CENGAGE Learning

Susanna S. Epp

Matemáticas discretas con aplicaciones

Cuarta Edición

MATEMÁTICAS DISCRETAS

MATEMÁTICAS DISCRETAS
CON APLICACIONES

CUARTA EDICIÓN

SUSANNA S. EPP
Universidad DePaul

Traducción:
Dra. Ana Elizabeth García Hernández
Universidad La Salle Morelia

Revisión técnica:
Dr. Ernesto Filio López
Unidad Profesional en Ingeniería y Tecnologías Avanzadas
Instituto Politécnico Nacional

M. en C. Manuel Robles Bernal
Escuela Superior de Física y Matemáticas
Instituto Politécnico Nacional

CENGAGE Learning™

Australia • Brasil • Corea • España • Estados Unidos • Japón • México • Reino Unido • Singapur

CENGAGE Learning™

Matemáticas discretas con aplicaciones, Cuarta edición
Susanna S. Epp

Presidente de Cengage Learning Latinoamérica:
Fernando Valenzuela Migoya

Director de producto y desarrollo Latinoamérica:
Daniel Oti Yvonett

Director editorial y de producción Latinoamérica:
Raúl D. Zendejas Espejel

Editor:
Sergio R. Cervantes González

Coordinadora de producción editorial:
Abril Vega Orozco

Editor de producción:
Omar A. Ramírez Rosas

Coordinador de manufactura:
Rafael Pérez González

Diseño de portada:
Hanh Luu

Imagen de portada:
Getty Images.com
(Collection OJO Images,
Photographer Martin Barraud)

Composición tipográfica:
JL Mau-Ro Impresos, Servicios Editoriales

Traducido del libro *Discrete Mathematics with Applications,* Fourth Edition.
Susanna S. Epp
Publicado en ingles por Brooks/Cole/ Cengage Learning
©2011
ISBN: 978-0-495-39132-6

Datos para catalogación bibliográfica:
Matemáticas discretas con aplicaciones, Cuarta edición
Susanna S. Epp
ISBN-13: 978-607-481-757-7
ISBN-10: 607-481-757-x

Visite nuestro sitio en:
http://latinoamerica.cengage.com

Impreso en México
1 2 3 4 5 6 7 15 14 13 12

A Jayne y Ernest

CONTENIDO

PREFACIO

Mi propósito al escribir este libro es proporcionar un tratamiento claro y accesible de las matemáticas discretas para estudiantes con mayor o menor dominio en ciencias de la computación, matemáticas, matemática educativa e ingeniería. El objetivo del libro es sentar las bases matemáticas para los cursos de ciencias de la computación, tales como estructuras de datos, algoritmos, teoría de las bases de datos relacionales, teoría de autómatas y lenguajes formales, diseño del compilador y criptografía y para los cursos de matemáticas tales como álgebra lineal y abstracta, combinaciones, probabilidad, lógica y teoría de conjuntos y teoría de números. Mediante el análisis combinado de teoría y práctica, he tratado de mostrar que la matemática tiene aplicaciones importantes además de ser interesante y hermosa por derecho propio.

Una buena formación en álgebra es el único prerrequisito, el curso puede ser tomado por estudiantes, ya sea antes o después de un curso de cálculo. Las ediciones anteriores del libro se han utilizado con éxito por estudiantes de cientos de instituciones en Norteamérica y Sudamérica, Europa, Medio Oriente, Asia y Australia.

Recientes recomendaciones curriculares de la Sociedad de cómputo del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE-CS) y de la Asociación de maquinaria computarizada (ACM) incluyen a las matemáticas discretas como la mayor parte de los "conocimientos básicos" de los estudiantes de ciencias computacionales y establecen que los estudiantes deben tomar por lo menos un curso de un semestre en el tema como parte de sus estudios de primer año, de preferencia con un curso de dos semestres cuando sea posible. Este libro incluye los temas recomendados por estas instituciones y se puede utilizar con eficacia, ya sea en un curso de uno o de dos semestres.

Hace tiempo, la mayoría de los temas de matemática discreta sólo se enseñaban en los últimos cursos de las licenciaturas. Descubrir la forma de presentar estos temas de manera que puedan ser entendidos por estudiantes de primer y segundo año fue el mayor y más interesante desafío al escribir este libro. La presentación se desarrolló durante un largo periodo de experimentación en el que mis alumnos fueron de muchas maneras mis maestros. Sus preguntas, comentarios y trabajos escritos me mostraron los conceptos y técnicas que se les dificultaban y su reacción a mi exposición me mostró lo que funcionaba para construir su conocimiento y para fomentar su interés. Muchos de los cambios en esta edición son el resultado de la interacción continua con los estudiantes.

Temas de un curso de Matemáticas discretas

La matemática discreta describe procesos que consisten en una secuencia de pasos individuales. Esto contrasta con el cálculo, que describe los procesos que cambian de forma continua. Mientras que las ideas del cálculo fueron fundamentales para la ciencia y la tecnología de la revolución industrial, las ideas de la matemática discreta son la base de la ciencia y la tecnología de la era de la computadora. Los temas principales de un primer curso de matemáticas discretas son la lógica y la demostración, la inducción y la recursión, las estructuras discretas, las combinaciones y la probabilidad discreta, los algoritmos y su análisis y las aplicaciones y el modelado.

Lógica y demostración Probablemente el objetivo más importante de un primer curso de matemáticas discretas es ayudar a los estudiantes a desarrollar la capacidad de pensamiento abstracto. Esto significa aprender a utilizar las formas válidas de argumentación lógica y evitar

errores comunes de lógica, apreciando lo que significa a la razón las definiciones, a sabiendas de cómo utilizar los argumentos directos e indirectos para deducir nuevos resultados a partir de los conocidos como verdaderos y ser capaz de trabajar con representaciones simbólicas, como si fueran objetos concretos.

Inducción y recursión Un desarrollo interesante de los últimos años ha sido la mayor apreciación de la fuerza y belleza del "pensamiento recursivo". Pensar de forma recursiva significa enfrentar un problema suponiendo que problemas similares más pequeños ya han sido resueltos y saber cómo colocar las soluciones en conjunto para resolver un problema mayor. Esta forma de pensamiento es ampliamente utilizada en el análisis de algoritmos, donde las relaciones de recurrencia que resultan del pensamiento recursivo a menudo dan lugar a fórmulas que se demuestran con inducción matemática.

Estructuras discretas Las estructuras de matemáticas discretas son estructuras abstractas que describen, clasifican y muestran las relaciones subyacentes entre los objetos matemáticos discretos. Las estudiadas en este libro son los conjuntos de números enteros y racionales, conjuntos generales, álgebras booleana, funciones, relaciones, grafos y árboles, lenguajes formales y expresiones regulares y autómatas de estado finito.

Combinación y probabilidad discreta Las combinaciones son la matemática de conteo y del arreglo de objetos y la probabilidad es el estudio de las leyes relativas a la medición de eventos aleatorios o al azar. La probabilidad discreta trata situaciones que implican conjuntos discretos de objetos, tales como encontrar la probabilidad de obtener un cierto número de caras cuando una moneda imparcial se lanza un número determinado de veces. Se necesita habilidad en el uso de probabilidad y las combinaciones en casi cualquier disciplina en donde se aplica la matemática, de economía a biología, a ciencia de la computación, a química y física, o a la gestión empresarial.

Algoritmos y su análisis La palabra *algoritmo* fue en gran parte desconocida hasta la mitad del siglo XX, sin embargo, ahora es una de las primeras palabras encontradas en el estudio de la ciencia de la computación. Para resolver un problema en una computadora, es necesario encontrar un algoritmo o secuencia paso a paso de instrucciones para que la computadora las siga. Diseñar un algoritmo requiere una comprensión de las matemáticas subyacentes del problema a resolver. Determinar si un algoritmo es correcto o no requiere de un uso sofisticado de la inducción matemática. El cálculo de la cantidad de tiempo o espacio de memoria que necesita el algoritmo al compararlo con otros algoritmos que producen la misma salida requiere del conocimiento de combinaciones, relaciones de recurrencia, funciones y notaciones O, Ω y Θ.

Aplicaciones y modelado Los temas matemáticos se entienden mejor cuando se ven en muchos diferentes contextos y se utilizan para resolver problemas en muchas y diferentes situaciones de aplicación. Una de las lecciones profundas de las matemáticas es que el mismo modelo matemático se puede utilizar para resolver problemas en situaciones que parecen ser superficialmente diferentes. Uno de los objetivos de este libro es mostrar a los alumnos la utilidad práctica extraordinaria de algunos conceptos matemáticos muy abstractos.

Características especiales de este libro

Razonamiento matemático La característica que más distingue a este libro de otros textos de matemática discreta es que enseña —explícitamente, pero de una manera que sea accesible para estudiantes de primer y segundo año de universidad— la lógica no hablada y el razonamiento que subyacen en el pensamiento matemático. Durante muchos años he enseñado una transición intensamente interactiva de los cursos de matemáticas abstractas a las matemáticas de las carreras de ciencia de la computación. Esta experiencia me mostró que es posible enseñar a la mayoría de

los estudiantes a comprender y construir argumentos matemáticos sencillos, los obstáculos para hacerlo no se deben tratar a la ligera. Para tener éxito, un texto para este curso debe abordar con amplitud las dificultades de los estudiantes con la lógica y el lenguaje directo. También debe incluir suficientes ejemplos concretos y ejercicios para que los estudiantes puedan desarrollar los modelos mentales necesarios para conceptualizar problemas más abstractos. El tratamiento de lógica y demostración en este libro combina el sentido común y el rigor de una manera que explica lo esencial, sin embargo, evita sobrecargar a los estudiantes con detalles formales.

Enfoque en espiral al desarrollo del concepto Una serie de conceptos en este libro aparecen en formas cada vez más sofisticadas en los capítulos sucesivos para ayudar a los estudiantes a desarrollar la capacidad de hacer frente eficazmente a niveles cada vez mayores de abstracción. Por ejemplo, cuando los estudiantes encuentran las matemáticas relativamente avanzadas del pequeño teorema de Fermat en la sección 8.4, ya se han introducido a la lógica del discurso matemático de los capítulos 1, 2 y 3, donde aprendieron los métodos básicos de la demostración y los conceptos *mod* y *div* en el capítulo 4, han explorando *mod* y *div* como funciones en el capítulo 7 y se han familiarizado con las relaciones de equivalencia en las secciones 8.2 y 8.3. Este método construye una revisión útil y desarrolla madurez matemática de forma natural.

Apoyo a los estudiantes Los estudiantes de facultades y universidades, inevitablemente, tienen que aprender mucho por sí mismos. Aunque con frecuencia es frustrante, aprender a aprender a través de autoestudio es un paso crucial para el éxito final de una carrera profesional. Este libro tiene una serie de características para facilitar la transición de los estudiantes para el aprendizaje independiente.

Ejemplos resueltos
El libro contiene más de 500 ejemplos resueltos, que se han escrito usando un formato de problema-solución y se han colocado de acuerdo al tipo y dificultad de los ejercicios. Muchas de las soluciones para los problemas de demostración se han desarrollado en dos etapas: primera un análisis de cómo se podría pensar la demostración o la refutación y, a continuación un resumen de la solución, que está encerrado en un cuadro. Este formato permite a los estudiantes leer el problema y pasar si lo desean, de inmediato al resumen y regresar al análisis si tienen problemas para entender el resumen. El formato también ahorra tiempo a los estudiantes al releer el texto para preparar un examen.

Notas marginales y preguntas de autoevaluación
En los márgenes de todo el libro, se incluyen, notas acerca de temas de particular importancia y comentarios de precaución para ayudar a los estudiantes a evitar errores comunes. Entre el texto y los ejercicios, se encuentran, preguntas diseñadas para centrar la atención en las ideas principales de cada sección. Para mayor comodidad, las preguntas utilizan un formato de completar el espacio en blanco y las respuestas se encuentran inmediatamente después de los ejercicios.

Ejercicios
El libro contiene casi 2 600 ejercicios. Los conjuntos al final de cada sección se han diseñado para que los estudiantes con antecedentes muy diferentes y niveles de habilidad encuentren algunos ejercicios que puedan realizar seguramente con éxito y también algunos ejercicios que los desafiarán.

Soluciones a los ejercicios
Para proporcionar información adecuada para los estudiantes entre las sesiones de clase, el apéndice B contiene un gran número de soluciones completas a los ejercicios. Se les recomienda encarecidamente a los estudiantes, no consultar soluciones hasta que hayan intentado todo lo posible para responder a las preguntas por sí mismos. Sin embargo, una vez que lo han hecho, comparar sus respuestas con las dadas puede conducir a una comprensión

significativamente mejorada. Además, muchos problemas, entre ellos algunos de los más difíciles, tienen soluciones parciales o sugerencias para que los estudiantes puedan determinar si están en el camino correcto y si es necesario hacer ajustes. Hay también muchos ejercicios sin soluciones para ayudar a los estudiantes aprender a lidiar con problemas matemáticos en un entorno real.

Características de referencia
Muchos estudiantes me han escrito para decir que el libro les ayudó a tener éxito en sus cursos avanzados. Incluso uno me escribió diciendo que había utilizado tanto una edición que se le había roto y que de hecho compró un libro de la siguiente edición, la que sigue utilizando en un programa de maestría. Las figuras y las tablas que se incluyen se realizaron para ayudar a los lectores a una mejor comprensión. En la mayoría, se utiliza un segundo color para resaltar el significado. Mi criterio al presentar enunciados en las definiciones y teoremas; poner títulos a los ejercicios; dar significado a los símbolos y una lista de fórmulas de referencia en la contraportada es facilitar a los estudiantes el uso de este libro para repasar en un curso actual y como referencia en posteriores ediciones.

Apoyo al profesor He recibido una gran cantidad de valiosa información de los profesores que han utilizado las ediciones anteriores de este libro. Muchos aspectos del libro se han mejorado a través de sus sugerencias. Además de los siguientes artículos, hay un apoyo adicional para el profesor en el sitio web del libro, como se describe más adelante en este prefacio.

Ejercicios
La gran variedad de ejercicios con todos los niveles de dificultad permite a los profesores gran libertad para adaptar el curso a las habilidades de sus estudiantes. Los ejercicios con soluciones en la parte posterior del libro tienen números en azul y sus soluciones se presentan por separado en el *Manual de soluciones de estudiantes y Guía de estudio* tienen números que son múltiplos de tres. Hay ejercicios de cada tipo que se representan en este libro que no tienen una respuesta en uno u otro para que los profesores asignen cualquier mezcla de ejercicios que prefiera con y sin respuestas. El amplio número de ejercicios de todo tipo da a los profesores una opción importante de problemas para el uso de tareas y exámenes. Se les invita a los profesores a utilizar los muchos ejercicios establecidos como preguntas en lugar de "demuestre que" para motivar el análisis en clase acerca del papel de la demostración y del contraejemplo en la solución de problemas.

Secciones flexibles
La mayoría de las secciones se dividen en subsecciones para que un profesor que se sienta presionado por el tiempo pueda elegir para cubrir los incisos determinados y bien omitir el resto, o dejarlo para que los estudiantes lo estudien por su cuenta. La división en subsecciones también facilita a los profesores partir las secciones si desea pasar más de un día en ellas.

Presentación de los métodos de demostración
Es inevitable que las demostraciones y refutaciones en este libro parezcan fáciles a los profesores. Sin embargo, muchos estudiantes, las encuentran difíciles. Al mostrar a los estudiantes cómo descubrir y construir demostraciones y refutaciones, he tratado de describir los tipos de métodos que usan los matemáticos cuando enfrentan problemas difíciles en sus propias investigaciones.

Soluciones del profesor
Las soluciones completas del profesor para todos los ejercicios están disponibles para la enseñanza de cualquier curso con este libro a través del servicio de construcción de soluciones de Cengage. Los profesores pueden registrarse para ingresar en www.cengage.com/solutionbuilder.

Aspectos sobresalientes de la cuarta edición

Los cambios realizados en esta edición se basan en las sugerencias de los colegas y otros usuarios de mucho tiempo de las ediciones anteriores, en las interacciones continuas con mis alumnos y en el desarrollo en los campos de desarrollo de la ciencia computacional y de las matemáticas.

Reorganización

Un nuevo capítulo 1 introduce a los estudiantes a algunos de los términos precisos lo que es muy fundamental en el pensamiento matemático: el lenguaje de variables, conjuntos, relaciones y funciones. En respuesta a las peticiones de algunos profesores, el material básico ahora se coloca junto en los capítulos del 1 al 8, el capítulo de recursión ahora se unió al capítulo sobre la inducción. Los capítulos del 9 al 12 se colocaron juntos al final, ya que, aunque muchos profesores cubren uno o más de ellos, existe una considerable diversidad en sus opciones y algunos de los temas de estos capítulos se incluyen en otros cursos.

Mejora pedagógica

- El número de ejercicios ha aumentado a casi 2 600. Se han agregado alrededor de 300 ejercicios nuevos.
- Se han agregado ejercicios para temas donde los estudiantes parecían necesitar práctica adicional y se han modificado, cuando era necesario, para subsanar las dificultades de los alumnos.
- Se han incorporado en el apéndice B, respuestas completas adicionales para ayudar más a los estudiantes en los temas difíciles.
- Se ha reexaminado la presentación y se ha revisado donde era necesario.
- Se analizaron antecedentes históricos, se han ampliado resultados recientes y se ha aumentado el número de fotografías de matemáticos y científicos de la computación cuyas contribuciones se analizan en el libro.

Lógica y Teoría de conjuntos

- Ahora se incluye la definición de argumentos racionales y se hacen aclaraciones adicionales de la diferencia entre un argumento válido y una conclusión verdadera.
- Se han agregado ejemplos y ejercicios acerca de seguimiento de cuantificadores.
- Se han incorporado definiciones de uniones e intersecciones infinitas.

Introducción a la demostración

- Se han ampliado las instrucciones para demostraciones escritas y el análisis de los errores más comunes.
- Se han aclarado las descripciones de los métodos de demostración.
- Se han revisado y/o reubicado ejercicios para fomentar el desarrollo de la comprensión del estudiante.

Inducción y recursión

- Se ha mejorado el formato para esbozar demostraciones con inducción matemática.
- Se han reorganizado las secuencias de las subsecciones de la sección.

- Se han ampliado, los conjuntos de ejercicios para las secciones de inducción matemática fuerte, del principio del buen orden y de las definiciones recursivas.
- Se ha prestado más atención a la inducción estructural.

Teoría de Números

- Se ha ampliado una sección acerca de problemas abiertos en la teoría de números y se incluye un análisis adicional de los recientes descubrimientos matemáticos de la teoría de números.
- Se ha simplificado, la presentación en la sección acerca de aritmética modular y criptografía.
- Se ha aclarado el análisis de demostraciones de números primos.

Combinaciones y probabilidad discreta

- Se ha movido a este capítulo, el análisis del principio de las casillas.

Funciones

- Hay una mayor cobertura de funciones de más de una variable y de funciones que actúan sobre conjuntos.

Teoría de grafos

- Se ha actualizado la terminología de recorrido de un grafo.
- Ahora se ha incluido, el algoritmo de la ruta más corta de Dijkstra.
- Se han agregado ejercicios para introducir a los estudiantes en el coloreado de los grafos.

Sitio web acompañante

www.cengage.com/math/epp

Se ha desarrollado un sitio web para este libro que contiene información y materiales para los estudiantes y los profesores. Éste incluye:

- descripciones y enlaces a muchos sitios en Internet con información accesible sobre temas de matemáticas discretas,
- enlaces a aplicaciones (*applets*) que ilustran o permiten practicar conceptos de la matemática discreta,
- más ejemplos y ejercicios con soluciones,
- guías de repaso para los capítulos del libro.

Una sección especial para profesores contiene:

- sugerencias sobre cómo abordar el material de cada capítulo,
- soluciones a todos los ejercicios no totalmente resueltos en el apéndice B,
- ideas para proyectos y tareas escritas,
- diapositivas de PowerPoint,
- hojas de examen y ejercicios adicionales para pruebas y exámenes.

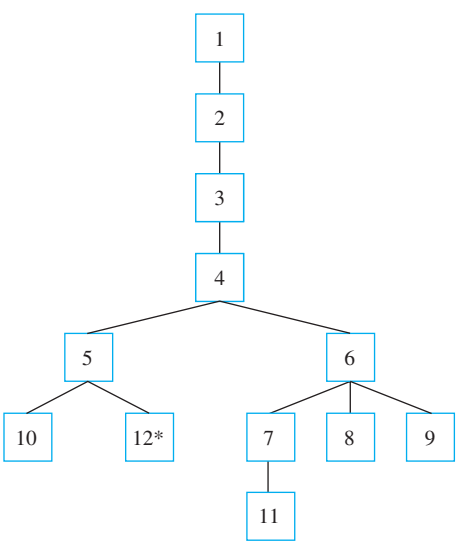
Organización

Este libro se puede utilizar efectivamente en un curso de uno o de dos semestres. Los capítulos contienen secciones básicas, secciones que cubren material matemático opcional y secciones que cubren aplicaciones opcionales. Los profesores tienen la flexibilidad de elegir cualquier mezcla que sirva mejor a las necesidades de sus estudiantes. En la tabla siguiente se muestra una división de las secciones en categorías.

Capítulo	Secciones básicas	Secciones que contienen material matemático opcional	Secciones que contienen aplicaciones opcionales de ciencia de la computación
1	1.1–1.3		
2	2.1–2.3	2.5	2.4, 2.5
3	3.1–3.4	3.3	3.3
4	4.1–4.4, 4.6	4.5, 4.7	4.8
5	5.1, 5.2, 5.6, 5.7	5.3, 5.4, 5.8	5.1, 5.5, 5.9
6	6.1	6.2–6.4	6.1, 6.4
7	7.1, 7.2	7.3, 7.4	7.1, 7.2, 7.4
8	8.1–8.3	8.4, 8.5	8.4, 8.5
9	9.1–9.4	9.5–9.9	9.3
10	10.1, 10.5	10.2–10.4, 10.6	10.1, 10.2, 10.5–10.7
11	11.1, 11.2	11.4	11.3, 11.5
12	12.1, 12.2	12.3	12.1–12.3

El siguiente diagrama de árbol muestra, aproximadamente, cómo dependen unos de otros los capítulos de este libro. Los capítulos en las diferentes ramas del árbol son lo suficientemente independientes por lo que los profesores necesitan hacer ajustes de menor importancia si se saltan capítulos, pero siguiendo caminos a lo largo de las ramas del árbol.

En la mayoría de los casos, cubriendo sólo las secciones básicas de los capítulos se tiene la preparación adecuada para moverse en el árbol.



∗La sección 8.3 se necesita en la sección 12.3 pero no para las secciones 12.1 y 12.2.

Reconocimientos

Tengo una deuda de gratitud con muchas personas de la Universidad DePaul, por su apoyo y aliento a lo largo de los años en que he trabajado en las ediciones de este libro. Algunos de mis colegas utilizaron las primeras versiones y ediciones anteriores y me dieron muchas excelentes sugerencias para su mejora. Por esto, estoy agradecida con Louis Aquila, J. Marshall Ash, Allan Berele, Jeffrey Bergen, William Chin, Barbara Cortzen, Constantine Georgakis, Sigrun Goes, Jerry Goldman, Lawrence Gluck, Leonid Krop, Carolyn Narasimhan, Walter Pranger, Eric Rieders, Ayse Sahin, Yuen-Fat Wong y, muy especialmente con, Jeanne LaDuke. Los miles de estudiantes a quienes he enseñado matemáticas discretas han tenido una profunda influencia en la presentación del libro. Al compartir sus pensamientos y procesos de pensamiento conmigo, ellos me enseñaron a enseñar mejor. Estoy muy agradecida por su ayuda. Estoy en deuda con la administración de la Universidad DePaul, en especial con mi decano, Charles Suchar y a mis antiguos decanos, Michael Mezey y Richard Meister, un agradecimiento especial al considerar la escritura de este libro un esfuerzo académico de mérito.

Mi agradecimiento a los revisores por sus valiosas sugerencias para la edición del libro: David Addis, Universidad Cristiana de Texas; Rachel Esselstein, Universidad Estatal de California, Bahía de Monterrey; William Marion, Universidad de Valparaíso; Michael McClendon, Universidad Central de Oklahoma; y Steven Miller, Universidad Brown. Por su ayuda con las ediciones anteriores del libro, estoy agradecida con Itshak Borosh, Universidad Texas A&M; Douglas M. Campbell, de la Universidad Brigham Young; David G. Cantor, de la Universidad de California en Los Angeles; C. Patrick Collier de la Universidad de Wisconsin-Oshkosh; Kevan H. Croteau, Universidad Francis Marion; Irinel Drogan de la Universidad de Texas en Arlington; Pablo Echeverría, Colegio Camden County; Henry A. Etlinger, Instituto de Tecnología de Rochester; Melvin J. Friske, Colegio Luterano de Wisconsin; William Gasarch de la Universidad de Maryland; Ladnor Geissinger de la Universidad de Carolina del Norte; Jerrold R. Griggs, Universidad de Carolina del Sur; Nancy Baxter Hastings, Colegio Dickinson; Lillian Hupert, Universidad Loyola de Chicago; Joseph Kolibal, Universidad del Sur de Mississippi; Benny Lo, Universidad Tecnológica Internacional, George Luger, de la Universidad de Nuevo México; Leonard T. Malinowski, Colegio de la comunidad Finger Lakes; John F. Morrison, Universidad Estatal de Towson; Paul Pederson, de la Universidad de Denver; George Peck, de la Universidad Estatal de Arizona; Roxy Peck, de la Universidad Politécnica Estatal de California en San Luis Obispo; Dix Pettey, de la Universidad de Missouri; Anthony Ralston, Universidad Estatal de Nueva York en Buffalo; Norman Richert, de la Universidad de Houston-Clear Lake; John Roberts, de la Universidad de Louisville y George Schultz, Colegio St. Petersburg Junior, Clearwater. Un agradecimiento especial a John Carroll, de la Universidad estatal de San Diego; al Dr. Joseph S. Fulda y Porter G. Webster, de la Universidad del Sur de Mississippi, a Peter Williams, de la Universidad estatal de California en San Bernardino y a Jay Zimmerman, de la Universidad de Towson para su inusual rigor y ánimo.

También me han ayudado inmensamente con las sugerencias de muchos profesores que generosamente me ofrecieron sus ideas para mejorar en base a sus experiencias con las ediciones anteriores del libro, en especial a Jonathan Goldstine, de la Universidad Estatal de Pensilvania; a David Hecker, de la Universidad St. Joseph; a Edward Huff, Colegio de la comunidad de Virginia del norte; a Robert Messer, del Colegio Albion; a Sophie Quigley, de la Universidad Ryerson; a Piotr RudNicki, de la Universidad de Alberta; a Anwar Shiek, del Colegio Diné; a Norton Starr, del Colegio Amherst; y Wee Eng, de la Universidad Nacional de Singapur. La producción de la tercera edición contó con la valiosa colaboración de Christopher Novak, de la Universidad de Michigan, Dearborn e Ian Crewe, Escuela colegiada Ascension. Con la tercera y cuarta ediciones estoy especialmente agradecida por las muchas excelentes sugerencias para mejorar hechas por Tom Jenkins, de la Universidad Brock, cuya asistencia en todo el proceso de producción fue muy valiosa.

Estoy en deuda con el personal de Brooks/Cole, especialmente a mi editor, Dan Seibert, por su asesoramiento serio y tranquilizador y por su tranquila dirección en el proceso de producción

y a mis editores anteriores, Stacy Green, Robert Pirtle, Barbara Holland y Bennett Heather, por su aliento y entusiasmo.

Conforme pasan los años me doy más cuenta de la profunda deuda que tengo con mis profesores de matemáticas para forjarme la manera en que percibo el tema. Quiero dar las gracias primero a mi esposo, Helmut Epp, quien, en una cita en la secundaria (¡!), me introdujo a la fuerza y belleza de los axiomas de campo y a ver que las matemáticas es un tema con ideas, así como las fórmulas y técnicas. En mi educación formal, estoy muy agradecida con Daniel Zelinsky y Ky Fan de la Universidad Northwestern y con Izaak Wirszup, I. N. Herstein y con Irving Kaplansky de la Universidad de Chicago, todos ellos, a su manera, me ayudaron a que apreciara la elegancia, rigor y emoción de las matemáticas.

A mi familia, le doy gracias sin medida. Agradezco a mi madre, cuyo interés en el funcionamiento de la inteligencia humana me inició hace muchos años en la pista que condujo finalmente a este libro y a mi difunto padre, cuya devoción por la palabra escrita ha sido una fuente constante de inspiración. Doy gracias a mis hijos y nietos por su afecto y alegre aceptación con las demandas que ha puesto este libro en mi vida. Y, sobre todo, agradezco a mi esposo, quien durante muchos años me ha animado con su fe en el valor de este proyecto y me apoyó con su amor y sabio consejo.

Susanna Epp

CAPÍTULO 1

HABLANDO MATEMÁTICAMENTE

Por tanto, estudiantes estudien matemáticas y no construyan sin fundamentos. —Leonardo da Vinci (1452-1519)

El objetivo de este libro es presentarle una forma matemática de pensar que le puede servir en muchas y diversas situaciones. Con frecuencia, cuando usted empieza a trabajar con un problema matemático, puede tener sólo una vaga sospecha de cómo proceder. Puede empezar por examinar ejemplos, hacer dibujos, jugar con la notación, releer el problema para centrarse en uno o más de sus detalles, etcétera. Sin embargo, al acercarse a la solución, su forma de pensar tiene que cristalizar. Y cuanto más necesite entender, más necesita un lenguaje que exprese las ideas matemáticas en forma clara, precisa y sin ambigüedades.

En este capítulo se le dará a conocer parte del lenguaje especial que es fundamental para mucho del pensamiento matemático, el lenguaje de las variables, conjuntos, relaciones y funciones. Este capítulo se ha pensado como el entrenamiento antes de un importante evento deportivo. Su objetivo es calentar sus músculos mentales, para que pueda hacer su mejor esfuerzo.

1.1 Variables

A veces a una variable se le considera como un ente matemático como "John Doe", ya que se puede utilizar como un marcador de posición cuando se quiere hablar de algo como 1) imagine que tiene uno o más valores pero no sabe cuáles son, o 2) desea que todo lo que se dice sea igualmente válido para todos los elementos en un conjunto dado, por lo que no quiere limitarse a considerar sólo un valor determinado, concreto para ellos. Para mostrar el primer uso, considere lo siguiente

> ¿Hay un número con la siguiente propiedad: al duplicar éste y sumarle 3 se obtiene el mismo resultado que si se eleva al cuadrado?

En esta frase se puede introducir una variable para reemplazar la palabra "éste" que puede resultar ambigua:

$$\text{¿Hay un número } x \text{ con la propiedad de que } 2x + 3 = x^2?$$

La ventaja de utilizar una variable es que le permite dar un nombre temporal a lo que está buscando, para que pueda realizar cálculos concretos con ésta para ayudar a descubrir sus posibles valores. Para enfatizar el papel de la variable como un marcador de posición, podría escribir lo siguiente:

$$\text{¿Hay un número } \square \text{ con la propiedad de que } 2\cdot\square + 3 = \square^2?$$

La caja vacía le puede ayudar a imaginar llenarla con diferentes valores, algunos de los cuales podrían hacer que los dos lados sean iguales y otros no.

Para mostrar el segundo uso de las variables, considere el enunciado siguiente:

> No importa qué número elija, si éste es mayor que 2,
> entonces su cuadrado es mayor que 4.

En este caso la introducción de una variable para dar un nombre temporal al número (arbitrario) le permite mantener la generalidad del enunciado y sustituyendo todos los casos de la palabra "éste" por lo que el nombre de la variable asegura que se evite la posible ambigüedad:

> No importa qué número n se elija, si n es mayor que 2,
> entonces n^2 es mayor que 4.

Ejemplo 1.1.1 Escritura de enunciados usando variables

Utilice variables para reescribir las siguientes frases de manera más formal.

a. ¿Hay números con la propiedad de que la suma de sus cuadrados es igual al cuadrado de su suma?

b. Dado cualquier número real, su cuadrado es no negativo.

Solución

Nota En el inciso *a*) la respuesta es sí. Por ejemplo, $a = 1$ y $b = 0$ lo cumplen. ¿Puedes pensar en otros números que también lo cumplan?

a. ¿Hay números a y b con la propiedad de que $a^2 + b^2 = (a + b)^2$?
O: ¿Hay números a y b tales que $a^2 + b^2 = (a + b)^2$?
O: ¿Existen dos números a y b tales que $a^2 + b^2 = (a + b)^2$?

b. Dado cualquier número real r, r^2 es no negativo.
O: Para cualquier número real r, $r^2 \geq 0$.
O: Para todos los números reales r, $r^2 \geq 0$. ■

Algunos tipos importantes de enunciados matemáticos

Tres de los tipos más importantes de enunciados en matemáticas son enunciados universales, enunciados condicionales y enunciados existenciales:

> Un **enunciado universal** dice que una cierta propiedad es verdadera para todos los elementos de un conjunto. (Por ejemplo: *Todos los números positivos son mayores que cero*).
>
> Un **enunciado condicional**, dice que si una cosa es verdad, otra cosa también tiene que ser verdad. (Por ejemplo: *Si 378 es divisible entre 18, entonces 378 es divisible entre 6*).
>
> Dada una propiedad que puede o no puede ser verdad, un **enunciado existencial**, dice que hay al menos una cosa para la cual la propiedad es verdadera. (Por ejemplo: *Hay un número primo que es par*).

En las secciones siguientes vamos a definir cada tipo de enunciado cuidadosamente y lo analizaremos detalladamente. El objetivo aquí es que comprenda que las combinaciones de estos enunciados se pueden expresar de muchas maneras diferentes. Una forma es utilizar el lenguaje ordinario, el lenguaje cotidiano y otra es expresar el enunciado usando una o más variables. Los ejercicios están diseñados para ayudarle a empezar a sentirse cómodo en la traducción de un modo a otro.

Enunciados universales condicionales

Los enunciados universales tienen alguna variación de las palabras "para todo" y los enunciados condicionales contienen versiones de las palabras "si-entonces". Un ***enunciado universal condicional*** es un enunciado que es a la vez universal y condicional. Por ejemplo:

Para todos los animales a, si a es perro, entonces a es un mamífero.

Uno de los hechos más importantes acerca de los enunciados universales condicionales es que se pueden reescribir de manera que parezcan solamente universales o solamente condicionales. Por ejemplo, el enunciado anterior se puede reescribir de un modo que haga explícito su carácter condicional, pero que su naturaleza universal esté implícita:

Si a es un perro, entonces a es un mamífero.
O: Si un animal es un perro, entonces el animal es un mamífero.

El enunciado también se puede expresar haciendo explícita su naturaleza universal e implícita su naturaleza condicional:

Para todos los perros a, a es un mamífero.
O: Todos los perros son mamíferos.

El punto crucial es que la capacidad de traducir entre diferentes maneras de expresar enunciados universales condicionales es muy útil para hacer matemáticas y en muchas partes de la ciencia computacional.

Ejemplo 1.1.2 Reescritura de un enunciado condicional universal

Llene los espacios en blanco para escribir el siguiente enunciado:

Para todos los números reales x, si x es distinto de cero entonces x^2 es positivo.

a. Si un número real es no cero, entonces su cuadrado ____.

b. Para todos los números reales diferentes de cero x, ____.

c. Si x ____, entonces ____.

d. El cuadrado de cualquier número real distinto de cero es ____.

e. Todos los números reales distintos de cero tienen ____.

Nota Si introduce x en la primera parte del enunciado, asegúrese de incluirla en la segunda parte del enunciado.

Solución

a. es positivo
b. x^2 es positivo
c. es un número real distinto de cero, x^2 es positivo
d. positivo
e. cuadrados positivos (*o*: los cuadrados son positivos) ■

Enunciados universales existenciales

Un ***enunciado universal existencial*** es un enunciado que es universal porque su primera parte dice que una cierta propiedad es verdadera para todos los objetos de un tipo dado y es existencial porque su segunda parte asegura la existencia de algo. Por ejemplo:

Todo número real tiene un inverso aditivo.

Nota Para que un número b sea un inverso aditivo de un número a significa que $a + b = 0$.

En este enunciado la propiedad "tiene un inverso aditivo" se aplica universalmente a todos los números reales. "Tiene un inverso aditivo", asegura la existencia de algo —un inverso aditivo— para cada número real. Sin embargo, la naturaleza del inverso aditivo depende del número real, diferentes números reales tienen diferentes inversos aditivos. Sabiendo que un inverso aditivo es un número real, puede volver a escribir esta enunciado de diferentes maneras, algunas menos formales y algunas más formales*:

Todos los números reales tienen inversos aditivos.
O: Para todos los números reales r, hay un inverso aditivo de r.
O: Para todos los números reales r, existe un número real s tal que s es un inverso aditivo de r.

Nombrar a las variables simplifica las referencias en el análisis siguiente. Por ejemplo, después de la tercera versión del enunciado podría escribir lo siguiente: Cuando r es positivo, s es negativo, cuando r es negativo, s es positivo y cuando r es igual a cero, s también es cero.

Una de las razones más importantes del uso de variables en matemáticas es que le da la posibilidad de referirse a las cantidades de forma inequívoca a través de un argumento matemático largo, mientras que no se restrinja a considerar sólo valores específicos de ellas.

Ejemplo 1.1.3 Reescritura de un enunciado universal existencial

Llene los espacios en blanco al reescribir el siguiente enunciado: Cada olla tiene una tapa.

a. Todas las ollas ____.

b. Para todas las ollas P, hay ____.

c. Para todas las ollas P, hay una tapa L tal que ____.

Solución

a. tienen tapas

b. una tapa de P

c. L es una tapa de P ■

Enunciados universales existenciales

Un **enunciado universal existencial** es un enunciado que es existencial porque su primera parte asegura que existe un determinado objeto y es universal porque su segunda parte dice que el objeto satisface una cierta propiedad de todas las cosas de una cierta clase. Por ejemplo:

Hay un entero positivo que es menor o igual a cada número entero positivo:

Este enunciado es verdadero porque el número uno es un entero positivo y satisface la propiedad de ser menor o igual a cada número entero positivo. Podemos reescribir el enunciado de varias maneras, algunas menos formales y algunas más formales:

Algún entero positivo es menor o igual que cada número entero positivo.
O: Hay un entero positivo m que es menor o igual a cada número entero positivo.
O: Hay un entero positivo m tal que todo entero positivo es mayor o igual a m.
O: Hay un entero positivo m con la propiedad de que para todos los enteros positivos n, $m \leq n$.

*Se podría utilizar un condicional para ayudar a expresar este enunciado, posponemos la complejidad adicional para un capítulo posterior.

Ejemplo 1.1.4 Reescritura de un enunciado universal existencial

Llene los espacios en blanco para escribir el siguiente enunciado en tres formas diferentes:

Hay una persona en mi clase que tiene al menos la misma edad que cada una las personas de mi clase.

a. Alguna ____ es por lo menos de la misma edad que ____.

b. Hay una persona p en mi clase tal que p ____.

c. Hay una persona p en mi clase con la propiedad de que para cada persona q en mi clase, p es ____.

Solución

a. persona en mi clase, cada una de las personas en mi clase

b. tiene la misma edad que cada una de las personas de mi clase

c. tiene por lo menos la misma edad que q. ■

Algunos de los conceptos matemáticos más importantes, tales como la definición de límite de una sucesión, se pueden definir usando sólo enunciados universales, existenciales y condicionales y requieren el uso de los tres enunciados "para todo", "existe" y "si-entonces". Por ejemplo, si $a_1, a_2, a_3, \ldots$ es una sucesión de números reales, se dice que

el límite de a_n cuando n tiende a infinito es L

lo que significa que

para todo número real positivo ε, **existe** un número entero N tal que **para todo** entero n, **si** $n > N$ **entonces** $-\varepsilon < a_n - L < \varepsilon$.

Autoexamen

Las respuestas a las preguntas del autoexamen se ubican al final de cada sección.

1. Un enunciado universal asegura que una cierta propiedad es ____ para ____.
2. Un enunciado condicional asegura que si una cosa ____ entonces alguna otra cosa ____.
3. Dada una propiedad que puede o no ser verdad, un enunciado existencial asegura que ____ para la que la propiedad es verdadera.

Conjunto de ejercicios 1.1

El apéndice B contiene soluciones ya sea totales o parciales de todos los ejercicios con números azules. Cuando la solución no está completa, el ejercicio tiene una ***H*** al lado de éste. Una ✶ al lado de un número indica que el ejercicio es más difícil de lo habitual. Tenga cuidado de no adquirir el hábito de recurrir a las soluciones demasiado rápido. Haga todo lo posible por realizar los ejercicios por su cuenta antes de que los revise. Vea el prefacio para obtener referencias de fuentes adicionales de asistencia y estudio.

En los ejercicios del 1 al 6, llene los espacios en blanco utilizando una variable o variables para reescribir el enunciado dado.

1. ¿Hay un número real cuyo cuadrado es -1?
   a. Existe un número real x tal que ____?
   b. ¿Existe ____ tal que $x^2 = -1$?

2. ¿Hay un número entero que tiene un residuo de 2 cuando se divide entre 5 y un residuo de 3 cuando se divide entre 6?
   a. ¿Existe un entero n tal que n tiene ____?
   b. ¿Existe ____ tal que si n se divide entre 5, el residuo es 2 y si ____?

Nota: Hay números enteros con esta propiedad. ¿Puede pensar en uno?

3. Dados dos números reales, existe un número real en medio.
   a. Dados dos números reales a y b, existe un número real c tal que c es _____.
   b. Para cualquiera de los dos _____, _____ tales que $a < c < b$.

4. Dado cualquier número real, existe un número real que es mayor.
   a. Dado cualquier número real r, existe _____ s tal que s es _____.
   b. Para cualquier _____, _____ tal que $s > r$.

5. El recíproco de cualquier número real positivo es positivo.
   a. Dado cualquier número real positivo r, el recíproco de _____.
   b. Para cualquier número real r, si r es _____, entonces _____.
   c. Si un número real r _____, entonces _____.

6. La raíz cúbica de cualquier número real negativo es negativa.
   a. Dado cualquier número real negativo s, la raíz cúbica de _____ .
   b. Para cualquier número real s, si s es _____, entonces _____.
   c. Si un número real s _____, entonces _____.

7. Reescriba los siguientes enunciados de manera menos formal, sin usar variables. Determine, lo mejor que pueda, si los enunciados son verdaderos o falsos.
   a. Hay números reales u y v con la propiedad de que $u + v < u - v$.
   b. Hay un número real x tal que $x^2 < x$.
   c. Para todos los enteros positivos n, $n^2 \geq n$.
   d. Para todos los números reales a y b, $|a + b| \leq |a| + |b|$.

En cada uno de los ejercicios del 8 al 13, llene los espacios en blanco para reescribir el enunciado dado.

8. Para todos los objetos J, si J es un cuadrado entonces J tiene cuatro lados.
   a. Todos los cuadrados _____.
   b. Todo cuadrado _____.
   c. Si un objeto es un cuadrado, entonces _____.
   d. Si J _____, entonces J _____.
   e. Para todos los cuadrados J, _____.

9. Para todas las ecuaciones E, si E es cuadrática entonces E tiene como máximo dos soluciones reales.
   a. Todas las ecuaciones cuadráticas _____.
   b. Toda ecuación cuadrática _____.
   c. Si una ecuación es cuadrática, entonces _____.
   d. Si E _____, entonces E _____.
   e. Para todas las ecuaciones cuadráticas E, _____

10. Todo número real distinto de cero tiene un recíproco.
   a. Todos los números reales distintos de cero _____.
   b. Para todos los números reales r distintos de cero, hay_____ para r.
   c. Para todos los números reales r distintos de cero, hay un número real s tal que _____.

11. Todo número positivo tiene una raíz cuadrada positiva.
   a. Todos los números positivos _____.
   b. Para cualquier número positivo e, existe _____ para e.
   c. Para todos los números positivos e, hay un número positivo r tal que _____.

12. Hay un número real cuyo producto con todo número real no cambia al número.
   a. Alguno _____ tiene la propiedad de que su _____.
   b. Hay un número r tal que el producto de r _____.
   c. Hay un número real r con la propiedad de que para todo número real s, _____.

13. Hay un número real cuyo producto con todos los números reales es igual a cero.
   a. Alguno _____ tiene la propiedad de que su _____.
   b. Hay un número real a tal que el producto de a _____.
   c. Hay un número real a con la propiedad de que para todo número real b, _____.

Respuestas del autoexamen

1. verdadera, todos los elementos de un conjunto 2. Es verdad, también tiene que ser verdad 3. hay por lo menos una cosa

1.2 El lenguaje de los conjuntos

. . . cuando intentamos expresar con símbolos matemáticos una condición propuesta en palabras. Primero, debemos entender a fondo la condición. Y después, debemos familiarizarnos con las formas de expresión matemática. —George Polyá (1887-1985)

El uso de la palabra *conjunto* como un término matemático formal fue introducido en 1879 por Georg Cantor (1845-1918). Para la mayoría de los propósitos matemáticos podemos

pensar en un conjunto intuitivamente, como Cantor lo hizo, simplemente como una colección de elementos. Por ejemplo, si C es el conjunto de todos los países que se encuentran actualmente en las Naciones Unidas, entonces Estados Unidos es un elemento de C y si I es el conjunto de todos los enteros del 1 al 100, entonces el número 57 es un elemento de I.

• Notación

Si S es un conjunto, la notación $\boldsymbol{x \in S}$ significa que x es un elemento de S. La notación $\boldsymbol{x \notin S}$ significa que x no es un elemento de S. Un conjunto se puede especificar usando la **notación en lista del conjunto** al escribir todos los elementos entre llaves. Por ejemplo **{1, 2, 3}**, denota el conjunto cuyos elementos son 1, 2 y 3. A veces se utiliza una variante de la notación para describir un conjunto muy grande, como cuando escribimos **{1, 2, 3, . . . , 100}** para referirnos al conjunto de todos los enteros del 1 al 100. Una notación similar también puede describir un conjunto infinito, como cuando escribimos **{1, 2, 3, . . .}** para referirnos al conjunto de todos los enteros positivos. (El símbolo **. . .** se llama **puntos suspensivos** y se lee "y así sucesivamente").

El **axioma de extensión**, dice que un conjunto está completamente determinado por los elementos que están en él —no por el orden en el que se podrían utilizar o por el hecho de que algunos elementos podrían listarse más de una vez.

Ejemplo 1.2.1 Uso de la notación en lista del conjunto

a. Sea $A = \{1, 2, 3\}$, $B = \{3, 1, 2\}$ y $C = \{1, 1, 2, 3, 3, 3\}$. ¿Cuáles son los elementos de A, B y C? ¿Cómo están relacionados A, B y C?

b. ¿Es $\{0\} = 0$?

c. ¿Cuántos elementos están en el conjunto $\{1, \{1\}\}$?

d. Para cada entero no negativo n, sea $U_n = \{n, -n\}$. Encuentre U_1, U_2 y U_0.

Solución

a. A, B y C tienen exactamente los mismos tres elementos: 1, 2 y 3. Por tanto, A, B y C son simplemente diferentes formas de representar el mismo conjunto.

b. $\{0\} \neq 0$ porque $\{0\}$ es un conjunto con un elemento, a saber, 0, mientras que 0 es sólo el símbolo que representa al número cero.

c. El conjunto $\{1, \{1\}\}$ tiene dos elementos: 1 y el conjunto cuyo único elemento es 1.

d. $U_1 = \{1, -1\}$, $U_2 = \{2, -2\}$, $U_0 = \{0, -0\} = \{0, 0\} = \{0\}$.

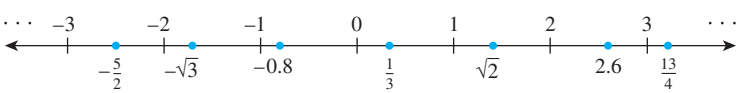
A algunos conjuntos de números se les refiere con tanta frecuencia que se les da nombres simbólicos especiales. Estos se resumen en la tabla de la página siguiente.

Símbolo	Conjunto
R	conjunto de todos los números reales
Z	conjunto de todos los enteros
Q	conjunto de todos los números racionales, o cocientes de enteros

Nota La **Z** es la primera letra de la palabra alemana enteros, *Zahlen*. Esta se usa para el conjunto de todos los enteros y no se debe usar como una abreviatura de la palabra *entero*.

La adición de un superíndice $+$ o $-$ o las letras *no negativo* indican que sólo los elementos positivos o negativos o no negativos del conjunto, respectivamente, se van a incluir. Por tanto $\mathbf{R}^+$ denota el conjunto de números reales positivos y $\mathbf{Z}^{\text{no negativo}}$ indica al conjunto de enteros no negativos: 0, 1, 2, 3, 4 y así sucesivamente. Algunos autores se refieren al conjunto de los enteros no negativos como el conjunto de **números naturales** y lo denotan por **N**. Otros autores llaman sólo a los enteros positivos, números naturales. Para evitar esta confusión, simplemente evitamos el uso de la frase *números naturales* en este libro.

El conjunto de números reales generalmente se describe como el conjunto de todos los puntos en una recta, como se muestra a continuación. El número 0 corresponde al punto medio, llamado el *origen*. Se marca una unidad de distancia y cada punto a la derecha del origen corresponde a un número real positivo que se encuentran calculando la distancia desde el origen. Cada punto a la izquierda del origen corresponde a un número real negativo, que se denota calculando su distancia del origen y poniendo un signo menos delante del número resultante. Por tanto, el conjunto de números reales se divide en tres partes: el conjunto de números reales positivos, el conjunto de números reales negativos y el número 0. *Observe que 0 no es ni positivo ni negativo*. Se han etiquetado algunos pocos números reales correspondientes a los puntos en la recta que se muestra a continuación.



La recta numérica real se llama *continua* porque se supone que no tiene huecos. Al conjunto de enteros corresponde un conjunto de puntos situados a intervalos fijos a lo largo de la recta real. Así, cada número entero es un número real y ya que los números enteros están separados unos de otros, el conjunto de los enteros se llama *discreto*. El nombre de *matemáticas discretas* proviene de la distinción entre los objetos matemáticos continuos y discretos.

Otra forma de definir un conjunto es utilizar lo que se conoce como la *notación constructiva del conjunto*.

Nota Leemos la llave izquierda como "el conjunto de todos" y la línea vertical como "tal que". Sin embargo, en todos los demás contextos matemáticos, no utilizamos una línea vertical para indicar las palabras "tal que"; abreviamos "tal que" como "t. q." o "t. qu." o "$\cdot \ni \cdot$".

• Notación constructiva del conjunto

Sea S un conjunto y sea $P(x)$ una propiedad que los elementos de S pueden o no pueden satisfacer. Podemos definir un nuevo conjunto como **el conjunto de todos los elementos x en S tal que $P(x)$ es verdadera**. Definimos este conjunto de la siguiente manera:

$$\{x \in S \mid P(x)\}$$

el conjunto de todas las — tal que

De vez en cuando vamos a escribir $\{x \mid P(x)\}$, sin precisar más acerca de dónde proviene el elemento x. Resulta que el uso incontrolado de esta notación puede dar lugar a contradicciones reales en la teoría de conjuntos. Vamos a analizar uno de estos en la sección 6.4 y se tratará con cuidado el uso de esta notación exclusivamente como una conveniencia en caso de que el conjunto S se deba especificar si es necesario.

Ejemplo 1.2.2 Uso de la notación constructiva del conjunto

Dado que **R** denota el conjunto de todos los números reales, **Z** el conjunto de todos los enteros y $\mathbf{Z}^+$ el conjunto de todos los enteros positivos, describa cada uno de los siguientes conjuntos.

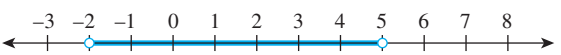
a. $\{x \in \mathbf{R} \mid -2 < x < 5\}$

b. $\{x \in \mathbf{Z} \mid -2 < x < 5\}$

c. $\{x \in \mathbf{Z}^+ \mid -2 < x < 5\}$

Solución

a. $\{x \in \mathbf{R} \mid -2 < x < 5\}$ es el intervalo abierto de los números reales (estrictamente) entre -2 y 5. Se ilustran de la siguiente manera:



b. $\{x \in \mathbf{Z} \mid -2 < x < 5\}$ es el conjunto de todos los enteros (estrictamente) entre -2 y 5. Es igual al conjunto $\{-1, 0, 1, 2, 3, 4\}$.

c. Dado que todos los números enteros en $\mathbf{Z}^+$ son positivos, $\{x \in \mathbf{Z}^+ \mid -2 < x < 5\} = \{1, 2, 3, 4\}$. ■

Subconjuntos

Una relación básica entre conjuntos es la de subconjunto

• Definición

Si A y B son conjuntos, entonces A se llama un **subconjunto** de B, que se escribe como $A \subseteq B$, si y sólo si, cada elemento de A es también un elemento de B.

Simbólicamente:

$A \subseteq B$ significa que Para todos los elementos x, si $x \in A$ entonces, $x \in B$.

Las frases *A está contenido en B* y *B contiene a A* son formas alternativas de decir que A es un subconjunto de B.

De la definición de subconjunto se deduce que un conjunto A que no es un subconjunto de un conjunto B significa que hay al menos un elemento de A que no es un elemento de B. Simbólicamente:

$A \not\subseteq B$ significa que Hay al menos un elemento x tal que $x \in A$ y $x \notin B$.

• Definición

Sean A y B conjuntos. A es un **subconjunto propio** de B si y sólo si, cada elemento de A está en B, pero hay al menos un elemento de B que no está en A.

Ejemplo 1.2.3 Subconjuntos

Sea $A = \mathbf{Z}^+$, $B = \{n \in \mathbf{Z} \mid 0 \leq n \leq 100\}$ y $C = \{100, 200, 300, 400, 500\}$. Evalúe si los siguientes enunciados son verdaderos o falsos.

a. $B \subseteq A$
b. C es un subconjunto propio de A
c. C y B tienen al menos un elemento en común
d. $C \subseteq B$ e. $C \subseteq C$

Solución

a. Falso. Cero no es un entero positivo. Por tanto cero está en B, pero no está en A y así $B \not\subseteq A$,

b. Verdadero. Cada elemento de C es entero positivo y, así, está en A, pero hay elementos en A que no están en C. Por ejemplo, 1 está en A y no en C.

c. Verdadero. Por ejemplo, 100 está tanto en C como B.

d. Falso. Por ejemplo, 200 está en C, pero no en B.

e. Verdadero. Cada elemento de C está en C. En general, la definición de subconjunto implica que todos los conjuntos son subconjuntos de sí mismos.

Ejemplo 1.2.4 Distinción entre $\in$ y $\subseteq$

¿Cuál de los siguientes enunciados son verdaderos?

a. $2 \in \{1, 2, 3\}$ b. $\{2\} \in \{1,2, 3\}$ c. $2 \subseteq \{1, 2, 3\}$
d. $\{2\} \subseteq \{1, 2, 3\}$ e. $\{2\} \subseteq \{\{1\}, \{2\}\}$ f. $\{2\} \in \{\{1\}, \{2\}\}$

Solución Sólo *a*), *d*) y *f*) son verdaderos.

Para que *b*) sea verdadero, el conjunto $\{1, 2, 3\}$ tendría que contener al elemento $\{2\}$. Pero, los únicos elementos de $\{1, 2, 3\}$ son 1, 2 y 3 y 2 no es igual a $\{2\}$. Por tanto *b*) es falso.

Para que *c*) sea verdadero, el número 2 tendría que ser un conjunto y todos los elementos en el conjunto de dos tendrían que ser un elemento de $\{1, 2, 3\}$. Este no es el caso, por lo que *c*) es falso.

Para que *e*) sea verdadero, todos los elementos en el conjunto que contienen sólo el número 2 tendría que ser un elemento del conjunto cuyos elementos son $\{1\}$ y $\{2\}$. Pero 2 no es igual a $\{1\}$ o a $\{2\}$ y así *e*) es falsa. ■

Productos cartesianos

Problemy monthly, julio 1959

Kazimierz Kuratowski (1896-1980)

Con la introducción de la teoría de conjuntos de Georg Cantor en el siglo XIX, comenzó a parecer posible poner a las matemáticas con fundamentos lógicos firmes mediante el desarrollo de todas sus diferentes ramas de la teoría de conjuntos y lógica. Un obstáculo importante fue el uso de conjuntos para definir un par ordenado, ya que la definición de un conjunto no se ve afectada por el orden en el que se listan a sus elementos. Por ejemplo, $\{a, b\}$ y $\{b, a\}$ representan el mismo conjunto, mientras que en un par ordenado queremos ser capaces de indicar qué elemento es primero.

En 1914, El matemático alemán Félix Hausdorff (1868-1942) y Norbert Wiener (1894-1964), un joven estadounidense que había recibido recientemente su doctorado de Harvard hicieron un importante adelanto. Ambos dieron definiciones que mostraban que un par ordenado se puede definir como un cierto tipo de sistema, pero ambas definiciones son algo complicadas. Por último, en 1921, el matemático polaco Kazimierz Kuratowski (1896-1980)

publicó la siguiente definición, que se ha vuelto común. Se dice que un par ordenado es un conjunto de la forma

$$\{\{a\}, \{a, b\}\}.$$

Este conjunto tiene elementos, $\{a\}$ y $\{a, b\}$. Si $a \neq b$, entonces los dos conjuntos son distintos y a está en ambos conjuntos, mientras que b no lo está. Esto nos permite distinguir entre a y b y decir que a es el primer elemento del par ordenado y b es el segundo elemento del par. Si $a = b$, entonces simplemente podemos decir que a es a la vez el primero y el segundo elemento del par. En este caso el conjunto que define el par ordenado será $\{\{a\}, \{a, a\}\}$, que es igual a $\{\{a\}\}$.

Sin embargo, no fue hasta mucho tiempo después que se han utilizado los pares ordenados ampliamente en las matemáticas, que los matemáticos se dieron cuenta de que era posible definirlos totalmente en términos de conjuntos, y, en cualquier caso, la notación de conjunto sería complicada para utilizarse habitualmente. La notación habitual de los pares ordenados dada por $\{\{a\}, \{a, b\}\}$ se escribe más simplemente como (a, b).

• Notación

Dados los elementos a y b, el símbolo (a, b) denota el **par ordenado** formado por a y b junto con las especificaciones de que a es el primer elemento del par y b es el segundo elemento. Dos pares ordenados (a, b) y (c, d) son iguales si y sólo si, $a = c$ y $b = d$. Simbólicamente:

$$(a, b) = (c, d) \quad \text{significa que} \quad a = c \text{ y } b = d.$$

Ejemplo 1.2.5 Pares ordenados

a. ¿Es $(\mathrm{l}, 2) = (2, 1)$?

b. ¿Es $\left(3, \frac{5}{10}\right) = \left(\sqrt{9}, \frac{1}{2}\right)$?

c. ¿Cuál es el primer elemento de $(1, 1)$?

Solución

a. No. Por definición de la igualdad de pares ordenados,

$$(1, 2) = (2, 1) \text{ si y sólo si, } 1 = 2 \text{ y } 2 = 1.$$

Pero $1 \neq 2$ y así los pares ordenados no son iguales.

b. Sí. Por definición de la igualdad de pares ordenados,

$$\left(3, \frac{5}{10}\right) = \left(\sqrt{9}, \frac{1}{2}\right) \text{ si y sólo si, } 3 = \sqrt{9} \text{ y } \frac{5}{10} = \frac{1}{2}.$$

Debido a que estas ecuaciones son verdaderas, los pares ordenados son iguales.

c. En el par ordenado $(1, 1)$, el primero y los segundos elementos son ambos 1.

• Definición

Dados los conjuntos A y B, el **producto cartesiano de A y B**, denotado por $A \times B$ y que se lee como "A cruz B", es el conjunto de todos los pares ordenados (a, b), tal que a está en A y b está en B. Simbólicamente:

$$A \times B = \{(a, b) \mid a \in A \text{ y } b \in B\}.$$

Ejemplo 1.2.6 Productos cartesianos

Sean $A = \{1, 2, 3\}$ y $B = \{u, v\}$.

a. Encuentre $A \times B$

b. Determine $B \times A$

c. Encuentre $B \times B$

d. ¿Cuántos elementos hay en $A \times A$, $B \times A$ y $B \times B$?

e. Sea $\mathbf{R}$ el conjunto de todos los números reales. Describa $\mathbf{R} \times \mathbf{R}$.

Solución

a. $A \times B = \{(1, u), (2, u), (3, u), (1, v), (2, v), (3, v)\}$

b. $B \times A = \{(u, 1), (u, 2), (u, 3), (v, 1), (v, 2), (v, 3)\}$

c. $B \times B = \{(u, u), (u, v), (v, u), (v, v)\}$

Nota ¡Este es el porqué tiene sentido llamar al producto cartesiano un producto!

d. $A \times B$ tiene seis elementos. Observe que éste es el número de elementos en A veces el número de elementos de B. $B \times A$ tiene seis elementos, el número de elementos en B veces el número de elementos en A. $B \times B$ tiene cuatro elementos, el número de elementos en B veces el número de elementos en B.

e. $\mathbf{R} \times \mathbf{R}$ es el conjunto de todos los pares ordenados (x, y) donde x y y son números reales. Si los ejes horizontal y vertical se dibujan en un plano y se marca una unidad de longitud, entonces cada par ordenado de $\mathbf{R} \times \mathbf{R}$ corresponde a un único punto en el plano, con el primer y segundo elemento del par indicando, respectivamente, las posiciones horizontal y vertical del punto. El término **plano cartesiano** se utiliza con frecuencia para referirse a un plano con este sistema de coordenadas, como se muestra en la figura 1.2.1.

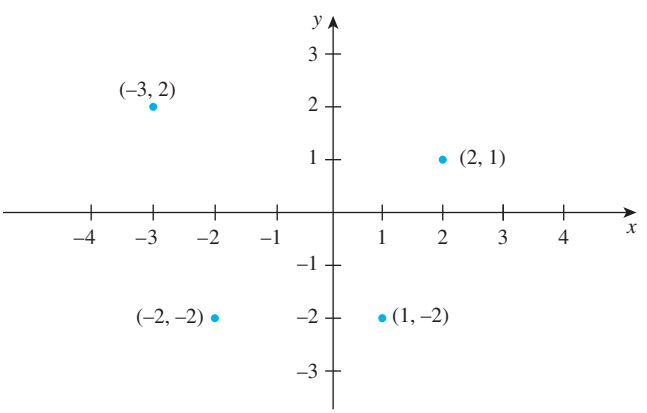


Figura 1.2.1: Un plano cartesiano

Autoexamen

1. Cuando los elementos de un conjunto están dados usando la notación de lista del conjunto, el orden en que se listan _____.
2. El símbolo $\mathbf{R}$ denota _____.
3. El símbolo $\mathbf{Z}$ denota _____.
4. El símbolo $\mathbf{Q}$ denota _____.
5. La notación $\{x \mid P(x)\}$ se lee _____.
6. Que un conjunto A sea un subconjunto de un conjunto B significa que, _____.
7. Dados los conjuntos A y B, el producto cartesiano $A \times B$ es _____.

Conjunto de ejercicios 1.2

1. ¿Cuáles de los siguientes conjuntos son iguales?

$A = \{a, b, c, d\}$ $\quad B = \{d, e, a, c\}$
$C = \{d, b, a, c\}$ $\quad D = \{a, a, d, e, c, e\}$

2. Escriba cómo se lee cada uno de los siguientes enunciados.
   a. $\{x \in \mathbf{R}^+ \mid 0 < x < 1\}$
   b. $\{x \in \mathbf{R} \mid x \leq 0 \text{ o } x \geq 1\}$
   c. $\{n \in \mathbf{Z} \mid n \text{ es un factor de } 6\}$
   d. $\{n \in \mathbf{Z}^+ \mid n \text{ es un factor de } 6\}$

3. a. ¿Es $4 = \{4\}$?
   b. ¿Cuántos elementos hay en el conjunto $\{3, 4, 3, 5\}$?
   c. ¿Cuántos elementos hay en el conjunto $\{1, \{1\}, \{1, \{1\}\}\}$?

4. a. ¿Es $2 \in \{2\}$?
   b. ¿Cuántos elementos hay en el conjunto $\{2, 2, 2, 2\}$?
   c. ¿Cuántos elementos hay en el conjunto $\{0, \{0\}\}$?
   d. ¿Es $\{0\} \in \{\{0\}, \{1\}\}$?
   e. ¿Es $0 \in \{\{0\}, \{1\}\}$?

***H* 5.** ¿Cuál de los siguientes conjuntos son iguales?

$A = \{0, 1, 2\}$
$B = \{x \in \mathbf{R} \mid -1 \leq x < 3\}$
$C = \{x \in \mathbf{R} \mid -1 < x < 3\}$
$D = \{x \in \mathbf{Z} \mid -1 < x < 3\}$
$E = \{x \in \mathbf{Z}^+ \mid -1 < x < 3\}$

***H* 6.** Para cada entero n, sea $T_n = \{n, n^2\}$. ¿Cuántos elementos están en cada uno de T_2, T_{-3}, T_1 y T_0? Justifique sus respuestas.

7. Use la notación de lista de conjuntos para indicar los elementos de cada uno de los siguientes conjuntos.
   a. $S = \{n \in \mathbf{Z} \mid n = (-1)^k$, para algún entero $k\}$.
   b. $T = \{m \in \mathbf{Z} \mid m = 1 + (-1)^i$, para algún entero $i\}$.
   c. $U = \{r \in \mathbf{Z} \mid 2 \leq r \leq -2\}$
   d. $V = \{s \in \mathbf{Z} \mid s > 2 \text{ o } s < 3\}$
   e. $W = \{t \in \mathbf{Z} \mid 1 < t < -3\}$
   f. $X = \{u \in \mathbf{Z} \mid u \leq 4 \text{ o } u \geq 1\}$

8. Sea $A = \{c, d, f, g\}$, $B = \{f, j\}$ y $C = \{d, g\}$. Responda cada una de las siguientes preguntas. Dé razones para cada una de sus respuestas.
   a. ¿Es $B \subseteq A$? b. ¿Es $C \subseteq A$?
   c. ¿Es $C \subseteq C$? d. ¿Es C un subconjunto propio de A?

9. **a.** ¿Es $3 \in \{1, 2, 3\}$? **b.** ¿Es $1 \subseteq \{1\}$?
   c. ¿Es $\{2\} \in \{1, 2\}$? d. ¿Es $\{3\} \in \{1, \{2\}, \{3\}\}$?
   e. ¿Es $1 \in \{1\}$? f. ¿Es $\{2\} \subseteq \{1, \{2\}, \{3\}\}$?
   g. ¿Es $\{1\} \subseteq \{1, 2\}$? h. ¿Es $1 \in \{\{1\}, 2\}$?
   i. ¿Es $\{1\} \subseteq \{1, \{2\}\}$? j. ¿Es $\{1\} \subseteq \{1\}$?

10. **a.** ¿Es $((-2)^2, -2^2) = (-2^2, (-2)^2)$?
    b. ¿Es $(5, -5) = (-5, 5)$?
    c. ¿Es $(8 - 9, \sqrt[3]{-1}) = (-1, -1)$?
    d. ¿(Es $\left(\frac{-2}{-4}, (-2)^3\right) = \left(\frac{3}{6}, -8\right)$?

11. Sea $A = \{w, x, y, z\}$ y $B = \{a, b\}$. Utilice la notación de lista del conjunto para escribir cada uno de los siguientes conjuntos, e indique el número de elementos que hay en cada conjunto:
   a. $A \times B$ b. $B \times A$
   c. $A \times A$ d. $B \times B$

12. Sea $S = \{2, 4, 6\}$ y $T = \{1,3, 5\}$. Utilice la notación de lista del conjunto para escribir cada uno de los siguientes conjuntos, e indique el número de elementos que hay en cada conjunto:
   a. $S \times T$ b. $T \times S$
   c. $S \times S$ d. $T \times T$

Respuestas del autoexamen

1. no importa 2. el conjunto de todos los números reales 3. el conjunto de todos los enteros 4. el conjunto de todos los números racionales 5. el conjunto de todas las x tal que $P(x)$ 6. cada elemento de A es un elemento de B 7. el conjunto de todos los pares ordenados (a, b) tal que a está en A y b se encuentra en B

1.3 El lenguaje de las relaciones y funciones

Las matemáticas son un lenguaje. —Josiah Willard Gibbs (1839-1903)

Hay muchos tipos de relaciones en el mundo. Por ejemplo, decimos que dos personas están relacionadas por la sangre si comparten un antepasado común y que están relacionadas por matrimonio si una comparte un antepasado común con el cónyuge de la otra. También hablamos de la relación entre estudiante y profesor, entre personas que trabajan para el mismo jefe y entre personas que comparten un origen étnico común.

Del mismo modo, los objetos de las matemáticas pueden estar relacionados de diversas maneras. Un conjunto A se puede decir que está relacionado con un conjunto B si A es un subconjunto de B, o si A no es un subconjunto de B, o si A y B tienen al menos un elemento en común. Se puede decir que un número x está relacionado con un número y si $x < y$, o si

x es un factor de y, o si $x^2 + y^2 = 1$. Se puede decir que dos identificadores en un programa de computadora están relacionados si tienen los mismos primeros ocho caracteres, o si utilizan la misma posición de memoria para almacenar sus valores cuando se ejecuta el programa. ¡Y la lista podría continuar!

Sea $A = \{0, 1, 2\}$ y $B = \{1, 2, 3\}$ y digamos que un elemento x de A está relacionado con un elemento y en B, si y sólo si, x es menor que y. Usamos la notación $x\ R\ y$ como una abreviatura de la frase "x está relacionada con y". Entonces,

$$\begin{array}{llll} 0\ R\ 1 & \text{ya que} & 0 < 1, & \\ 0\ R\ 2 & \text{ya que} & 0 < 2, & \\ 0\ R\ 3 & \text{ya que} & 0 < 3, & \\ 1\ R\ 2 & \text{ya que} & 1 < 2, & \\ 1\ R\ 3 & \text{ya que} & 1 < 3 & \text{y} \\ 2\ R\ 3 & \text{ya que} & 2 < 3. & \end{array}$$

Por otro lado, si la notación $x\ \not R\ y$ representa la frase "x no está relacionada con y", entonces

$$\begin{array}{llll} 1\ \not R\ 1 & \text{ya que} & 1 \not< 1, & \\ 2\ \not R\ 1 & \text{ya que} & 2 \not< 1 & \text{y} \\ 2\ \not R\ 2 & \text{ya que} & 2 \not< 2, & \end{array}$$

Recuerde que el producto cartesiano de A y B, $A \times B$, consiste de todos los pares ordenados, cuyo primer elemento se encuentra en A y cuyo segundo elemento se encuentra en B:

$$A \times B = \{(x, y) \mid x \in A \text{ y } y \in B\}.$$

En este caso,

$$A \times B = \{(0, 1), (0, 2), (0, 3), (1, 1), (1, 2), (1, 3), (2, 1), (2, 2), (2, 3)\}.$$

Los elementos de algunos pares ordenados de $A \times B$ están relacionados, mientras que los elementos de otros pares ordenados no lo están. Considere el conjunto de todos los pares ordenados en $A \times B$ cuyos elementos están relacionados

$$\{(0, 1), (0, 2), (0, 3), (1, 2), (1, 3), (2, 3)\}.$$

Observe que el conocimiento de que los pares ordenados se encuentran en este grupo es equivalente a saber qué elementos están relacionados con qué. La relación misma por tanto se puede considerar como el conjunto de pares ordenados cuyos elementos están relacionados por la condición dada. La definición matemática formal de la relación, sobre la base de esta idea, fue presentada por el matemático y lógico estadounidense C. S. Pierce en el siglo XIX.

• Definición

Sean A y B conjuntos. Una **relación R de A a B** es un subconjunto de $A \times B$. Dando un par ordenado (x, y) en $A \times B$, **x está relacionada con y por R**, que se escribe $x\ R\ y$, si y sólo si (x, y), está en R. El conjunto A se llama el dominio de R y el conjunto B se llama su codominio.

La notación para una relación R se puede escribir simbólicamente de la siguiente manera:

$$x\ R\ y \quad \text{significa que} \quad (x, y) \in R.$$

La notación $x\ \not R\ y$ significa que x no se relaciona con y por R:

$$x\ \not R\ y \quad \text{significa que} \quad (x, y) \notin R.$$

Ejemplo 1.3.1 Una relación como un subconjunto

Sea $A = \{1, 2\}$ y $B = \{1, 2, 3\}$ y se define una relación R de A a B de la siguiente manera: Dado cualquier $(x, y) \in A \times B$,

$$(x, y) \in R \quad \text{significa que,} \quad \frac{x - y}{2} \text{ es un entero.}$$

a. De manera explícita establezca qué pares ordenados están en $A \times B$ y cuáles están en R.

b. ¿Es 1 R 3? ¿Es 2 R 3? ¿Es 2 R 2?

c. ¿Cuáles son el dominio y el codominio de R?

Solución

a. $A \times B = \{(1, 1), (1, 2), (1,3), (2, 1), (2, 2), (2, 3)\}$. Para determinar explícitamente la composición de R, examine cada par ordenado en $A \times B$ para ver si sus elementos cumplen la condición de definición de R.

$(1, 1) \in R$, porque $\frac{1-1}{2} = \frac{0}{2} = 0$, que es un entero.
$(1, 2) \notin R$, porque $\frac{1-2}{2} = \frac{-1}{2}$, que no es un entero.
$(1, 3) \in R$, porque $\frac{1-3}{2} = \frac{-2}{2} = -1$, que es un entero.
$(2, 1) \notin R$, porque $\frac{2-1}{2} = \frac{1}{2}$, que no es un entero.
$(2, 2) \in R$, porque $\frac{2-2}{2} = \frac{0}{2} = 0$, que es un entero.
$(2, 3) \notin R$, porque $\frac{2-3}{2} = \frac{-1}{2}$, que no es un entero.

Por tanto

$$R = \{(1, 1), (1, 3), (2, 2)\}$$

b. Sí, 1 R 3, ya que $(1, 3) \in$ R.
No, 2 $\not R$ 3, ya que $(2, 3) \notin R$.
Sí, 2 R 2 porque $(2, 2) \in R$.

c. El dominio de R es $\{1, 2\}$ y el codominio es $\{1, 2, 3\}$. ■

Ejemplo 1.3.2 La relación de la circunferencia

Defina una relación C de $\mathbf{R}$ a $\mathbf{R}$ de la siguiente manera: Para cualquier $(x, y) \in \mathbf{R} \times \mathbf{R}$,

$$(x, y) \in C \quad \text{significa que} \quad x^2 + y^2 = 1.$$

a. ¿Es (l, 0) $\in C$? ¿Es (0, 0) $\in C$? ¿Es $\left(-\frac{1}{2}, \frac{\sqrt{3}}{2}\right) \in C$? ¿Es -2 C 0? ¿Es 0 C O (-1)? ¿Es 1 C 1?

b. ¿Cuáles son el dominio y el codominio de C?

c. Dibuje una gráfica para C trazando los puntos de C en el plano cartesiano.

Solución

a. Sí, $(1, 0) \in C$ ya que $1^2 + 0^2 = 1$.
No, $(0, 0) \notin C$ ya que $0^2 + 0^2 = 0 \neq 1$.
Sí, $\left(-\frac{1}{2}, \frac{\sqrt{3}}{2}\right) \in C$ ya que $\left(-\frac{1}{2}\right)^2 + \left(\frac{\sqrt{3}}{2}\right)^2 = \frac{1}{4} + \frac{3}{4} = 1$.
No, $-2 \not C$ 0 ya que $(-2)^2 + 0^2 = 4 \neq 1$.
Sí, 0 C (-1) ya que $0^2 + (-1)^2 = 1$.
No, 1 $\not C$ 1 ya que $1^2 + 1^2 = 2 \neq 1$.

b. El dominio y el codominio de C son ambos $\mathbf{R}$, el conjunto de todos los números reales.

c.

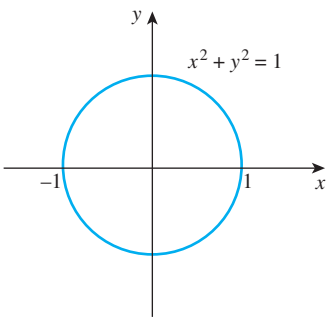


Diagrama de flechas de una relación

Supongamos que R es una relación de un conjunto A a un conjunto B. El **diagrama de flechas para R** se obtiene de la siguiente manera:

1. Se representan los elementos de A como puntos en una región y los elementos de B como puntos en otra región.
2. Para cada x en A y y en B, dibuje una flecha de x a y si y sólo si, x está relacionada con y por R. Simbólicamente:

Se dibuja una flecha de x a y
si y sólo si, $x\ R\ y$
si y sólo si, $(x, y) \in R$.

Ejemplo 1.3.3 Diagramas de flechas de relaciones

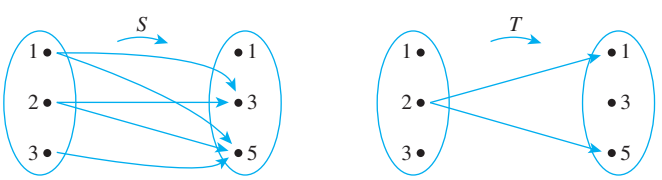
Sea $A = \{1, 2, 3\}$ y $B = \{1, 3, 5\}$ y defina las relaciones S y T de A a B de la siguiente manera: Para toda $(x, y) \in A \times B$,

$(x, y) \in S$ significa que $x < y$ S es una relación "menor que".

$T = \{(2, 1), (2, 5)\}$

Dibuje diagramas de flechas para S y T.

Solución



Estos ejemplos de relaciones muestran que es posible tener varias flechas que salen de un mismo elemento de A apuntando en direcciones diferentes. Además, es muy posible tener un elemento de A que no tenga una flecha que salga de ella.

Funciones

En el punto 1.2 se demostró que los pares ordenados se pueden definir en términos de conjuntos y se definieron los productos cartesianos en términos de pares ordenados. En esta sección presentamos las relaciones como subconjuntos del producto cartesiano. Así, ahora podemos definir las funciones de una manera que sólo dependan del concepto de conjunto. Aunque esta definición no está, obviamente, relacionada con la forma en que se

suele trabajar con funciones en matemáticas, es satisfactoria desde el punto teórico y a los científicos de la computación les gusta porque es especialmente adecuada para trabajar con funciones en una computadora.

• Definición

Una función *F* de un conjunto *A* a un conjunto *B* es una relación con el dominio A y codominio B que satisface las siguientes dos propiedades:

1. Para cada elemento x en A, existe un elemento y en B tal que $(x, y) \in F$.
2. Para todos los elementos x de A y y y z en B,

$$\text{si } (x, y) \in F \text{ y } (x, z) \in F, \quad \text{entonces} \quad y = z.$$

Las propiedades 1) y 2) se pueden enunciar de manera menos formal de la siguiente manera: Una relación F de A a B es una función si y sólo si:

1. Cada elemento de A es el primer elemento de un par ordenado de F.
2. No hay dos pares ordenados distintos en F que tengan el mismo primer elemento.

En la mayoría de situaciones matemáticas pensamos en una función como el envío de elementos de un conjunto, el dominio, a los elementos de otro conjunto, el codominio. Debido a la definición de la función, cada elemento en el dominio corresponde a uno y sólo uno de los elementos del codominio.

Más precisamente, si F es una función de un conjunto A a un conjunto B, entonces dado cualquier elemento x en A, la propiedad 1) de la definición de función se garantiza que hay al menos un elemento de B que está relacionado con x por F y la propiedad 2) garantiza que hay a lo más un elemento. Esto hace que sea posible dar el elemento que corresponde a x un nombre especial.

• Notación

Si A y B son conjuntos y F es una función de A a B, entonces dado cualquier elemento x en A, el único elemento en B que está relacionado con x por F se denota, $\boldsymbol{F(x)}$, que se lee **"F de x"**.

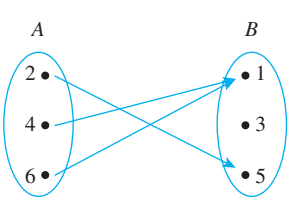
Ejemplo 1.3.4 Funciones y relaciones en conjuntos finitos

Sea $A = \{2, 4, 6\}$ y $B = \{1, 3, 5\}$. ¿Cuál de las relaciones R, S y T que se definen a continuación son funciones de A a B?

a. $R = \{(2, 5), (4, 1), (4, 3), (6, 5)\}$

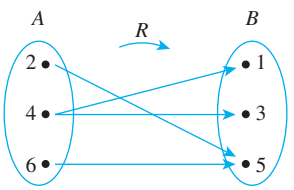
b. Para toda $(x, y) \in A \times B$, $(x, y) \in S$ significa que $y = x + 1$.

c. T está definida por el diagrama de flechas

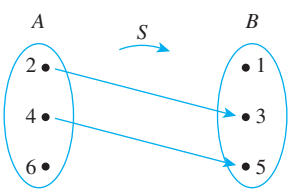


Solución

a. R no es una función, ya que no cumple la propiedad 2). Los pares ordenados (4, 1) y (4, 3) tienen el mismo primer elemento, pero diferentes segundos elementos. Puede ver esto gráficamente si se dibuja el diagrama de flechas para R. Hay dos flechas que salen de 4: Una apunta hacia 1 y la otra apunta hacia 3.



b. S no es una función, ya que no cumple la propiedad 1). No es verdad que cada elemento de A es el primer elemento de un par ordenado en S. Por ejemplo, $6 \in A$, pero no hay y en B tal que $y = 6 + 1 = 7$. También puede ver esto gráficamente dibujando el diagrama de flechas para S.



Nota En el inciso *c*), $T(4) = T(6)$. Esto ilustra el hecho de que, aunque ningún elemento del dominio de una función pueda estar relacionado con más de un elemento del codominio, diferentes elementos en el dominio puede estar relacionados con el mismo elemento en el codominio.

c. T es una función: Cada elemento de $\{2, 4, 6\}$ está relacionado con algún elemento en $\{1, 3, 5\}$ y no hay ningún elemento en $\{2, 4, 6\}$ que esté relacionado con más de un elemento de $\{1, 3, 5\}$. Cuando estas propiedades se expresan en términos del diagrama de flechas, se convierten en 1) hay una flecha que sale de cada elemento del dominio y 2) ningún elemento del dominio tiene más de una flecha que sale de ella. Así se puede escribir $T(2) = 5$, $T(4) = 1$ y $T(6) = 1$. ■

Ejemplo 1.3.5 Funciones y relaciones en conjuntos de números reales

a. En el ejemplo 1.3.2 de la relación de la circunferencia C se definió de la siguiente manera:

$$\text{Para toda } (x, y) \in \mathbf{R} \times \mathbf{R}, \quad (x, y) \in C \quad \text{significa que} \quad x^2 + y^2 = 1.$$

¿C es una función? Si es así, determine $C(0)$ y $C(1)$.

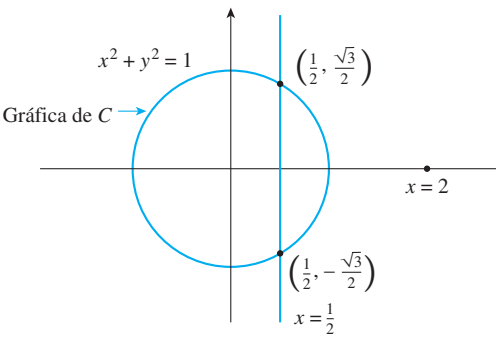
b. Defina una relación de $\mathbf{R}$ a $\mathbf{R}$ como sigue:

$$\text{Para toda } (x, y) \in \mathbf{R} \times \mathbf{R}, \quad (x, y) \in \quad L \text{ significa que} \quad y = x - 1.$$

¿L es una función? Si es así, determine $L(0)$ y $L(1)$.

Solución

a. La gráfica de C, que se muestra en la página siguiente, indica que C no cumple cualquiera de las propiedades de función. Para ver por qué C no cumple la propiedad 1), observamos que hay muchos números reales x tal que $(x, y) \notin C$ para cualquier y.



Por ejemplo, cuando $x = 2$, no hay ningún número real y tal que

$$x^2 + y^2 = 2^2 + y^2 = 4 + y^2 = 1$$

porque si la hubiera, entonces tendría que ser verdad que

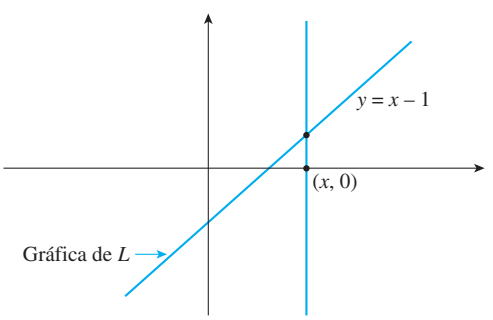
$$y^2 = -3.$$

que no es el caso para cualquier número real y.

Para ver por qué C no cumple la propiedad 2), observe que para algunos valores de x hay dos valores distintos de y tal que $(x, y) \in C$. Una forma de ver esto gráficamente es observar que hay rectas verticales, tal como $x = \frac{1}{2}$, que intersectan la gráfica de C en dos puntos separados: $\left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$ y $\left(\frac{1}{2}, -\frac{\sqrt{3}}{2}\right)$.

b. L es una función. Para cada número real x, $y = x - 1$ es un número real y así que hay un número real y con $(x, y) \in L$. También si $(x, y) \in L$ y $(x, z) \in L$, entonces $y = x - 1$ y $z = x - 1$ así que $y = z$. En particular, $L(0) = 0 - 1 = -1$ y $L(1) = 1 - 1 = 0$.

También puede consultar estos resultados inspeccionando la gráfica de L, que se muestra a continuación. Observe que para todo número real x, la recta vertical que pasa por $(x, 0)$ pasa a través de la gráfica de L exactamente una vez. Esto indica tanto que cada número real x es el primer elemento de un par ordenado en L y también que no hay dos pares ordenados distintos en L que tengan el mismo primer elemento.



■

Máquinas de funciones

Otra manera útil de pensar en una función es como una máquina. Suponga que f es una función de X a Y y que se da una entrada x de X. Imagine que f es una máquina que procesa x de una cierta manera que produce la salida $f(x)$. Esto se muestra, en la figura 1.3.1 de la página siguiente.

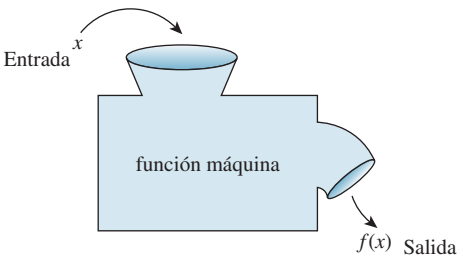


Figura 1.3.1

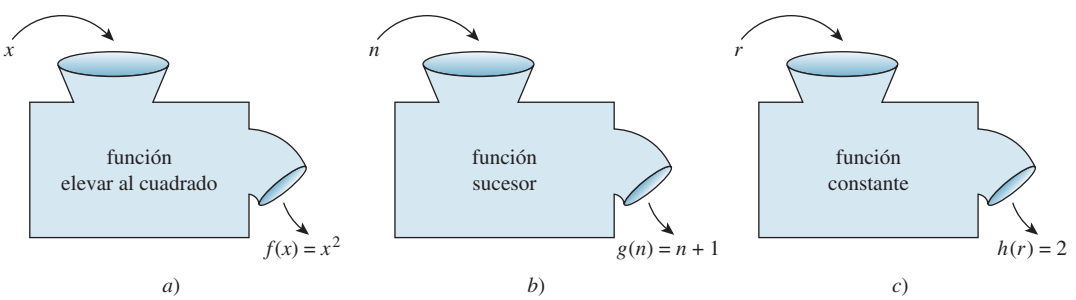
Ejemplo 1.3.6 Funciones definidas por fórmulas

La función f **elevar al cuadrado** de $\mathbf{R}$ a $\mathbf{R}$ se define por la fórmula $f(x) = x^2$ para todos los números reales x. Esto significa que no importa qué número real sea la entrada que se sustituye por x, la salida de f será el cuadrado de ese número. Esta idea se puede representar al escribir $f(\square) = \square^2$. En otras palabras, f envía cada número real x a x^2, o, simbólicamente, $f: x \to x^2$. Observe que la variable x es una variable muda y se podría sustituir con cualquier otro símbolo, siempre que la sustitución se haga en todas las partes en que x aparece.

La **función sucesor** g de $\mathbf{Z}$ a $\mathbf{Z}$ se define por la fórmula $g(n) = n + 1$. Por tanto, no importa qué número entero se sustituya por n, la salida de g será el número más uno: $g(\square) = \square + 1$. En otras palabras, g envía cada entero n a $n + 1$, o, simbólicamente, $g: n \to n + 1$.

Un ejemplo de una **función constante** es la función h de $\mathbf{Q}$ a $\mathbf{Z}$ definida por la fórmula $h(r) = 2$ para todos los números racionales r. Esta función envía cada número racional r a 2. En otras palabras, no importa qué entrada sea, la salida es siempre 2: $h(\square) = 2$ o $h: r \to 2$.

Las funciones f, g y h, están representadas por las funciones máquina de la figura 1.3.2.



a) *b)* *c)*

Figura 1.3.2 ■

Una función es una entidad por derecho propio. Se puede considerar como una cierta relación entre conjuntos o como una máquina de entrada/salida que opera de acuerdo a una regla dada. Esta es la razón por la que generalmente una función se denota por un solo símbolo o por una cadena de símbolos, tales como f, G, log o sen.

Una relación es un subconjunto de un producto cartesiano y una función es un tipo especial de relación. En concreto, si f y g son funciones de un conjunto A a un conjunto B, entonces

$$f = \{(x, y) \in A \times B \mid y = f(x)\} \qquad \text{y} \qquad g = \{(x, y) \in A \times B \mid y = g(x)\}.$$

De lo que se deduce que

f es igual a g, que se escribe $f = g$, si y sólo si, $f(x) = g(x)$ para toda x en A.

Ejemplo 1.3.7 Igualdad de funciones

Defina $f: \mathbf{R} \to \mathbf{R}$ y $g: \mathbf{R} \to \mathbf{R}$ con las fórmulas siguientes:

$$f(x) = |x| \quad \text{para toda } x \in \mathbf{R}.$$
$$g(x) = \sqrt{x^2} \quad \text{para toda } x \in \mathbf{R}.$$

¿Es $f = g$?

Solución

Sí. Ya que el valor absoluto de cualquier número real es igual a la raíz cuadrada de su cuadrado, $|x| = \sqrt{x^2}$ para toda $x \in \mathbf{R}$. Por tanto $f = g$. ■

Autoexamen

1. Dados los conjuntos A y B, una relación de A a B es _____.
2. Una función F de A a B es una relación de A a B que satisface las siguientes propiedades:
   a. para cada elemento x de A, existe _____.
   b. para todos los elementos x de A y y y z en B, si _____ entonces _____.
3. Si F es una función de A a B y x es un elemento de A, entonces $F(x)$ es _____.

Conjunto de ejercicios 1.3

1. Sea $A = \{2, 3, 4\}$ y $B = [6, 8, 10\}$ y defina una relación R de A a B como sigue: Para toda $(x, y) \in A \times B$,

$$(x, y) \in R \quad \text{significa que} \quad \frac{y}{x} \text{ es un número entero.}$$

a. ¿Es $4\ R\ 6$? ¿Es $4\ R\ 8$? ¿Es $(3, 8) \in R$? ¿Es $(2, 10) \in R$?
b. Escriba R como un conjunto de pares ordenados.
c. Escriba el dominio y el codominio de R.
d. Dibuje un diagrama de flechas para R.

2. Sea $C = D = \{-3, -2, -1, 1, 2, 3\}$ y defina una relación S de C a D de la siguiente manera: Para toda $(x, y) \in C \times D$,

$$(x, y) \in S \quad \text{significa que} \quad \frac{1}{x} - \frac{1}{y} \text{ es un número entero.}$$

a. ¿Es $2\ S\ 2$? ¿Es $-1\ S\ -1$? ¿Es $(3, 3) \in S$? ¿Es $(3, -3) \in S$?
b. Escriba S como un conjunto de pares ordenados.
c. Escriba el dominio y el codominio de S.
d. Dibuje un diagrama de flechas para S.

3. Sea $E = \{1, 2, 3\}$ y $F = \{-2, -1, 0\}$ y defina una relación T de E a F de la siguiente manera: Para toda $(x, y) \in E \times F$,

$$(x, y) \in T \quad \text{significa que} \quad \frac{x - y}{3} \text{ es un número entero.}$$

a. ¿Es $3\ T\ 0$? ¿Es $1\ T\ (-1)$? ¿Es $(2, -1) \in T$? ¿Es $(3, -2) \in T$?
b. Escriba T como un conjunto de pares ordenados.
c. Escriba el dominio y el codominio de T.
d. Dibuje un diagrama de flechas para T.

4. Sea $G = \{-2, 0, 2\}$ y $H = \{4, 6, 8\}$ y defina una relación V de G a H de la siguiente manera: Para toda $(x, y) \in G \times H$,

$$(x, y) \in V \quad \text{significa que} \quad \frac{x - y}{4} \text{ es un número entero.}$$

a. ¿Es $2\ V\ 6$? ¿Es $(-2)V(-6)$? ¿Es $(0, 6) \in V$? ¿Es $(2,4) \in V$?
b. Escriba V como un conjunto de pares ordenados.
c. Escriba el dominio y el codominio de V.
d. Dibuje un diagrama de flechas para V.

5. Defina una relación S de $\mathbf{R}$ a $\mathbf{R}$ como sigue:
Para toda $(x, y) \in \mathbf{R} \times \mathbf{R}$,

$$(x, y) \in S \quad \text{significa que} \quad x \geq y.$$

a. ¿Es $(2, 1) \in S$? ¿Es $(2, 2) \in S$? ¿Es $2\ S\ 3$? ¿Es $(-1)\ S\ (-2)$?
b. Dibuje la gráfica de S en el plano cartesiano.

6. Defina una relación R de $\mathbf{R}$ a $\mathbf{R}$ de la siguiente manera: Para toda $(x, y) \in \mathbf{R} \times \mathbf{R}$,

$$(x, y) \in R \quad \text{significa que} \quad y = x^2.$$

a. ¿Es $(2, 4) \in R$? ¿Es $(4, 2) \in R$? ¿Es $(-3)R\ 9$? ¿Es $9\ R\ (-3)$?
b. Dibuje la gráfica de R en el plano cartesiano.

7. Sea $A = \{4, 5, 6\}$ y $B = \{5, 6, 7)$ y defina las relaciones R, S y T de A a B como sigue:
Para toda $(x, y) \in A \times B$,

$(x, y) \in R$ significa que $x \geq y$.

$(x, y) \in S$ significa que $\dfrac{x - y}{2}$ es un número entero.

$T = \{(4, 7), (6, 5), (6, 7)\}$.

a. Dibuje diagramas de flechas para R, S y T.
b. Indique si alguna de las relaciones R, S y T son funciones.

8. Sea $A = \{2, 4\}$ y $B = \{1, 3, 5\}$ y defina las relaciones U, V y W de A a B de la siguiente manera: Para toda $(x, y) \in A \times B$,

$(x, y) \in U$ significa que $y - x > 2$.

$(x, y) \in V$ significa que $y - 1 = \dfrac{x}{2}$.

$W = \{(2, 5), (4, 1), (2, 3)\}$.

a. Dibuje diagramas de flechas para U, V y W.
b. Indique si alguna de las relaciones U, V y W son funciones.

9. a. Encuentre todas las relaciones de $\{0,1\}$ a $\{1\}$.
b. Encuentre todas las funciones de $\{0,1\}$ a $\{1\}$.
c. ¿Qué fracción de las relaciones de $\{0,1\}$ a $\{1\}$ son funciones?

10. Determine cuatro relaciones de $\{a, b\}$ a $\{x, y\}$ que no sean funciones de $\{a, b\}$ a $\{x, y\}$.

11. Defina una relación P de $\mathbf{R}^+$ a $\mathbf{R}$ de la siguiente manera: Para todos los números reales x y y con $x > 0$,

$$(x, y) \in P \quad \text{significa que} \quad x = y^2.$$

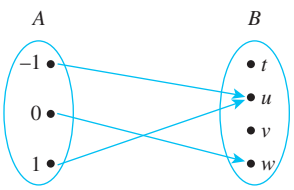
¿P es una función? Explique.

12. Defina una relación T de $\mathbf{R}$ a $\mathbf{R}$ de la siguiente manera: Para todos los números reales x y y,

$$(x, y) \in T \quad \text{significa que} \quad y^2 - x^2 = 1.$$

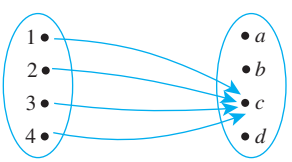
¿T es una función? Explique.

13. Sea $A = \{-1, 0, 1\}$ y $B = \{t, u, v, w\}$. Defina una función $F: A \to B$ con el siguiente diagrama de flechas:



a. Escriba el dominio y el codominio de F.
b. Determine $F(-1)$, $F(0)$ y $F(1)$.

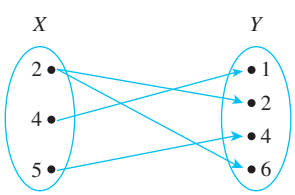
14. Sea $C = \{1, 2, 3, 4\}$ y $D = \{a, b, c, d\}$. Defina una función $G: C \to D$ con el siguiente diagrama de flechas:



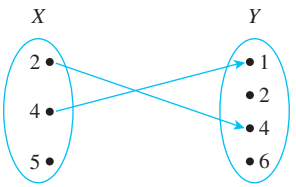
a. Escriba el dominio y el codominio de G.
b. Determine $G(1)$, $G(2)$, $G(3)$ y $G(4)$.

15. Sea $X = \{2, 4, 5\}$ $Y = \{1, 2, 4, 6\}$. ¿Cuál de los siguientes diagramas de flechas determinan las funciones de X a Y?

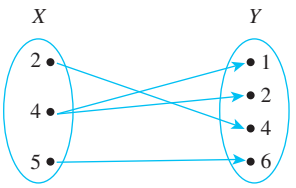
a.



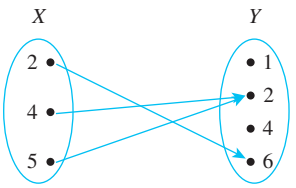
b.



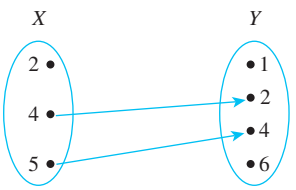
c.



d.



e.



16. Sea f la función elevar al cuadrado definida en el ejemplo 1.3.6. Determine $f(-1)$, $f(0)$ y $f\left(\frac{1}{2}\right)$.

17. Sea g la función sucesor definida en el ejemplo 1.3.6. Encuentre $g(-1000)$, $g(0)$ y $g(999)$.

18. Sea h la función constante definida en el ejemplo 1.3.6. Encuentre $h\left(-\frac{12}{5}\right)$, $h\left(\frac{0}{1}\right)$ y $h\left(\frac{9}{17}\right)$.

19. Defina las funciones f y g de $\mathbf{R}$ a $\mathbf{R}$ por las fórmulas siguientes: Para toda $x \in R$,

$$f(x) = 2x \quad \text{y} \quad g(x) = \frac{2x^3 + 2x}{x^2 + 1}.$$

¿Es $f = g$? Explique.

20. Defina las funciones H y K de $\mathbf{R}$ a $\mathbf{R}$ por las fórmulas siguientes: Para toda $x \in \mathbf{R}$,

$$H(x) = (x - 2)^2 \quad \text{y} \quad K(x) = (x - 1)(x - 3) + 1.$$

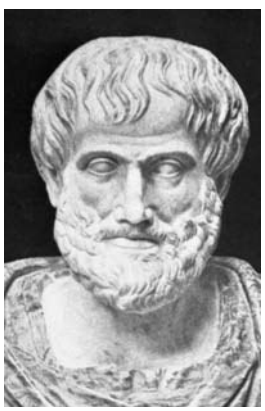
¿Es $H = K$? Explique.

Respuestas del autoexamen

1. un subconjunto del producto cartesiano $A \times B$ 2. a. un elemento de B tal que $(x, y) \in F$ (es decir, tal que x está relacionado con y por F) b. $(x, y) \in F$ y $(x, z) \in F$; $y = z$ 3. el único elemento de B que está relacionado con x por F

CAPÍTULO 2

LA LÓGICA DE LOS ENUNCIADOS COMPUESTOS



Bettmann/CORBIS

Aristóteles
(384 a.C.-322 a.C.)

Los primeros grandes tratados de lógica fueron escritos por el filósofo griego Aristóteles. Eran un conjunto de reglas para el razonamiento deductivo que estaban destinadas a servir de base para el estudio de todas las ramas del conocimiento. En el siglo XVII, el filósofo y matemático alemán Gottfried Leibniz concibió la idea de utilizar símbolos para mecanizar el proceso del razonamiento deductivo de la misma manera que la notación algebraica había mecanizado el proceso de razonamiento de los números y sus relaciones. La idea de Leibniz se realizó en el siglo XIX por los matemáticos ingleses George Boole y Augustus De Morgan, quienes fundaron el moderno tema de la lógica simbólica. Con investigación continúa hasta nuestros días, la lógica simbólica ha proporcionado, entre otras cosas, la base teórica para muchas áreas de la ciencia computacional, tales como el diseño de circuitos lógicos digitales (vea las secciones 2.4 y 2.5), la teoría de base de datos relacionales (vea la sección 8.1), la teoría de autómatas y la computabilidad (vea la sección 7.4 y el capítulo 12) y la inteligencia artificial (vea las secciones 3.3, 10.1 y 10.5).

2.1 Forma lógica y equivalencia lógica

La lógica es una ciencia de las leyes necesarias del pensamiento, sin la cual no se comprende ni se razona. —Immanuel Kant, 1785

El concepto central de la lógica deductiva es el concepto de forma de argumento. Un argumento es una secuencia de enunciados destinados a demostrar la verdad de una frase. La frase al final de la secuencia se llama la *conclusión* y los enunciados anteriores se llaman *premisas*. Para tener confianza en la conclusión que obtiene de un argumento, debe asegurarse de que las premisas sean aceptables por sus propios méritos o que son consecuencia de otros enunciados que se sabe que son verdaderos.

En lógica, la forma de un argumento se distingue de su contenido. El análisis lógico no le ayudará a determinar el valor intrínseco del contenido de un argumento, pero le ayudará a analizar la forma de un argumento para determinar si la verdad de la conclusión se desprende *necesariamente* de la verdad de las premisas. Por esta razón, la lógica a veces se define como la ciencia de la inferencia necesaria o la ciencia del razonamiento.

Considere los siguientes dos argumentos, por ejemplo. Aunque su contenido es muy diferente, su forma lógica es la misma. Ambos argumentos son *válidos* en el sentido de que si sus premisas son verdaderas, entonces sus conclusiones también deben ser verdaderas. (En la sección 2.3 aprenderá cómo comprobar si un argumento es válido).

Argumento 1 Si la sintaxis del programa es defectuosa o si los resultados de la ejecución del programa dan como resultado una división entre cero, la computadora va a generar un mensaje de error. Por tanto, si la computadora no genera un mensaje de error, entonces,

la sintaxis del programa es correcta y la ejecución del programa no da como resultado una división entre cero.

Argumento 2 Si x es un número real tal que $x < -2$ o $x > 2$, entonces $x^2 > 4$. Por tanto, si $x^2 \not> 4$, entonces $x \not< -2$ y $x \not> 2$.

Para mostrar la forma lógica de estos argumentos, utilizamos letras del alfabeto (tal como p, q y r) para representar las frases componentes y la expresión "no p" se refiere a la frase "Este no es el caso que p". Entonces, la *forma lógica común* de ambos argumentos anteriores es la siguiente:

Si p o q, entonces r.
Por tanto, si no r, entonces no p y no q.

Ejemplo 2.1.1 Identificación de forma lógica

Complete los espacios en blanco para que el argumento *b*) tenga que la misma forma que el argumento *a*). Después represente la forma más común de los argumentos usando letras para presentar los enunciados compuestos.

a. Si Jane es una estudiante de la carrera de matemáticas o Jane es una estudiante de la carrera de ciencia computacional, entonces, Jane tendrá 150 en matemáticas.
Jane es una estudiante de ciencia computacional.
Por tanto, Jane tendrá 150 en matemáticas.

b. Si la lógica es fácil o ___1)___, entonces ___2)___.
Voy a estudiar mucho.
Por tanto, voy a obtener una A en este curso.

Solución

1. Voy a estudiar mucho.
2. Voy a obtener una *A* en este curso.

Forma común: Si p o q, entonces r.

q.

Por tanto, r. ■

Enunciados

La mayoría de las definiciones de la lógica formal se han desarrollado de acuerdo con la lógica natural o intuitiva utilizada por personas que han sido educadas para pensar con claridad y utilizar el lenguaje con cuidado. Las diferencias que existen entre la lógica formal e intuitiva son necesarias para evitar la ambigüedad y obtener consistencia.

En cualquier teoría matemática, se definen nuevos términos usando los que se han definido previamente. Sin embargo, este proceso tiene que comenzar en alguna parte. Unos pocos términos iniciales permanecen necesariamente indefinidos. En lógica, las palabras, *enunciado*, *verdadero* y *falso* son términos iniciales indefinidos.

• Definición

Un **enunciado** (o **proposición**) es una frase que es verdadera o falsa, pero no ambas.

Por ejemplo, "Dos más dos son cuatro" y "Dos más dos son cinco", ambos son enunciados, el primero porque es verdad y el segundo porque es falso. Por otro lado, lo verdadero o

lo falso de "Él es un estudiante universitario" depende de la referencia para el pronombre *él*. Para algunos valores de *él* la frase es verdadera, para otros es falsa. Si la frase estuviera precedida de otros enunciados que hacen referencia clara al pronombre, entonces la frase sería un enunciado. Considerada en sí mismo, sin embargo, la frase no es ni verdadera ni falsa, por lo que no es un enunciado. En la sección 3.1, analizaremos la forma de transformar las frases de esta forma en enunciados.

Del mismo modo, "$x + y > 0$" no es un enunciado, porque para algunos valores de x y y la frase es verdadera, mientras que para otros es falsa. Por ejemplo, si $x = 1$ y $y = 2$, la frase es verdadera, si $x = -1$ y $y = 0$, la frase es falsa.

Enunciados compuestos

Ahora introducimos tres símbolos que se utilizan para construir expresiones lógicas más complicadas a partir de otras más simples. El símbolo $\sim$ denota *no*, $\wedge$ denota *y* y $\vee$ denota *o*. Dado un enunciado p, la frase "$\sim p$" se lee "no p" o "No es el caso que p" y se llama **negación de *p***. En algunos lenguajes de programación se utiliza el símbolo $\neg$ en lugar de $\sim$. Dado otro enunciado q, la frase "$p \wedge q$" se lee "p y q" y se llama **conjunción de *p* y *q***. La frase "$p \vee q$" se lee "p o q" y se llama **disyunción de *p* y *q***.

En las expresiones que incluyen al símbolo $\sim$, así como a $\wedge$ o a $\vee$, el **orden de las operaciones** especifica que $\sim$ se realiza primero. Por ejemplo, $\sim p \wedge q = (\sim p) \wedge q$. En expresiones lógicas, como en las expresiones algebraicas ordinarias, el orden de las operaciones se pueden controlar usando paréntesis. Así $\sim(p \wedge q)$ representa la negación de la conjunción de p y q. En esto, como en la mayoría de los tratamientos de lógica, los símbolos $\wedge$ y $\vee$ se consideran iguales en orden de operación y una expresión tal como $p \wedge q \vee r$ se considera ambigua. Esta expresión se debe escribir como $(p \wedge q) \vee r$ o como $p \wedge (q \vee r)$ para tener sentido.

Muchas palabras en español se traducen en lógica como $\wedge$, $\vee$ o $\sim$. Por ejemplo, la palabra, *pero* se traduce como *y* cuando vincula dos cláusulas independientes, como en "Jim es alto pero él no es pesado". En general, la palabra, *pero* se utiliza en lugar de *y* cuando la parte de la frase que sigue es, en cierta forma, inesperada. Otro ejemplo es el de las palabras *"ni-ni"*. Cuando Shakespeare escribió: "Ni un prestatario ni el prestamista son", significaba que, "No es un prestatario y no es un prestamista". Así que si p y q son enunciados, entonces,

p pero q	significa	p y q
ni p ni q	significa	$\sim p$ y $\sim q$.

Ejemplo 2.1.2 Traducción de español a símbolos: *Pero* y *Ni-ni*

Escriba cada una de las siguientes frases simbólicamente, haciendo h = "Hace calor" y s = "Hay sol".

a. No hace calor, pero hay sol.

b. No hace calor ni hay sol.

Solución

a. La frase dada es equivalente a "No hace calor y hay sol", que se puede escribir simbólicamente como $\sim h \wedge s$.

b. Decir que ni hace calor ni hay sol significa que no hace calor y no hay sol. Por tanto, la frase dada puede escribirse simbólicamente como $\sim h \wedge \sim s$. ■

La notación de las desigualdades involucra los enunciados *y* y *o*. Por ejemplo, si x, a y b son números reales dados, entonces,

$x \leq a$	significa	$x < a$	o	$x = a$
$a \leq x \leq b$	significa	$a \leq x$	y	$x \leq b$.

Observe que la desigualdad $2 \leq x \leq 1$ no la satisface ningún número real, ya que

$$2 \leq x \leq 1 \quad \text{significa} \quad 2 \leq x \quad \text{y} \quad x \leq 1,$$

y es falsa, para cualquier número x. Por la forma, el punto dado x, a y b son números reales *particulares*, que aseguran que las frases tales como "$x < a$" y "$x \geq b$" son ya sea verdaderas o falsas y por tanto se trata de enunciados.

Ejemplo 2.1.3 *Y*, *O* y desigualdades

Supongamos que x es un número real particular. Sea que p, q y r, simbolicen "$0 < x$", "$x < 3$" y "$x = 3$", respectivamente. Escriba las siguientes desigualdades simbólicamente:

a. $x \leq 3$ b. $0 < x < 3$ c. $0 < x \leq 3$

Solución

a. $q \vee r$ b. $p \wedge q$ c. $p \wedge (q \vee r)$ ■

Valores de verdad

En los ejemplos 2.1.2 y 2.1.3 construimos frases compuestas de enunciados compuestos y los términos *no*, *y* y *o*. Sin embargo, si esas frases son enunciados, deben tener **valores de verdad** bien definidos —que deben ser ya sea verdaderos o falsos. Ahora definimos dichas frases compuestas como enunciados especificando sus valores de verdad en términos de los enunciados que los componen.

La negación de un enunciado es un enunciado que expresa exactamente lo que significa que el enunciado sea falso.

• Definición

Si p es un enunciado variable, la **negación** de p es "no p" o "No es el caso que p" y se denota $\sim p$. Tiene valores de verdad opuestos a p: si p es verdadera, $\sim p$ es falsa, si p es falsa, $\sim p$ es verdadera.

Los valores de verdad para la negación se resumen en una *tabla de verdad*.

Tabla de verdad para $\sim p$

p	$\sim p$
V	F
F	V

En el lenguaje común la frase "Hace calor y hay sol" se entiende que es verdadera cuando se satisfacen ambas condiciones —que hace calor y que está soleado. Si hace calor, pero no hay sol, o si está soleado pero no hace calor, o si ni hace calor ni está soleado, se entiende que la frase es falsa. La definición formal de los valores de verdad para un enunciado y concuerda con este razonamiento general.

• Definición

Si p y q son enunciados variables, la **conjunción** de p y q que es "p y q" se denota por $p \wedge q$. Es verdadera cuando y sólo cuando, tanto p como q son verdaderos. Si ya sea p o q es falso, o si ambas son falsos, entonces $p \wedge q$ es falso.

Los valores de verdad para la conjunción también se pueden resumir en una tabla de verdad. La tabla se obtiene considerando las cuatro combinaciones posibles de los valores de verdad de p y q. Cada combinación se presenta en un renglón de la tabla, el correspondiente valor de verdad para todo el enunciado se coloca en la columna que está en el extremo derecho en ese renglón. Observe que el único renglón que contiene una V es el primero ya que la única forma de que un enunciado y sea verdadero es que ambos enunciados componentes sean verdaderos.

Tabla de verdad para $p \wedge q$

p	q	$p \wedge q$
V	V	V
V	F	F
F	V	F
F	F	F

Por la forma, el orden de los valores de verdad de p y q en la tabla anterior es VV, VF, FV, FF. No es absolutamente necesario escribir los valores de verdad en este orden, aunque se acostumbra hacerlo. Utilizaremos este orden para todas las tablas de verdad que implican dos enunciados variables. En el ejemplo 2.1.5 mostraremos el orden estándar para tablas de verdad que implican tres enunciados variables.

En el caso de los enunciado de disyunción de la forma "p o q" —la lógica intuitiva ofrece dos interpretaciones alternativas. En el lenguaje común *o* a veces se utiliza en un sentido exclusivo (p o q pero no ambas) y, a veces en un sentido inclusivo (p o q o ambas). Un camarero que le dice que puede ser "café, té, o leche" utiliza la palabra *o* en un sentido exclusivo: Generalmente hay que pagar más si desea más de una bebida. Por otra parte, un camarero que ofrece "crema o azúcar" utiliza la palabra *o* en un sentido inclusivo: Tiene derecho a crema y a azúcar si lo desea.

Los matemáticos y lógicos evitan la posible ambigüedad acerca del significado de la palabra *o* en el entendimiento de lo que significa "y/o" inclusivo. El símbolo $\vee$ proviene de la palabra latina *vel*, que significa *o* en un sentido inclusivo. Para expresar *o* exclusivo; se utiliza la frase p o q, *pero no ambos*.

• Definición

Si p y q son enunciados variables, la **disyunción** de p y q es "p o q", que se denota por $p \vee q$. Es verdadera cuando ya sea que p sea verdad, o que q sea verdad, o que ambas p y q sean verdaderas; es falsa sólo cuando p y q son falsas.

Nota El enunciado "$2 \leq 2$" significa que 2 es menor que 2 o 2 es igual a 2. Es verdadero, ya que $2 = 2$.

La tabla de verdad para la disyunción es:

Tabla de verdad para $p \vee q$

p	q	$p \wedge q$
V	V	V
V	F	V
F	V	V
F	F	F

Evaluando la verdad de los enunciados compuestos más generales

Ahora que se han asignado valores de verdad a $\sim p$, $p \wedge q$ y $p \vee q$, considere cómo asignar valores de verdad a expresiones más complicadas, tales como $\sim p \vee q$, $(p \vee q) \sim (p \wedge q)$ y $(p \wedge q) \vee r$. Estas expresiones se llaman *formas de enunciado* (o *formas proposicionales*). En la sección 2.4, se analiza, la estrecha relación entre las formas de enunciado y las *expresiones booleanas*.

• Definición

Una **forma de enunciado** (o **forma proposicional**) es una expresión formada por enunciados variables (tales como p, q y r) y conectores lógicos (por ejemplo, $\sim$, $\wedge$ y $\vee$) que se convierten en un enunciado cuando los enunciados reales se sustituyen por enunciados compuestos variables. La **tabla de verdad** para un enunciado dado presenta los valores de verdad que corresponden a todas las posibles combinaciones de los valores de verdad de sus enunciados compuestos variables.

Para calcular los valores de verdad para una forma de enunciado, se siguen reglas similares a las utilizadas para evaluar expresiones algebraicas. Para cada combinación de valores de verdad para los enunciados variables, primero se evalúan las expresiones dentro de los paréntesis más internos, después se evalúan las expresiones dentro del siguiente conjunto de paréntesis hacia el exterior y así sucesivamente hasta tener los valores de verdad de la expresión completa.

Ejemplo 2.1.4 Tabla de verdad para *O-exclusivo*

Construya la tabla de verdad para la forma de enunciado $(p \vee q) \wedge \sim(p \wedge q)$. Considere que cuando se utiliza o en su sentido exclusivo, el enunciado "p o q" significa "p o q pero no ambos" o "p o q y no ambos p y q", que se traduce en símbolos como $(p \vee q) \wedge \sim(p \wedge q)$. Esto a veces se abrevia como $p \oplus q$ o p XOR q.

Solución Etiquete columnas tituladas p, q, $p \vee q$, $p \wedge q$, $\sim(p \wedge q)$ y $(p \vee q) \wedge \sim(p \wedge q)$. Llene las columnas p y q con todas las posibles combinaciones lógicas de V y F. Después, utilice las tablas de verdad para $\vee$ y $\wedge$ para completar las columnas $p \vee q$ y $p \wedge q$ con los valores de verdad correspondiente. Después llene la columna $\sim(p \wedge q)$ tomando los opuestos de los valores de verdad de $p \wedge q$. Por ejemplo, la entrada de $\sim(p \wedge q)$ en el primer renglón es F, ya que en el primer renglón el valor de verdad de $p \wedge q$ es V. Por último, llene la columna $(p \vee q) \wedge \sim(p \wedge q)$ considerando la tabla de verdad para un enunciado y junto con los valores de verdad calculados para $p \vee q$ y $\sim(p \wedge q)$. Por ejemplo, la entrada en el primer renglón es F ya que la entrada para $p \vee q$ es V, la entrada de $\sim(p \wedge q)$ es F y un enunciado y es falso a menos que ambos componentes sean verdaderos. La entrada en el segundo renglón es V ya que ambos componentes son verdaderos en este renglón.

Tabla de verdad para *O Exclusiva*: $(p \vee q) \wedge \sim(p \wedge q)$

p	q	$p \vee q$	$p \wedge q$	$\sim(p \wedge q)$	$(p \vee q) \wedge \sim(p \wedge q)$
V	V	V	V	F	F
V	F	V	F	V	V
F	V	V	F	V	V
F	F	F	F	V	F

■

Ejemplo 2.1.5 Tabla de verdad para $(p \wedge q) \vee \sim r$

Construya una tabla de verdad para la forma de enunciado $(p \wedge q) \vee \sim r$.

Solución Titule columnas con p, q, r, $p \wedge q$, $\sim r$ y $(p \wedge q) \vee \sim r$. Introduzca las ocho combinaciones lógicas posibles de valores de verdad para p, q, r y en las tres columnas más hacia la izquierda. Después, llene los valores de verdad para $p \wedge q$ y para $\sim r$. Complete la tabla considerando los valores de verdad de $(p \wedge q)$ y para $\sim r$ y la definición de un enunciado o. Puesto que un enunciado o es falso sólo cuando ambos componentes son falsos, los únicos renglones con entrada F son los renglones tercero, quinto y séptimo, porque esos son los únicos renglones en los que las expresiones $p \wedge q$ y $\sim r$ son falsas. La entrada de todos los otros renglones es V.

p	q	r	$p \wedge q$	$\sim r$	$(p \wedge q) \vee \sim r$
V	V	V	V	F	V
V	V	F	V	V	V
V	F	V	F	F	F
V	F	F	F	V	V
F	V	V	F	F	F
F	V	F	F	V	V
F	F	V	F	F	F
F	F	F	F	V	V

■

El punto esencial de asignación de valores de verdad a los enunciados compuestos es que le permite —usando sólo la lógica— juzgar la verdad de un enunciado compuesto en base a su conocimiento de la verdad de sus partes componentes. La lógica no ayuda a determinar la verdad o falsedad de los enunciados compuestos. Más bien, la lógica ayuda a enlazar estas piezas de información separadas en un todo coherente.

Equivalencia lógica

Los enunciados

6 es mayor que 2 y 2 es menor que 6

son dos maneras diferentes de decir la misma cosa. ¿Por qué? Debido a la definición de las frases *mayor que* y *menor que*. Por el contrario, aunque los enunciados

1) Los perros ladran y los gatos maúllan y 2) Los gatos maúllan y los perros ladran

son dos maneras diferentes de decir lo mismo, la razón no tiene que ver con la definición de las palabras. Tiene que ver con la forma lógica de los enunciados. Cualquiera de los dos enunciados cuyas formas lógicas se relacionan en la misma forma como 1) y 2) bien podría ser ambos verdaderos o ser ambos falsos. Puede ver esto examinando la tabla de verdad siguiente, donde las variables de enunciado p y q se sustituyen por los enunciados compuestos "Los perros ladran" y "Los gatos maúllan", respectivamente. La tabla muestra que para cada combinación de valores de verdad de p y q, $p \wedge q$ es verdadera cuando y sólo cuando, $p \wedge q$ es verdadera. En tal caso, las formas de enunciado se llaman *lógicamente equivalentes* y decimos que 1) y 2) son *enunciados lógicamente equivalentes*.

p	q	$p \wedge q$	$q \wedge p$
V	V	V	V
V	F	F	F
F	V	F	F
F	F	F	F

$p \wedge q$ y $q \wedge p$ siempre tiene el mismo valor de verdad, por lo que son lógicamente equivalentes

• Definición

Dos *formas de enunciado* se llaman **lógicamente equivalentes** si y sólo si, tienen los mismos valores de verdad para cada posible sustitución de enunciados por sus enunciados de variables. La equivalencia lógica de las formas de enunciado P y Q se denota escribiendo $P \equiv Q$.

Dos *enunciados* se llaman **lógicamente equivalentes** si y sólo si, tienen formas lógicas equivalentes cuando componentes idénticos de enunciados variables se utilizan para reemplazar los enunciados compuestos idénticos.

Prueba de si dos formas de enunciado P y Q son lógicamente equivalentes

1. Se construye una tabla de verdad con una columna para los valores de verdad de P y otra columna para los valores de verdad de Q.
2. Compruebe cada combinación de valores de verdad de enunciado de variables para ver si el valor de verdad de P es igual que el valor de verdad de Q.
   a. Si en cada renglón el valor de verdad de P es el igual al valor de verdad de Q, entonces P y Q son lógicamente equivalentes.
   b. Si en algún renglón P tiene un valor de verdad diferente de Q, entonces P y Q no son lógicamente equivalentes.

Ejemplo 2.1.6 Propiedad doblemente negativa: $\sim(\sim p) \equiv p$

Construya una tabla de verdad para demostrar que la negación de la negación de un enunciado es lógicamente equivalente al enunciado, anotando en la tabla con una frase de explicación.

Solución

p	$\sim p$	$\sim(\sim p)$
V	F	V
F	V	F

p y $\sim(\sim p)$ siempre tienen los mismos valores de verdad, por lo que son lógicamente equivalentes

■

Hay dos maneras de mostrar que las formas de enunciado de P y Q *no* son lógicamente equivalentes. Como se indicó anteriormente, una es utilizar una tabla de verdad para buscar renglones para que sus valores de verdad sean diferentes. La otra forma es encontrar enunciados concretos para cada una de las dos formas, una de las cuales es verdadera y la otra es falsa. El siguiente ejemplo muestra estas dos maneras.

Ejemplo 2.1.7 Demostración de la no equivalencia

Demuestre que las formas de enunciado $\sim(p \wedge q)$ y $\sim p \wedge \sim q$ no son lógicamente equivalentes.

Solución

a. Este método utiliza una tabla de verdad con una frase de explicación.

p	q	$\sim p$	$\sim q$	$p \wedge q$	$\sim(p \wedge q)$		$\sim p \wedge \sim q$
V	V	F	F	V	F		F
V	F	F	V	F	V	$\neq$	F
F	V	V	F	F	V	$\neq$	F
F	F	V	V	F	V		T

$\sim(p \wedge q)$ y $\sim p \wedge \sim q$ tienen valores de verdad diferentes en los renglones 2 y 3 por lo que no son lógicamente equivalentes

b. Este método utiliza un ejemplo para mostrar que $\sim(p \wedge q)$ y $\sim p \wedge \sim q$ no son lógicamente equivalentes. Sea p el enunciado "$0 < 1$" y sea q el enunciado "$1 < 0$". Entonces,

$$\sim(p \wedge q) \quad \text{es} \quad \text{"Este no es el caso de que } 0 < 1 \text{ y } 1 < 0\text{"},$$

lo cual es verdadero. Por otra parte,

$$\sim p \wedge \sim q \quad \text{es} \quad \text{"}0 \not< 1 \quad \text{y} \quad 1 \not< 0\text{"}.$$

que es falso. Este ejemplo muestra que hay enunciados concretos que pueden sustituirse por p y q para hacer una de las formas de enunciado verdadera y la otra falsa. Por tanto, las formas de enunciado no son lógicamente equivalentes. ■

Ejemplo 2.1.8 Negaciones de *Y* y *O*: Leyes de De Morgan

Para que el enunciado "John es alto y Jim es pelirrojo" sea verdadero, ambos componentes deben ser verdaderos. Por lo que si el enunciado es falso, uno de los componentes o ambos deben ser falsos. Así pues, la negación se puede escribir como "John no es alto o Jim no es pelirrojo". En general, la negación de la conjunción de los dos enunciados es lógicamente equivalente a la disyunción de sus negaciones. Es decir, las formas de enunciados $\sim(p \wedge q)$ y $\sim p \vee \sim q$ son lógicamente equivalentes. Compruebe esto utilizando tablas de verdad.

Solución

p	q	$\sim p$	$\sim q$	$p \wedge q$	$\sim(p \wedge q)$	$\sim p \vee \sim q$
V	V	F	F	V	F	F
V	F	F	V	F	V	V
F	V	V	F	F	V	V
F	F	V	V	F	V	V

$\sim(p \wedge q)$ y $\sim p \vee \sim q$ siempre tienen los mismos valores de verdad, por lo que son lógicamente equivalentes

Culver Pictures

Augustus De Morgan (1806-1871)

Simbólicamente,

$$\sim(p \wedge q) \equiv \sim p \vee \sim q.$$

En los ejercicios al final de esta sección se le pide que muestre que la ley análoga a la negación de la disyunción de dos enunciados es lógicamente equivalente a la conjunción de sus negaciones:

$$\sim(p \vee q) \equiv \sim p \wedge \sim q.$$

■

Las dos equivalencias lógicas del ejemplo 2.1.8 se conocen como las **leyes de De Morgan** de la lógica en honor de Augustus De Morgan, quien fue el primero en establecerlas formalmente en términos matemáticos.

Leyes de De Morgan

La negación de un enunciado y es lógicamente equivalente al enunciado o en el que cada componente es negado.

La negación de un enunciado o es lógicamente equivalente al enunciado y en el que cada componente es negado.

Ejemplo 2.1.9 Aplicación de las Leyes de De Morgan

Escriba negaciones para cada una de los siguientes enunciados:

a. John tiene una altura de 6 pies y pesa por lo menos 200 libras.

b. El autobús llegó tarde o el reloj de Tom estaba retrasado.

Solución

a. John no tiene una altura de 6 pies o pesa menos de 200 libras.

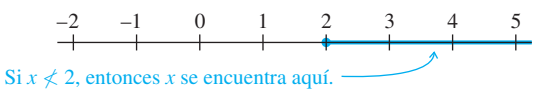
b. El autobús no llegó tarde y el reloj de Tom no estaba retrasado.

Ya que el enunciado "ni p ni q" significa lo mismo que "$\sim p$ y $\sim q$", una respuesta alternativa para *b*) es "Ni el autobús llegó tarde, ni el reloj de Tom estaba retrasado." ■

Si x es un número real dado, digamos que x no es menor a 2 ($x \not< 2$) significa que x no se encuentra a la izquierda de 2 en la recta numérica. Esto equivale a decir que $x = 2$, o que x se encuentra a la derecha de 2 en la recta numérica ($x = 2$ o $x > 2$). Por tanto,

$$x \not< 2 \quad \text{es equivalente a} \quad x \geq 2.$$

Gráficamente,



Del mismo modo,

$$x \not> 2 \quad \text{es equivalente a} \quad x \leq 2,$$
$$x \not\leq 2 \quad \text{es equivalente a} \quad x > 2 \quad \text{y}$$
$$x \not\geq 2 \quad \text{es equivalente a} \quad x < 2.$$

Ejemplo 2.1.10 Desigualdades y leyes de De Morgan

Utilice las leyes de De Morgan para escribir la negación de $-1 < x \leq 4$.

Solución El enunciado dado es equivalente a

$$-1 < x \quad \text{y} \quad x \leq 4.$$

¡Precaución! La negación de $-1 < x \leq 4$ *no* es $-1 \not< x \not< 4$. Tampoco es $-1 \geq x > 4$.

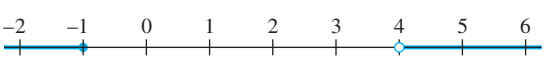
Por las leyes de De Morgan, la negación es

$$-1 \not< x \quad \text{o} \quad x \not\leq 4,$$

lo que equivale a

$$-1 \geq x \quad \text{o} \quad x > 4.$$

Gráficamente, si $-1 \geq x$ o $x > 4$, entonces x se encuentra en la región sombreada de la recta numérica, como se muestra a continuación.



■

Las leyes de De Morgan se utilizan con frecuencia al escribir programas de computadora. Por ejemplo, supongamos que quiere que su programa elimine todos los archivos modificados fuera de un rango dado de fechas, por ejemplo de la fecha 1 a la fecha 2 inclusive. Se podría utilizar el hecho que

$$\sim(\mathit{fecha1} \leq \mathit{modificación\_archivo\_fecha} \leq \mathit{fecha2})$$

es equivalente a

(*archivo_modificación_fecha* < *fecha*1) o (*fecha*2 < *archivo_modificación_fecha*).

Ejemplo 2.1.11 Un ejemplo preventivo

De acuerdo a las leyes de De Morgan, la negación de

p: Jim es alto y Jim es delgado

es $\sim p$: Jim no es alto o Jim no es delgado

porque la negación de un enunciado y es el enunciado o en el que los dos componentes son negados.

Por desgracia, puede surgir un aspecto potencialmente confuso del idioma español cuando se están tomando negaciones de este tipo. Considere que el enunciado p se puede escribir en forma más compacta como

p': Jim es alto y delgado.

Cuando está así escrito, otra manera de negar esto, es

$\sim(p')$: Jim no es alto y delgado.

¡Precaución! Aunque las leyes de la lógica son muy útiles, se deben utilizar como una ayuda para pensar, no como un sustituto mecánico.

Pero en esta forma la negación se ve como un enunciado y. ¿No se violan las leyes de De Morgan?

En realidad no se violan. La razón es que en la lógica formal las palabras y y o sólo se permiten entre enunciados completos, no entre fragmentos de frases.

Una lección que aprender de este ejemplo es que cuando se aplican las leyes de De Morgan, se deben tener enunciados completos a cada lado de cada y en cualquier lado de cada o. ■

Tautologías y contradicciones

Se ha dicho que toda la matemática se reduce a tautologías. Aunque esto es formalmente cierto, el mayor trabajo de los matemáticos es pensar que sus temas tienen sustancia y forma. Sin embargo, una comprensión intuitiva de las tautologías lógicas básicas es parte de las herramientas necesarias para cualquier persona que razona con matemáticas.

• Definición

Una **tautología** es una forma de enunciado que siempre es verdadera, independientemente de los valores de verdad de los enunciados individuales sustituidos por sus enunciados variables. Un enunciado cuya forma es una tautología es un **enunciado tautológico**.

Una **contradicción** es una forma de enunciado que siempre es falso, independientemente de los valores de verdad de los enunciados individuales de los enunciados variables sustituidos. Un enunciado cuya forma es una contradicción es un **enunciado contradictorio**.

De acuerdo con esta definición, lo verdadero de un enunciado tautológico y la falsedad de un enunciado contradictorio se deben a la estructura lógica de los propios enunciados y son independientes de los significados de los enunciados.

Ejemplo 2.1.12 Tautologías y contradicciones

Demuestre que el enunciado de la forma $p \vee \sim p$ es una tautología y que el enunciado de la forma $p \wedge \sim p$ es una contradicción.

Solución

p	$\sim p$	$p \vee \sim p$	$p \wedge \sim p$
V	F	V	F
F	V	V	F
		↑ todas V así que $p \vee \sim p$ es una tautología,	↑ todas F así que $p \vee \sim p$ es una contradicción

■

Ejemplo 2.1.13 Equivalencia lógica que involucra tautologías y contradicciones

Si **t** es una tautología y **c** es una contradicción, demuestre que $p \wedge \mathbf{t} \equiv p$ y $p \wedge \mathbf{c} \equiv \mathbf{c}$.

Solución

p	t	$p \wedge$ t	p	c	$p \wedge$ c
V	V	V	V	F	F
F	V	F	F	F	F
		↑ valores iguales, por tanto $p \wedge \mathbf{t} \equiv p$		↑ valores iguales, por tanto $p \wedge \mathbf{c} \equiv \mathbf{c}$	

■

Resumen de las equivalencias lógicas

El conocimiento de enunciados lógicamente equivalentes es muy útil para la construcción de argumentos. Con frecuencia sucede que es difícil ver cómo se deduce una conclusión de una forma de un enunciado, mientras que es fácil ver cómo se deduce de una forma lógicamente equivalente del enunciado. En el teorema 2.1.1 se resumen una serie de equivalencias lógicas para futuras referencias.

Teorema 2.1.1 Equivalencias lógicas

En cualquier enunciado variable dado p, q y r, con una tautología **t** y una contradicción **c**, son válidas las siguientes equivalencias lógicas.

1.	*Leyes conmutativas:*	$p \wedge q \equiv q \wedge p$	$p \vee q \equiv q \vee p$
2.	*Leyes asociativas:*	$(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$	$(p \vee q) \vee r \equiv p \vee (q \vee r)$
3.	*Leyes distributivas:*	$p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$	$p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$
4.	*Leyes de la identidad:*	$p \wedge \mathbf{t} \equiv p$	$p \vee \mathbf{c} \equiv p$
5.	*Leyes de negación:*	$p \vee \sim p \equiv \mathbf{t}$	$p \wedge \sim p \equiv \mathbf{c}$
6.	*Ley de la doble negación:*	$\sim(\sim p) \equiv p$	
7.	*Leyes de idempotencia:*	$p \wedge p \equiv p$	$p \vee p \equiv p$
8.	*Leyes universales acotadas:*	$p \vee \mathbf{t} \equiv \mathbf{t}$	$p \wedge \mathbf{c} \equiv \mathbf{c}$
9.	*Leyes de De Morgan:*	$\sim(p \wedge q) \equiv \sim p \vee \sim q$	$\sim(p \vee q) \equiv \sim p \wedge \sim q$
10.	*Leyes de absorción:*	$p \vee (p \wedge q) \equiv p$	$p \wedge (p \vee q) \equiv p$
11.	*Negaciones de* **t** *y* **c**:	$\sim \mathbf{t} \equiv \mathbf{c}$	$\sim \mathbf{c} \equiv \mathbf{t}$

Las demostraciones de las leyes 4 y 6, las primeras partes de las leyes 1 y 5 y la segunda parte de la ley 9 ya se han presentado como ejemplo en el libro. Las demostraciones de las otras partes del teorema se dejan como ejercicios. De hecho, se puede demostrar que las primeras cinco leyes del teorema 2.1.1 forman un núcleo a partir del cual se pueden deducir las demás leyes. Las primeras cinco leyes son los axiomas de una estructura matemática conocida como álgebra booleana, que se analiza en la sección 6.4.

Las equivalencias del teorema 2.1.1 son las leyes generales del pensamiento que se producen en todas las áreas del quehacer humano. También se pueden utilizar como una manera formal para reescribir formas de enunciado complicadas en formas de enunciado más sencillas.

Ejemplo 2.1.14 Simplificación de formas de enunciado

Utilice el teorema 2.1.1 para comprobar la equivalencia lógica

$$\sim(\sim p \wedge q) \wedge (p \vee q) \equiv p.$$

Solución Use las leyes del teorema 2.1.1 para reemplazar la forma de enunciado de la izquierda, por expresiones lógicamente equivalentes. Cada vez que haga esto, obtiene una forma de enunciado lógicamente equivalente. Continúe haciendo reemplazos hasta obtener la forma de enunciado de la derecha.

$$\begin{aligned}
\sim(\sim p \wedge q) \wedge (p \vee q) &\equiv (\sim(\sim p) \vee \sim q) \wedge (p \vee q) && \text{por las leyes de De Morgan}\\
&\equiv (p \vee \sim q) \wedge (p \vee q) && \text{por la ley de doble negación}\\
&\equiv p \vee (\sim q \wedge q) && \text{por la ley distributiva}\\
&\equiv p \vee (q \wedge \sim q) && \text{por la ley conmutativa para } \wedge\\
&\equiv p \vee \mathbf{c} && \text{por la ley de negación}\\
&\equiv p && \text{por la ley de identidad.}
\end{aligned}$$

■

Es útil tener habilidad en la simplificación de formas de enunciado para la construcción lógicamente eficiente de programas de computadora y en el diseño de circuitos lógicos digitales.

Aunque las propiedades del teorema 2.1.1 se pueden utilizar para demostrar la equivalencia lógica de dos formas de enunciado, no se pueden utilizar para demostrar formas de enunciado que no son lógicamente equivalentes. Por otra parte, las tablas de verdad siempre se pueden utilizar para determinar tanto equivalencia como no equivalencia y las tablas de verdad son fáciles de programar en una computadora. Sin embargo, cuando se utilizan tablas de verdad, la comprobación de equivalencia siempre requiere de 2^n pasos, donde n es el número de variables. A veces se puede ver rápidamente que hay dos formas de enunciado que son equivalentes por el teorema 2.1.1, mientras que se necesitaría un poco de cálculo para mostrar su equivalencia con tablas de verdad. Por ejemplo, se deduce inmediatamente de la ley asociativa para $\wedge$ que $p \wedge (\sim q \wedge \sim r) \equiv (p \wedge \sim q) \wedge \sim r$, mientras que la comprobación de la tabla de verdad requiere construir una tabla de ocho renglones.

Autoexamen

Las respuestas a las preguntas del autoexamen se presentan al final de cada sección.

1. Un enunciado y es verdadero si y sólo si ambos componentes son _____.
2. Un enunciado o es falso si y sólo si, ambos componentes son _____.
3. Dos formas de enunciado son lógicamente equivalentes si y sólo si, siempre tienen _____.
4. Las leyes de De Morgan dicen 1) que la negación de un enunciado y es lógicamente equivalente al enunciado _____ en el que cada componente es _____ y 2) la negación de un enunciado o es lógicamente equivalente al enunciado _____ en el que cada componente es _____.
5. Una tautología es un enunciado que siempre es _____.
6. Una contradicción es un enunciado que siempre es _____.

Conjunto de ejercicios 2.1

En cada uno de los ejercicios del 1 al 4 represente la forma común de cada argumento con letras para representar frases componentes y llene los espacios en blanco para que el argumento del enunciado *b*) tenga la misma forma lógica que el argumento del inciso *a*).

1. a. Si todos los números enteros son racionales, entonces el número 1 es racional. Todos los números enteros son racionales. Por tanto, el número 1 es racional.
b. Si todas las expresiones algebraicas se pueden escribir en notación de prefijo, entonces _____.
_____.
Por tanto $(a + 2b)\ (a^2 - b)$, puede escribirse en notación de prefijo.

2. a. Si todos los programas de computadora contienen errores, entonces este programa contiene un error.
Este programa no contiene un error.
Por tanto, no es el caso de que todos los programas de computadora tengan errores.
b. Si_____, entonces_____.
2 no es impar.
Por tanto, no es el caso de que todos los números primos sean impares.

3. a. Este número es par o este número es impar.
Este número no es par.
Por tanto, este número es impar.
b. _____o la lógica es confusa.
Mi mente no funciona.
Por tanto,_____.

4. a. Si n es divisible entre 6, entonces n es divisible entre 3.
Si n es divisible entre 3, entonces la suma de los dígitos de n es divisible entre 3.
Por tanto, si n es divisible entre 6, entonces la suma de los dígitos de n es divisible entre 3. (Suponga que n es un entero fijo dado.)
b. Si esta función es _____ entonces, esta función es derivable.
Si esta función es ____ entonces esta función es continua.
Por tanto, si esta función es un polinomio, entonces esta función es ____.

5. Indique cuál de las siguientes frases son enunciados.
a. 1024 es el menor número de cuatro dígitos que es un cuadrado perfecto.
b. Ella es una estudiante de la licenciatura en matemáticas.
c. $128 = 2^6$ d. $x = 2^6$

Escriba los enunciados del 6 al 9 en forma simbólica con los símbolos $\sim$, $\vee$, $\wedge$ y las letras indicadas para representar enunciados compuestos.

6. Sea s = "las acciones están aumentando" y i = "las tasas de interés se mantienen estables".
a. Las acciones están aumentando, pero las tasas de interés son constantes.
b. Ni las acciones aumentan ni las tasas de interés son estables.

7. Juan estudia la licenciatura en matemáticas pero no estudia la licenciatura en ciencias computacionales (m = "Juan estudia la licenciatura en matemáticas", c = "Juan estudia la licenciatura en ciencias computacionales").

8. Sea h = "Juan es sano", w = "Juan es rico" y s = "Juan es sabio".
a. Juan es sano y rico, pero no sabio.
b. Juan no es rico pero, es sano y sabio.
c. Juan ni es sano, rico, ni sabio.
d. Juan ni es rico ni sabio, pero es saludable.
e. Juan es rico, pero no es sano y sabio.

9. O este polinomio tiene grado 2 o tiene un grado 3, pero no ambos (n = "Este polinomio tiene grado 2", k = "Este polinomio tiene grado 3").

10. Sea p el enunciado "La BANDERAFINDATOS está apagada", q el enunciado "ERROR es igual a 0" y r el enunciado "la SUMA es menor que 1 000". Exprese las siguientes frases en notación simbólica.
a. La BANDERAFINDATOS está apagada, ERROR es igual a 0 y SUMA es menor que 1 000.
b. La BANDERAFINDATOS está apagada pero ERROR no es igual a 0.
c. La BANDERAFINDATOS está apagada, sin embargo, ERROR no es 0 o SUMA es mayor o igual a 1 000.
d. La BANDERAFINDATOS está encendida y ERROR es igual a 0 pero SUMA es mayor que o igual a 1 000.
e. Ya sea que BANDERAFINDATOS está encendida o que sea el caso de que tanto ERROR es 0 como SUMA es menor que 1 000.

11. En la frase siguiente, la palabra *o* se utiliza en sentido inclusivo o exclusivo? Un equipo gana los partidos decisivos si gana dos partidos consecutivos o un total de *tres* partidos.

En los ejercicios del 12 al 15, escriba las tablas de verdad para las formas de enunciado.

12. $\sim p \wedge q$ 13. $\sim(p \wedge q) \vee (p \vee q)$

14. $p \wedge (q \wedge r)$ 15. $p \wedge (\sim q \vee r)$

En los ejercicios del 16 al 24, determine si las formas de enunciado son lógicamente equivalentes. En cada caso, construya una tabla de verdad e incluya una frase que justifique su respuesta. Su frase debe mostrar que entiende el significado de equivalencia lógica.

16. $p \vee (p \wedge q)$ y p 17. $\sim(p \wedge q)$ y $\sim p \wedge \sim q$

18. $p \vee \mathbf{t}$ y $\mathbf{t}$ 19. $p \wedge \mathbf{t}$ y p

20. $p \wedge \mathbf{c}$ y $p \vee \mathbf{c}$

21. $(p \wedge q) \wedge r$ y $p \wedge (q \wedge r)$

*Para los ejercicios con números o letras azules, las soluciones están dadas en el apéndice B. El símbolo ***H*** indica que sólo se da una sugerencia o una solución parcial. El símbolo ✶ indica que el ejercicio es más difícil de lo normal.

22. $p \wedge (q \vee r)$ y $(p \wedge q) \vee (p \wedge r)$

23. $(p \wedge q) \vee r$ y $p \wedge (q \vee r)$

24. $(p \vee q) \vee (p \wedge r)$ y $(p \vee q) \wedge r$

En los ejercicios del 25 al 31, utilice las leyes de De Morgan para escribir las negaciones de los enunciados.

25. Hal estudia la licenciatura en matemáticas y la hermana de Hal estudiante de la licenciatura en ciencia computacional.

26. Sam es un cinturón de color naranja y Kate es un cinturón rojo.

27. El conector está suelto o el equipo esté desconectado.

28. El dígito de las unidades de 4^{67} es 4 o es 6.

29. Este programa de computadora tiene un error de lógica en las primeras diez líneas o se ejecuta con un conjunto incompleto de datos.

30. El dólar está en su punto más alto de todos los tiempos y el mercado de valores está en un mínimo histórico.

31. El tren llegó tarde o mi reloj se adelantó.

En los enunciados del 32 al 37, suponga que x es un número real dado y utilice las leyes de De Morgan para escribir las negaciones.

32. $-2 < x < 7$

33. $-10 < x < 2$

34. $x < 2$ o $x > 5$

35. $x \leq -1$ o $x > 1$

36. $1 > x \geq -3$

37. $0 > x \geq -7$

En los ejercicios 38 y 39, imagine que *num_ordenes* y *num_existencias* son valores dados, como podría ocurrir en la ejecución de un programa de computadora. Escriba las negaciones de los siguientes enunciados.

38. (*num_ordenes* $>$ 100 y *num_existencias* $\leq$ 500) o *num_existencias* $<$ 200

39. (*num_ordenes* $<$50 y *num_existencias* $>$ 300) o (50 $\leq$ *num_ordenes* $<$ 75 y *num_existencias* $>$ 500)

En los ejercicios del 40 al 43, utilice tablas de verdad para establecer cuál de las formas de enunciado son tautologías y cuáles son contradicciones.

40. $(p \wedge q) \vee (\sim p \vee (p \wedge \sim q))$

41. $(p \wedge \sim q) \wedge (\sim p \vee q)$

42. $((\sim p \wedge q) \wedge (q \wedge r)) \wedge \sim q$

43. $(\sim p \vee q) \vee (p \wedge \sim q)$

En los ejercicios 44 y 45, determine si los enunciados en los incisos *a*) y *b*) son lógicamente equivalentes.

44. Suponga que x es un número real dado.
a. $x < 2$ o no es el caso de que $1 < x < 3$.
b. $x \leq 1$ o bien $x < 2$ o $x \geq 3$.

45. a. Bob estudia dos carreras en matemáticas y en ciencias de la computación y Ann es una estudiante de la licenciatura en matemáticas, pero Ann no estudia dos carreras en matemáticas y en ciencias de la computación.
b. No es el caso de que tanto Bob como Ann estudien dos carreras en matemáticas y en ciencia computacional, pero es el caso de que Ann es una estudiante de la licenciatura en matemáticas y que Bob estudia dos carreras en matemáticas y en ciencias de la computación.

✶ 46. En el ejemplo 2.1.4, se introdujo el símbolo $\oplus$ para denotar *exclusivo o*, por lo que $p \oplus q \equiv (p \vee q) \wedge \sim(p \wedge q)$. Por tanto la tabla de verdad para *exclusivo o* es la siguiente:

p	q	$p \oplus q$
V	V	F
V	F	V
F	V	V
F	F	F

a. Encuentre formas de enunciado más simples que sean lógicamente equivalente a $p \oplus p$ y $(p \oplus p) \oplus p$.
b. ¿Es $(p \oplus q) \oplus r \equiv p \oplus (q \oplus r)$? Justifique su respuesta.
c. ¿Es $(p \oplus q) \wedge r \equiv (p \wedge r) \oplus (q \wedge r)$? Justifique su respuesta.

✶ **47.** En la lógica y en el español habitual, una doble negación es equivalente a un positivo. Hay un uso del español bastante común en el que un "doble positivo" es equivalente a un negativo. ¿Cuál es éste? ¿Puedes pensar en otros?

En los ejercicios 48 y 49 que se presentan a continuación, se deduce una equivalencia lógica del teorema 2.1.1. Dé una razón para cada paso.

48.
$$\begin{aligned} (p \wedge \sim q) \vee (p \wedge q) &\equiv p \wedge (\sim q \vee q) && \text{por } a) \\ &\equiv p \wedge (q \vee \sim q) && \text{por } b) \\ &\equiv p \wedge \mathbf{t} && \text{por } c) \\ &\equiv p && \text{por } d) \end{aligned}$$
Por tanto, $(p \wedge \sim q) \vee (p \wedge q) \equiv p$.

49.
$$\begin{aligned} (p \vee \sim q) \wedge (\sim p \vee \sim q) & \\ &\equiv (\sim q \vee p) \wedge (\sim q \vee \sim p) && \text{por } a) \\ &\equiv \sim q \vee (p \wedge \sim p) && \text{por } b) \\ &\equiv \sim q \vee \mathbf{c} && \text{por } c) \\ &\equiv \sim q && \text{por } d) \end{aligned}$$
Por tanto $(p \vee \sim q) \wedge (\sim p \vee \sim q) \equiv \sim q$.

Utilice el teorema 2.1.1 para comprobar la equivalencia lógica en los ejercicios 50 al 54. Dé una razón para cada paso.

50. $(p \wedge \sim q) \vee p \equiv p$

51. $p \wedge (\sim q \vee p) \equiv p$

52. $\sim(p \vee \sim q) \vee (\sim p \wedge \sim q) \equiv \sim p$

53. $\sim((\sim p \wedge q) \vee (\sim p \wedge \sim q)) \vee (p \wedge q) \equiv p$

54. $(p \wedge (\sim(\sim p \vee q))) \vee (p \wedge q) \equiv p$

Respuestas del autoexamen

1. verdaderos 2. falsos 3. los mismos valores verdaderos 4. *o*; negado, *y*; negado 5. verdadero 6. falso

2.2 Enunciados condicionales

. . . el razonamiento hipotético implica la subordinación de lo real a la esfera de lo posible . . . —Jean Piaget, 1972

Cuando usted hace una inferencia lógica o una deducción, razona *de* una hipótesis *a* una conclusión. Su objetivo es ser capaz de decir: "*Si* tal y tal es conocido, *entonces* algo u otro debe ser el caso".

Sean p y q los enunciados. Una frase de la forma "Si p entonces q" se denota simbólicamente por "$p \rightarrow q$"; p se llama la *hipótesis* y q se llama la *conclusión*. Por ejemplo, considere el enunciado siguiente:

$$\underbrace{\text{Si } 4\,686 \text{ es divisible entre } 6}_{\text{hipótesis}}, \quad \text{entonces} \quad \underbrace{4\,686 \text{ es divisible entre } 3}_{\text{conclusión}}$$

Esta frase se llama *condicional* ya que la verdad del enunciado q está condicionado a la verdad del enunciado p.

La notación $p \rightarrow q$ indica que $\rightarrow$ es un conector, como $\wedge$ o $\vee$, que se puede utilizar para unir enunciados para crear nuevos enunciados. Por tanto, para definir $p \rightarrow q$ como un enunciado, tenemos que especificar los valores de verdad para $p \rightarrow q$ conforme se especifican los valores de verdad para $p \wedge q$ y para $p \vee q$. Como es el caso con otros conectores, la definición formal de los valores de verdad para $\rightarrow$ (si-entonces) se basa en su sentido cotidiano, intuitivo. Consideremos un ejemplo.

Supongamos que va a una entrevista de trabajo en un almacén y el dueño le hace la siguiente promesa:

Si se presenta a trabajar el lunes por la mañana, entonces conseguirá el trabajo.

¿Bajo qué circunstancias se justifica diciendo que el dueño habló falsamente? Es decir, ¿en qué circunstancias la frase anterior es falsa? La respuesta es: *Se* presentó a trabajar el lunes por la mañana y *no* consiguió el trabajo.

Después de todo, la promesa del dueño sólo dice que usted conseguirá el trabajo, *si* cumple una determinada condición (ir a trabajar el lunes por la mañana); no dice nada acerca de lo que ocurre si *no* se cumple la condición. Así que si la condición no se cumple, no es justo decir que la promesa es falsa, independientemente de si se consigue o no el trabajo.

El ejemplo anterior tiene la intención de convencernos de que *la única combinación de circunstancias en las que llamarían un enunciado condicional falso se produce cuando la hipótesis es verdadera y la conclusión es falsa*. En todos los otros casos, no llamaría falsa a la frase. Esto implica que el único renglón de la tabla de verdad para $p \rightarrow q$ que se debe llenar con una F es el renglón donde p es V y q es F. Ningún otro renglón debe contener una F. Pero cada renglón de una tabla de verdad se debe llenar, ya sea con una V o con una F. Por tanto todos los otros renglones de la tabla de verdad para $p \rightarrow q$ se deben llenar con V.

Tabla de verdad para $p \rightarrow q$

p	q	$p \rightarrow q$
V	V	V
V	F	F
F	V	V
F	F	V

• Definición

Si p y q son enunciados variables, el **condicional** de q por p es "si p, entonces q" o "p implica q" y se denota $p \rightarrow q$. Es falso cuando p es verdadero y q es falso, en cualquier caso es verdadero. Llamamos a p la **hipótesis** (o **antecedente**) de la condicional y a q la **conclusión** (o **consecuente**).

Un enunciado condicional que es verdadero por el hecho de que su hipótesis es falsa con frecuencia se llama **vacíamente verdadera** o **verdadera por defecto**. Así, el enunciado "Si se presenta a trabajar el lunes por la mañana, entonces conseguirá el trabajo" es vacíamente verdadera si no se presenta a trabajar el lunes por la mañana. En general, cuando la parte "si" de un enunciado si-entonces es falsa, el enunciado como un todo se dice que es verdadero, independientemente de si la conclusión es verdadera o falsa.

Ejemplo 2.2.1 Un enunciado condicional con una hipótesis falsa

Considere el enunciado:

$$\text{Si } 0 = 1, \text{ entonces } 1 = 2.$$

Por extraño que parezca, ya que la hipótesis de este enunciado es falsa, el enunciado como un todo es verdadero. ■

El filósofo Willard Van Orman Quine aconseja no utilizar la frase "p implica q" para significar "$p \rightarrow q$" porque la palabra *implica* sugiere que q puede ser lógicamente deducido de p y esto no suele ser el caso. Sin embargo, la frase es utilizada por mucha gente, probablemente debido a que es un sustituto conveniente para el símbolo $\rightarrow$. Y, por supuesto, en muchos casos, se puede deducir una conclusión de una hipótesis, aun cuando la hipótesis es falsa.

Nota Por ejemplo, si $0 = 1$, entonces, sumando 1 a ambos lados de la ecuación, se puede deducir que $1 = 2$

En las expresiones que incluyen $\rightarrow$, así como otros operadores lógicos, tales como $\wedge$, $\vee$ y $\sim$, el **orden de las operaciones** es que $\rightarrow$ se realiza al último. Así, de acuerdo con la especificación del orden de las operaciones de la sección 2.1, primero se realiza $\sim$, después $\wedge$ y $\vee$ y finalmente $\rightarrow$.

Ejemplo 2.2.2 Tabla de verdad para $p \vee \sim q \rightarrow \sim p$

Construya una tabla de verdad para la forma de enunciado $p \vee \sim q \rightarrow \sim p$.

Solución Por el orden de las operaciones antes mencionadas, las siguientes dos expresiones son equivalentes: $p \vee \sim q \rightarrow \sim p$ y $(p \vee (\sim q)) \rightarrow (\sim p)$ y este orden regula la construcción de la tabla de verdad. Primero complete las cuatro combinaciones posibles de valores de verdad de p y q, después escriba los valores de verdad para $\sim p$ y $\sim q$ usando la definición de negación. Después llene la columna $p \vee \sim q$ utilizando la definición de $\vee$. Por último, llene la columna $p \vee \sim q \rightarrow \sim p$ utilizando la definición de $\rightarrow$. Los únicos renglones en los que la hipótesis $p \vee \sim q$ es verdadera y la conclusión de $\sim p$ es falsa son el primer y segundo renglón. Así ponga F en los dos renglones y V en los otros dos renglones.

		conclusión		premisas	
p	q	$\sim p$	$\sim q$	$p \vee \sim q$	$p \vee \sim q \rightarrow \sim p$
V	V	F	F	V	F
V	F	F	V	V	F
F	V	V	F	F	V
F	F	V	V	V	V

■

Equivalencias lógicas que involucran →

Imagine que está tratando de resolver un problema relacionado con tres enunciados: p, q y r. Supongamos que sabe que la verdad de r se deduce de la verdad de p *y también* que la verdad de r se deduce de la verdad de q. Entonces no importa si p o q es el caso, se debe deducir la verdad de r. El método de análisis de división en casos se basa en esta idea.

Ejemplo 2.2.3 División en casos: Demuestre que $p \vee q \to r \equiv (p \to r) \wedge (q \to r)$

Utilice tablas de verdad para mostrar la equivalencia lógica de las formas de enunciado $p \vee q \to r$ y $(p \to r) \wedge (q \to r)$. Anote en la tabla una frase de la explicación.

Solución Primero llene en las ocho combinaciones posibles de valores de verdad para p, q y r. Después llene las columnas para $p \vee q$, $p \to r$ y $q \to r$ utilizando las definiciones de *o* y *si-entonces*. Por ejemplo la columna $p \to r$ tiene F en el segundo y cuarto renglón, porque estos son los renglones en los que p es verdadera y q es falsa. Después llene la columna $p \vee q \to r$ utilizando la definición *si-entonces*. Los renglones en los que la hipótesis $p \vee q$ es verdadera y la conclusión r es falsa son el segundo, cuarto y sexto. Así F va en estos renglones y V en todos los demás. La tabla completa muestra que $p \vee q \to r$ y $(p \to r) \wedge (q \to r)$ tienen valores de verdad iguales para cada combinación de valores de verdad de p, q y r. Por tanto las dos formas de enunciado son lógicamente equivalentes.

p	q	r	$p \vee q$	$p \to r$	$q \to r$	$p \vee q \to r$	$(p \to r) \wedge (q \to r)$
V	V	V	V	V	V	V	V
V	V	F	V	F	F	F	F
V	F	V	V	V	V	V	V
V	F	F	V	F	V	F	F
F	V	V	V	V	V	V	V
F	V	F	V	V	F	F	F
F	F	V	F	V	V	V	V
F	F	F	F	V	V	V	V

$p \vee q \to r$ y $(p \to r) \wedge (q \to r)$ siempre tienen los mismos valores de verdad, así que son lógicamente equivalentes ■

Representación de si-entonces como o

En el ejercicio 13*a*) al final de esta sección se le pide que use tablas de verdad para demostrar que

$$p \to q \equiv \sim p \vee q.$$

La equivalencia lógica de "si p entonces q" y "no p o q" se utiliza ocasionalmente en el lenguaje cotidiano. A continuación se presenta un ejemplo.

Ejemplo 2.2.4 Aplicación de la equivalencia entre $\sim p \vee q$ y $p \to q$

Reescriba el siguiente enunciado en la forma si-entonces.

O llega a tiempo al trabajo o lo despiden.

Solución Sea $\sim p$

Llega a tiempo al trabajo.

y q sea

Está despedido.

Entonces, el enunciado dado es $\sim p \vee q$. También p es.

No llegó a tiempo al trabajo.

Así que la versión equivalente si-entonces, $p \rightarrow q$, es

No llegó a tiempo al trabajo, entonces está despedido. ■

La negación de un enunciado condicional

Por definición, $p \rightarrow q$ es falsa si y sólo si, su hipótesis p, es verdadera y su conclusión, q, es falsa. De lo que se deduce

> La negación de "si p, entonces q" es lógicamente equivalente a "p y no q".

Esto se puede reescribir simbólicamente de la siguiente manera:

$$\sim(p \rightarrow q) \equiv p \wedge \sim q$$

También se puede obtener este resultado a partir de la equivalencia lógica $p \rightarrow q \equiv \sim p \vee q$. Tome la negación de ambos lados para obtener

$$\begin{aligned} \sim(p \rightarrow q) &\equiv \sim(\sim p \vee q) \\ &\equiv \sim(\sim p) \wedge (\sim q) && \text{por las leyes de De Morgan} \\ &\equiv p \wedge \sim q && \text{por la ley doble negación} \end{aligned}$$

Otra forma de obtener este resultado es la construcción de tablas de verdad para $\sim(p \rightarrow q)$ y para $p \wedge \sim q$ para comprobar que tienen el mismo valor de verdad. (Vea el ejercicio 13*b*) al final de esta sección.)

Ejemplo 2.2.5 Negaciones de enunciados *si-entonces*

Escriba las negaciones de cada uno de los siguientes enunciados:

a. Si mi automóvil está en el taller de reparaciones, entonces no puedo ir a clase.

b. Si Sara vive en Atenas, entonces, ella vive en Grecia.

Solución

a. Mi automóvil está en el taller de reparaciones y puedo ir a clase.

b. Sara vive en Atenas y no vive en Grecia. (Sara podría vivir en Atenas, Georgia; Atenas, Ohio; o Atenas, Wisconsin.) ■

¡Precaución! Recuerde que **la negación de un enunciado si-entonces no empieza con la palabra *si*.**

Es tentador escribir la negación de un enunciado si-entonces como otro enunciado si-entonces. ¡Por favor, resista la tentación!

El contrapositivo de un enunciado condicional

Una de las leyes más fundamentales de la lógica es la equivalencia entre un enunciado condicional y su contrapositivo.

• Definición

El **contrapositivo** de un enunciado condicional de la forma "si p entonces q" es

Si $\sim q$ entonces $\sim p$.

Simbólicamente,

El contrapositivo de $p \to q$ es $\sim q \to \sim p$.

El hecho es que

Un enunciado condicional es lógicamente equivalente a su contrapositivo.

En el ejercicio 26 al final de esta sección, se le pide que establezca esta equivalencia.

Ejemplo 2.2.6 Escriba el contrapositivo

Escriba cada uno de los siguientes enunciados en su forma contrapositiva equivalente:

a. Si Howard puede atravesar a nado el lago, entonces, Howard puede nadar a la isla.

b. Si hoy es domingo de Pascua, entonces mañana es lunes.

Solución

a. Si Howard no puede nadar a la isla, entonces, Howard no puede cruzar nadando el lago.

b. Si mañana no es lunes, entonces hoy no es domingo de Pascua. ■

Cuando está tratando de resolver ciertos problemas, puede encontrar la forma contrapositiva de un enunciado condicional con la que es más fácil trabajar que con el enunciado original. Sustituyendo un enunciado con su contrapositivo puede dar el empuje extra que ayuda en la búsqueda de una solución. Esta equivalencia lógica es también la base para una de las leyes más importantes de la deducción, el *modus tollens* (que se explica en la sección 2.3) y para el método contrapositivo de la demostración (que se explica en la sección 4.6).

El converso y la contraria de un enunciado condicional

El hecho de que un enunciado condicional y su contrapositivo sean lógicamente equivalentes es muy importante y tiene una amplia aplicación. Dos variantes de un enunciado condicional *no* son lógicamente equivalentes al enunciado.

• Definición

Suponga un enunciado condicional dado de la forma "Si p entonces q".

1. El **converso** es "si q entonces p".
2. El **contrario** es "si $\sim p$ entonces $\sim q$".

Simbólicamente,

$$\text{El converso de } p \to q \text{ es } q \to p.$$

y

$$\text{El contrario de } p \to q \text{ es } \sim p \to \sim q.$$

Ejemplo 2.2.7 Escritura del converso y del contrario

Escriba el converso y el contrario de cada uno de los siguientes enunciados:

a. Si Howard puede nadar atravesando del lago, entonces, Howard puede nadar a la isla.

b. Si hoy es domingo de Pascua, mañana es lunes.

Solución

a. *Converso*: Si Howard puede nadar a la isla, entonces, Howard puede atravesar a nado el lago.
Contrario: Si Howard no puede cruzar a nado el lago, entonces, Howard no puede nadar a la isla.

b. *Converso*: Si mañana es lunes, entonces hoy es domingo de Pascua.
Contrario: Si hoy no es domingo de Pascua, entonces mañana no es lunes. ■

¡Precaución! Muchas personas creen que si un enunciado condicional es verdadero, entonces su converso e inverso también deben ser verdaderos. ¡Esto no es correcto!

Observe que, aunque el enunciado "Si hoy es domingo de Pascua, mañana es lunes" siempre es verdadero, tanto su converso como su contrario son falsos para cada domingo excepto el domingo de Pascua.

1. Un enunciado condicional y su converso *no* son lógicamente equivalentes.
2. Un enunciado condicional y su contrario *no* son lógicamente equivalentes.
3. El converso y el contrario de un enunciado condicional son lógicamente equivalentes entre sí.

En los ejercicios 24, 25 y 27 al final de esta sección, se le pide utilizar tablas de verdad para comprobar los enunciados del cuadro anterior. Considere que la verdad del enunciado de 3 también se deduce de la observación de que el contrario de un enunciado condicional es el contrapositivo de su converso.

Sólo si y el bicondicional

Decir "p sólo si q" significa que p *sólo* puede tener lugar si q también ocurre. Es decir, si q no ocurre, entonces p no puede ocurrir. Otra forma de decir esto es que si ocurre p, entonces q también debe ocurrir (por equivalencia lógica entre un enunciado y su contrapositivo).

• Definición

Si p y q son enunciados,

p **sólo si** q significa "si no q entonces no p".

o, equivalentemente,

"si p, entonces q".

Ejemplo 2.2.8 Convertir *sólo si* a *si-entonces*

Reescriba el siguiente enunciado en la forma si-entonces de dos maneras, una de las cuales es el contrapositivo de la otra.

John romperá el récord mundial para la carrera de una milla sólo si corre la milla en menos de cuatro minutos.

Solución *Versión* 1: Si John no corre la milla en menos de cuatro minutos, entonces no romperá el récord mundial.

Versión 2: Si John bate el récord mundial, entonces tendrá que correr la milla en menos de cuatro minutos. ■

¡Precaución! "p sólo si q" *no* significa "p si q".

Observe que es posible que "p sólo si q" sea verdadero en el momento en que "p si q" es falso. Por ejemplo, decir que John va a romper el récord mundial sólo si corre la milla en menos de cuatro minutos no quiere decir que John romperá el récord mundial si corre la milla en menos de cuatro minutos. Su tiempo puede ser menor de cuatro minutos, pero aún no lo suficientemente rápido para romper el récord.

• Definición

Dados los enunciados de variables p y q, el **bicondicional de p y q** es "p si y sólo si q" y se denota por $p \leftrightarrow q$. Es verdadero, si tanto p como q tienen los mismos valores de verdad y es falso si p y q tienen valores de verdad opuestos. Las palabras *si y sólo si* a veces se abrevian como **iff**.

El bicondicional tiene la siguiente tabla de verdad:

Tabla de verdad para $p \leftrightarrow q$

p	q	$p \leftrightarrow q$
V	V	V
V	F	F
F	V	F
F	F	V

El orden de las operaciones $\leftrightarrow$ es igual que con $\rightarrow$. Como con $\wedge$ y $\vee$, la única manera para indicar la prioridad entre ellos es el uso de paréntesis. En la página siguiente, se muestra la jerarquía completa de las operaciones de los cinco operadores lógicos.

Orden de operaciones para los operadores lógicos

1. $\sim$	Primero evalúe las negaciones.
2. $\wedge$, $\vee$	Segundo evalúe $\wedge$ y $\vee$. Cuando ambos están presentes, el paréntesis puede ser necesario.
3. $\rightarrow$, $\leftrightarrow$	Tercero evalúe $\rightarrow$ y $\leftrightarrow$. Cuando ambos están presentes, el paréntesis puede ser necesario.

De acuerdo con las definiciones por separado de *sí* y sólo *si*, que dicen que "p si y sólo si, q" debe significar lo mismo que decir tanto "p si q" como "p sólo si q". La siguiente tabla de verdad muestra en la anotación que este es el caso:

Tabla de verdad, que demuestra que $p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$

p	q	$p \rightarrow q$	$q \rightarrow p$	$p \leftrightarrow q$	$(p \rightarrow q) \wedge (q \rightarrow p)$
V	V	V	V	V	V
V	F	F	V	F	F
F	V	V	F	F	F
F	F	V	V	V	V

$p \leftrightarrow q$ y $(p \rightarrow q) \wedge (q \rightarrow p)$ siempre tienen los mismos valores de verdad, por lo que son lógicamente equivalentes

Ejemplo 2.2.9 *Si* y *sólo si*

Reescriba el enunciado siguiente como una conjunción de dos enunciados si-entonces:

> Este programa de computadora es correcto si y sólo si, produce respuestas correctas para todos los posibles conjuntos de datos de entrada.

Solución Si este programa es correcto, entonces produce las respuestas correctas para todos los posibles conjuntos de datos de entrada y si este programa produce las respuestas correctas para todos los posibles conjuntos de datos de entrada, entonces es correcto. ■

Condiciones necesarias y suficientes

Las frases *condición necesaria* y *condición suficiente*, tal como se utilizan en el español formal, corresponden exactamente con sus definiciones en lógica.

• Definición

Si r y s son enunciados:

r es una **condición suficiente** para s	significa	"si r entonces s".
r es una **condición necesaria** para s	significa	"si no r entonces no s".

En otras palabras, decir que "r es una condición suficiente para s" significa que la aparición de r es *suficiente* para garantizar la presencia de s. Por otro lado, decir "r es condición necesaria para s" significa que si r no se produce, entonces, s no puede ocurrir:

La ocurrencia de r es *necesaria* para obtener la ocurrencia de s. Considere que debido a la equivalencia entre un enunciado y su contrapositivo,

r es una condición necesaria para s	también significa	"si s entonces r".

En consecuencia,

r es una condición necesaria y suficiente para s significa "r si y sólo si, s".

Ejemplo 2.2.10 Interpretación de condiciones necesarias y suficientes

Considere el enunciado "Si John es elegible para votar, entonces tiene por lo menos 18 años de edad". La verdad de la condición de "John es elegible para votar" es *suficiente* para garantizar la verdad de la condición que "John tiene por lo menos 18 años de edad". Además, la condición de "John tiene por lo menos 18 años de edad" es *necesaria* para que la condición de "John tiene derecho a votar" sea verdad. Si John fuera menor de 18 años, entonces no tendrían derecho a voto. ■

Ejemplo 2.2.11 Conversión de una condición suficiente para la forma si-entonces

Reescriba el siguiente enunciado en la forma "Si A entonces B":

> El nacimiento de Pía en territorio de EE.UU. es una condición suficiente para que ella sea ciudadana de EE.UU.

Solución Si Pía nació en territorio de EE.UU., entonces es ciudadana de EE.UU. ■

Ejemplo 2.2.12 Conversión de una condición necesaria para la forma si-entonces

Utilice la contraposición para reescribir el enunciado siguiente de dos maneras:

> Que George tenga la edad de 35 es una condición necesaria para ser presidente de Estados Unidos.

Solución *Versión* 1: Si George no tiene la edad de 35 años, entonces no puede ser presidente de Estados Unidos.
Versión 2: Si George puede ser presidente de Estados Unidos, entonces tiene la edad de 35 años. ■

Observaciones

1. *En lógica, no se requiere que la hipótesis y la conclusión sean temas relacionados.*
   En el lenguaje común nunca decimos cosas como "Si las computadoras son máquinas, entonces, Babe Ruth fue un jugador de béisbol" o "Si $2 + 2 = 5$, entonces Mickey Mouse es el presidente de Estados Unidos". Se formula una frase como "si p, entonces q" sólo si existe alguna relación de contenido entre p y q.
   Sin embargo, en la lógica, las dos partes de un enunciado condicional no necesitan tener significados relacionados. ¿La razón? Si hubiera dicho requisito, ¿qué lo haría cumplir? Lo que una persona percibe como dos cláusulas no relacionadas a otra persona le pueden parecer relacionadas. Tendría que haber un árbitro central para comprobar cada frase condicional antes de que alguien la use, para estar seguro de que sus cláusulas tenían la relación adecuada. Eso es poco práctico, ¡en pocas palabras!

Por tanto un enunciado como "si las computadoras son máquinas, entonces, Babe Ruth fue un jugador de béisbol" se permite, e incluso se llama verdadero porque tanto su hipótesis como su conclusión son verdaderas. Del mismo modo, el enunciado "Si $2 + 2 = 5$, entonces, Mickey Mouse es el presidente de Estados Unidos" se permite y se llama verdadero porque la hipótesis es falsa, aunque hacerlo puede parecer ridículo.

En matemáticas sucede con frecuencia que una definición cuidadosamente formulada cubre con éxito situaciones para las que fue concebida principalmente, posteriormente satisface algunos casos extremos que el formulador no tenía en mente. Pero esas son excepciones y es importante adquirir el hábito de explorar plenamente las definiciones de buscar y entender *todas* sus instancias, aún las más inusuales.

2. *En lenguaje informal, los condicionales simples se utilizan con frecuencia para significar bicondicionales*.

   El enunciado formal de "*p* si y sólo si, *q*" rara vez se utiliza en el lenguaje ordinario: Con frecuencia, cuando las personas intentan el bicondicional dejan de lado el *sí y sólo si* o el *sí y*. Esto es, dicen ya sea "*p* si *q*" o "*p* sólo si *q*", cuando en realidad significa "*p* si y sólo si, *q*". Por ejemplo, considere el enunciado "tendrá postre si y sólo si, come su cena". Lógicamente, es equivalente a la conjunción de los dos enunciados.

   Enunciado 1: Si come la cena, tendrá postre.

   Enunciado 2: Tendrá postre sólo si se come su cena.

   o

   Si no come la cena, entonces no tendrá postre.

Ahora, ¿Cuántos padres en la historia del mundo han dicho a sus hijos "tendrás postre, si y sólo si, comes tu cena"? ¡No muchos! La mayoría dicen, "Si comes la cena, tendrás un postre" (éstas tienen enfoque positivo; hacen hincapié en la recompensa) o "Tendrás postre sólo si comes tu cena" (éstas tienen enfoque negativo; destacan el castigo). Sin embargo, los padres que prometen premiar sugieren también el castigo y los que amenazan con castigo sin duda darán la recompensa si se gana. Ambos grupos de padres esperan que sus enunciados condicionales se interpreten como bicondicionales.

Dado que con frecuencia (correctamente) interpretamos los enunciados condicionales como bicondicionales, no es sorprendente que podamos llegar a creer (erróneamente) que los enunciados condicionales son siempre lógicamente equivalentes a sus contrarios y conversos. Sin embargo, en contextos formales, los enunciados deben tener interpretaciones inequívocas. Los enunciados si-entonces no pueden algunas veces significar "si-entonces" y otras veces significar "si y sólo si". Cuando se utiliza el lenguaje en matemáticas, ciencias, o en otras situaciones donde la precisión es importante, es esencial interpretar los enunciados si-entonces de acuerdo a la definición formal y no confundirlos con sus conversos y contrarios.

Autoexamen

1. Un enunciado *si-entonces* es falso si y sólo si, la hipótesis es _____ y la conclusión es _____.
2. La negación de "si *p*, entonces *q*" es _____.
3. El converso de "si *p*, entonces *q*" es _____.
4. El contrapositivo de "si *p*, entonces *q*" es _____.
5. El contrario de "si *p*, entonces *q*" es _____.
6. Un enunciado condicional y su contrapositivo son _____.
7. Un enunciado condicional y su converso no son _____.
8. "*R* es una condición suficiente para *S*" significa si _____ entonces _____".
9. "*R* es una condición necesaria para *S*" significa "si _____ entonces _____".
10. "*R* sólo si *S*" significa "si _____ entonces _____".

Conjunto de ejercicios 2.2

En los ejercicios 1 al 4, reescriba los enunciados en la forma si-entonces.

1. Este bucle se repetirá exactamente N veces, si no contiene un **alto** o un **siga**.

2. Estoy a tiempo para el trabajo si tomo el autobús de las 8:05.

3. Se detiene o dispararé.

4. Arregle mi techo o no voy a pagar el alquiler.

En los ejercicios del 5 al 11, construya tablas de verdad para las formas de enunciado.

5. $\sim p \vee q \rightarrow \sim q$ 6. $(p \vee q) \vee (\sim p \wedge q) \rightarrow q$

7. $p \wedge \sim q \rightarrow r$ 8. $\sim p \vee q \rightarrow r$

9. $p \wedge \sim r \leftrightarrow q \vee r$ 10. $(p \rightarrow r) \leftrightarrow (q \rightarrow r)$

11. $(p \rightarrow (q \rightarrow r)) \leftrightarrow ((p \wedge q) \rightarrow r)$

12. Use la equivalencia lógica establecida en el ejemplo 2.2.3, $p \vee q \rightarrow r \equiv (p \rightarrow r) \wedge (q \rightarrow r)$, reescriba el siguiente enunciado. (Supongamos que x representa un número real fijo).

Si $x > 2$ o $x < -2$, entonces $x^2 > 4$.

13. Utilice tablas de verdad para comprobar la equivalencia lógica siguiente. Incluya algunas palabras de explicación con sus respuestas.

a. $p \rightarrow q \equiv \sim p \vee q$ b. $\sim(p \rightarrow q) \equiv p \wedge \sim q$.

H 14. **a.** Muestre que las siguientes formas de enunciados son lógicamente equivalentes.

$$p \rightarrow q \vee r, \quad p \wedge \sim q \rightarrow r \quad \text{y} \quad p \wedge \sim r \rightarrow q$$

b. Utilice las equivalencias lógicas establecidas en el inciso *a*) para reescribir la siguiente frase de dos maneras diferentes. (Suponga que n representa un entero fijo.)

Si n es primo, entonces n es impar o n es 2.

15. Determine si las siguientes formas de enunciado son lógicamente equivalentes:

$$p \rightarrow (q \rightarrow r) \quad \text{y} \quad (p \rightarrow q) \rightarrow r$$

En los ejercicios 16 y 17, escriba cada uno de los dos enunciados en forma simbólica y determine si son lógicamente equivalentes. Incluya una tabla de verdad y algunas palabras de explicación.

16. Si pagó el precio completo y no compró en la librería Corona. No compró en la librería Corona o pagó el precio completo.

17. Si 2 es un factor de n y 3 es un factor de n, entonces 6 es un factor de n. 2 no es un factor de n o 3 no es un factor de n o 6 es un factor de n.

18. Escriba cada uno de los siguientes tres enunciados en forma simbólica y determine qué pares son lógicamente equivalentes. Incluya tablas de verdad y algunas palabras de explicación.

Si camina como un pato y habla como un pato, entonces es un pato.

O bien no camina como un pato o no habla como un pato, o es un pato.

Si no camina como un pato y no habla como un pato, entonces no es un pato.

19. ¿Verdadero o falso? La negación de "Si Susana es la madre de Luis, entonces, Ali es su primo" es "Si Susana es la madre de Luis, entonces, Ali no es su primo".

20. Escribe negaciones para cada uno de los siguientes enunciados. (Suponga que todas las variables representan cantidades fijas o entidades, según corresponda.)

a. Si P es un cuadrado, entonces P es un rectángulo.

b. Si hoy es la víspera de Año Nuevo, entonces, mañana es enero.

c. Si la expansión decimal de r es finita, entonces r es racional.

d. Si n es primo, entonces n es impar *o* n es 2.

e. Si x es no negativo, entonces x es positivo o x es 0.

f. Si Tom es el padre de Ana, entonces, Jim es su tío y Susana es su tía.

g. Si n es divisible entre 6, entonces n es divisible entre 2 y n es divisible entre 3.

21. Supongamos que p y q son enunciados tal que $p \rightarrow q$ es falso. Encuentre los valores verdaderos de cada uno de los siguientes enunciados:

a. $\sim p \rightarrow q$ b. $p \vee q$ c. $q \rightarrow p$

H 22. Escriba contrapositivos para los enunciados del ejercicio 20.

H 23. Escriba el converso y el contrario de cada enunciado del ejercicio 20.

En los ejercicios del 24 al 27, utilice tablas de verdad para establecer la verdad de cada enunciado.

24. Un enunciado condicional no es lógicamente equivalente a su converso.

25. Un enunciado condicional no es lógicamente equivalente a su contrario.

26. Un enunciado condicional y su contrapositivo son lógicamente equivalentes entre sí.

27. El converso y el contrario de un enunciado condicional son lógicamente equivalentes entre sí.

H 28. "¿Significa que piensa que puede encontrar la respuesta a esto?" le dijo la Liebre de Marzo.

"Exactamente", dijo Alicia.

"Entonces debes decir lo que quieres decir", prosiguió la Liebre de Marzo.

"Lo hago", respondió rápidamente Alicia, "por lo menos —al menos yo digo lo que quiero decir— que es la misma cosa, tú sabes".

"No es lo mismo ¡es un poco!" dijo el Sombrerero. "¿Por qué, podría decir también que 'veo lo que como' es lo mismo que ¡yo como lo que veo!"

—De "Una loca fiesta de té" en *Alicia en el País de las Maravillas*, de Lewis Carroll.

El Sombrerero está en lo correcto. "Yo digo lo que quiero decir" no es lo mismo que "quiero decir lo que digo". Reescriba cada una de estas dos frases en la forma si-entonces y explique la relación lógica entre ellas. (Se le referencia a este ejercicio en la introducción del capítulo 4.)

Si las formas de enunciado P y Q son lógicamente equivalentes, entonces $P \leftrightarrow Q$ es una tautología. Por el contrario, si $P \leftrightarrow Q$ es una tautología, entonces P y Q ¡son lógicamente equivalentes! En los ejercicios 29 al 31, use $\leftrightarrow$ para convertir cada una de las equivalencias lógicas en una tautología. Después, utilice una tabla de verdad para comprobar cada tautología.

29. $p \rightarrow (q \vee r) \equiv (p \wedge \sim q) \rightarrow r$

30. $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$

31. $p \rightarrow (q \rightarrow r) \equiv (p \wedge q) \rightarrow r$

Reescriba cada uno de los enunciados en los ejercicios 32 y 33 como una conjunción de dos enunciados si-entonces.

32. Esta ecuación de segundo grado tiene dos raíces reales distintas si y sólo si, su discriminante es mayor que cero.

33. Este entero es par si y sólo si, es igual a dos veces un número entero.

Reescriba los enunciados de los ejercicios 34 y 35 en la forma si-entonces de dos maneras, una de las cuales es el contrapositivo del otro.

34. Los Cachorros van a ganar el campeonato sólo si ganan el partido de mañana.

35. A Sam se le permitirá participar en la carrera de botes Signe sólo si él es un experto navegante.

36. Teniendo una gran visión de su educación, va a la corporación Prestigio y pregunta qué debe estudiar en la universidad para que se le contrate cuando se gradúe. El director de personal responde que se le contratará *sólo si* hace una carrera de matemáticas o en ciencias de la computación, obtiene un promedio de B o mejor y toma el curso de contabilidad. De hecho, lo hace, estudia matemáticas, obtiene un promedio de B^+ y estudia contabilidad. Regresa a la compañía Prestigio, hace una solicitud formal y es rechazada. ¿El director de personal le mintió?

Algunos lenguajes de programación utilizan enunciados de la forma "r a menos que s" significa que mientras s no suceda, entonces r ocurrirá. Más formalmente:

Definición: Si r y s son enunciados,

r* a menos que *s significa que si $\sim s$ entonces r.

En los ejercicios del 37 al 39, reescriba los enunciados en la forma si-entonces.

37. El pago se efectuará en la quinta a menos que se conceda una nueva audiencia.

38. Ann irá a menos que llueva.

39. Esta puerta no se abrirá a menos que se introduzca un código de seguridad.

Reescriba los enunciados 40 y 41 en la forma si-entonces.

40. Tomar el autobús a las 8:05 es una condición suficiente para que yo llegue a tiempo al trabajo.

41. Tener dos ángulos de 45° es una condición suficiente para que este triángulo sea un triángulo rectángulo.

Utilice el contrapositivo para reescribir los enunciados de los ejercicios 42 y 43 en la forma si-entonces de dos maneras.

42. Ser divisible entre 3 es una condición necesaria para que este número sea divisible entre 9.

43. Hacer la tarea con regularidad es una condición necesaria para que Jim apruebe el curso.

Observe que "una condición suficiente para s es r" significa que r es una condición suficiente para s y que "una condición necesaria para s es r" significa que r es una condición necesaria para s. Reescriba los enunciados de los ejercicios 44 y 45 en la forma si-entonces.

44. Una condición suficiente para que el equipo de Jon gane el campeonato es que gane el resto de sus juegos.

45. Una condición necesaria para que este programa de computadora esté correcto es que no se produzcan mensajes de error durante la corrida.

46. "Si el compuesto X está hirviendo, entonces, su temperatura debe ser de al menos 150 °C". Suponiendo que este enunciado sea verdadero, cuál de los siguientes enunciados también debe ser verdadero?
   - **a.** Si la temperatura del compuesto X es al menos de 150 °C, el compuesto X está hirviendo.
   - **b.** Si la temperatura del compuesto X es menor de 150 °C, entonces, el compuesto X no está hirviendo.
   - c. El compuesto X hierve sólo si su temperatura es de al menos150 °C.
   - d. Si el compuesto X no está hirviendo, entonces, su temperatura es inferior a 150 °C.
   - e. Una condición necesaria para que el compuesto X hierva es que su temperatura es por lo menos de 150 °C.
   - f. Una condición suficiente para que el compuesto X hierva es que su temperatura sea por lo menos de 150 °C.

En los ejercicios 47 a 50 *a*) use las equivalencias lógicas $p \rightarrow q \equiv \sim p \vee q$ y $p \leftrightarrow q = (\sim p \vee q) \wedge (\sim q \vee p)$ para reescribir las formas de enunciado dado sin utilizar el símbolo $\rightarrow$ o $\leftrightarrow$ y *b*) utilice la equivalencia lógica $p \vee q \equiv \sim(\sim p \wedge \sim q)$ para reescribir cada forma de enunciado usando solamente $\wedge$ y $\sim$.

47. $p \wedge \sim q \rightarrow r$ 48. $p \vee \sim q \rightarrow r \vee q$

49. $(p \rightarrow r) \leftrightarrow (q \rightarrow r)$

50. $(p \rightarrow (q \rightarrow r)) \leftrightarrow ((p \wedge q) \rightarrow r)$

51. ¿Dada cualquier forma de enunciado, es posible encontrar una forma lógicamente equivalente que sólo use $\sim$ y $\wedge$? Justifique su respuesta.

Respuestas del autoexamen

1. verdadera; falsa 2. $p \wedge \sim q$ 3. si q entonces p 4. si $\sim q$ entonces $\sim p$ 5. si $\sim p$ entonces $\sim q$ 6. lógicamente equivalentes 7. lógicamente equivalentes 8. R; S 9. S; R 10. R; S

2.3 Argumentos válidos y no válidos

"Por el contrario", continuó Patachún, "si fuera así, podría ser y si así fuera, sería, pero como no lo es, no es. Es lógico". —Lewis Carroll, *A través del espejo*

En las matemáticas y en lógica un argumento no es una disputa. Es una secuencia de instrucciones que terminan en una conclusión. En esta sección se muestra cómo determinar si un argumento es válido, es decir, si la conclusión se deduce *necesariamente* de los enunciados anteriores. Demostraremos que esta decisión sólo depende de la forma de un argumento, no de su contenido.

En la sección 2.1, se mostró que la forma lógica de un argumento puede abstraerse de su contenido. Por ejemplo, el argumento

Si Sócrates es un hombre, entonces Sócrates es mortal.
Sócrates es un hombre.
$\therefore$ Sócrates es mortal.

tiene la forma resumida

Si p, entonces q
p
$\therefore q$

Cuando considere la forma abstracta de un argumento, piense en p y q como variables con las cuales se pueden sustituir los enunciados. Una forma de argumento se llama *válida* si y sólo si, una vez que se sustituyen los enunciados que hacen todas las premisas verdaderas, la conclusión también es verdadera.

• Definición

Un **argumento** es una secuencia de enunciados y una **forma de argumento** es una secuencia de formas de enunciado. Todos los enunciados en un argumento y todas las formas de enunciado en una forma de argumento, a excepción de la final, se llaman **premisas** (o **suposiciones** o **hipótesis**). El enunciado final o forma de enunciado se llama la **conclusión**. El símbolo $\therefore$, que se lee "por tanto", se coloca normalmente justo antes de la conclusión.

Decir que una *forma de argumento* es **válida** significa que no importan qué argumentos particulares sean sustituidos por los enunciados variables en sus premisas, si las premisas resultantes son todas verdaderas, entonces la conclusión también es verdadera. Decir que un *argumento* es **válido** significa que su forma es válida.

El hecho crucial acerca de un argumento válido es que lo verdadero de su conclusión se deduce *necesariamente* o *inevitablemente* o *por la forma lógica sólo* de lo verdadero de sus premisas. Es imposible tener un argumento válido con premisas verdaderas y una falsa conclusión. Cuando un argumento es válido y sus premisas son verdaderas, se dice que lo verdadero de la conclusión *se infiere o se deduce* de lo verdadero de las premisas. Si una conclusión "no es necesariamente así", entonces no es una deducción válida.

Prueba de la validez de una forma de argumento

1. Identifique las premisas y la conclusión de la forma de argumento.
2. Construya una tabla de verdad que muestre los valores de verdad de todas las premisas y la conclusión.
3. Un renglón de la tabla de verdad en el que todas las premisas son verdaderas se llama un **renglón crítico**. Si hay un renglón crítico en el que la conclusión es falsa, entonces es posible que un argumento de la forma dada tenga premisas verdaderas y una conclusión falsa, por lo que la forma del argumento es no válida. Si la conclusión en *cada* renglón crítico es verdadera, entonces la forma del argumento es válida.

Ejemplo 2.3.1 Determinación de validez o no validez

Determine si la siguiente forma de argumento es válida o no válida sacando una tabla de verdad, indicando qué columnas representan las premisas y cuáles representan la conclusión y anotando en la tabla una frase de la explicación. Cuando complete la tabla sólo tiene que indicar los valores de verdad para la conclusión en los renglones en que todas las premisas son verdaderas (los renglones críticos), porque los valores verdaderos de la conclusión en otros renglones son irrelevantes para la validez o no validez del argumento.

$$p \to q \vee \sim r$$
$$q \to p \wedge r$$
$$\therefore p \to r$$

Solución La tabla de verdad muestra que a pesar de que existen varias situaciones en los que las premisas y la conclusión son verdaderas (renglones 1, 7 y 8), hay una situación (renglón 4) donde las premisas son verdaderas y la conclusión es falsa.

						premisas		conclusión
p	q	r	$\sim r$	$q \vee \sim r$	$p \wedge r$	$p \to q \vee \sim r$	$q \to p \wedge r$	$p \to r$
V	V	V	F	V	V	V	V	V
V	V	F	V	V	F	V	F	
V	F	V	F	F	V	F	V	
V	F	F	V	V	F	V	V	F
F	V	V	F	V	F	V	F	
F	V	F	V	V	F	V	F	
F	F	V	F	F	F	V	V	V
F	F	F	V	V	F	V	V	V

Este renglón muestra que un argumento de esta forma puede tener premisas verdaderas y una conclusión falsa. Por tanto esta forma de argumento es no válida

■

Modus ponens y Modus tollens

Una forma de argumento que consiste en dos premisas y una conclusión se le llama un **silogismo**. La primera y segunda premisas se llaman la **premisa mayor** y la **premisa menor**, respectivamente.

La forma más famosa del silogismo en lógica se llama **modus ponens**. Tiene la siguiente forma:

Si p entonces q.
p
$\therefore q$

Este es un argumento de esta forma:

Si la suma de los dígitos de 371 487 es divisible entre 3, entonces 371 487 es divisible entre 3.
La suma de los dígitos de 371 487 es divisible entre 3.
$\therefore$ 371 487 es divisible por 3.

El término *modus ponens* en latín significa "método de afirmación" (la conclusión es una afirmación). Mucho antes de que viera su primera tabla de verdad, sin duda, que se convenció con argumentos de esta forma. Sin embargo, es instructivo demostrar que el *modus ponens* es una forma válida de argumento si no hay otra razón que la de confirmar el acuerdo entre la definición formal de validez y el concepto intuitivo. Para hacer esto, se construye una tabla de verdad para las premisas y la conclusión.

		premisas		conclusión	
p	q	$p \rightarrow q$	p	q	
V	V	V	V	V	← renglón crítico
V	F	F	V		
F	V	V	F		
F	F	V	F		

El primer renglón es el único en la que ambas premisas son verdaderas y la conclusión de ese renglón también es verdadera. De ahí que la forma del argumento es válida.

Ahora consideremos otra forma de argumento válido llamada **modus tollens**. Tiene la siguiente forma:

Si p entonces q.
$\sim q$
$\therefore \sim p$

Un ejemplo del *modus tollens* es:

Si Zeus es humano, entonces Zeus es mortal.
Zeus no es mortal.
$\therefore$ Zeus no es humano.

Una explicación intuitiva de la validez del *modus tollens* utiliza la demostración por contradicción. Dice así:

Supongamos

1) Si Zeus es humano, entonces Zeus es mortal, y
2) Zeus no es mortal.

¿Zeus necesariamente debe ser no humano?

¡Sí!

Porque, si Zeus fuera humano, entonces por 1) iba a ser mortal.

Pero por 2) no es mortal.

Por tanto, Zeus no puede ser humano.

Modus tollens es latín y significa "método de la negación" (la conclusión es una negación). La validez del *modus tollens* es que se puede demostrar que se deduce del *modus ponens*, junto con el hecho de que un enunciado condicional es lógicamente equivalente a su contrapositivo. O se puede establecer formalmente usando una tabla de verdad. (Vea el ejercicio 13.)

Estudios realizados por psicólogos cognitivos han demostrado que, si bien casi el 100% de los estudiantes universitarios tienen una comprensión sólida e intuitiva del *modus ponens*, menos de 60% son capaces de aplicar *modus tollens* correctamente.* Sin embargo, en el razonamiento matemático, el *modus tollens* se utiliza casi con tanta frecuencia como el *modus ponens*. Por tanto, es importante estudiar cuidadosamente la forma del *modus tollens* para aprender a utilizarlo de manera eficaz.

Ejemplo 2.3.2 Reconociendo el modus ponens y el modus tollens

Utilice el *modus ponens* o el *modus tollens* para llenar los espacios en blanco de los siguientes argumentos para que se conviertan en inferencias válidas.

a. Si hay más palomas que casilleros, por lo menos dos palomas se posan en el mismo casillero.
Hay más palomas que casilleros.
$\therefore$ _____.

b. Si 870 232 es divisible entre 6, entonces es divisible entre 3.
870 232 no es divisible entre 3.
$\therefore$ _____.

Solución

a. Al menos dos palomas se posan en el mismo casillero. por el *modus ponens*

b. 870 232 no es divisible entre 6. por el *modus tollens* ■

Formas adicionales de argumento válido: reglas de inferencia

Una ***regla de inferencia*** es una forma de argumento, que es válida. Así el *modus ponens* y el *modus tollens* son reglas de inferencia. Los siguientes son ejemplos de reglas de inferencia que se utilizan con frecuencia en el razonamiento deductivo.

Ejemplo 2.3.3 Generalización

Las siguientes formas de argumento son válidas:

a. p $\quad\therefore p \vee q$ b. q $\quad\therefore p \vee q$

Estas formas de argumento se utilizan para hacer generalizaciones. Por ejemplo, de acuerdo con la primera, si p es verdadero, entonces, más generalmente, "p o q" es verdadero para *cualquier* otro enunciado q. Como un ejemplo, supongamos que le han dado el trabajo de contar a los estudiantes de clase social alta en su escuela. Pregunta en qué clase se encuentra Antón y le dicen que es un joven rico.

* *Psicología Cognitiva y sus implicaciones*, 3a. ed. por John R. Anderson (Nueva York: Freeman, 1990), páginas 292-297.

Razona de la siguiente manera:

Anton es un joven rico.

$\therefore$ (en general) Anton es un joven rico o Anton es un adulto rico.

Sabiendo que la clase social alta significa joven o adulto rico, agrega a Antón a su lista. ■

Ejemplo 2.3.4 Especialización

Las siguientes formas de argumento son válidas:

a. $p \wedge q$ b. $p \wedge q$

$\therefore p$ $\therefore q$

Estas formas de argumento se utilizan para la especialización. Cuando se clasifican objetos de acuerdo con alguna propiedad, con frecuencia se sabe mucho más de ellos que si tienen o no esa propiedad. Cuando esto sucede, descarte la información extraña conforme se concentra en la propiedad particular de interés.

Por ejemplo, supongamos que usted está buscando una persona que sabe algoritmos gráficos para trabajar en su proyecto. Descubre que Ana sabe tanto análisis numérico como algoritmos gráficos. Razona de la siguiente manera:

Ana sabe análisis numérico y Ana sabe algoritmos gráficos.

$\therefore$ (en particular) Ana sabe algoritmos gráficos.

En consecuencia, la invita a trabajar con usted en su proyecto. ■

Tanto la generalización como la especialización se utilizan con frecuencia en matemáticas hechas a la medida para ajustar las hipótesis de los teoremas conocidos con el fin de obtener nuevas conclusiones. La eliminación, la transitividad y la demostración por división en casos son también herramientas ampliamente utilizadas.

Ejemplo 2.3.5 Eliminación

Las siguientes formas de argumento son válidas:

a. $p \vee q$ b. $p \vee q$

$\sim q$ $\sim p$

$\therefore p$ $\therefore q$

Digamos que estas formas de argumento tienen sólo dos posibilidades y si se puede descartar una, la otra debe ser el caso. Por ejemplo, supongamos que sabe que para un determinado número x,

$$x - 3 = 0 \quad \text{o} \quad x + 2 = 0.$$

Si también sabe que x no es negativo, entonces $x \neq -2$, por lo que

$$x + 2 \neq 0.$$

Por eliminación, entonces puede concluir que

$$\therefore x - 3 = 0.$$ ■

Ejemplo 2.3.6 Transitividad

La siguiente forma de argumento es válida:

$$\begin{array}{l} p \to q \\ q \to r \\ \therefore p \to r \end{array}$$

Muchos de los argumentos en matemáticas contienen cadenas de enunciados si-entonces. Del hecho de que un enunciado implica un segundo y el segundo implica un tercero, se puede concluir que el primer enunciado implica el tercero. Por ejemplo:

Si 18 486 es divisible entre 18, entonces 18 486 es divisible entre 9.
Si 18 486 es divisible entre 9, entonces la suma de los dígitos de 18 486 es divisible entre 9.
$\therefore$ Si 18 486 es divisible entre 18, entonces la suma de los dígitos de 18 486 es divisible entre 9. ■

Ejemplo 2.3.7 Demostración por división en casos

La siguiente forma de argumento es válida:

$$\begin{array}{l} p \vee q \\ p \rightarrow r \\ q \rightarrow r \\ \therefore r \end{array}$$

Sucede con frecuencia que sabe que una cosa u otra es verdad. Si puede demostrar que en cualquier caso se deduce una conclusión verdadera, entonces, esta conclusión también debe ser verdadera. Por ejemplo, supongamos que sabemos que x es un número real dado distinto de cero. La propiedad de tricotomía de los números reales, dice que cualquier número es positivo, negativo o cero. Por tanto (por eliminación) usted sabe que x es positivo o que x es negativo. Puede deducir que $x^2 > 0$ argumentando de la siguiente manera:

x es positivo o x es negativo.
Si x es positivo, entonces $x^2 > 0$.
Si x es negativo, entonces $x^2 > 0$.
$\therefore x^2 > 0$. ■

Las reglas de inferencia válida se utilizan constantemente en la solución de problemas. A continuación se presenta un ejemplo de la vida cotidiana.

Ejemplo 2.3.8 Aplicación: una deducción más compleja

Está a punto de salir para la escuela en la mañana y descubre que no tiene sus lentes. Sabe que los siguientes enunciados son verdaderos:

a. Si yo estaba leyendo el periódico en la cocina, entonces, mis lentes están sobre la mesa de la cocina.
b. Si los lentes están sobre la mesa de la cocina, entonces los vi en el desayuno.
c. No he visto mis lentes en el desayuno.
d. Yo estaba leyendo el periódico en la sala o estaba leyendo el periódico en la cocina.
e. Si yo estaba leyendo el periódico en la sala entonces, mis lentes están sobre la mesa del café.

¿Dónde están los lentes?

Solución Sea RK = Yo estuve leyendo el periódico en la cocina.
GK = Mis lentes están sobre la mesa de la cocina.
SB = Vi mis lentes en el desayuno.
RL = Estuve leyendo el periódico en la sala.
GC = Mis lentes están sobre la mesa del café.

A continuación se presenta una secuencia de pasos que puede utilizar para llegar a la respuesta, junto con las reglas de inferencia que le permiten sacar la conclusión de cada etapa:

1.	$RK \rightarrow GK$	por *a*)
	$GK \rightarrow SB$	por *b*)
	$\therefore RK \rightarrow SB$	por transitividad
2.	$RK \rightarrow SB$	por la conclusión de 1)
	$\sim SB$	por *c*)
	$\therefore \sim RK$	por *modus tollens*
3.	$RL \vee RK$	por *d*)
	$\sim RK$	por la conclusión de 2)
	$\therefore RL$	por eliminación
4.	$RL \rightarrow GC$	por *e*)
	RL	por la conclusión de 3)
	$\therefore GC$	por *modus ponens*

Así los lentes están en la mesa del café. ■

Falacias

Una **falacia** es un error en el razonamiento que da lugar a un argumento no válido. Tres falacias comunes son **usar premisas ambiguas** y tratarlas como si fueran no ambiguas, **razonamiento circular** (suponiendo que se ha demostrado sin tener que deducirlo de las premisas) y **saltar a una conclusión** (sin bases adecuadas). En esta sección se analizan otras dos falacias, *error converso* y *error contrario*, que dan lugar a argumentos que superficialmente se parecen a los que son válidos por el *modus ponens* y *modus tollens*, pero no son, en realidad, válidos.

Como en los ejemplos anteriores, puede demostrar que un argumento es no válido por la construcción de una tabla de verdad para la forma del argumento y la búsqueda de al menos un renglón crítico en el que todas las premisas son verdad, pero la conclusión es falsa. Otra forma es encontrar un argumento de la misma forma con premisas verdaderas y una conclusión falsa.

> Para que un argumento sea válido, todos los argumentos de la misma forma cuyas premisas son verdaderas todas deben tener una conclusión verdadera. De ello se deduce que un argumento sea invalidado significa que hay un argumento de esa forma, cuyas premisas son todas verdaderas y cuya conclusión es falsa.

Ejemplo 2.3.9 Error converso

Demuestre que el siguiente argumento es no válido:

Si Zeke es un tramposo, entonces, Zeke se sienta en la fila de atrás.

Zeke se sienta en la fila de atrás.

$\therefore$ Zeke es un tramposo.

Solución Muchas personas reconocen la invalidez del argumento anterior de forma intuitiva, con un razonamiento como éste: La primera premisa da información acerca de Zeke *si* se sabe que es un tramposo. No da ninguna información acerca de él si no es que ya sabe que

es un tramposo. Uno ciertamente puede imaginarse una persona que no es tramposa, pero que se sienta en la fila de atrás. Entonces, si el nombre de esa persona se sustituye por Zeke, la primera premisa es verdadera por defecto y la segunda premisa también es verdadera, pero la conclusión es falsa.

La forma general del argumento anterior es la siguiente:

$$p \rightarrow q$$
$$q$$
$$\therefore p$$

En el ejercicio 12*a*) al final de esta sección se le pide que utilice una tabla de verdad para demostrar que esta forma de argumento no es válida. ■

La falacia subyacente a esta forma de argumento no válido se llama **error converso**, porque la conclusión del argumento se deduce de las premisas si la premisa $p \rightarrow q$ se sustituyera por su converso. Sin embargo, esta sustitución no está permitida, ya que un enunciado condicional no es lógicamente equivalente a su converso. El error converso también se conoce como *la falacia de afirmar la consecuencia*.

Otro error común en el razonamiento se llama *error contrario*.

Ejemplo 2.3.10 Error inverso

Considere el siguiente argumento:

Si las tasas de interés están subiendo, los precios de la bolsa bajarán.

Las tasas de interés no están subiendo.

$\therefore$ Los precios de las acciones de mercado no bajarán.

Considere que este argumento tiene la forma siguiente:

$$p \rightarrow q$$
$$\sim p$$
$$\therefore \sim q$$

¡Precaución! En lógica, las palabras *verdadera* y *válido* tienen significados muy diferentes. Un argumento válido puede tener una conclusión falsa y un argumento inválido puede tener una conclusión verdadera.

En el ejercicio 12*b*) al final de esta sección, le pedimos que presente una tabla de verdad de comprobación de la invalidez de esta forma de argumento.

La falacia subyacente a esta forma de argumento inválido se llama **error contrario** ya que la conclusión del argumento que se deduce de las premisas $p \rightarrow q$ se sustituyó por su contraria. Sin embargo, este reemplazo no está permitido, ya que, un enunciado condicional no es lógicamente equivalente a su contrario. El error contrario también se conoce como la *falacia de negar el antecedente*. ■

A veces la gente agrupa las ideas de validez y de verdad. Si un argumento parece válido, aceptan la conclusión como verdadera. Y si un argumento parece capcioso (en realidad una expresión usual para inválido), piensan que la conclusión debe ser falsa. ¡Esto no es correcto!

Ejemplo 2.3.11 Un argumento válido con una falsa premisa y una conclusión falsa

El argumento que se presenta a continuación es válido por *modus ponens*. Pero su principal premisa es falsa y también lo es su conclusión.

Si John Lennon fue una estrella de rock, entonces, John Lennon era pelirrojo.

John Lennon fue una estrella de rock.

$\therefore$ John Lennon era pelirrojo. ■

Ejemplo 2.3.12 Un argumento no válido con premisas verdaderas y una conclusión verdadera

El argumento que se presenta a continuación es no válido por error converso, pero tiene una conclusión verdadera.

Si Nueva York es una ciudad grande, entonces Nueva York tiene edificios altos.
Nueva York tiene edificios altos.
$\therefore$ Nueva York es una ciudad grande. ■

• Definición

Un argumento se llama **sólido**, si y sólo si, es válido y todas sus premisas son verdaderas. Un argumento que no es sólido se llama **no sólido**.

Lo importante a destacar es que la validez es una característica de las formas de argumento: Si un argumento es válido, también lo es cualquier otro argumento que tiene la misma forma. Del mismo modo, si un argumento es no válido, también lo es cualquier otro argumento que tiene la misma forma. Lo que caracteriza a un argumento válido es que ningún argumento cuya forma es válida puede tener todas las premisas verdaderas y una conclusión falsa. Para cada argumento válido, hay argumentos de esa forma con todas las premisas verdaderas y una conclusión verdadera, con al menos una premisa falsa y una conclusión verdadera y con al menos una premisa falsa y una conclusión falsa. Por otra parte, para cada argumento no válido, hay argumentos de esa forma con todas las combinaciones de valores verdaderos de las premisas y la conclusión, incluyendo todas las premisas verdaderas y una conclusión falsa. La conclusión es que sólo podemos estar seguros de que la conclusión de un argumento es válido cuando sabemos que el argumento es sólido, es decir, cuando sabemos que el argumento es válido y dispone de todas las premisas verdaderas.

Contradicciones y argumentos válidos

El concepto de contradicción lógica se puede utilizar para hacer inferencias a través de una técnica de razonamiento llamada *regla de contradicción*. Supongamos que p es algún enunciado cuya verdad quiere deducir.

Regla de contradicción

Si puede mostrar que la suposición de que el enunciado p es falso conduce lógicamente a una contradicción, entonces se puede concluir que p es verdadera.

Ejemplo 2.3.13 Regla de contradicción

Muestre que la siguiente forma de argumento es válida:

$\sim P \rightarrow \mathbf{c}$, donde $\mathbf{c}$ es una contradicción
$\therefore p$

Solución Construya una tabla de verdad para la premisa y la conclusión de este argumento.

			premisas	conclusión
p	$\sim p$	$\mathbf{c}$	$\sim p \rightarrow \mathbf{c}$	p
V	F	F	V	V
F	V	F	F	

Hay un único renglón crítico en el que la premisa es verdadera y en este renglón la conclusión es también verdadera. Por tanto esta forma de argumento es válida. ■

La regla de contradicción es el corazón lógico del método de la demostración por contradicción. Una ligera variación también proporciona la base para resolver muchos rompecabezas lógicos mediante la eliminación de respuestas contradictorias: *Si una suposición conduce a una contradicción, entonces esa suposición debe ser falsa.*

Ejemplo 2.3.14 Caballeros y bribones

El lógico Raymond Smullyan describe una isla que contiene dos tipos de personas, caballeros que siempre dicen la verdad y bribones que siempre mienten.* Visita la isla y se le acercan dos nativos que hablan con usted de la siguiente manera:

A dice: *B* es un caballero.

B dice: *A* y yo somos del tipo opuesto.

¿Qué son *A* y *B*?

Solución *A* y *B* los dos son bribones. Para ver esto, razone de la siguiente forma: Suponga que *A* es un caballero.

∴ Lo que dice *A* es verdad.	por definición de *caballero*
∴ *B* también es un caballero.	Eso es lo que dijo *A*.
∴ Lo que *B* dice también es verdadero.	por definición de *caballero*
∴ *A* y *B* son de tipo opuesto.	Eso es lo que *B* dice.
∴ Hemos llegado a la siguiente contradicción: *A* y *B* son dos caballeros y *A* y *B* son de tipo opuesto.	
∴ La suposición es falsa.	por regla de contradicción
∴ *A* no es un caballero.	negación de la suposición
∴ *A* es un bribón.	por eliminación: dado que todos los habitantes son caballeros o bribones, ya que *A* no es un caballero, es un bribón.
∴ Lo que *A* dice es falso.	
∴ *B* no es un caballero.	
∴ B es también un bribón.	por eliminación.

Indiana University Archives

Raymond Smullyan (nacido en 1919)

Este razonamiento muestra que si el problema no tiene solución, entonces *A* y *B* deben ser bribones. Sin embargo, es concebible, que el problema no tenga solución. El enunciado del problema podría ser inherentemente contradictorio. Sin embargo, si vemos hacia atrás en la solución, se puede ver que se resuelve que tanto *A* como *B* son bribones. ■

Resumen de reglas de inferencia

La tabla 2.3.1 resume algunas de las más importantes reglas de inferencia.

* Raymond Smullyan ha escrito una encantadora serie de caprichosos pero profundos libros de rompecabezas lógicos que empiezan con *¿Cuál es el nombre del libro*? (Englewood Cliffs, New Jersey: Prentice-Hall, 1978). Otras buenas fuentes de rompecabezas lógicos son los excelentes libros de Martin Gardner, tales como *¡Ajá! Visión* y *¡Ajá! Lo tengo* (Nueva York: W. H. Freeman, 1978, 1982).

Tabla 2.3.1 Formas de argumento válidas

Modus Ponens	$p \to q$ p $\therefore q$	**Eliminación**	**a.** $p \vee q$ $\sim q$ $\therefore p$ **b.** $p \vee q$ $\sim p$ $\therefore q$
Modus Tollens	$p \to q$ $\sim q$ $\therefore \sim p$	**Transitividad**	$p \to q$ $q \to r$ $\therefore p \to r$
Generalización	**a.** p $\therefore p \vee q$ **b.** q $\therefore p \vee q$	**Demostración por división en casos**	$p \vee q$ $p \to r$ $q \to r$ $\therefore r$
Especialización	**a.** $p \wedge q$ $\therefore p$ **b.** $p \wedge q$ $\therefore q$		
Conjunción	p q $\therefore p \wedge q$	**Regla de contradicción**	$\sim p \to c$ $\therefore p$

Autoexamen

1. Que un argumento sea válido significa que todos los argumentos de la misma forma cuyas premisas _____ tienen una _____ conclusión.
2. Que un argumento es no válido significa que hay un argumento de la misma forma cuyas premisas _____ y cuya conclusión _____ .
3. Que un argumento sea sólido significa que es _____ y sus premisas _____. En este caso podemos estar seguros de que su conclusión _____.

Conjunto de ejercicios 2.3

Use el *modus ponens* o *modus tollens* para llenar los espacios en blanco en los ejercicios 1 al 5 para producir inferencias válidas.

1. Si $\sqrt{2}$ es racional, entonces $\sqrt{2} = a/b$ para algunos enteros a y b.
No es verdad que $\sqrt{2} = a/b$ para algunos enteros a y b.
$\therefore$ _____.

2. Si $1 - 0.99999\ldots$ es menor que todo número real positivo, entonces éste es igual a cero.
_____.
$\therefore$ El número $1 - 0.99999\ldots$ es igual a cero.

3. Si lógica es fácil, entonces soy el tío de un mono.
Yo no soy el tío de un mono.
$\therefore$ _____.

4. Si esta figura es un cuadrilátero, entonces la suma de sus ángulos interiores es 360°.
La suma de los ángulos interiores de esta figura no es 360°.
$\therefore$ _____.

5. Si ellos no estaban seguros de la dirección, entonces habrían telefoneado.
_____.
$\therefore$ Ellos estaban seguros de la dirección.

Utilice tablas de verdad para determinar si las formas de argumento en los ejercicios 6 al 11 son válidas. Indique qué columnas representan las premisas y cuáles representan la conclusión e incluya una frase de explicación de cómo la tabla de verdad apoya su respuesta. Su explicación debe demostrar que entiende lo que significa que una forma de argumento sea válida o no válida.

6. $p \to q$
$q \to p$
$\therefore p \vee q$

7. p
$p \to q$
$\sim q \vee r$
$\therefore r$

8. $p \vee q$
$p \to \sim q$
$p \to r$
$\therefore r$

9. $p \wedge q \to \sim r$
$p \vee \sim q$
$\sim q \to p$
$\therefore \sim r$

10. $p \to r$
$q \to r$
$\therefore p \vee q \to r$

11. $p \to q \vee r$
$\sim q \vee \sim r$
$\therefore \sim p \vee \sim r$

12. Utilice tablas de verdad para demostrar que las siguientes formas de argumento son no válidas.

a. $p \to q$
q
$\therefore p$
(error converso)

b. $p \to q$
$\sim p$
$\therefore \sim q$
(error contrario)

Utilice tablas de verdad para demostrar que el argumento de las formas referidas en los ejercicios del 13 al 21 son válidas. Indique qué columnas representan las premisas y cuáles representan a la conclusión, e incluya una frase que explique cómo la tabla de verdad apoya su respuesta. Su explicación debe demostrar que usted entiende lo que significa que una forma de argumento sea válida.

13. *Modus tollens*:

$$p \to q$$
$$\sim q$$
$$\therefore \sim p$$

14. Ejemplo 2.3.3*a*)

15. Ejemplo 2.3.3*b*)

16. Ejemplo 2.3.4*a*)

17. Ejemplo 2.3.4*b*)

18. Ejemplo 2.3.5*a*)

19. Ejemplo 2.3.5*b*)

20. Ejemplo 2.3.6

21. Ejemplo 2.3.7

Utilice símbolos para escribir la forma lógica de cada argumento en los ejercicios 22 y 23 y después use una tabla de verdad para poner a prueba la validez del argumento. Indique qué columnas representan las premisas y cuáles representan a la conclusión, e incluya algunas palabras de explicación que demuestren que entiende el significado de validez.

22. Si Tom no está en el equipo A, entonces, Hua está en el equipo B.
Si Hua no está en el equipo B, entonces, Tom está en el equipo A.
$\therefore$ Tom no está en el equipo A o Hua no está en el equipo B.

23. Oleg estudia la licenciatura en matemáticas o Oleg estudia la licenciatura en economía.
Si Oleg estudia la licenciatura en matemáticas, entonces a Oleg se le requiere que curse Matemáticas 362.
$\therefore$ Oleg estudia la licenciatura en economía o a Oleg no se le requiere que curse Matemáticas 362.

Algunos de los argumentos de los ejercicios 24 a 32 son válidos, mientras que otros muestran el error converso o contrario. Utilice símbolos para escribir la forma lógica de cada argumento. Si el argumento es válido, identifique la regla de inferencia que garantiza su validez. En caso contrario, deberá indicar si se comete error converso o error contrario.

24. Si Jules resuelve este problema correctamente, entonces Jules ha obtenido la respuesta 2.
Jules ha obtenido la respuesta 2
$\therefore$ Jules ha resuelto este problema correctamente.

25. Este número real es racional o es irracional.
Este número real no es racional.
$\therefore$ Este número real es irracional.

26. Si voy al cine, no voy a terminar mi tarea. Si no termino mi tarea, no voy a hacer bien el examen de mañana.
$\therefore$ Si voy al cine, no voy a hacer bien el examen de mañana.

27. Si este número es mayor que 2, entonces su cuadrado es mayor que 4.
Este número no es mayor que 2.
$\therefore$ El cuadrado de este número no es mayor que 4.

28. Si hay tantos números racionales como número irracionales, entonces el conjunto de todos los números irracionales es infinito.
El conjunto de todos los números irracionales es infinito.
$\therefore$ Hay tantos números racionales como números irracionales.

29. Si al menos uno de estos dos números es divisible entre 6, entonces el producto de estos dos números es divisible entre 6.
Ninguno de estos dos números es divisible entre 6.
$\therefore$ El producto de estos dos números no es divisible entre 6.

30. Si este programa de computadora es correcto, entonces produce la salida correcta cuando se ejecuta con los datos de prueba que me dio el profesor.
Este programa de computadora genera la salida correcta cuando se ejecuta con los datos de prueba que me dio mi profesor.
$\therefore$ Este programa de computadora es correcto.

31. Sandra sabe Java y Sandra sabe C++.
$\therefore$ Sandra sabe C++.

32. Si me dan una gratificación de Navidad, compraré un estéreo.
Si vendo mi moto, compraré un estéreo.
$\therefore$ Si me dan gratificación de Navidad o vendo mi moto, entonces voy a comprar un estéreo.

33. Dé un ejemplo (diferente del ejemplo 2.3.11) de un argumento válido con una conclusión falsa.

34. Dé un ejemplo (diferente del ejemplo 2.3.12) de un argumento inválido con una conclusión verdadera.

35. Explique en sus propias palabras lo que distingue una forma válida de argumento de una inválida.

36. Dada la siguiente información sobre un programa de computadora, encuentre el error en el programa.
a. Hay una variable no declarada o hay un error de sintaxis en las primeras cinco líneas.
b. Si hay un error de sintaxis en las primeras cinco líneas, entonces, falta un punto y coma o el nombre de una variable está mal escrito.
c. No falta un punto y coma.
d. No está mal escrito el nombre de una variable.

37. En la parte trasera de un viejo armario descubre una nota firmada por un pirata famoso por su extraño sentido del humor y amor a los rompecabezas lógicos. En la nota escribió que él había escondido el tesoro en algún lugar de la propiedad. Hizo una lista de cinco enunciados verdaderos (del *a* al *e* que se muestran a continuación) y desafió al lector a usarlos para averiguar la ubicación del tesoro.

a. Si esta casa está al lado de un lago, entonces el tesoro no está en la cocina.
b. Si el árbol en el patio delantero es un olmo, entonces el tesoro está en la cocina.
c. Esta casa está al lado de un lago.
d. El árbol del patio delantero es un olmo o el tesoro está enterrado bajo el asta de la bandera.
e. Si el árbol del patio trasero es un roble, el tesoro está en el garaje.

¿Dónde está escondido el tesoro?

38. Usted está visitando la isla que se describe en el ejemplo 2.3.14 y tienen los siguientes encuentros con los nativos.

a. Dos nativos *A* y *B* se dirigen a usted de la siguiente manera:
A dice: Los dos somos caballeros.
B dice: *A* es un bribón.
¿Qué son *A* y *B*?

b. Se le acercan otros dos nativos *C* y *D*, pero sólo habla *C*.
C dice: Los dos son bribones.
¿Qué son *C* y *D*?

c. Después se encuentra con los nativos *E* y *F*.
E, dice: *F* es un bribón.
F dice: *E* es un bribón.
¿Cuántos bribones hay?

H d. Por último, se encuentra con un grupo de seis indígenas, *U*, *V*, *W*, *X*, Y y *Z*, que le hablan de la siguiente manera:
U dice: Ninguno de nosotros es un caballero.
V dice: Por lo menos tres de nosotros son caballeros.
W dice: A lo más tres de nosotros son caballeros.
X dice: Exactamente cinco de nosotros son caballeros.
Y dice: Exactamente dos de nosotros son caballeros.
Z dice: Exactamente uno de nosotros es un caballero.
¿Cuáles son caballeros y cuáles son bribones?

39. El famoso detective Percule Hoirot fue llamado para resolver un misterioso asesinato desconcertante. Él determinó los siguientes hechos:

a. Lord Hazelton, el hombre muerto, fue asesinado por un golpe en la cabeza con un candelabro de bronce.
b. Ya sea Lady Hazelton o una criada, Sara, estaba en el comedor en el momento del asesinato.
c. Si el cocinero estaba en la cocina en el momento del asesinato, el mayordomo mató a Lord Hazelton con una dosis letal de estricnina.
d. Si Lady Hazelton se encontraba en el comedor en el momento del asesinato, entonces el chofer asesinó a Lord Hazelton.
e. Si el cocinero no estaba en la cocina en el momento en que se cometió el asesinato, entonces, Sara no estaba en el comedor cuando se cometió el asesinato.
f. Si Sara estaba en el comedor en el momento que se cometió el asesinato, el *sumiller* mató a Lord Hazelton.

¿Es posible que el detective deduzca la identidad del asesino de estos hechos? Si es así, ¿quién cometió el asesinato de Lord Hazelton? (Suponga que sólo había una causa de la muerte).

40. Tiburón, un líder del hampa, fue asesinado por uno de su propia banda de cuatro secuaces. El detective Brillante entrevistó a los hombres y determinó que todos estaban mintiendo a excepción de uno. Dedujo quién mató a Tiburón con base en los siguientes enunciados:

a. Puños: El zurdo mató a Tiburón.
b. Grasa: Músculos no mató a Tiburón.
c. Zurdo: Músculos jugaba dados con Puños cuando Tiburón cayó.
d. Músculos: Zurdo no mató a Tiburón.

¿Quién mató a Tiburón?

En los ejercicios del 41 al 44 se dan un conjunto de premisas y una conclusión. Use las formas de argumento válidas que se presentan en la tabla 2.3.1 para deducir la conclusión de las premisas, dando una razón para cada paso como en el ejemplo 2.3.8. Suponga que todas las variables son enunciados variables.

41. a. $\sim p \vee q \rightarrow r$
b. $s \vee \sim q$
c. $\sim t$
d. $p \rightarrow t$
e. $\sim p \wedge r \rightarrow \sim s$
f. $\therefore \sim q$

43. a. $\sim p \rightarrow r \wedge \sim s$
b. $t \rightarrow s$
c. $u \rightarrow \sim p$
d. $\sim w$
e. $u \vee w$
f. $\therefore \sim t$

42. a. $p \vee q$
b. $q \rightarrow r$
c. $p \wedge s \rightarrow t$
d. $\sim r$
e. $\sim q \rightarrow u \wedge s$
f. $\therefore t$

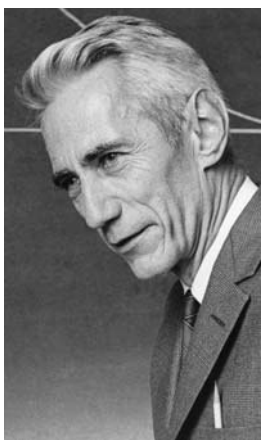
44. a. $p \rightarrow q$
b. $r \vee s$
c. $\sim s \rightarrow \sim t$
d. $\sim q \vee s$
e. $\sim s$
f. $\sim p \wedge r \rightarrow u$
g. $w \vee t$
h. $\therefore u \wedge w$

Respuestas del autoexamen

1. todas son verdaderas; verdadera 2. todas son verdaderas; es falsa 3. válida; todas son verdaderas; es verdadera

2.4 Aplicación: circuitos lógicos digitales

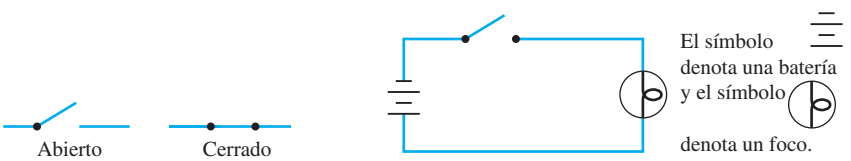
¡Sólo conecte! —E. M. Forster, *Regreso a Howards End*


MIT Museum

Claude Shannon
(1916-2001)

En la década de 1930, un joven estudiante de graduados del Instituto Tecnológico de Massachusetts, llamado Claude Shannon observó una analogía entre el funcionamiento de dispositivos de conmutación, tales como conmutador telefónico: circuitos y las operaciones de conectores lógicos. Utilizó esta analogía con un éxito sorprendente para resolver problemas de diseño de circuitos y lo escribió en su tesis de maestría, que fue publicada en 1938.

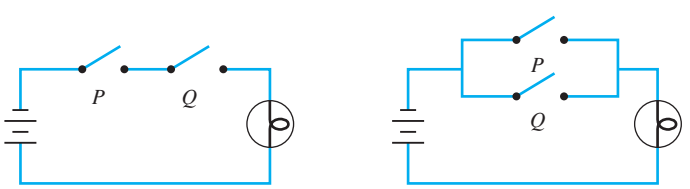
El dibujo de la figura 2.4.1*a*) muestra la presencia de dos posiciones de un interruptor simple. Cuando se cierra el interruptor, la corriente puede fluir de una terminal a la otra, cuando está abierto, la corriente no puede fluir. Imagínese que dicho interruptor es parte del circuito que se muestra en la figura 2.4.1*b*). El foco se enciende si y sólo si, la corriente fluye a través de él. Y esto ocurre si y sólo si, el interruptor está cerrado.



a) *b*)

Figura 2.4.1

Ahora consideremos los circuitos más complicados de las figuras 2.4.2*a*) y 2.4.2*b*).



Interruptores "en serie" Interruptores "en paralelo"

a) *b*)

Figura 2.4.2

En el circuito de la figura 2.4.2*a*) la corriente fluye y se enciende el foco, si y sólo si, *ambos* interruptores P y Q están cerrados. Los interruptores de este circuito se dice que están **en serie.** En el circuito de la figura 2.4.2*b*) la corriente fluye y el foco se enciende si y sólo si *al menos uno* de los interruptores P o Q está cerrado. Los interruptores de este circuito se dice que están en **paralelo**. En la tabla 2.4.1 se describen todos los posibles comportamientos de estos circuitos.

Tabla 2.4.1

***a*) Interruptores en serie**

Interruptores		Foco
P	***Q***	**Estado**
cerrado	cerrado	encendido
cerrado	abierto	apagado
abierto	cerrado	apagado
abierto	abierto	apagado

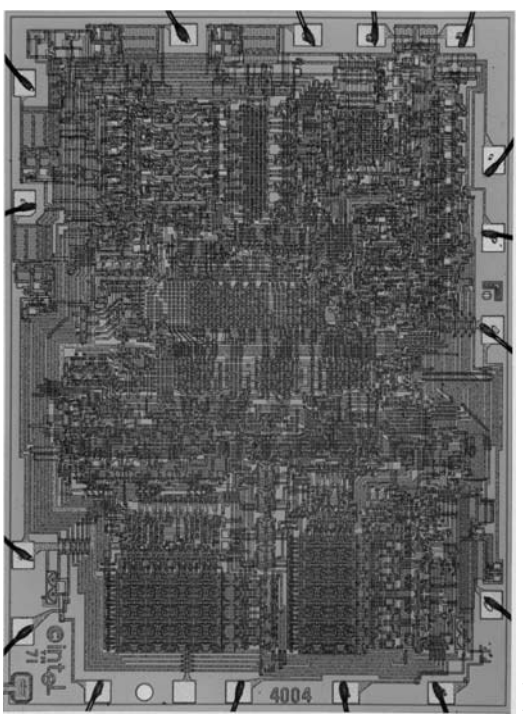
***b*) Interruptores en paralelo**

Interruptores		Foco
P	***Q***	**Estado**
cerrado	cerrado	encendido
cerrado	abierto	encendido
abierto	cerrado	encendido
abierto	abierto	apagado

Observe que si las palabras *cerrado* y *encendido* se sustituyen por V y *abierto* y cerrado se reemplazan por F, la tabla 2.4.1*a*) se convierte en la tabla de verdad para *y* y la tabla 2.4.1*b*) se convierte en la tabla de verdad para *o*. En consecuencia, el circuito de interruptores de la figura 2.4.2*a*) se dice que corresponde a la expresión lógica $P \wedge Q$ y el de la figura 2.4.2*b*) se dice que corresponden a $P \vee Q$.

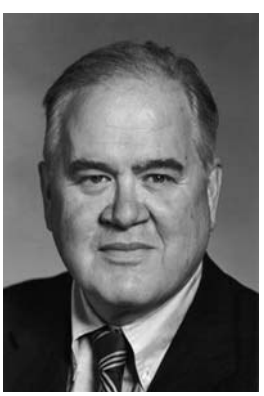
Circuitos más complicados corresponden a expresiones lógicas más complicadas. Esta correspondencia se ha utilizado ampliamente en el diseño y estudio de los circuitos.

En la década de 1940 y 1950, se reemplazaron los interruptores por dispositivos electrónicos, con estados físicos de abierto y cerrado correspondientes con los estados electrónicos, tales como alto y bajo voltajes. La nueva tecnología electrónica condujo al desarrollo de modernos sistemas digitales tales como computadoras electrónicas, sistemas electrónicos de conmutación telefónica, control de semáforos, calculadoras electrónicas y mecanismos de control utilizados en cientos de otros tipos de equipos electrónicos. Los componentes electrónicos básicos de un sistema digital se llaman *circuitos lógicos digitales*. La palabra *lógica* indica el importante papel de la lógica en el diseño de estos circuitos y la palabra *digital* indica que los circuitos de procesan en señales discretas, o por separado, señales opuestas a las continuas.



Intel

El Intel 4004, introducido en 1971, es generalmente considerado como el primer microprocesador comercialmente disponible o unidad central de procesamiento (CPU) contenido en un chip del tamaño de una uña. Constaba de 2 300 transistores y podía ejecutar 70 000 instrucciones por segundo, esencialmente la misma potencia de cálculo que la primera computadora electrónica, la ENIAC, construida en 1946, que ocupaba toda una habitación. Los modernos microprocesadores consisten de varios CPUs en un solo chip, contienen cerca de mil millones de transistores y muchos cientos de millones de circuitos lógicos y pueden calcular cientos de millones de instrucciones por segundo.



Courtesy of IBM

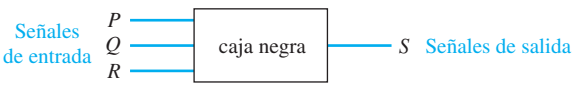
John W. Tukey (1915-2000)

Los ingenieros eléctricos continúan utilizando el lenguaje de la lógica cuando se refieren a los valores de las señales producidas por un interruptor electrónico como "verdadero" o "falso". Pero por lo general utilizan los símbolos 1 y 0 en lugar de V y F para indicar estos valores. Los símbolos 0 y 1 se llaman **bits**, abreviatura de dígi**tos bi**narios. Esta terminología se introdujo en 1946 por el estadístico John W. Tukey.

Cajas negras y puertas

Las combinaciones de señales de bits (1 y 0) se pueden transformar en otras combinaciones de señales de bits (1 y 0) a través de varios circuitos. Ya que se utilizan en muchas

diferentes tecnologías en la construcción del circuito, los ingenieros informáticos y diseñadores de sistemas digitales encontraron útil pensar en ciertos circuitos básicos como cajas negras. El interior de una caja negra contiene la implementación detallada del circuito que con frecuencia se ignora, mientras la atención se centra en la relación entre las señales de **entrada** y **salida**.



El funcionamiento de una caja negra se especifica completamente construyendo una tabla de entrada/salida que enumera todas sus posibles señales de entrada junto con sus señales de salida correspondientes. Por ejemplo, la caja negra de la figura anterior tiene tres señales de entrada. Puesto que cada una de estas señales puede tomar el valor 1 o 0, hay ocho posibles combinaciones de las señales de entrada. Una posible correspondencia de las señales de entrada y salida es la siguiente:

Una tabla de entrada/salida

Entrada			Salida
P	***Q***	***R***	***S***
1	1	1	1
1	1	0	0
1	0	1	0
1	0	0	1
0	1	1	0
0	1	0	1
0	0	1	1
0	0	0	0

Por ejemplo, el tercer renglón, indica que para las entradas $P = 1$, $Q = 0$ y $R = 1$, la salida S es 0.

Un método eficiente para el diseño de circuitos más complicados es construir conectando circuitos cajas negras menos complicados. Tres de estos circuitos se conocen como las puertas NOT, AND y OR.

Una **puerta NOT** (o **inversor**) es un circuito con una señal de entrada y una señal de salida. Si la señal de entrada es 1, la señal de salida es 0. Por el contrario, si la señal de entrada es 0, entonces, la señal de salida es 1. Una **puerta AND** es un circuito con dos señales de entrada y una señal de salida. Si las dos señales de entrada son 1, entonces la señal de salida es 1. De lo contrario, la señal de salida es 0. Una **puerta OR** también cuenta con dos señales de entrada y una señal de salida. Si las dos señales de entrada son 0, entonces la señal de salida es 0. De lo contrario, la señal de salida es 1.

Las acciones de las puertas NOT, AND y OR se resumen en la figura 2.4.3, donde P y Q representan las señales de entrada y R representa la señal de salida. Debe quedar claro en la figura 2.4.3 que las acciones de las puertas NOT, AND y OR en las señales corresponden exactamente con las de los conectores lógicos $\sim$, $\wedge$ y $\vee$ de los enunciados, si el símbolo 1 se identifica con V y el símbolo 0 se identifica con F.

Las puertas se pueden combinar en los circuitos de muchas maneras. Si se obedecen las reglas que se muestran en la página siguiente, el resultado es un **circuito combinacional**, uno cuya salida en cualquier momento se determina completamente por su entrada en ese momento sin considerar a las entradas anteriores.

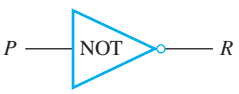
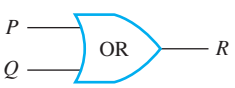
<table>
<tr><th>Tipo de puerta</th><th>Representación simbólica</th><th>Acción</th></tr>
<tr><td>NOT</td><td> 
</td><td>
<table>
<tr><th>Entrada</th><th>Salida</th></tr>
<tr><th>P</th><th>R</th></tr>
<tr><td>1</td><td>0</td></tr>
<tr><td>0</td><td>1</td></tr>
</table>
</td></tr>
<tr><td>AND</td><td> 
</td><td>
<table>
<tr><th colspan="2">Entrada</th><th>Salida</th></tr>
<tr><th>P</th><th>Q</th><th>R</th></tr>
<tr><td>1</td><td>1</td><td>1</td></tr>
<tr><td>1</td><td>0</td><td>0</td></tr>
<tr><td>0</td><td>1</td><td>0</td></tr>
<tr><td>0</td><td>0</td><td>0</td></tr>
</table>
</td></tr>
<tr><td>OR</td><td> 
</td><td>
<table>
<tr><th colspan="2">Entrada</th><th>Salida</th></tr>
<tr><th>P</th><th>Q</th><th>R</th></tr>
<tr><td>1</td><td>1</td><td>1</td></tr>
<tr><td>1</td><td>0</td><td>1</td></tr>
<tr><td>0</td><td>1</td><td>1</td></tr>
<tr><td>0</td><td>0</td><td>0</td></tr>
</table>
</td></tr>
</table>

Figura 2.4.3

Reglas para un circuito combinacional

Nunca combine dos cables de entrada. 2.4.1

Un único cable de entrada se puede separar en dos y utilizarlo como entrada para dos puertas separadas. 2.4.2

Un cable de salida se puede utilizar como entrada. 2.4.3

La no salida de una puerta puede eventualmente alimentar de nuevo esa puerta. 2.4.4

La regla (2.4.4) se viola en circuitos más complejos, llamados **circuitos secuenciales**, cuya salida en un momento dado depende tanto de la entrada en ese momento como también de las entradas anteriores. Estos circuitos se analizan en la sección 12.2.

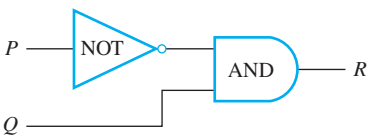
La tabla de entrada/salida para un circuito

Si le dan un conjunto de señales de entrada para un circuito, puede encontrar su salida siguiendo el circuito puerta por puerta.

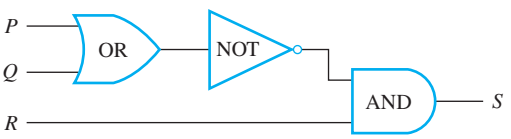
Ejemplo 2.4.1 Determinación de salida para una entrada dada

Indique la salida de los circuitos que se muestra a continuación para las señales de entrada dadas.

a. Señales de entrada: $P = 0$ y $Q = 1$

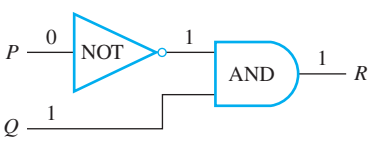


b. Señales de entrada: $P = 1$, $Q = 0$ y $R = 1$

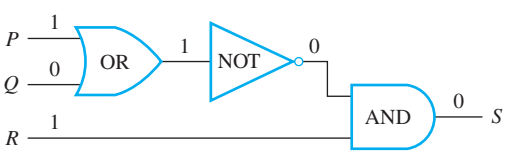


Solución

a. Muévase de izquierda a derecha a través del diagrama, siga la acción de cada puerta en las señales de entrada. La puerta NOT cambia de $P = 0$ a 1, por lo que ambas entradas a la puerta AND son 1, por lo que la salida de R es 1. Esto se muestra indicado en el diagrama, como se muestra a continuación.



b. La salida de la puerta OR es 1 ya que una de las señales de entrada, P, es 1. La puerta NOT cambia este 1 en un 0, por lo que las dos entradas a la puerta AND son 0 y R = 1. Por tanto la salida de S es 0. A continuación se muestra el seguimiento.

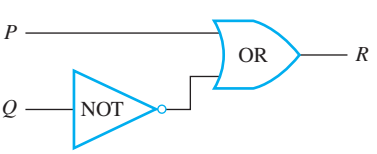


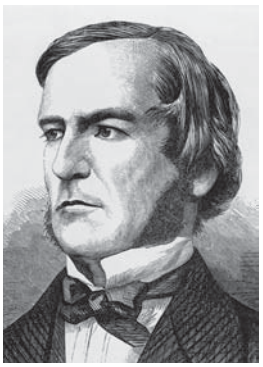
■

Para construir la tabla completa de entrada/salida de un circuito, siga el circuito para encontrar las señales de salida correspondientes a cada posible combinación de señales de entrada.

Ejemplo 2.4.2 Construcción de tabla de entrada/salida para un circuito

Construya la tabla de entrada/salida del siguiente circuito.




CORBIS

George Boole
(1815-1864)

Solución Enliste las cuatro combinaciones posibles de las señales de entrada y encuentre la salida para cada una siguiendo el circuito.

Entrada		Salida
P	***Q***	***R***
1	1	1
1	0	1
0	1	0
0	0	1

■

La expresión booleana correspondiente a un circuito

En lógica, variables tales como p, q y r representan enunciados y un enunciado puede tener uno de los dos valores de verdad: V (verdadero) o F (falso). Una forma de enunciado es una expresión, tal como $p \wedge (\sim q \vee r)$, compuesto por variables de enunciado y conectores lógicos.

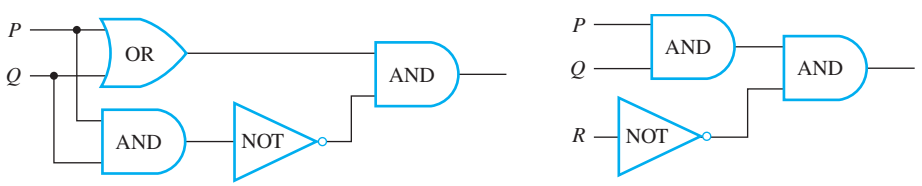
Como se indicó anteriormente, uno de los fundadores de la lógica simbólica fue el matemático inglés George Boole. En su honor, cualquier variable, tal como un enunciado variable o una señal de entrada, que puede tomar uno de los dos valores, se llama una **variable booleana**. Una expresión compuesta de variables booleanas y conectores $\sim$, $\wedge$ y $\vee$ se denomina una **expresión booleana**.

Dado un circuito que consiste de la combinación de las puertas NOT, AND y OR, se puede obtener una expresión booleana correspondiente siguiendo las acciones de las puertas de las variables de entrada.

Nota Estrictamente hablando sólo expresiones significativas tales como $(\sim p \wedge q) \vee (p \wedge r)$ y $\sim(\sim(p \wedge q) \vee r)$ se permiten como booleanas, no sin sentido como $p \sim q$ $((rs \vee \wedge q\sim$. Usamos la recursión para dar una cuidadosa definición de las expresiones booleanas de la sección 5.9.

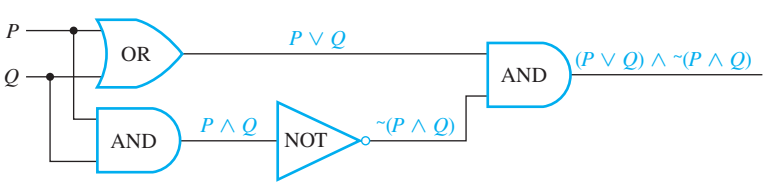
Ejemplo 2.4.3 Determinación de una expresión booleana para un circuito

Encuentre las expresiones booleanas que corresponden a los circuitos que se muestran a continuación. Un punto indica una soldadura de dos alambres, cables que se cruzan sin un punto se supone que no se tocan.



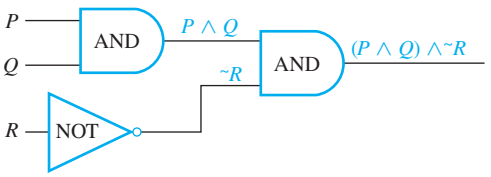
Solución

a. Dé seguimiento a través del circuito de izquierda a derecha, indicando la salida de cada puerta simbólicamente, como se muestra a continuación.



La expresión final obtenida $(P \vee Q) \wedge \sim(P \wedge Q)$, es la expresión para o exclusivo: P o Q, pero no ambos.

b. La expresión booleana correspondiente al circuito es $(P \wedge Q) \wedge \sim R$, como se muestra a continuación.



Observe que la salida del circuito que se muestra en el ejemplo 2.4.3*b*) es 1 exactamente para una combinación de las entradas ($P = 1$, $Q = 1$ y $R = 0$) y es 0 para todas las entradas de otras combinaciones. Por esta razón, el circuito se puede decir que "reconoce" una combinación particular de entradas. La columna de salida de la tabla de entrada/salida tiene un 1 en exactamente un renglón y 0 en todos los otros renglones.

• Definición

Un **reconocedor** es un circuito que genera un 1 para exactamente una combinación particular de señales de entrada y salidas 0 para las demás combinaciones.

Tabla de entrada/salida para un reconocedor

P	Q	R	$(P \wedge Q) \wedge \sim R$
1	1	1	0
1	1	0	1
1	0	1	0
1	0	0	0
0	1	1	0
0	1	0	0
0	0	1	0
0	0	0	0

El circuito correspondiente a una expresión booleana

Los ejemplos anteriores muestran cómo encontrar una expresión booleana correspondiente a un circuito. El siguiente ejemplo muestra cómo construir un circuito correspondiente a una expresión booleana.

Ejemplo 2.4.4 Construcción de circuitos de las expresiones booleanas

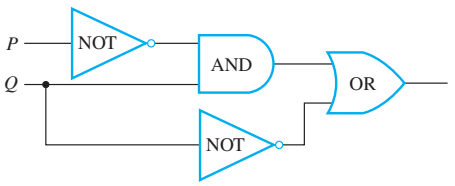
Construya circuitos para las siguientes expresiones booleanas.

a. $(\sim P \wedge Q) \vee \sim Q$ b. $((P \wedge Q) \wedge (R \wedge S)) \wedge T$

Solución

a. Escriba las variables de entrada en una columna en el lado izquierdo del diagrama. Después en el lado derecho del diagrama a la izquierda, trabaje de la parte más externa hacia la más interna. Ya que la última operación ejecutada cuando se evaluó $(\sim P \wedge Q) \vee \sim Q$ es $\vee$, ponga una puerta OR en el extremo derecho del diagrama. Una entrada de esta puerta es $\sim P \wedge Q$, por lo que dibuje una puerta AND a la izquierda de la puerta

OR y muestre su salida entrando en la puerta OR. Puesto que una entrada a la puerta AND es $\sim P$, dibuje una línea de P a una puerta NOT y de ahí a la puerta AND. Ya que la otra entrada a la puerta AND es Q, dibuje una línea de Q directamente a la puerta AND. La otra entrada a la puerta OR es $\sim Q$, por lo que dibuje una línea de Q a la puerta NOT y de la puerta NOT a la puerta OR. Se obtiene el circuito que se muestra a continuación.



b. Para iniciar la construcción de este circuito, ponga una puerta AND en el extremo derecho para la $\wedge$ entre $((P \wedge Q) \wedge (R \wedge S))$ y T. A la izquierda de donde puso la puerta AND corresponde al $\wedge$ entre $P \wedge Q$ y $R \wedge S$. A la izquierda de donde puso la puerta AND corresponde a los $\wedge$ entre P y Q y entre R y S. En la figura 2.4.4 se muestra el circuito.

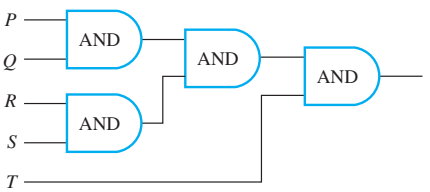


Figura 2.4.4 ■

Esto se deduce del teorema 2.1.1 que todas las formas de agregar paréntesis para $P \wedge Q \wedge R \wedge \mathrm{S} \wedge T$ son lógicamente equivalentes. Así, por ejemplo,

$$((P \wedge Q) \wedge (R \wedge S)) \wedge T \equiv (P \wedge (Q \wedge R)) \wedge (S \wedge T)$$

También se deduce del circuito de la figura 2.4.5, que corresponde a $(P \wedge (Q \wedge R)) \wedge (S \wedge T)$, que tiene la misma tabla de entrada/salida que el circuito de la figura 2.4.4, que corresponde a $((P \wedge Q) \wedge (R \wedge S)) \wedge T$.

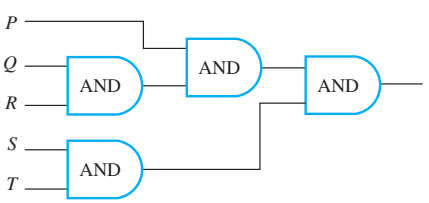


Figura 2.4.5

Cada uno de los circuitos en las figuras 2.4.4 y 2.4.5 es, por tanto, una implementación de la expresión $P \wedge Q \wedge R \wedge S \wedge \mathrm{T}$. Este circuito recibe el nombre de **puerta AND de entrada múltiple** y se representa por el diagrama que se muestra en la figura 2.4.6. Las **puertas OR de entrada múltiple** se construyen de manera similar.

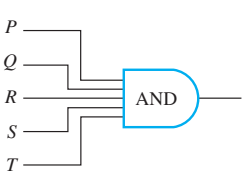


Figura 2.4.6

Determinación de un circuito que corresponde a una tabla dada de entrada/salida

Hasta el momento, hemos analizado la forma de construir la tabla de entrada/salida de un circuito, cómo encontrar la expresión booleana correspondiente para un circuito dado y cómo construir el circuito que corresponde a una expresión booleana dada. Ahora trataremos el tema de cómo diseñar un circuito (o encontrar una expresión booleana) que corresponda a una tabla dada de entrada/salida. La forma de hacerlo es poner varios reconocedores juntos en paralelo.

Ejemplo 2.4.5 Diseño de un circuito para una tabla dada de entrada/salida

Diseñe un circuito para la siguiente tabla de entrada/salida:

Entrada			Salida
P	***Q***	***R***	***S***
1	1	1	1
1	1	0	0
1	0	1	1
1	0	0	1
0	1	1	0
0	1	0	0
0	0	1	0
0	0	0	0

Solución Primero construya una expresión booleana con esta tabla como su tabla de verdad. Para hacer esto identifique cada renglón para el que la salida es 1 —en este caso el primero, tercero y cuarto renglones. Para cada uno de estos renglones construya una expresión y que produzca un 1 (o verdadero) para la combinación exacta de valores de entrada para ese renglón y un 0 (o falso) para todas las otras combinaciones de los valores de entrada. Por ejemplo, la expresión para el primer renglón es $P \wedge Q \wedge R$ porque $P \wedge Q \wedge R$ es 1 si $P = 1$ y $Q = 1$ y $R = 1$ y es 0 para todos los demás valores de P, Q y R. La expresión del tercer renglón es $P \wedge \sim Q \wedge R$ ya que $P \wedge \sim Q \wedge R$ es 1 si $P = 1$ y $Q = 0$ y $R = 1$ y es 0 para todos los demás valores de P, Q y R. Del mismo modo la expresión del cuarto renglón es $P \wedge \sim Q \wedge \sim R$.

Ahora, cualquier expresión booleana con la tabla dada como su tabla de verdad tiene el valor 1 en el caso $P \wedge Q \wedge R = 1$, o en caso de $P \wedge \sim Q \wedge R = 1$, o en caso $P \wedge \sim Q \wedge \sim R = 1$ y en ningún otro caso. De lo que se deduce que una expresión booleana con la tabla de verdad dada es

$$(P \wedge Q \wedge R) \vee (P \wedge \sim Q \wedge R) \vee (P \wedge \sim Q \wedge \sim R). \qquad 2.4.5$$

El circuito correspondiente a esta expresión tiene el diagrama que se muestra en la figura 2.4.7. Observe que la expresión (2.4.5) es una disyunción de términos en los que ellos mismos son conjunciones en los que una de P o $\sim P$, una de Q o $\sim Q$ y una de R o $\sim R$ todas aparecen. Se dice que tales expresiones están en **forma normal disyuntiva** o en **forma de suma de productos**.

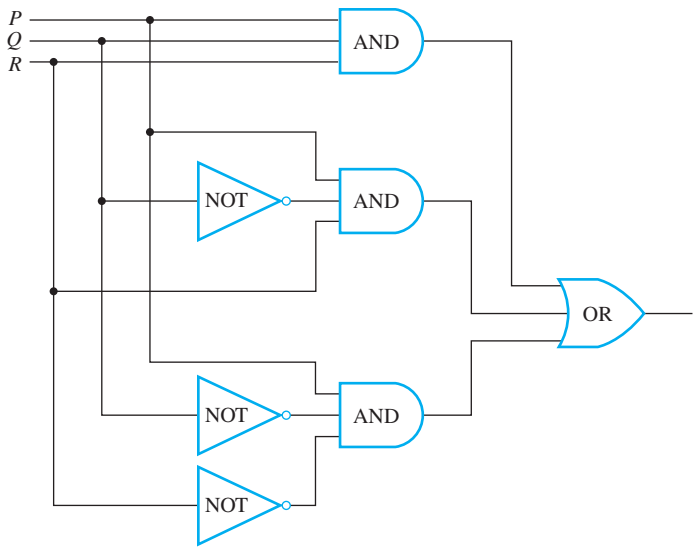


Figura 2.4.7

Simplificación de circuitos combinacionales

Considere los dos circuitos combinacionales que se muestran en la figura 2.4.8.

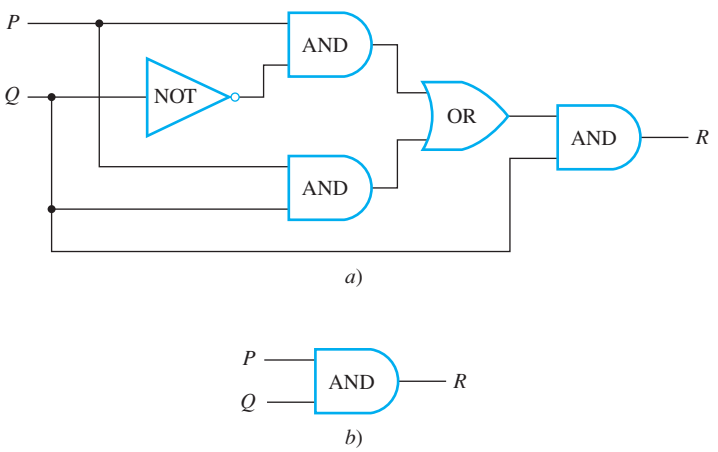


Figura 2.4.8

Si sigue al circuito *a*), encontrará que su tabla de entrada/salida es

Entrada		Salida
P	***Q***	***R***
1	1	1
1	0	0
0	1	0
0	0	0

que es igual que la tabla de entrada/salida para el circuito *b*). Así, estos dos circuitos hacen el mismo trabajo en el sentido de que se transforman las mismas combinaciones de señales

de entrada en las mismas señales de salida. Sin embargo, el circuito *b*) es más simple que el circuito *a*), ya que contiene muchas menos puertas lógicas. Por tanto, como parte de un circuito integrado, ocupan menos espacio y requieren de menos energía.

• Definición

Dos circuitos lógicos digitales son **equivalentes** si y sólo si, sus tablas de entrada/salida son idénticas.

Puesto que las formas de enunciado lógicamente equivalentes tienen tablas de verdad idénticas, se puede determinar que dos circuitos son equivalentes encontrando las expresiones booleanas correspondiente a los circuitos y demostrando que estas expresiones, consideradas como formas de enunciado, son lógicamente equivalentes. El ejemplo 2.4.6 muestra cómo funciona este procedimiento para los circuitos *a*) y *b*) en la figura 2.4.8.

Ejemplo 2.4.6 Demuestre que dos circuitos son equivalentes

Encuentre las expresiones booleanas para cada circuito de la figura 2.4.8. Utilice el teorema 2.1.1 para demostrar que estas expresiones son lógicamente equivalentes cuando se le considera como formas de enunciado.

Solución Las expresiones booleanas que corresponden a los circuitos *a*) y *b*) son $((P \wedge \sim Q) \vee (P \wedge Q)) \wedge Q$ y $P \wedge Q$, respectivamente. Por el teorema 2.1.1,

$$
\begin{aligned}
&((P \wedge \sim Q) \vee (P \wedge Q)) \wedge Q \\
&\quad \equiv (P \wedge (\sim Q \vee Q)) \wedge Q && \text{por la ley distributiva} \\
&\quad \equiv (P \wedge (Q \vee \sim Q)) \wedge Q && \text{por la ley conmutativa para } \vee \\
&\quad \equiv (P \wedge \mathbf{t}) \wedge Q && \text{por la ley de negación} \\
&\quad \equiv P \wedge Q && \text{por la ley de identidad.}
\end{aligned}
$$

De lo que se deduce que las tablas de verdad para $((P \wedge \sim Q) \vee (P \wedge Q)) \wedge Q$ y $P \wedge Q$ son iguales: Por lo que las tablas de entrada y salida de los circuitos correspondientes a estas expresiones son iguales y así los circuitos son equivalentes. ■

En general, se puede simplificar un circuito combinacional determinando la correspondiente expresión booleana, utilizando las propiedades que se listan en el teorema 2.1.1 para encontrar una expresión booleana que es más corta y lógicamente equivalente a la misma (cuando ambos son considerados como formas de enunciado) y la construcción del circuito correspondiente a esta corta expresión booleana.

Puertas NAND y NOR

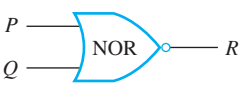
Harvard University Archives

H. M. Sheffer (1882-1964)

Otra forma de simplificar un circuito consiste en encontrar un circuito equivalente que utilice el menor número de diferentes tipos de puertas lógicas. Dos puertas que no se presentaron antes pero que son particularmente útiles para esto son: las puertas NAND y NOR. Una puerta NAND es una sola puerta que actúa como una puerta AND seguida de una puerta NOT. Una puerta NOR actúa como una puerta OR seguida de una puerta NOT. Así, la señal de salida de la puerta NAND es 0 cuando y sólo cuando, ambas señales de entrada son 1 y la señal de salida para una puerta NOR es 1 cuando y sólo cuando, ambas señales son 0. Los correspondientes símbolos lógicas de estas puertas son | (para NAND) y ↓ (para NOR) donde | se llama **trazo de Sheffer** (en honor de H. M. Sheffer, 1882-1964) y ↓ se llama una **flecha de Peirce** (en honor de C. S. Peirce, 1839-1914; consulte la página 101). Así

$$P \mid Q \equiv \sim(P \wedge Q) \quad \text{y} \quad P \downarrow Q \equiv \sim(P \vee Q).$$

La tabla que se presenta a continuación resume las acciones de las puertas NAND y NOR.

<table>
<tr><th>Tipo de puerta</th><th>Representación simbólica</th><th>Acción</th></tr>
<tr><td>NAND</td><td> 
</td><td>
<table>
<tr><th colspan="2">Entrada</th><th>Salida</th></tr>
<tr><th>P</th><th>Q</th><th>R = P | Q</th></tr>
<tr><td>1</td><td>1</td><td>0</td></tr>
<tr><td>1</td><td>0</td><td>1</td></tr>
<tr><td>0</td><td>1</td><td>1</td></tr>
<tr><td>0</td><td>0</td><td>1</td></tr>
</table>
</td></tr>
<tr><td>NOR</td><td> 
</td><td>
<table>
<tr><th colspan="2">Entrada</th><th>Salida</th></tr>
<tr><th>P</th><th>Q</th><th>R = P ↓ Q</th></tr>
<tr><td>1</td><td>1</td><td>0</td></tr>
<tr><td>1</td><td>0</td><td>0</td></tr>
<tr><td>0</td><td>1</td><td>0</td></tr>
<tr><td>0</td><td>0</td><td>1</td></tr>
</table>
</td></tr>
</table>

Se puede demostrar que cualquier expresión booleana es equivalente a escribir completamente con trazos de Sheffer o con flechas de Peirce. Por tanto, cualquier circuito lógico digital es equivalente a utilizar sólo las puertas NAND o sólo puertas NOR. El ejemplo 2.4.7 desarrolla parte de la deducción de este resultado, el resto se deja para los ejercicios.

Ejemplo 2.4.7 Reescritura de expresiones usando el trazo de Sheffer

Utilice el teorema 2.1.1 y la definición del trazo de Sheffer para mostrar que

a. $\sim P \equiv P \mid P$ y b. $P \vee Q \equiv (P \mid P) \mid (Q \mid Q)$.

Solución

a $\sim P \equiv \sim(P \wedge P)$ por la ley idempotencia para $\wedge$
$\equiv P \mid P$ por definición, de $\mid$.

b. $P \vee Q \equiv \sim(\sim(P \vee Q))$ por la ley de doble negación
$\equiv \sim(\sim P \wedge \sim Q)$ por las leyes de De Morgan
$\equiv \sim((P \mid P) \wedge (Q \mid Q))$ por el inciso *a*)
$\equiv (P \mid P) \mid (Q \mid Q)$ por la definición de $\mid$. ■

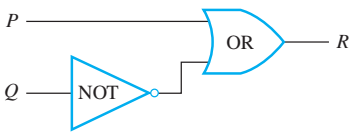
Autoexamen

1. La tabla de entrada/salida para un circuito lógico digital es una tabla que muestra _____.
2. La expresión booleana que corresponde a un circuito lógico digital es _____.
3. Un reconocedor es un circuito de lógico digital que _____.
4. Dos circuitos lógicos digitales son equivalentes si y sólo si, _____.
5. Una puerta NAND se construye mediante la colocación de una puerta _____ inmediatamente después de una puerta _____.
6. Una puerta NOR se construye colocando de una puerta _____ inmediatamente después de una puerta _____.

Conjunto de ejercicios 2.4

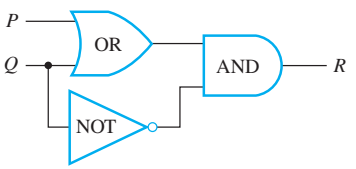
Dé las señales de salida de los circuitos de los ejercicios 1 al 4 como están indicados.

1.



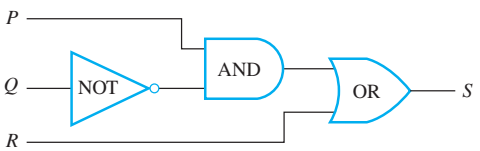
señales de entrada: $P = 1$ y $Q = 1$

2.



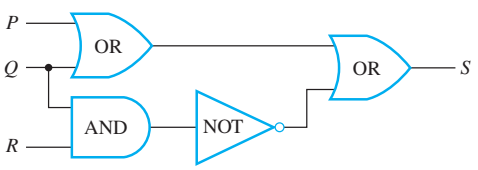
señales de entrada: $P = 1$ y $Q = 0$

3.



señales de entrada: $P = 1$, $Q = 0$, $R = 0$

4.



señales de entrada: $P = 0$, $Q = 0$, $R = 0$

En los ejercicios 5 al 8 escriba la tabla de entrada/salida para el circuito en el ejercicio al que se hace referencia.

5. Ejercicio 1

6. Ejercicio 2

7. Ejercicio 3

8. Ejercicio 4

En los ejercicios 9 al 12 determine la expresión booleana que corresponde al circuito en el ejercicio al que se hace referencia.

9. Ejercicio 1

10. Ejercicio 2

11. Ejercicio 3

12. Ejercicio 4

Construya circuitos para las expresiones booleanas de los ejercicios 13 al 17.

13. $\sim P \vee Q$

14. $\sim(P \vee Q)$

15. $P \vee (\sim P \wedge \sim Q)$

16. $(P \wedge Q) \vee \sim R$

17. $(P \wedge \sim Q) \vee (\sim P \wedge R)$

Para cada una de las tablas de los ejercicios 18 al 21, construya *a*) una expresión booleana que tenga la tabla dada como su tabla de verdad y *b*) un circuito que tenga la tabla dada como su tabla de entrada/salida.

18.

P	*Q*	*R*	*S*
1	1	1	0
1	1	0	1
1	0	1	0
1	0	0	0
0	1	1	1
0	1	0	0
0	0	1	0
0	0	0	0

19.

P	*Q*	*R*	*S*
1	1	1	0
1	1	0	1
1	0	1	0
1	0	0	1
0	1	1	0
0	1	0	1
0	0	1	0
0	0	0	0

20.

P	*Q*	*R*	*S*
1	1	1	1
1	1	0	0
1	0	1	1
1	0	0	0
0	1	1	0
0	1	0	0
0	0	1	0
0	0	0	1

21.

P	*Q*	*R*	*S*
1	1	1	0
1	1	0	1
1	0	1	0
1	0	0	0
0	1	1	1
0	1	0	1
0	0	1	0
0	0	0	0

22. Diseñe un circuito para tener señales de entrada P, Q y R y salida 1 si y sólo si, P y Q tienen el mismo valor y Q y R tienen valores opuestos.

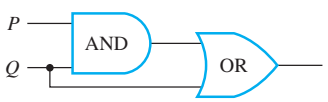
23. Diseñe un circuito para tener señales de entrada P, Q y R y salida 1 si y sólo si, todos las tres P, Q y R tienen el mismo valor.

24. Las luces de un salón de clases están controladas por dos interruptores: uno en la parte trasera y el otro en la parte del frente del salón. Mover cualquiera de los interruptores a la posición opuesta apagará las luces si se encuentran encendidas y las encenderá si están apagadas. Suponga que las luces se han instalado de modo que cuando ambos interruptores están en la posición hacia abajo, las luces están apagadas. Diseñe un circuito para controlar los interruptores.

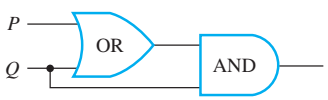
25. Un sistema de alarma tiene tres paneles de control diferentes en tres lugares diferentes. Para habilitar el sistema, los interruptores en al menos dos de los paneles deben estar en la posición de encendido. Si menos de dos están en la posición de encendido, el sistema está desactivado. Diseñe un circuito para controlar los interruptores.

Utilice las propiedades que se presentan en el teorema 2.1.1 para demostrar que cada par de circuitos en los ejercicios 26 a 29 tienen la misma tabla de entrada/salida. (Encuentre las expresiones booleanas para los circuitos y demuestre que son lógicamente equivalentes cuando se les considera como formas de enunciado.)

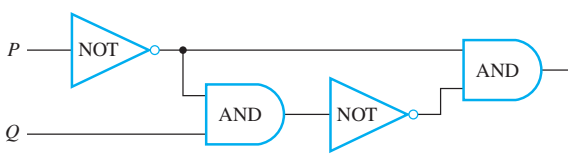
26. a.



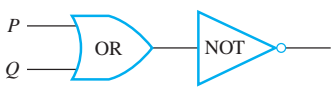
b.



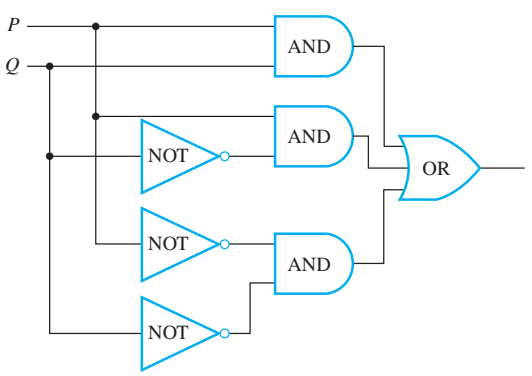
27. a.



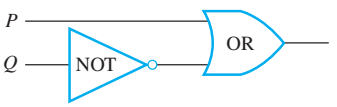
b.



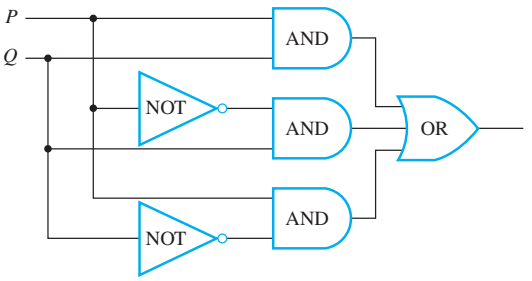
28. a.



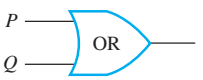
b.



29. a.



b.



Para los circuitos correspondientes a las expresiones booleanas en cada uno de los ejercicios 30 y 31 hay un circuito equivalente con a lo más dos puertas lógicas. Encuentre dicho circuito.

30. $(P \wedge Q) \vee (\sim P \wedge Q) \vee (\sim P \wedge \sim Q)$

31. $(\sim P \wedge \sim Q) \vee (\sim P \wedge Q) \vee (P \wedge \sim Q)$

32. La expresión booleana para el circuito en el ejemplo 2.4.5 es

$$(P \wedge Q \wedge R) \vee (P \wedge \sim Q \wedge R) \vee (P \wedge \sim Q \wedge \sim R)$$

(una forma normal disyuntiva). Determine un circuito con un máximo de tres puertas lógicas que es equivalente a este circuito.

33. a. Demuestre que para el trazo de Sheffer |,

$$P \wedge Q \equiv (P \mid Q) \mid (P \mid Q).$$

b. Utilice los resultados del ejemplo 2.4.7 y el inciso *a*) para escribir $P \wedge (\sim Q \vee R)$ utilizando sólo trazos Sheffer.

34. Demuestre que las equivalencias lógicas siguientes mantienen la flecha de Peirce $\downarrow$, donde $P \downarrow Q \equiv \sim(P \vee Q)$.

a. $\sim P \equiv P \downarrow P$

b. $P \vee Q \equiv (P \downarrow Q) \downarrow (P \downarrow Q)$

c. $P \wedge Q \equiv (P \downarrow P) \downarrow (Q \downarrow Q)$

H **d.** Escriba $P \rightarrow Q$ usando sólo flechas de Peirce.

e. Escriba $P \leftrightarrow Q$, usando sólo flechas de Peirce.

Respuestas del autoexamen

1. La señal(es) de salida que corresponden a todas las combinaciones posibles de las señales de entrada al circuito 2. una expresión booleana que representa las señales de entrada como variables e indica las acciones sucesivas de las puertas lógicas en las señales de entrada 3. tiene salidas a 1 para exactamente una combinación particular de señales de entrada y salidas 0 para todas las otras combinaciones 4. tienen la misma tabla de entrada/salida 5. NOT; AND 6. NOT; OR

2.5 Aplicación: sistemas numéricos y circuitos para suma

Contar en binario es igual que contar en decimal, si tienen todos pulgares. —Glaser y Way

En la escuela primaria, aprendió el significado de la notación decimal: para interpretar una cadena de dígitos decimales como un número, mentalmente multiplique cada dígito por su valor de posición. Por ejemplo, 5049 tiene un 5 en el lugar de los millares, un 0 en el lugar de las centenas, un 4 en el lugar de las decenas y un 9 en el lugar de las unidades. Por tanto

$$5049 = 5 \cdot (1000) + 0 \cdot (100) + 4 \cdot (10) + 9 \cdot (1).$$

Usando la notación exponencial, está ecuación se puede escribir como

$$5049 = 5 \cdot 10^3 + 0 \cdot 10^2 + 4 \cdot 10^1 + 9 \cdot 10^0.$$

De manera más general, la notación decimal se basa en el hecho de que cualquier número entero positivo puede ser escrito de manera única como una suma de productos de la forma

$$d \cdot 10^n,$$

donde cada n es un entero no negativo y cada d es uno de los dígitos decimales de 0, 1, 2, 3, 4, 5, 6, 7, 8, o 9. La palabra *decimal* proviene de la raíz latina *deci*, que significa "diez". La notación decimal (o de base 10) expresa un número como una cadena de dígitos en la que cada dígito indica la posición de la potencia de 10 por la que se multiplica. La posición que está más a la derecha es el lugar de las unidades (o el lugar de 10^0), a la izquierda está el lugar de las decenas (o el lugar 10^1), a la izquierda está el lugar de las centenas (o el lugar 10^2) y así sucesivamente, como se muestra a continuación.

Lugar	10^3 miles	10^2 centenas	10^1 decenas	10^0 unidades
Dígito decimal	5	0	4	9

Representación binaria de números

No hay nada sagrado acerca del número 10, usamos el 10 como base de nuestro sistema de numeración habitual ya que sucede que tenemos diez dedos. De hecho, cualquier número entero mayor de 1 puede servir como base para un sistema de numeración. En ciencia computacional, la **notación de base 2**, o la **notación binaria** es de especial importancia ya que las señales utilizadas en electrónica moderna están siempre en uno de los dos estados. (La raíz latina *bi* significa "dos".)

En la sección 5.4, se demuestra que cualquier número entero se puede representar como una suma única de productos de la forma

$$d \cdot 2^n,$$

donde cada n es un entero y cada d es uno de los dígitos binarios (o bits) 0 o 1. Por ejemplo,

$$27 = 16 + 8 + 2 + 1$$
$$= 1 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0.$$

En notación binaria, como en notación decimal, se escriben sólo los dígitos binarios y no las potencias de la base. En notación binaria, entonces,

$$1 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0$$
$$27_{10} = 11011_2$$

donde los subíndices indican la base, ya sea 10 o 2, en el que está escrito el número. Los lugares en notación binaria corresponden con las distintas potencias de 2. La posición más a la derecha es el lugar de los unos (o lugar 2^0), a la izquierda está el lugar de los dos (o lugar 2^1), a la izquierda está el lugar de los cuatro (o lugar 2^2) y así sucesivamente, como se muestra a continuación.

Lugar	2^4 dieciseises	2^3 ochos	2^2 cuatros	2^1 dos	2^0 unos
Dígito binario	1	1	0	1	1

Al igual que en la notación decimal, se puede agregar o quitar ceros a la izquierda al gusto. Por ejemplo,

$$003_{10} = 3_{10} = 1 \cdot 2^1 + 1 \cdot 2^0 = 11_2 = 011_2.$$

Ejemplo 2.5.1 Notación binaria de números enteros del 1 al 9

Deduzca la notación binaria de los enteros de 1 a 9.

Solución

$$\begin{aligned}
1_{10} &= 1 \cdot 2^0 = 1_2 \\
2_{10} &= 1 \cdot 2^1 + 0 \cdot 2^0 = 10_2 \\
3_{10} &= 1 \cdot 2^1 + 1 \cdot 2^0 = 11_2 \\
4_{10} &= 1 \cdot 2^2 + 0 \cdot 2^1 + 0 \cdot 2^0 = 100_2 \\
5_{10} &= 1 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 = 101_2 \\
6_{10} &= 1 \cdot 2^2 + 1 \cdot 2^1 + 0 \cdot 2^0 = 110_2 \\
7_{10} &= 1 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 111_2 \\
8_{10} &= 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 0 \cdot 2^0 = 1000_2 \\
9_{10} &= 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2^1 + 1 \cdot 2^0 = 1001_2
\end{aligned}$$

■

Una lista de potencias de 2 es útil para hacer conversiones de binario a decimal y de decimal a binario. Vea la tabla 2.5.1.

Tabla 2.5.1 Potencias de 2

Potencias de 2	2^{10}	2^9	2^8	2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
Forma decimal	1024	512	256	128	64	32	16	8	4	2	1

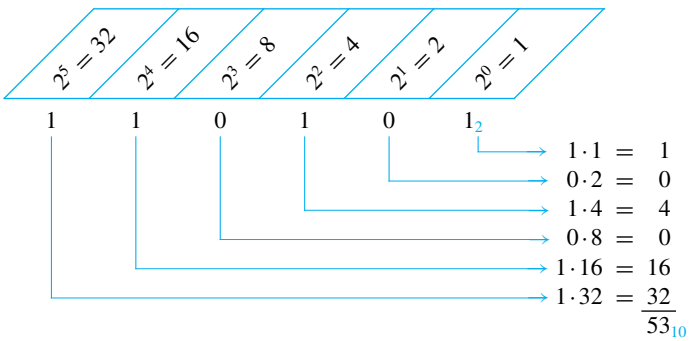
Ejemplo 2.5.2 Conversión de un binario a un número decimal

Represente 110101_2 en notación decimal.

Solución

$$\begin{aligned} 110101_2 &= 1\cdot 2^5 + 1\cdot 2^4 + 0\cdot 2^3 + 1\cdot 2^2 + 0\cdot 2^1 + 1\cdot 2^0 \\ &= 32 + 16 + 4 + 1 \\ &= 53_{10} \end{aligned}$$

Por otra parte, se puede utilizar el esquema que se muestra a continuación.



■

Ejemplo 2.5.3 Conversión de un decimal a un número binario

Represente 209 en notación binaria.

Solución Use la tabla 2.5.1 para escribir 209 como suma de potencias de 2, iniciando con la mayor potencia de 2 que es menor que 209 y continúe reduciendo a potencias menores.

Puesto que 209 está entre 128 y 256, la mayor potencia de 2 que es menor de 209 es 128. Por lo que

$$209_{10} = 128 + \text{un número menor.}$$

Ahora $209 - 128 = 81$ y 81 está entre 64 y 128, por lo que la mayor potencia de 2 que es menor que 81 es 64. Por tanto

$$209_{10} = 128 + 64 + \text{un número menor.}$$

Continuando de esta manera, se obtiene

$$\begin{aligned} 209_{10} &= 128 + 64 + 16 + 1 \\ &= 1\cdot 2^7 + 1\cdot 2^6 + 0\cdot 2^5 + 1\cdot 2^4 + 0\cdot 2^3 + 0\cdot 2^2 + 0\cdot 2^1 + 1\cdot 2^0. \end{aligned}$$

Para cada potencia de 2 que se presenta en la suma, hay un 1 en la posición correspondiente del número binario. Para cada potencia de 2 que falta de la suma, hay un 0 en la posición correspondiente del número binario. Por tanto

$$209_{10} = 11010001_2$$ ■

En la sección 5.1 se analiza otro procedimiento para convertir de decimal a notación binaria.

¡Precaución! No se lee 10_2 como "diez"; este es el número dos. Lea 10_2 como "uno cero base dos".

Suma y resta binaria

Los métodos de cálculo de aritmética binaria son análogos a los de aritmética decimal. En aritmética binaria el número 2 ($= 10_2$ en notación binaria) desempeña un papel similar al del número 10 en aritmética decimal.

Ejemplo 2.5.4 Suma en notación binaria

Sume 1101_2 y 111_2 usando notación binaria.

Solución Ya que $2_{10} = 10_2$ y $1_{10} = 1_2$, la traducción de $1_{10} + 1_{10} = 2_{10}$ en notación binaria es

$$\begin{array}{r} 1_2 \\ +\ 1_2 \\ \hline 10_2 \end{array}$$

De lo que se deduce que la suma de dos 1 juntos, da como resultado llevar un 1 cuando se usa la notación binaria. Sumar tres 1 juntos, también da como resultado en llevar un 1 ya que $3_{10} = 11_2$ ("uno uno base dos").

$$\begin{array}{r} 1_2 \\ +\ 1_2 \\ +\ 1_2 \\ \hline 11_2 \end{array}$$

Así, la suma se puede realizar de la siguiente manera:

$$\begin{array}{rcccc} & 1 & 1 & 1 & \leftarrow \text{renglón de lo que se lleva} \\ & 1 & 1 & 0 & 1_2 \\ + & & 1 & 1 & 1_2 \\ \hline 1 & 0 & 1 & 0 & 0_2 \end{array}$$

■

Ejemplo 2.5.5 Resta en notación binaria

Reste 1011_2 de 11000_2 usando notación binaria.

Solución En la resta decimal el hecho de que $10_{10} - 1_{10} = 9_{10}$ se usa para prestar a través de varias columnas. Por ejemplo, considere lo siguiente:

$$\begin{array}{rcccc} & 9 & 9 & & \\ & \not{1} & 1 & & \leftarrow \text{renglón de préstamos} \\ & \not{1}0 & 0 & 0 & 0_{10} \\ - & & 5 & 8_{10} & \\ \hline & 9 & 4 & 2_{10} & \end{array}$$

En la resta binaria, también puede ser necesario pedir prestado a través de más de una columna. Pero cuando usted pide prestado un 1_2 de 10_2, lo que queda es 1_2.

$$\begin{array}{r} 10_2 \\ -\ 1_2 \\ \hline 1_2 \end{array}$$

Así, la resta se puede realizar de la siguiente manera:

$$\begin{array}{rcccc} & 0 & 1 & 1 & \\ & \not{1} & \not{1} & 1 & \leftarrow \text{renglón de préstamos} \\ 1 & \not{1} & 0 & 0 & 0_2 \\ - & & 1 & 0 & 1_2 \\ \hline & & 1 & 1 & 0_2 \end{array}$$

■

Circuitos para el cálculo de sumas

Considere el tema de diseñar un circuito para generar la suma de dos dígitos binarios P y Q. Tanto P como Q puede ser ya sea 0 o 1. Y se conocen los siguientes hechos:

$$1_2 + 1_2 = 10_2,$$
$$1_2 + 0_2 = 1_2 = 01_2,$$
$$0_2 + 1_2 = 1_2 = 01_2,$$
$$0_2 + 0_2 = 0_2 = 00_2.$$

De lo que se deduce que el circuito a diseñar debe tener dos salidas —una para el dígito binario de la izquierda (este se llama **lo que se lleva**) y uno para el dígito binario de la derecha (este se llama **la suma**). La salida de lo que se lleva es 1 si P y Q son 1; es 0 de otra manera. Así, lo que se lleva se puede producir usando el circuito de puerta AND que corresponde a la expresión booleana $P \wedge Q$. La salida de la suma es 1 si ya sea P o Q, pero no ambas, es 1. La suma puede, por tanto, producirse usando un circuito que corresponde a la expresión booleana para *o exclusivo*: $(P \vee Q) \wedge \sim(P \wedge Q)$. (Vea el ejemplo 2.4.3*a*).) Por tanto, un circuito para sumar dos dígitos binarios P y Q se puede construir como se muestra en la figura 2.5.1. Este circuito se llama **semisumador**.

SEMISUMADOR

Circuito

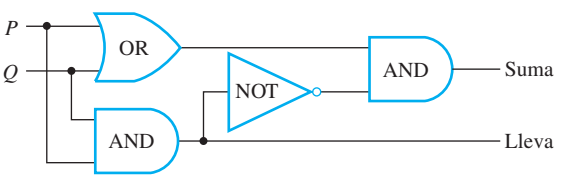


Tabla de entrada/salida

P	Q	Lleva	Suma
1	1	1	0
1	0	0	1
0	1	0	1
0	0	0	0

Figura 2.5.1 **Circuito para sumar $P + Q$, donde P y Q son dígitos binarios**

Ahora consideremos el problema de cómo construir un circuito para sumar dos números enteros binarios, cada uno con más de un dígito. Ya que la adición de dos dígitos binarios puede dar como resultado llevar a la siguiente columna a la izquierda, puede ser necesario añadir tres binarios en ciertos puntos. En el ejemplo siguiente, la suma en la columna de la derecha es la suma de dos dígitos binarios, y, debido a lo que se lleva, la suma en la columna de la izquierda es la suma de los tres dígitos binarios.

$$\begin{array}{rrr} & 1 & \leftarrow \text{renglón de lo que se lleva} \\ & 1 & 1_2 \\ + & 1 & 1_2 \\ \hline 1 & 1 & 0_2 \end{array}$$

Así, con el fin de construir un circuito que sume varios números dígitos binarios, es necesario incorporar un circuito que calcule la suma de tres dígitos binarios. Tal circuito se llama un **sumador completo**. Considere una suma general de tres dígitos binarios P, Q y R que da como resultado en llevar C (o el dígito en el extremo izquierdo) y una suma S (el dígito en el extremo derecho).

$$\begin{array}{rr} & P \\ + & Q \\ + & R \\ \hline & CS \end{array}$$

El funcionamiento del sumador completo se basa en el hecho de que la suma es una operación binaria: Sólo se pueden agregar dos números a la vez. Por tanto P es el primero agregado a Q y después el resultado se suma a R. Por ejemplo, considere la siguiente suma:

$$\left.\begin{array}{r} 1_2 \\ +\ 0_2 \end{array}\right\} 1_2 + 0_2 = 01_2 \qquad \left.\begin{array}{r} 01_2 \\ +\ 1_2 \\ \hline 10_2 \end{array}\right\} 1_2 + 1_2 = 10_2$$

El proceso que se muestra aquí se puede dividir en pasos que utilizan circuitos de semisumador.

Paso 1: Sume P y Q utilizando un semisumador para obtener un número binario de dos dígitos.

$$\begin{array}{r} P \\ +\ Q \\ \hline C_1 S_1 \end{array}$$

Paso 2: Sume R a la suma C_1S_1 de P y Q.

$$\begin{array}{r} C_1 S_1 \\ +\ R \\ \hline \end{array}$$

Para esto, proceda como se muestra a continuación:

Paso 2a: Sume R a S_1 utilizando un semisumador para obtener el número de dos dígitos C_2S.

$$\begin{array}{r} S_1 \\ +\ R \\ \hline C_2 S \end{array}$$

Entonces S es el dígito del extremo derecho de la suma total de P, Q y R.

Paso 2b: Determine el dígito del extremo izquierdo, C, de la suma total de la siguiente manera: En primer lugar observe que es imposible que tanto C_1 como C_2 sean 1. Si $C_1 = 1$, entonces P y Q son 1 y así $S_1 = 0$. En consecuencia, la suma de S_1 y R da un número binario C_2S_1 donde $C_2 = 0$. Después observamos que C será un 1 en el caso de que la suma de P y Q da como resultado llevar un 1 o en el caso de que la suma de S_1 (el dígito del extremo derecho de $P + Q$) y R da como resultado llevar 1. En otras palabras, $C = 1$ si y sólo si, $C_1 = 1$ o $C_2 = 1$. De lo que se deduce que el circuito que se muestra en la figura 2.5.2 calculará la suma de tres dígitos binarios.

SEMISUMADOR

Circuito

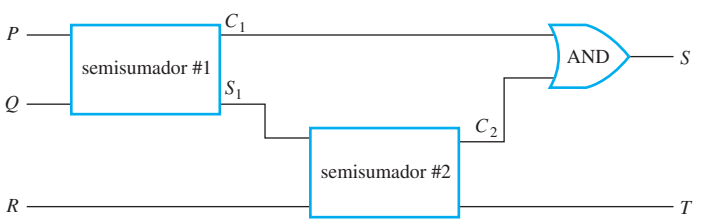


Tabla de entrada/salida

P	*Q*	*R*	*C*	*S*
1	1	1	1	1
1	1	0	1	0
1	0	1	1	0
1	0	0	0	1
0	1	1	1	0
0	1	0	0	1
0	0	1	0	1
0	0	0	0	0

Figura 2.5.2 Circuito para sumar $P + Q + R$, donde P, Q y R son dígitos binarios

Dos sumadores completos y un semisumador se pueden utilizar juntos para construir un circuito que va a sumar dos números binarios de tres dígitos *PQR* y *STU* para obtener la suma *W X Y Z*. Esto se muestra en la figura 2.5.3. Tal circuito se llama un **sumador en paralelo**. Los sumadores en paralelo pueden construirse para sumar números binarios de cualquier longitud finita.

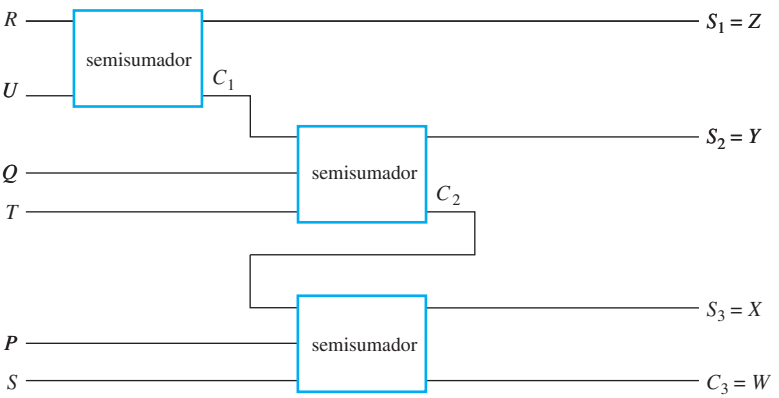


Figura 2.5.3 Un sumador en paralelo para sumar *PQR* y *STU* para obtener *W X Y Z*

Complementos de dos y la representación en computadora de enteros negativos

En general, se utiliza un número fijo de bits para representar números enteros en una computadora y estos son necesarios para representar números enteros negativos y no negativos. A veces un bit particular, normalmente el del extremo izquierdo, se utiliza como un indicador de señal y los bits restantes se toman como el valor absoluto del número en notación binaria. El problema con este enfoque es que los procedimientos para la suma de los números resultantes son un poco complicados y la representación del 0 no es única. Un método más común, usando *complementos de dos* permite sumar enteros con bastante facilidad y da como resultado una representación única del 0. Los complementos de dos de un entero con respecto a una longitud de bits fija se definen como sigue:

• Definición

Dado un número entero positivo a, los **complementos de dos de *a* respecto de una longitud de bits fija** n es la representación binaria de n bits de

$$2^n - a.$$

Longitudes de bits de 16 y 32 son las más comúnmente utilizadas en la práctica. Sin embargo, ya que los principios son los mismos para todas las longitudes de bits, utilizamos una longitud de 8 bits por simplicidad en este análisis. Por ejemplo, ya que

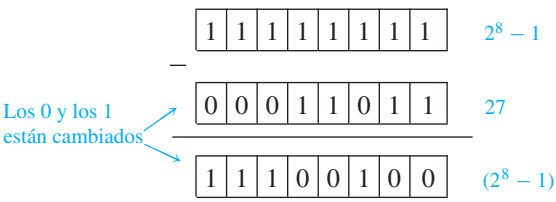
$$(2^8 - 27)_{10} = (256 - 27)_{10} = 229_{10} = (128 + 64 + 32 + 4 + 1)_{10} = 11100101_2,$$

el complemento de dos de 8 bits de 27 es 11100101_2.

Resulta que hay una manera conveniente para calcular complementos de dos que implican menos aritmética que la aplicación directa de la definición. Para una representación de 8 bits se basa en tres hechos:

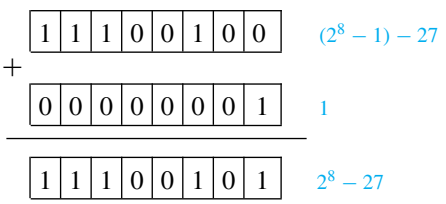
1. $2^8 - a = [(2^8 - 1) - a] + 1$.
2. La representación binaria de $2^8 - 1$ es 11111111_2.
3. Restar un número binario de 8 bits a de 11111111_2 sólo cambia todos los 0 en a a 1 y todos los 1 a 0. (El número resultante se llama el **complemento de uno** del número dado.)

Por ejemplo, por 2) y 3), con $a = 27$



2.5.1

y así, en notación binaria de la diferencia $(2^8 - 1) - 27$ es 11100100_2. Pero por 1) con $a = 27$, $2^8 - 27 = [(2^8 - 1) - 27] + 1$ y por lo que si sumamos 1 a (2.5.1), se obtiene la representación binaria de 8 bits, de $2^8 - 27$, que es el complemento de dos de 8 bits de 27:



En general,

Para encontrar el complemento de dos de 8 bits de un entero positivo a es a lo más igual a 255:

- Escriba la representación binaria de 8 bits para a.
- Mueva los bits (es decir, cambie todos los 1 por 0 y todos los 0 por 1).
- Sume 1 en notación binaria.

Ejemplo 2.5.6 Determinación de un complemento de dos

Encuentre el complemento de dos de 8 bits de 19.

Solución Escriba la representación binaria de 8 bits para el 19, cambie todas los 0 por 1 y todos los 1 por 0 y sume 1.

$$19_{10} = (16 + 2 + 1)_{10} = 00010011_2 \xrightarrow{\text{voltee los bits}} 11101100 \xrightarrow{\text{sume 1}} 11101101$$

Para comprobar este resultado, observe que

$$11101101_2 = (128 + 64 + 32 + 8 + 4 + 1)_{10} = 237_{10} = (256 - 19)_{10} = (2^8 - 19)_{10},$$

que *es* el complemento de 19. ■

Observe que, ya que

$$2^8 - (2^8 - a) = a$$

el *complemento de dos del complemento de dos de un número es el número mismo* y por tanto,

> Para determinar la representación decimal del número entero con un complemento dado de dos de 8 bits:
>
> - Encuentre el complemento de dos del complemento de dos dado.
> - Escriba el equivalente decimal del resultado.

Ejemplo 2.5.7 Determinación de un número con un complemento de dos dado

¿Cuál es la representación decimal del número entero con el complemento de dos 10101001?

Solución

$$10101001_2 \xrightarrow{\text{voltee los bits}} 01010110$$
$$\xrightarrow{\text{sume 1}} 01010111_2 = (64 + 16 + 4 + 2 + 1)_{10} = 87_{10}$$

Para comprobar este resultado, observe que el número dado es

$$10101001_2 = (128 + 32 + 8 + 1)_{10} = 169_{10} = (256 - 87)_{10} = (2^8 - 87)_{10},$$

que es el complemento de dos de 87. ■

Representación 8 bits de un número

Ahora considere el complemento de dos de un entero n que satisface la desigualdad $1 \leq n \leq 128$. Entonces,

$$-1 \geq -n \geq -128$$

ya que la multiplicación por -1 invierte la dirección de la desigualdad

y

$$2^8 - 1 \geq 2^8 - n \geq 2^8 - 128$$

sumando 2^8 en todas las partes de la desigualdad.

Pero $2^8 - 128 = 256 - 128 = 128 = 2^7$. Por tanto

$$2^7 \leq \text{complemento de dos de } n < 2^8.$$

De lo que se deduce que el complemento de dos de 8 bits de un número entero de 1 a 128 bits tiene un bit principal de 1. Observe también que la representación ordinaria de 8 bits de un entero de 0 a 127 tiene un bit principal de 0. En consecuencia, se pueden usar ocho bits para representar los números enteros no negativos y negativos, representando cada número entero no negativo hasta 127 usando la notación ordinaria binaria de 8 bits y representando cada número entero negativo entre -1 y -128 como el complemento de dos de su valor absoluto. Es decir, para cualquier entero a de -128 a 127,

> La representación de 8 bits de a
>
> $$= \begin{cases} \text{representación binaria de 8 bits de } a & \text{si } a \geq 0 \\ \text{representación binaria de 8 bits de } 2^8 - |a| & \text{si } a < 0 \end{cases}.$$

En la tabla 2.5.2 se muestran las representaciones.

Tabla 2.5.2

Entero	Representación de 8 bits (ordinaria 8 bits notación binaria si es no negativo o 8 bits complemento de dos del valor absoluto si es negativo)	Forma decimal del complemento de dos para enteros negativos
127	01111111	
126	01111110	
⋮	⋮	
2	00000010	
1	00000001	
0	00000000	
−1	11111111	$2^8 - 1$
−2	11111110	$2^8 - 2$
−3	11111101	$2^8 - 3$
⋮	⋮	⋮
−127	10000001	$2^8 - 127$
−128	10000000	$2^8 - 128$

Suma en computadora con enteros negativos

A continuación se presenta un ejemplo de cómo complemento de dos permiten sumar circuitos para realizar la resta. Suponga que queremos calcular 72 − 54. Primero observe que esto es lo mismo que 72 + (−54) y que las representaciones binarias de 8 bits de 72 y −54 son 01001000 y 11001010, respectivamente. Así si se suma las representaciones binarias de 8 bits para los dos números, se obtiene

$$\begin{array}{rcccccccc} & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ + & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ \hline 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \end{array}$$

Y si trunca el 1 principal, se obtiene 00010010. Esta es la representación binaria de 8 bits de 18, que ¡es la respuesta correcta!

La descripción que se muestra a continuación explica cómo utilizar este método para sumar cualquiera de dos números enteros entre −128 y 127. Es fácil generalizar para aplicar las representaciones de 16 bits y 32 bits para obtener la suma de enteros entre −2 000 000 000 y 2 000 000 000.

Para sumar dos números enteros en el rango de −128 a 127 cuya suma está también en el rango de −128 a 127:

- Convierta los dos números enteros a sus representaciones de 8 bits (que representan los números enteros negativos usando los complementos de dos de sus valores absolutos).
- Sume los enteros resultantes usando suma binaria ordinaria.
- Trunque cualquier 1 principal (desbordamiento) que se presente en la posición 2^8ava.
- Convierta el resultado de nuevo a la forma decimal (interpretando los números enteros de 8 bits con un 0 principal como no negativo y enteros de 8 bits con 1 principales como negativo).

Para ver por qué este resultado es verdadero, considere cuatro casos: 1) ambos enteros son no negativos 2) un entero es no negativo y el otro entero es negativo y el valor absoluto del entero no negativo es menor que el del negativo, 3) un entero es no negativo y el otro es negativo y el valor absoluto del entero negativo es menor o igual que el del no negativo y 4) ambos enteros son negativos.

Caso 1 (ambos son enteros no negativos): Este caso es fácil porque si dos números enteros de 0 a 127 se escriben en sus representaciones de 8 bits y si su suma también está en el rango de 0 a 127, entonces, la representación de los 8 bits de su suma tiene un 0 principal y es por tanto interpretado correctamente como un entero no negativo. El siguiente ejemplo muestra lo que sucede cuando se suman 38 y 69.

$$\begin{array}{rcl} & \boxed{0}\boxed{0}\boxed{1}\boxed{0}\boxed{0}\boxed{1}\boxed{1}\boxed{0} & 38 \\ + & & \\ & \boxed{0}\boxed{1}\boxed{0}\boxed{0}\boxed{0}\boxed{1}\boxed{0}\boxed{1} & 69 \\ \hline & \boxed{0}\boxed{1}\boxed{1}\boxed{0}\boxed{1}\boxed{0}\boxed{1}\boxed{1} & 107 \end{array}$$

Los casos 2) y 3), ambos implican la suma de un entero negativo y de un no negativo. Para ser concretos, sea a el entero no negativo y sea $-b$ el entero negativo y supongamos que tanto a como $-b$ están en el rango de -128 a 127. La observación crucial es que la suma de las representaciones de 8 bits de a y $-b$ es equivalente a calcular

$$a + (2^8 - b)$$

ya que la representación de 8 bits de $-b$ es la representación binaria de $2^8 - b$.

Caso 2 (a es negativa y $-b$ es negativo y $|a| < |b|$): En este caso, observe que a $= |a| <$ $|b| =$ b y

$$a + (2^8 - b) = 2^8 - (b - a),$$

y la representación binaria de este número es la representación de los 8 bits $-(b - a) =$ $a + (-b)$. Debemos tener cuidado en comprobar que $2^8 - (b - a)$ está entre 2^7 y 2^8. Pero esto es porque

$$2^7 = 2^8 - 2^7 \leq 2^8 - (b - a) < 2^8 \qquad \text{ya que } 0 < b - a \leq b \leq 128 = 2^7.$$

Por tanto en caso de que $|a| < |b|$, sumando las representaciones de 8 bits de a y de $-b$ se obtiene la representación de 8 bits de $a + (-b)$.

Ejemplo 2.5.8 Cálculo de $a + (-b)$ donde $0 \leq a < b \leq 128$

Utilice las representaciones de 8 bits para calcular $39 + (-89)$.

Solución

Paso 1: Cambie a decimal las representaciones de 8 bits utilizando el complemento de dos para representar a -89.

Ya que $39_{10} = (32 + 4 + 2 + 1)_{10} = 100111_2$, la representación de 8 bits de 39 es 00100111. Ahora la representación de 8 bits de -89 es el complemento de dos de 89. Este se obtiene de la siguiente manera:

$$89_{10} = (64 + 16 + 8 + 1)_{10} = 01011001_2 \xrightarrow{\text{voltee los bits}}$$

$$10100110 \xrightarrow{\text{sume 1}} 10100111$$

Así la representación de 8 bits de −89 es 10100111.

Paso 2: Sume las representaciones de 8 bits en notación binaria y trunque el uno en la posición 2^8ava si es que existe:

$$\begin{array}{r} \boxed{0}\boxed{0}\boxed{1}\boxed{0}\boxed{0}\boxed{1}\boxed{1}\boxed{1} \\ + \\ \boxed{1}\boxed{0}\boxed{1}\boxed{0}\boxed{0}\boxed{1}\boxed{1}\boxed{1} \\ \hline \boxed{1}\boxed{1}\boxed{0}\boxed{0}\boxed{1}\boxed{1}\boxed{1}\boxed{0} \end{array}$$

No hay un 1 en la 2^8ava posición para truncarlo. →

Paso 3: Encuentre el equivalente decimal del resultado. Ya que su bit principal es 1, este número es la representación de 8 bits de un entero negativo.

$$11001110 \xrightarrow{\text{voltee los bits}} 00110001 \xrightarrow{\text{sume 1}} 00110010$$
$$\leftrightarrow -(32 + 16 + 2)_{10} = -50_{10}$$

Observe que puesto que $39 - 89 = -50$, este procedimiento da la respuesta correcta. ■

Caso 3 (a es no negativo y −b es negativo y |b| ≤ |a|): En este caso, observamos que $b = |b| \leq |a| = a$ y

$$a + (2^8 - b) = 2^8 + (a - b).$$

También

$$2^8 \leq 2^8 + (a - b) < 2^8 + 2^7 \qquad \text{ya que } 0 \leq a - b \leq a < 128 = 2^7.$$

Así la representación binaria de $a + (2^8 - b) = 2^8 + (a - b)$ tiene un 1 principal en la novena (2^8ava) posición. Este 1 principal conduce con frecuencia a lo que se llama un "desbordamiento", ya que no caben en el formato entero de 8 bits. Ahora, restando 2^8 de $2^8 + (a - b)$ es equivalente a truncar el 1 principal en la posición 2^8ava de la representación binaria del número. Sin embargo,

$$[a + (2^8 - b)] - 2^8 = 2^8 + (a - b) - 2^8 = a - b = a + (-b).$$

Por tanto en caso de que $|a| \geq |b|$, agregando las representaciones de 8 bits de a y $-b$ y truncando el 1 principal (que está seguro de que está presente) se obtiene la representación de 8 bits de $a + (-b)$.

Ejemplo 2.5.9 Cálculo de $a + (-b)$ donde $1 \leq b \leq a \leq 127$

Utilice las representaciones de 8 bits para calcular $39 + (-25)$.

Solución

Paso 1: Cambio de decimal a las representaciones de 8 bits utilizando el complemento de dos para representar a −25.

Como en el ejemplo 2.5.8, la representación de 8 bits de 39 es 00100111. Ahora la representación de 8 bits de −25 es el complemento de dos de 25, que se obtiene de la siguiente manera:

$$25_{10} = (16 + 8 + 1)_{10} = 00011001_2 \xrightarrow{\text{voltee los bits}}$$
$$11100110 \xrightarrow{\text{sume 1}} 11100111$$

Así que la representación de 8 bits de −25 es 11100111.

Paso 2: Sume las representaciones de 8 bits en notación binaria y trunque el 1 en la 2^8ava posición si es que existe:

$$\begin{array}{rr} & \boxed{0}\boxed{0}\boxed{1}\boxed{0}\boxed{0}\boxed{1}\boxed{1}\boxed{1} \\ + & \\ & \boxed{1}\boxed{1}\boxed{1}\boxed{0}\boxed{0}\boxed{1}\boxed{1}\boxed{1} \\ \hline \text{Trunque} \rightarrow & 1\ \boxed{0}\boxed{0}\boxed{0}\boxed{0}\boxed{1}\boxed{1}\boxed{1}\boxed{0} \end{array}$$

Paso 3: Encuentre el equivalente decimal del resultado:

$$00001110_2 = (8 + 4 + 2)_{10} = 14_{10}.$$

Ya que $39 - 25 = 14$, esta es la respuesta correcta. ■

Caso 4 (ambos enteros son negativos): Este caso implica la suma de dos números enteros negativos en el rango de -1 a -128 cuya suma también está en este rango. Para especificar, considere la suma $(-a) + (-b)$ donde a, b y ab están todas en el rango de 1 a 128. En este caso las representaciones de 8 bits de $-a$ y $-b$ son las representaciones de 8 bits, de $2^8 - a$ y $2^8 - b$. Así si las representaciones de 8 bits de $-a$ y $-b$ se suman, el resultado es

$$(2^8 - a) + (2^8 - b) = [2^8 - (a + b)] + 2^8.$$

Recordemos que truncar un 1 principal en la novena (2^8ava) posición de un número binario es al restar 2^8. Así que cuando se trunca el 1 principal de la representación de 8 bits de $(2^8 - a) + (2^8 - b)$, el resultado es $2^8 - (a + b)$, que es la representación de 8 bits de $-(a + b) = (-a) + (-b)$. (En el ejercicio 37 se le pide que muestre que la suma $(2^8 - a) + (2^8 - b)$ *tiene* un 1 principal en la novena (2^8ava) posición.)

Ejemplo 2.5.10 Cálculo de $(-a) + (-b)$ donde $1 \leq a, b \leq 128$ y $1 \leq a + b \leq 128$

Utilice las representaciones de 8 bits para calcular $(-89) + (-25)$.

Solución

Paso 1: Cambio de decimal a las representaciones de 8 bits usando los complementos de dos para representar a -89 y -25.

Las representaciones de 8 bits de -89 y -25 se mostraron en los ejemplos 2.5.8 y 2.5.9 de 10100111 y 11100111, respectivamente.

Paso 2: Sume las representaciones de 8 bits en notación binaria y trunque el 1 en la 2^8ava posición si es que existe:

$$\begin{array}{rr} & \boxed{1}\boxed{0}\boxed{1}\boxed{0}\boxed{0}\boxed{1}\boxed{1}\boxed{1} \\ + & \\ & \boxed{1}\boxed{1}\boxed{1}\boxed{0}\boxed{0}\boxed{1}\boxed{1}\boxed{1} \\ \hline \text{Trunque} \rightarrow & 1\ \boxed{1}\boxed{0}\boxed{0}\boxed{0}\boxed{1}\boxed{1}\boxed{1}\boxed{0} \end{array}$$

Paso 3: Encuentre el equivalente decimal del resultado. Debido a que su bit principal es 1, este número es la representación de 8 bits de un entero negativo.

$$10001110 \xrightarrow{\text{voltee los bits}} 01110001 \xrightarrow{\text{sume 1}} 01110010_2$$
$$\leftrightarrow -(64 + 32 + 16 + 2)_{10} = -114_{10}$$

Ya que $(-89) + (-25) = -114$, esta es la respuesta correcta. ■

Notación hexadecimal

Ahora debería ser obvio que los números escritos en notación binaria ocupan mucho más espacio que los números escritos en notación decimal. Sin embargo, muchos aspectos del funcionamiento de la computadora pueden ser mejor analizados usando números binarios. La **notación hexadecimal** es mucho más compacta que la notación decimal y es mucho más fácil para convertir de ida y vuelta entre la notación hexadecimal y binaria que entre la notación binaria y la decimal. El palabra *hexadecimal* proviene del griego *hex-* que significa "seis" y la raíz latina *deci-*, que significa "diez". Por tanto hexadecimal se refiere a "dieciséis" y la notación hexadecimal también se llama **notación de base 16**. La notación hexadecimal se basa en el hecho de que cualquier número entero se puede expresar de manera única como una suma de números de la forma

$$d \cdot 16^n,$$

donde cada n es un entero no negativo y cada d es uno de los números enteros de 0 a 15. Con el fin de evitar ambigüedad, cada dígito hexadecimal se debe representar por un solo símbolo. Los enteros del 10 al 15 están representados por los símbolos A, B, C, D, E y F. En la tabla 2.5.3, se muestran los dieciséis dígitos hexadecimales, junto con sus equivalentes decimales y, para futura referencia, sus 4 bits equivalentes binarios.

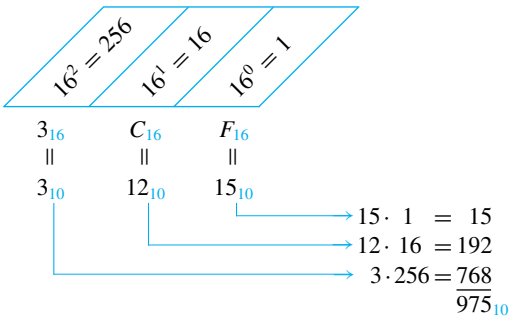
Tabla 2.5.3

Decimal	Hexadecimal	4-bit binario equivalente
0	0	0000
1	1	0001
2	2	0010
3	3	0011
4	4	0100
5	5	0101
6	6	0110
7	7	0111
8	8	1000
9	9	1001
10	A	1010
11	B	1011
12	C	1100
13	D	1101
14	E	1110
15	F	1111

Ejemplo 2.5.11 Convirtiendo de notación hexadecimal a decimal

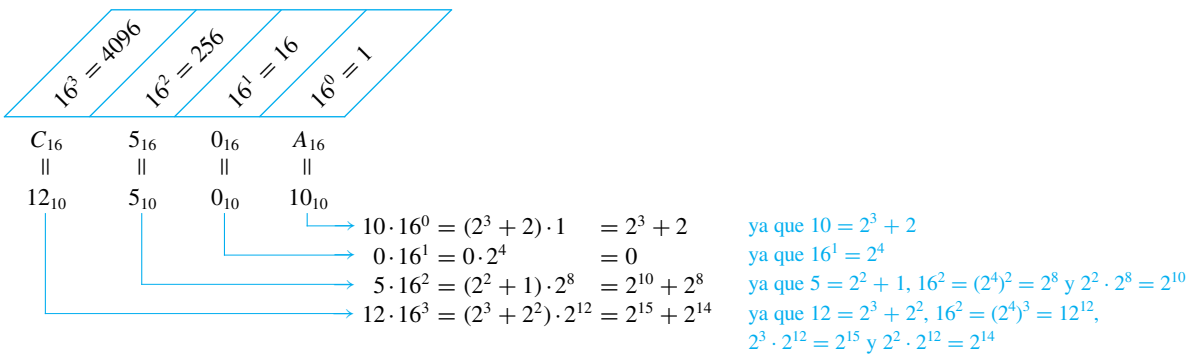
Convierta $3CF_{16}$ a la notación decimal.

Solución Aquí se puede utilizar un esquema similar al introducido en el ejemplo 2.5.2.



Así $3CF_{16} = 975_{10}$. ■

Ahora considere como convertir de la notación hexadecimal a la notación binaria. En el ejemplo que se muestra a continuación los números se reescriben usando potencias de 2 y se aplican las leyes de los exponentes. El resultado sugiere un procedimiento general.



Pero

$$(2^{15} + 2^{14}) + (2^{10} + 2^8) + 0 + (2^3 + 2)$$
$$= 1100\ 0000\ 0000\ 0000_2 + 0101\ 0000\ 0000_2 + 0000\ 0000_2 + 1010_2$$

por las reglas de escritura de los números binarios.

Por lo que

$$C50A_{16} = \underbrace{1100}_{C_{16}}\ \underbrace{0101}_{5_{16}}\ \underbrace{0000}_{0_{16}}\ \underbrace{1010_2}_{A_{16}}$$

por las reglas de la suma de números binarios.

El procedimiento que se muestra en este ejemplo se puede generalizar. De hecho, la siguiente secuencia de pasos, siempre dará la respuesta correcta:

Para convertir un entero de la notación hexadecimal a la binaria:

- Escriba cada digito hexadecimal del entero a la notación binaria de 4 bits.
- Yuxtaponga los resultados.

Ejemplo 2.5.12 Conversión de notación hexadecimal a binaria

Convierta $B09F_{16}$ a notación binaria.

Solución $B_{16} = 11_{10} = 1011_2$, $0_{16} = 0_{10} = 0000_2$, $9_{16} = 9_{10} = 1001_2$ y $F_{16} = 15_{10} = 1111_2$. En consecuencia,

$$\begin{array}{cccc} \text{B} & \text{0} & \text{9} & \text{F} \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow \\ 1011 & 0000 & 1001 & 1111 \end{array}$$

y la respuesta es 1011000010011111_2. ■

Para convertir números enteros escritos en notación binaria a notación hexadecimal, invierta los pasos del procedimiento anterior.

> Para convertir un número entero de notación binaria a hexadecimal:
>
> - Agrupe los dígitos del número binario en conjuntos de cuatro, empezando por la derecha y agregando ceros principales según sea necesario.
> - Convierta los números binarios en cada conjunto de cuatro de dígitos hexadecimales. Yuxtaponga los dígitos hexadecimales.

Ejemplo 2.5.13 Conversión de notación binaria a hexadecimal

Convierta 100110110101001_2 a la notación hexadecimal.

Solución Primero agrupe los dígitos binarios en grupos de cuatro, trabajando de derecha a izquierda y agregando 0 principales si es necesario.

$$0100 \quad 1101 \quad 1010 \quad 1001.$$

Convierta cada grupo de cuatro dígitos binarios en un dígito hexadecimal.

$$\begin{array}{cccc} 0100 & 1101 & 1010 & 1001 \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow \\ 4 & \text{D} & \text{A} & 9 \end{array}$$

Después yuxtaponga los dígitos hexadecimales.

$$4\text{DA}9_{16}$$ ■

Ejemplo 2.5.14 Lectura de un volcado de memoria

La unidad más pequeña de memoria direccionable en la mayoría de las computadoras es un byte, u ocho bits. En algunas operaciones de depuración de un volcado es de contenido de la memoria, es decir, se muestra o se imprime en orden el contenido de cada posición de memoria. Para ahorrar espacio y hacer la salida más fácil a ojo, se les dan las versiones hexadecimales del contenido de la memoria, en lugar de las versiones binarias. Supongamos, por ejemplo, que un segmento del volcado de memoria se parece a

$$\text{A3 BB 59 2E.}$$

¿Cuál es el contenido real de las cuatro posiciones de memoria?

Solución

$$A3_{16} = 10100011_2$$
$$BB_{16} = 10111011_2$$
$$59_{16} = 01011001_2$$
$$2E_{16} = 00101110_2$$

■

Autoexamen

1. Representar un entero no negativo en notación binaria significa escribirlo como una suma de productos de la forma _____, donde _____.
2. Para sumar enteros en notación binaria, se utilizan los hechos de que $1_2 + 1_2 =$ _____ y $1_2 + 1_2 + 1_2 =$ _____.
3. Para restar números enteros en notación binaria, se utiliza el hecho de que $10_2 - 1_2 =$ _____ y $11_2 - 1_2 =$ _____.
4. Un semisumador es un circuito digital lógico que _____ y un sumador completo es un circuito digital lógico que _____.
5. El complemento de dos de 8 bits de un entero positivo a es _____.
6. Para encontrar el complemento de dos de 8 bits de un entero positivo que es a lo más 255, usted _____, _____ y _____.
7. Si a es un entero con $-128 \leq a \leq 127$, la representación de 8 bits de a es _____ si $a \geq 0$ y es _____ si $a < 0$.
8. Para sumar dos números enteros en el rango de -128 a 127 —cuya suma también está en el rango de -128 a 127, usted _____, _____, _____ y _____.
9. Representar un entero no negativo en notación hexadecimal significa escribirlo como una suma de productos de la formas _____, donde _____.
10. Para convertir un número entero no negativo de la notación hexadecimal a la notación binaria, usted _____ y _____.

Conjunto de ejercicios 2.5

En los ejercicios 1 al 6 represente los números enteros decimales en notación binaria.

1. 19 2. 55 3. 87

4. 458 5. 1609 6. 1424

En los ejercicios del 7 al 12 represente los números enteros en notación decimal.

7. 1110_2 8. 10111_2 9. 110110_2

10. 1100101_2 11. 1000111_2 12. 1011011_2

En los ejercicios del 13 al 20 realice la aritmética usando la notación binaria.

13. $1011_2 + 101_2$

14. $1001_2 + 1011_2$

15. $101101_2 + 11101_2$

16. $110111011_2 + 1001011010_2$

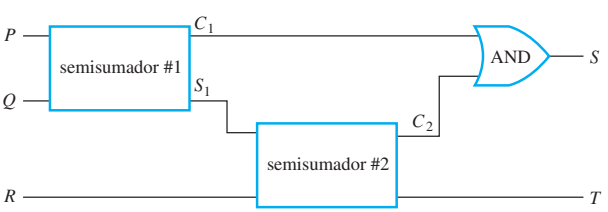
17. $10100_2 - 1101_2$

18. $11010_2 - 1101_2$

19. $101101_2 - 10011_2$

20. $1010100_2 - 10111_2$

21. De las señales de salida S y T para el circuito en la columna de la derecha si las señales de entrada P, Q y R se especifican. Considere que este *no* es el circuito de un sumador completo.
   a. $P = 1, Q = 1, R = 1$
   b. $P = 0, Q = 1, R = 0$
   c. $P = 1, Q = 0, R = 1$



22. Agregue $11111111_2 + 1_2$ y convierta el resultado a notación decimal, para comprobar que $11111111_2 = (2^8 - 1)_{10}$.

En los ejercicios del 23 al 26, encuentre los complementos de dos de 8 bits para los enteros.

23. 23 24. 67 **25.** 4 26. 115

En los ejercicios 27 al 30, encuentre las representaciones decimales de los enteros con representaciones de 8 bits.

27. 11010011 28. 10011001

29. 11110010 30. 10111010

En los ejercicios 31 al 36, utilice las representaciones de 8 bits para calcular las sumas.

31. $57 + (-118)$ **32.** $62 + (-18)$

33. $(-6) + (-73)$ 34. $89 + (-55)$

35. $(-5) + (-46)$ 36. $123 + (-94)$

✶ 37. Demuestre que si a, b y $a + b$ son enteros en el rango de 1 al 128, entonces,

$$(2^8 - a) + (2^8 - b) = (2^8 - (a + b)) + 2^8 \geq 2^8 + 2^7.$$

Explique por qué resulta que si se calcula la representación binaria de 8 bits de la suma de los negativos de dos números en el rango dado, el resultado es un número negativo.

En los ejercicios 38 al 40 convierta los enteros de notación hexadecimal a decimal.

38. $A2BC_{16}$ 39. $E0D_{16}$ 40. $39EB_{16}$

En los ejercicios 41 al 43 convierta los números enteros de notación hexadecimal a binaria.

41. $1C0ABE_{16}$ 42. $B53DF8_{16}$ 43. $4ADF83_{16}$

En los ejercicios 44 al 46 convierta los números enteros de notación binaria a hexadecimal.

44. 00101110_2 45. 1011011111000101_2

46. 1100100101100_2

47. **Notación octal:** Además de la notación binaria y hexadecimal, los científicos de la computación también usan la *notación octal* (base 8) para representar los números. La notación octal se basa en el hecho de que cualquier número entero se puede representar como una única suma de los números de la forma $d \cdot 8^n$, donde cada n es un entero no negativo y cada d es uno de los números enteros de 0 a 7. Así, por ejemplo, $5073_8 = 5 \cdot 8^3 + 0 \cdot 8^2 + 7 \cdot 8^1 + 3 \cdot 8^0 = 2619_{10}$.
   a. Convierta 61502_8 a notación decimal.
   b. Convierta 20763_8 a notación decimal.
   c. Describa los métodos para convertir enteros de notación octal a binaria y de binaria a octal que son similares a los métodos utilizados en los ejemplos 2.5.12 y 2.5.13 para convertir de un lado a otro de notación hexadecimal a binaria. Dé ejemplos que demuestren que estos métodos dan las respuestas correctas.

Respuestas del autoexamen

1. $d \cdot 2^n$: $d = 0$ o $d = 1$ y n es un entero no negativo 2. 10_2; 11_2 3. 1_2; 10_2
4. las salidas de la suma de dos dígitos binarios cualesquiera; las salidas de la suma de cualesquiera tres dígitos binarios
5. $2^8 - a$ 6. escriba la representación binaria de 8 bits de a; voltear los bits, sume 1 en notación binaria
7. la representación binaria de 8 bits de a, la representación binaria de 8 bits de $2^8 - a$
8. convierta ambos números enteros a sus representaciones binarias de 8 bits, sume los resultados utilizando la notación binaria; trunque cualquier 1 principal; convierta de nuevo a la forma decimal
9. $d \cdot 16^n$; $d = 0, 1, 2, \ldots 9, A, B, C, D, E, F$ y n es un entero no negativo
10. escriba cada dígito hexadecimal en notación binaria de 4 bits; yuxtaponga los resultados

Capítulo 3

LA LÓGICA DE ENUNCIADOS CUANTIFICADOS

En el capítulo 2 discutimos el análisis lógico de los enunciados compuestos, que están formados de enunciados simples unidos por los conectores, $\sim$, $\wedge$, $\vee$, $\rightarrow$ y $\leftrightarrow$. Dicho análisis ilumina muchos aspectos del razonamiento humano, pero no se puede utilizar para determinar la validez en la mayoría de las situaciones cotidianas y matemáticas. Por ejemplo, el argumento

Todos los hombres son mortales.
Sócrates es un hombre.
$\therefore$ Sócrates es mortal.

se percibe intuitivamente como correcto. Sin embargo, su validez no puede deducirse utilizando los métodos descritos en la sección 2.3. Para determinar la validez de ejemplos como éste, es necesario separar los enunciados en partes de la misma manera que se separan las frases declarativas en sujetos y predicados. Y se debe analizar y comprender el papel especial que desempeñan las palabras que denotan cantidades tales como "todos" o "algunos". El análisis simbólico de los predicados y los enunciados cuantificados se llama **cálculo de predicados**. El análisis simbólico de enunciados compuestos ordinarios (como el que se indica en las secciones de la 2.1 a la 2.3) se llama **cálculo de enunciados** (o **cálculo proposicional**).

3.1 Predicados y enunciados cuantificados I

. . . no fue sino hasta en los últimos años que se ha visto como fundamental que cualquier y alguno están en la naturaleza misma de las matemáticas. —A. N. Whitehead (1861-1947)

Como se indicó en la sección 2.1, la frase "Él es un estudiante universitario" no es un enunciado, ya que puede ser verdadero o falso, dependiendo del valor del pronombre *él*. Del mismo modo, la frase "$x + y$ es mayor que 0" no es un enunciado, porque su valor de verdad depende de los valores de las variables x y y.

En gramática, la palabra *predicado* se refiere a la parte de una frase que da información acerca del sujeto. En la frase "James es un estudiante del Colegio Bedford", la palabra *James* es el sujeto y la frase *es un estudiante del Colegio Bedford* es el predicado. El predicado es la parte de la frase de la que se ha eliminado al sujeto.

En lógica, los predicados se pueden obtener mediante la eliminación de todos o algunos de los nombres de un enunciado. Por ejemplo, sea que P signifique "es un estudiante del Colegio Bedford" y sea Q "es un estudiante de". Entonces, P y Q son *símbolos de predicado*. Las frases "x es un estudiante del Colegio Bedford" y "x es un estudiante en y" se simbolizan como $P(x)$ y como $Q(x, y)$, respectivamente, donde x y y son *variables del predicado* que toman valores en conjuntos apropiados. Cuando se sustituyen los valores concretos en lugar de las variables del predicado, se obtiene un enunciado. Para simplificar, se define un *predicado* como un símbolo de predicado junto con variables de predicado. En algunos otros tratados de lógica, a estos objetos se les conoce como **funciones proposicionales** o **frases abiertas**.

• Definición

Un **predicado** es una frase que contiene un número finito de variables y se convierte en un enunciado cuando se sustituyen valores específicos en lugar de las variables. El **dominio** de una variable de predicado es el conjunto de todos los valores que se pueden sustituir en lugar de la variable.

Ejemplo 3.1.1 Determinación de los valores de verdad de un predicado

Sea $P(x)$ el predicado "$x^2 > x$" con dominio el conjunto $\mathbf{R}$ de todos los números reales. Escriba $P(2)$, $P(\frac{1}{2})$ y $P(-\frac{1}{2})$ e indique cuáles de los siguientes enunciados son verdaderos y cuáles son falsos.

Solución

$P(2)$: $2^2 > 2$, o $4 > 2$. Verdadero.

$P\left(\frac{1}{2}\right)$: $\left(\frac{1}{2}\right)^2 > \frac{1}{2}$, o $\frac{1}{4} > \frac{1}{2}$. Falso.

$P\left(-\frac{1}{2}\right)$: $\left(-\frac{1}{2}\right)^2 > -\frac{1}{2}$, o $\frac{1}{4} > -\frac{1}{2}$. Verdadero. ■

Cuando un elemento en el dominio de la variable de una variable de predicado se sustituye por la variable, el enunciado resultante es verdadero o falso. El conjunto de todos estos elementos que hacen que el predicado sea verdadero se llama *conjunto de verdad* del predicado.

• Definición

Si $P(x)$ es un predicado y x tiene dominio D, el **conjunto de verdad** de $P(x)$ es el conjunto de todos los elementos de D que hacen a $P(x)$ verdadero cuando se sustituyen por x. El conjunto de verdad de $P(x)$ se denota por

$$\{x \in D \mid P(x)\}.$$

Nota Recuerde que leemos estos símbolos como "el conjunto de todas las x en D tal que $P(x)$".

Ejemplo 3.1.2 Determinación del conjunto de verdad de un predicado

Sea $Q(n)$ el predicado "n es un factor de 8". Determine el conjunto de verdad de $Q(n)$ si

a. el dominio de n es el conjunto $\mathbf{Z}^+$ de todos los enteros positivos.

b. el dominio de n es el conjunto $\mathbf{Z}$ de todos los enteros.

Solución

a. El conjunto de verdad es $\{1, 2, 4, 8\}$ ya que éstos son exactamente los enteros positivos que dividen a 8 de manera exacta.

b. El conjunto de verdad es $\{1, 2, 4, 8, -1, -2, -4, -8\}$ porque los enteros negativos $-1, -2, -4$ y -8 también se dividen entre 8 sin dejar residuo. ■

El cuantificador universal: ∀

Una forma segura de cambiar predicados en los enunciados es asignar valores específicos a todas sus variables. Por ejemplo, si x representa el número 35, la frase "x es (exactamente) divisible entre 5" es un enunciado verdadero ya que $35 = 5 \cdot 7$. Otra forma de obtener enunciados de predicados es agregar **cuantificadores**. Los cuantificadores son palabras que se refieren a las cantidades tales como "algunos" o "todos" y nos dicen para cuántos elementos de un predicado dado es verdadero. El concepto formal de cuantificador se introdujo en la

Culver Pictures

Charles Sanders Peirce (1839-1914)

lógica simbólica a finales del siglo XIX por el filósofo, lógico e ingeniero norteamericano, Charles Sanders Peirce y, de forma independiente, por el lógico alemán Gottlob Frege.

El símbolo $\forall$ denota "para todo" y se llama **cuantificador universal**. Por ejemplo, otra forma de expresar la frase "Todos los seres humanos son mortales" es escribir

$$\forall \text{ los seres humanos } x,\ x \text{ es mortal.}$$

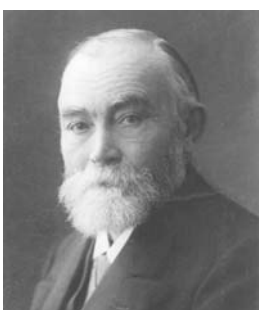
Cuando se introduce el símbolo x en la frase "$\forall$ los seres humanos x" se supone que piensa en x como un objeto individual, pero genérico, con todas las propiedades que comparten todos los seres humanos, pero no otras propiedades. Por tanto debe decir "x es mortal" en lugar de "x son mortales". En otras palabras, use el singular "es" más que el verbo en plural "son" cuando describa la propiedad que satisface x. Sea H el conjunto de todos los seres humanos, entonces puede simbolizar el enunciado más formalmente escribiendo

$$\forall x \in H,\ x \text{ es mortal,}$$

que se lee como "Para toda x en el conjunto de todos los seres humanos, x es mortal".

Nota Piense "para todo" cuando vea el símbolo $\forall$".

El dominio de la variable del predicado generalmente se indica entre el símbolo $\forall$ y el nombre de la variable (como en $\forall$ los seres humanos x) o inmediatamente después del nombre de la variable (como en $\forall x \in H$). Algunas otras expresiones que se pueden utilizar en lugar de *para toda* son *para cada*, *para un arbitrario*, *para cualquier*, *para cada una* y para *cualquier dada*. En una frase como "$\forall$ los números reales x y y, $x + y = y + x$" el símbolo $\forall$ se entiende que se refiere tanto a x como a y.*



Friedrich Schiller, Universitat Jena

Gottlob Frege (1848-1925)

Las oraciones que se cuantifican universalmente se definen como enunciados, dándoles los valores verdaderos que se especifican en la siguiente definición:

• Definición

Sea $Q(x)$ un predicado y D el dominio de x. Un **enunciado universal** es un enunciado de la forma "$\forall x \in D$, $Q(x)$". Se define como verdadero, si y sólo si, $Q(x)$ es verdadera para toda x en D. Se define como falso si y sólo si $Q(x)$ es falso para al menos un x en D. Un valor para x, para el cual $Q(x)$ es falso se llama un **contraejemplo** del enunciado universal.

Ejemplo 3.1.3 Verdad y falsedad de los enunciados universales

a. Sea $D = \{1, 2, 3, 4, 5\}$ y considere el enunciado

$$\forall x \in D,\ x^2 \geq x$$

Demuestre que este enunciado es verdadero.

b. Considere el enunciado

$$\forall x \in \mathbf{R},\ x^2 \geq x.$$

Encuentre un contraejemplo para demostrar que este enunciado es falso.

Solución

a. Compruebe que "$x^2 \geq x$" es verdadero para cada x dado en D.

$$1^2 \geq 1, \qquad 2^2 \geq 2, \qquad 3^2 \geq 3, \qquad 4^2 \geq 4, \qquad 5^2 \geq 5.$$

Por tanto "$\forall x \in D$, $x^2 \geq x$" es verdadero.

*Las versiones más formales de la lógica simbólica requerirían escribir un $\forall$ separado para cada variable: "$\forall x \in \mathbf{R}(\forall y \in \mathbf{R}(x + y = y + x))$".

b. *Contraejemplo*: Tome $x = \frac{1}{2}$. Entonces x está en $\mathbf{R}$ (ya que $\frac{1}{2}$ es un número real) y

$$\left(\frac{1}{2}\right)^2 = \frac{1}{4} \not\geq \frac{1}{2}.$$

Por tanto "$\forall x \in \mathbf{R}$, $x^2 \geq 2$" es falso. ■

La técnica utilizada para mostrar la verdad del enunciado universal en el ejemplo 3.1.3*a*) se llama **método de agotamiento**. Consiste en demostrar la verdad del predicado por separado para cada elemento individual del dominio. (¡La idea es agotar las posibilidades antes de que usted se agote!). Este método puede, en teoría, utilizarse siempre que el dominio de la variable del predicado es finito. En los últimos años el predominio de las computadoras digitales ha aumentado considerablemente la conveniencia de utilizar el método de agotamiento. Los sistemas computacionales expertos o sistemas basados en el conocimiento, utilizan este método para obtener respuestas a muchas de las preguntas formuladas a las mismas. Sin embargo, ya que la mayoría de conjuntos matemáticos son infinitos, el método de agotamiento rara vez se puede utilizar para obtener resultados matemáticos en general.

El cuantificador existencial: ∃

El símbolo ∃ denota "existe" y se llama **cuantificador existencial**. Por ejemplo, la frase "Hay un estudiante de matemáticas 140" se puede escribir como

∃ una persona p tal que p es un estudiante en Matemáticas 140,

o, más formalmente,

$\exists p \in P$ tal que p es un estudiante en Matemáticas 140,

Nota Piense "existe" cuando vea el símbolo ∃.

donde P es el conjunto de todas las personas. El dominio de la variable del predicado generalmente se indica ya sea entre el símbolo ∃ y el nombre de la variable o inmediatamente después del nombre de la variable. Las palabras *tal que* se insertan justo antes del predicado. Se pueden utilizar algunas otras expresiones en lugar de *existe* como son *hay una a*, *se puede encontrar una a*, *hay al menos una*, *para alguna* y *por lo menos una*. En una frase tal como "∃ m y n enteros tales que $m + n = m \cdot n$", se entiende que el símbolo ∃ se refiere tanto a m como a n.*

Las frases que se cuantifican existencialmente se definen como enunciados, al darles los valores de verdad que se detallan en la siguiente definición.

• Definición

Sea $Q(x)$ un predicado y D el dominio de x. Un **enunciado existencial** es un enunciado de la forma "$\exists x \in D$ tal que $Q(x)$". Que se define como verdadero, si y sólo si $Q(x)$ es verdadero para al menos una x en D. Es falso, si y sólo si, $Q(x)$ es falso para toda x en D.

Ejemplo 3.1.4 Verdad y falsedad de los enunciados existenciales

a. Considere el enunciado

$$\exists m \in \mathbf{Z}^+ \text{ tal que } m^2 = m.$$

Demuestre que este enunciado es verdadero.

*En la mayoría de las versiones más formales de lógica simbólica, las palabras *tal que* no se escriben (aunque se sobreentienden) y se utiliza un símbolo por separado ∃ para cada variable: "$\exists m \in \mathbf{Z}(\exists n \in \mathbf{Z}(m + n = m \cdot n))$".

b. Sea $E = \{5, 6, 7, 8\}$ y considere el enunciado

$$\exists m \in E \text{ tal que } m^2 = m$$

Demuestre que este enunciado es falso.

Solución

a. Observe que $1^2 = 1$. Así, "$m^2 = m$" es verdadero para al menos un número entero m. Por tanto "$\exists m \in \mathbf{Z}$ tal que $m^2 = m$" es verdadero.

b. Observe que $m^2 = m$ no es verdadero para cualquier entero m del 5 al 8:

$$5^2 = 25 \neq 5, \qquad 6^2 = 36 \neq 6, \qquad 7^2 = 49 \neq 7, \qquad 8^2 = 64 \neq 8.$$

Por lo que "$\exists m \in E$ tal que $m^2 = m$" es falso. ■

Lenguaje formal versus *lenguaje informal*

Es importante poder traducir del lenguaje informal al formal cuando se trata de dar sentido a conceptos matemáticos que son nuevos para usted. Es igualmente importante poder traducir del lenguaje informal al formal cuando se analiza un problema complicado.

Ejemplo 3.1.5 Traducción del lenguaje formal al informal

Reescriba los siguientes enunciados formales en diferentes formas equivalentes pero de manera más informal. No utilice el símbolo ∀ o ∃.

a. $\forall x \in \mathbf{R}$, $x^2 \geq 0$.

b. $\forall x \in \mathbf{R}$, $x^2 \neq -1$.

c. $\exists m \in \mathbf{Z}^+$ tal que $m^2 = m$.

Solución

Nota El nombre singular se usa para referirse al dominio cuando el símbolo ∀ se traduce como *todo*, *cualquier* o *cada uno*.

a. Todos los números reales tienen cuadrados no negativos.
O: Todo número real tiene un cuadrado no negativo.
O: Cualquier número real tiene un cuadrado no negativo.
O: El cuadrado de todo número real es no negativo.

b. Todos los números reales tienen cuadrados que no son iguales a -1.
O: No hay números reales que tengan cuadrados iguales a -1.
(Las palabras *ninguno es* o *no . . . son* son equivalentes a las palabras *todos no son*).

Nota En inglés común, el enunciado del inciso *c*) se podría considerar verdadero sólo si hay al menos dos números enteros positivos igual a sus propios cuadrados. En matemáticas, entendemos que los dos últimos enunciados del inciso *c*) significan lo mismo.

c. Hay un entero positivo cuyo cuadrado es igual a sí mismo.
O: Se puede encontrar al menos un número entero positivo igual a su propio cuadrado.
O: Algún entero positivo es igual a su propio cuadrado.
O: Algunos números enteros positivos son iguales a sus propios cuadrados. ■

Otra forma de recapitular los enunciados universales y existenciales de manera informal es colocar la cuantificación al final de la frase. Por ejemplo, en lugar de decir "Para cualquier número real x, x^2 es positivo", se podría decir "x^2 es positivo para cualquier número real x". En tal caso se dice que el cuantificador "sigue" al resto de la frase.

Ejemplo 3.1.6 Cuantificadores que siguen

Reescriba los enunciados siguientes de tal forma que el cuantificador siga al resto de la frase.

a. Para cualquier entero n, $2n$ es par.

b. Existe al menos un número real x tal que $x^2 \leq 0$.

Solución

a. $2n$ es par para cualquier entero n.

b. $x^2 \leq 0$ para algún número real x.
O: $x^2 \leq 0$ para al menos un número real x. ■

Ejemplo 3.1.7 Traducción del lenguaje informal al formal

Reescriba cada uno de los siguientes enunciados formalmente. Use cuantificadores y variables.

a. Todos los triángulos tienen tres lados.

b. Ningún perro tiene alas.

c. Algunos programas están estructurados.

Solución

a. $\forall$ triángulo t, t tiene tres lados.
O: $\forall t \in T$, t tiene tres lados (donde T es el conjunto de todos los triángulos).

b. $\forall$ perro d, d no tiene alas.
O: $\forall d \in D$, d no tiene alas (donde D es el conjunto de todos los perros).

c. $\exists$ un programa p tal que p está estructurado.
O: $\exists p \in P$ tal que p está estructurado (donde P es el conjunto de todos los programas). ■

Enunciados condicionales universales

Un argumento razonable puede decir que la forma más importante de enunciado en matemáticas es el **enunciado condicional universal**:

$$\forall x, \text{ si } P(x), \text{ entonces } Q(x).$$

La familiaridad con enunciados de esta forma es esencial si va a aprender a hablar con matemáticas.

Ejemplo 3.1.8 Escritura informal de enunciados condicionales universales

Reescriba el siguiente enunciado de manera informal, sin cuantificadores o variables.

$$\forall x \in \mathbf{R}, \text{ si } x > 2, \text{ entonces } x^2 > 4.$$

Solución Si un número real x es mayor que 2, entonces su cuadrado es mayor que 4.
O: Siempre que un número real es mayor que 2, su cuadrado es mayor que 4.
O: El cuadrado de cualquier número real mayor que 2 es mayor que 4.
O: Los cuadrados de todos los números reales mayores que 2 son mayores que 4. ■

Ejemplo 3.1.9 Escritura formal de enunciados condicionales universales

Reescriba cada uno de los siguientes enunciados en la forma

$$\forall \text{ \_\_\_\_\_}, \text{ si } \text{\_\_\_\_\_} \text{ entonces } \text{\_\_\_\_\_}.$$

a. Si un número real es un número entero, entonces es un número racional.

b. Todos los bytes tienen ocho bits.

c. No hay autobombas de color verde.

Solución

a. ∀ números reales x, si x es un número entero, entonces x es un número racional.
O: ∀ $x \in \mathbf{R}$, si $x \in \mathbf{Z}$ entonces $x \in \mathbf{Q}$.

b. ∀x, si x es un byte, entonces x tiene ocho bits.

c. ∀x, si x es una autobomba, entonces x no es verde.

Es común que, como en los incisos *b*) y *c*), omitir la identificación explícita del dominio de las variables del predicado en los enunciados condicionales universales. ■

Pensar con calma acerca del significado de los enunciados condicionales universales nos conduce a otro nivel de comprensión del porqué la tabla de verdad para un enunciado si-entonces se debe definir como es. Consideremos de nuevo el enunciado

$$\forall \text{ número real } x, \text{ si } x > 2 \text{ entonces } x^2 > 4.$$

Su experiencia e intuición le dice que este enunciado es verdadero. Pero eso significa que

$$\text{Si } x > 2 \text{ entonces } x^2 > 4$$

debe ser verdadero para cada número real x. En consecuencia, incluso debe ser verdadero para valores de x que hacen que su hipótesis "$x > 2$" sea falsa. En particular, ambos enunciados

$$\text{Si } 1 > 2, \text{ entonces } 1^2 > 4 \quad \text{y} \quad \text{Si } -3 > 2 \text{ entonces } (-3)^2 > 4$$

deben ser verdaderos. En ambos casos la hipótesis es falsa, pero en el primer caso, la conclusión "$1^2 > 4$" es falsa y en el segundo caso, la conclusión de la "$(-3)^2 > 4$" es verdadera. Por tanto, independientemente de que su conclusión sea verdadera o falsa, un enunciado si-entonces con una hipótesis falsa debe ser verdadero.

Observe también que la definición de argumento válido es un enunciado condicional universal:

∀ combinaciones de valores de verdad de los enunciados componentes,
si las premisas son todas verdaderas entonces la conclusión también es verdadera.

Formas equivalentes de los enunciados universal y existencial

Observe que los dos enunciados "∀ número real x, si x es un número entero, entonces x es racional" y "∀ entero x, x es racional" significan lo mismo. Ambos tienen la traducción informal "Todos los números enteros son racionales". De hecho, un enunciado de la forma

$$\forall x \in U, \text{ si } P(x), \text{ entonces } Q(x)$$

siempre se puede escribir en la forma

$$\forall x \in D,\ Q(x)$$

para un angosto U que está en el dominio D que consiste en todos los valores de la variable x que hacen que $P(x)$ sea verdadero. Por el contrario, un enunciado de la forma

$$\forall x \in D,\ Q(x)$$

se puede reescribir como

$$\forall x, \text{ si } x \text{ está en } D, \text{ entonces } Q(x).$$

Ejemplo 3.1.10 Formas equivalentes de enunciados universales

Reescriba el enunciado siguiente en las dos formas "$\forall x$, si _____ entonces _____" y "$\forall$ _____ x, _____": Todos los cuadrados son rectángulos.

Solución

$\forall x$, si x es un cuadrado entonces x es un rectángulo.
$\forall$ cuadrado x, x es un rectángulo. ■

Del mismo modo, un enunciado de la forma "$\exists x$ tal que $p(x)$ y $Q(x)$" se puede escribir como "$\exists x \varepsilon D$ tal que $Q(x)$", donde D es el conjunto de todas las x para los que $P(x)$ es verdadero.

Ejemplo 3.1.11 Formas equivalentes para los enunciados existenciales

Un **número primo** es un entero mayor que 1, cuyos únicos factores enteros positivos son el mismo y el 1. Considere el enunciado de "Hay un número entero que es a la vez primo y par". Sea que Primo(n) signifique "n es primo" y que Par(n) signifique "n es par". Use la notación Primo(n) y Par(n) para reescribir este enunciado en las dos formas siguientes:

a. $\exists n$ tal que _____ $\wedge$ _____.

b. $\exists$ _____ n tal que _____.

Solución

a. $\exists n$ tal que Primo(n) $\wedge$ Par(n).

b. Dos respuestas: $\exists$ un número primo n tal que Par(n).
$\exists$ un número par n tal que Primo(n). ■

Cuantificación implícita

Considere el enunciado

Si un número es un entero, entonces es un número racional.

Como se indicó antes, este enunciado es equivalente a un enunciado universal. Sin embargo, no contiene la palabra reveladora *todos* o *cada* o *cualquiera* o *cada uno*. La única pista para indicar su cuantificación universal proviene de la presencia del artículo indefinido *un*. Este es un ejemplo de cuantificación universal *implícita*.

La cuantificación existencial puede ser implícita. Por ejemplo, el enunciado "El número 24 puede ser escrito como la suma de dos números enteros pares" se puede expresar formalmente como "$\exists$ m y n enteros pares tales que $24 = m + n$".

La escritura matemática contiene muchos ejemplos de enunciados cuantificados implícitamente. Algunos ocurren, como en el primer ejemplo anterior, a través de la presencia de la palabra *uno* o *un*. Otros casos se producen en el contexto general de una frase que proporciona parte de su significado. Por ejemplo, en un curso de álgebra en el que la letra x siempre se usa para indicar un número real, el predicado

$$\text{Si } x > 2 \text{ entonces } x^2 > 4$$

se interpreta que significa lo mismo que el enunciado

$$\forall \text{ número real } x, \text{ si } x > 2, \text{ entonces } x^2 > 4.$$

Los matemáticos utilizan a menudo una doble flecha para indicar simbólicamente la cuantificación implícita. Por ejemplo, podrían expresar el enunciado anterior como

$$x > 2 \quad \Rightarrow \quad x^2 > 4.$$

• Notación

Sean $P(x)$ y $Q(x)$ predicados y supongamos que el dominio común de x es D.

- La notación $\boldsymbol{P(x) \Rightarrow Q(x)}$ significa que cada elemento del conjunto de verdad de $P(x)$ está en el conjunto de verdad de $Q(x)$, o, equivalentemente, $\forall x$, $P(x) \rightarrow Q(x)$.
- La notación $\boldsymbol{P(x) \Leftrightarrow Q(x)}$ significa que $P(x)$ y $Q(x)$ tienen conjuntos de verdad idénticos, o equivalentemente, $\forall x$, $P(x) \leftrightarrow Q(x)$.

Ejemplo 3.1.12 Uso de $\Rightarrow$ y $\Leftrightarrow$

Sea

$Q(n)$ "n es un factor de 8",

$R(n)$ "n es un factor de 4",

$S(n)$ "$n < 5$ y $n \neq 3$"

y supongamos que el dominio de n es $\mathbf{Z}^+$, el conjunto de los enteros positivos. Utilice los símbolos $\Rightarrow$ y $\Leftrightarrow$ para indicar las relaciones verdaderas entre $Q(n)$, $R(n)$ y $S(n)$.

Solución

1. Como se indicó en el ejemplo 3.1.2, el conjunto de verdad de $Q(n)$ es $\{1, 2, 4, 8\}$ cuando el dominio de n es $\mathbf{Z}^+$. Con un razonamiento similar el conjunto de verdad de $R(n)$ es $\{1, 2, 4\}$. Por tanto, es cierto que cada elemento del conjunto de verdad de $R(n)$ está en el conjunto de verdad de $Q(n)$, o, equivalentemente, $\forall n$ en $\mathbf{Z}^+$, $R(n) \rightarrow Q(n)$. Por tanto $R(n) \Rightarrow Q(n)$, o, equivalentemente

   $$n \text{ es un factor de } 4 \quad \Rightarrow \quad n \text{ es un factor de } 8.$$

2. El conjunto de verdad de $S(n)$ es $\{1, 2, 4\}$, que es idéntico al conjunto de verdad de $R(n)$, o, equivalentemente, $\forall n$ en $\mathbf{Z}^+$, $R(n) \leftrightarrow S(n)$. Por tanto $R(n) \Leftrightarrow S(n)$, o, equivalentemente,

   $$n \text{ es un factor de } 4 \quad \Leftrightarrow \quad n < 5 \text{ y } n \neq 3.$$

   Además, ya que cada elemento del conjunto de verdad de $S(n)$ está en el conjunto de verdad de $Q(n)$, o, equivalentemente, $\forall n$ en $\mathbf{Z}^+$, $S(n) \rightarrow Q(n)$, entonces, $S(n) \Rightarrow Q(n)$, o, equivalentemente,

   $$n < 5 \text{ y } n \neq 3 \quad \Rightarrow \quad n \text{ es un factor de } 8.$$ ■

Algunas preguntas de cuantificación pueden ser muy sutiles. Por ejemplo, un libro de matemáticas puede contener lo siguiente:

a. $(x + 1)^2 = x^2 + 2x + 1$. b. Resuelva $3x - 4 = 5$.

Aunque ni *a*) ni *b*) contiene la cuantificación explícita, se supone que el lector entiende que la x en *a*) está universalmente cuantificada, mientras que la x en *b*) está existencialmente cuantificada. Cuando se hace explícita la cuantificación, *a*) y *b*) se convierten en

a. $\forall$ número real x, $(x + 1)^2 = x^2 + 2x + 1$.

b. Demuestre (encontrando un valor) que $\exists$ un número real x tal que $3x - 4 = 5$.

La cuantificación de un enunciado, ya sea universal o existencial fundamentalmente determina cómo se puede aplicar el enunciado y qué método se debe utilizar para establecer su verdad. Por tanto, es importante estar alerta a la presencia de cuantificadores ocultos cuando esté leyendo matemáticas, para que interprete los enunciados de una manera lógicamente correcta.

Mundo de Tarski

El mundo de Tarski es un programa de computadora desarrollado por los científicos de la información Jon Barwise y John Etchemendy para ayudar a enseñar los principios de lógica. Se describe en su libro *El lenguaje de la lógica de primer orden*, que se acompaña de un CD que contiene el programa El mundo de Tarski, llamado así por el gran lógico Alfred Tarski.

Ejemplo 3.1.13 Investigando El mundo de Tarski

Alfred Tarski (1902-1983)

El programa El mundo de Tarski proporciona imágenes de bloques de diferentes tamaños, formas y colores, que se encuentran en una cuadrícula. En la figura 3.1.1 se muestra una figura de un arreglo de objetos en un mundo de Tarski bidimensional. La configuración se puede describir usando operadores lógicos y para la versión bidimensional notación tal como Triángulo(x), significa "x es un triángulo", Azul(y), significa "y es de color azul" y DerechaDe(x, y), significa "x está a la derecha de y (pero posiblemente en un diferente renglón)". Los objetos individuales pueden tener nombres, tales como a, b o c.

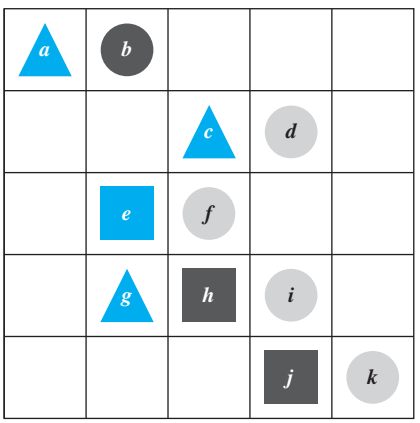


Figura 3.1.1

Determine la verdad o falsedad de cada uno de los enunciados siguientes. El dominio de todas las variables es el conjunto de objetos en el mundo de Tarski que se acaba de mostrar.

a. $\forall t$, Triángulo(t) $\rightarrow$ Azul(t).

b. $\forall x$, Azul(x) $\rightarrow$ Triángulo(x).

c. $\exists y$ tal que Cuadrado(y) $\wedge$ DerechaDe(d, y).

d. $\exists z$ tal que Cuadrado(z) $\wedge$ Gris(z).

Solución

a. Este enunciado es verdadero. Todos los triángulos son de color azul.

b. Este enunciado es falso. Como un contraejemplo, observe que e es de color azul y no es un triángulo.

c. Este enunciado es verdadero, ya que tanto e como h son cuadrados y d está a su derecha.

d. Este enunciado es falso. Todos los cuadrados son ya sea azules o negros. ■

Autoexamen

Las respuestas de las preguntas del autoexamen se encuentran al final de cada sección.

1. Si $P(x)$ es un predicado con dominio D, el conjunto de verdad de $P(x)$ se denota _____. Leemos estos símbolos como _____.
2. Algunas formas de expresar el símbolo $\forall$ en palabras son _____.
3. Algunas formas de expresar el símbolo $\exists$ en palabras son _____.
4. Un enunciado de la forma $\forall x \in D$, $Q(x)$ es verdadero si y sólo si, $Q(x)$ es _____ para _____.
5. Un enunciado de la forma $\exists x \in D$ tal que $Q(x)$ es verdadero si y sólo si, $Q(x)$ es _____ para _____.

Conjunto de ejercicios 3.1*

1. Un zoológico tiene siete perros de color café, dos perros de color negro, seis gatos grises, diez gatos negros, cinco pájaros azules, seis pájaros amarillos y un pájaro negro. Determine cuáles de los siguientes enunciados son verdaderos y cuáles son falsos.
   a. Hay un animal en el zoológico que es rojo.
   b. Todo animal en el zoológico o es un ave o es un mamífero.
   c. Todo animal en el zoológico es de color café, gris o negro.
   d. Hay un animal en el zoológico que no es ni un gato ni perro.
   e. Ningún animal en el zoológico es de color azul.
   f. Hay en el zoológico un perro, un gato y un pájaro que todos tienen el mismo color.

2. Indique cuáles de los siguientes enunciados son verdaderos y cuáles son falsos. Justifique su respuesta lo mejor que pueda.
   a. Todo número entero es un número real.
   b. 0 es un número real positivo.
   c. Para todos los números reales r, $-r$ es un número real negativo.
   d. Todo número real es un número entero.

3. Sea $P(x)$ el predicado "$x > 1/x$".
   a. Escriba $P(2)$, $P(\frac{1}{2})$, $P(-1)$, $P(-\frac{1}{2})$ y $P(-8)$ e indique cuáles de estos enunciados son verdaderos y cuáles son falsos.
   b. Busque el conjunto de verdad de $P(x)$ si el dominio de x es $\mathbf{R}$, el conjunto de todos los números reales.
   c. Si el dominio es el conjunto $\mathbf{R}^+$ de todos los números reales positivos, ¿cuál es el conjunto de verdad de $P(x)$?

4. Sea $Q(n)$ el predicado "$n^2 \leq 30$".
   a. Escriba $Q(2)$, $Q(-2)$, $Q(7)$ y $Q(-7)$ e indique cuáles de estos enunciados son verdaderos y cuáles son falsos.
   b. Encuentre el conjunto de verdad de $Q(n)$ si el dominio de n es $\mathbf{Z}$, el conjunto de todos los enteros.
   c. Si el dominio es el conjunto $\mathbf{Z}^+$ de todos los enteros positivos, ¿cuál es el conjunto de verdad de $Q(n)$?

5. Sea $Q(x, y)$ el predicado "Si $x < y$ entonces $x^2 < y^2$" con el dominio de x y y el conjunto $\mathbf{R}$ de números reales.
   a. Explique por qué $Q(x, y)$ es falso si $x = -2$ y $y = 1$.
   b. De valores diferentes a los del inciso *a*) para los que $Q(x, y)$ es falso.
   c. Explique por qué $Q(x, y)$ es verdadero si $x = 3$ y $y = 8$.
   d. Dé valores diferentes de los del inciso *c*) para los que $Q(x, y)$ sea verdadero.

6. Sea $R(m, n)$ el predicado "Si m es un factor de n^2 entonces m es un factor de n", con el dominio, de m y n es el conjunto $\mathbf{Z}$ de enteros.
   a. Explique por qué $R(m, n)$ es falso si $m = 25$ y $n = 10$.
   b. Dé valores diferentes a los del inciso *a*) para los cuales $R(m, n)$ es falso.
   c. Explique por qué $R(m, n)$ es verdadero si $m = 5$ y $n = 10$.
   d. Dé valores diferentes de los del inciso *c*) para los que $R(m, n)$ sea verdadero.

7. Determine el conjunto de verdad de cada predicado.
   a. predicado: $6/d$ es un entero, dominio: $\mathbf{Z}$
   b. predicado: $6/d$ es un entero, dominio: $\mathbf{Z}^+$
   c. predicado: $1 \leq x^2 \leq 4$, dominio: $\mathbf{R}$
   d. predicado: $1 \leq x^2 \leq 4$, dominio: $\mathbf{Z}$

8. Sea $B(x)$ "$-10 < x < 10$". Determine el conjunto de verdad de $B(x)$ para cada uno de los siguientes dominios.
   a. $\mathbf{Z}$ b. $\mathbf{Z}^+$ c. El conjunto de todos los enteros pares

Encuentre contraejemplos para mostrar que los enunciados de los ejercicios del 9 al 12 son falsos.

9. $\forall x \in \mathbf{R}$, $x > 1/x$.

10. $\forall a \in \mathbf{Z}$, $(a - 1)/a$ no es un número entero.

11. $\forall$ enteros positivos m y n, $m \cdot n \geq m + n$.

12. $\forall$ números reales x y y, $\sqrt{x + y} = \sqrt{x} + \sqrt{y}$.

13. Considere el siguiente enunciado:

$$\forall \text{ jugador de baloncesto } x, x \text{ es alto.}$$

¿Cuál de las siguientes formas de expresión son equivalentes de este enunciado?
   a. Todo jugador de baloncesto es alto.
   b. Entre todos los jugadores de baloncesto, algunos son altos.
   c. Algunas de las personas altas son jugadores de baloncesto.
   d. Cualquier persona alta es un jugador de baloncesto.
   e. Todas las personas que son jugadores de baloncesto son altos.
   f. Cualquier persona que es un jugador de baloncesto es una persona alta.

*Para los ejercicios con números o letras azules, las soluciones están dadas en el apéndice B. El símbolo **H** indica que sólo se da una sugerencia o una solución parcial. El símbolo ✶ indica que el ejercicio es más difícil de lo normal.

14. Considere el siguiente enunciado:

$$\exists x \in \mathbf{R} \text{ tal que } x^2 = 2.$$

¿Cuál de las siguientes son formas equivalentes de expresar este enunciado?

a. El cuadrado de todo número real es 2.
b. Algunos números reales tienen cuadrado 2.
c. El número x tiene cuadrado 2, para algún número real x.
d. Si x es un número real, entonces $x^2 = 2$.
e. Algún número real tiene cuadrado 2.
f. Hay por lo menos un número real cuyo cuadrado es 2.

H 15. Reescriba los siguientes enunciados de manera informal en al menos dos formas diferentes sin necesidad de utilizar variables o cuantificadores.

a. $\forall$ los rectángulos x, x es un cuadrilátero.
b. $\exists$ un conjunto A tal que A tiene 16 subconjuntos.

16. Reescriba cada uno de las siguientes enunciados en la forma "$\forall$ ____ x, ____ ".

a. Todos los dinosaurios se extinguieron.
b. Cada número real es positivo, negativo o cero.
c. Ninguno de los números irracionales son números enteros.
d. Los que no son lógicos son perezosos.
e. El número 2 147 581 953 no es igual al cuadrado de ningún número entero.
f. El número -1 no es igual al cuadrado de cualquier número real.

17. Reescriba cada una de las siguientes frases en la forma "$\exists$ ____ x tal que ____ ".

a. Algunos ejercicios tienen respuestas.
b. Algunos números reales son racionales.

18. Sea D el conjunto de todos los estudiantes en su escuela y sea $M(s)$ "s es un estudiante de la licenciatura en matemáticas", sea $C(s)$ "s es un estudiante de ciencias de la computación" y sea $E(s)$ "s es un estudiante de ingeniería". Exprese cada uno de los siguientes enunciados utilizando cuantificadores, variables y los predicados $M(s)$, $C(s)$ y $E(s)$.

a. Hay un estudiante de ingeniería que es estudiante de matemáticas.
b. Cada estudiante de ciencias de la computación es un estudiante de ingeniería.
c. No hay estudiantes de ciencias de la computación que sean estudiantes de ingeniería.
d. Algunos estudiantes de ciencias de la computación también son estudiantes de matemáticas.
e. Algunos estudiantes de ciencias de la computación son estudiantes de ingeniería y otros no.

19. Considere el siguiente enunciado:

$$\forall \text{ entero } n, \text{ si } n^2 \text{ es par entonces } n \text{ es par.}$$

¿Cuál de las siguientes formas de expresión son equivalentes de este enunciado?

a. Todos los enteros tienen cuadrados pares y son pares.
b. Dado cualquier número entero cuyo cuadrado es par, ese entero en sí mismo es par.
c. Para todos los números enteros, hay algunos cuyo cuadrado es par.
d. Cualquier número entero con un cuadrado par es par.
e. Si el cuadrado de un número entero es par, entonces ese número entero es par.
f. Todos los números enteros tienen cuadrados pares.

H 20. Reescriba el siguiente enunciado de manera informal en al menos dos maneras diferentes sin necesidad de utilizar las variables o el símbolo $\forall$ o las palabras "para todo".

$\forall$ número real x, si x es positivo, entonces la raíz cuadrada de x es positiva.

21. Reescriba los siguientes enunciados tal que el cuantificador siga el resto de la frase.

a. Para cualquier gráfica G, el grado total de G es par.
b. Para cualquier triángulo isósceles T, los ángulos de la base de T son iguales.
c. Existe un número primo p tal que p es par.
d. Existe una función continua f tal que f no es derivable.

22. Reescriba cada uno de las siguientes enunciados en la forma "$\forall$ ____ x, si ____ entonces ____ ".

a. Todos los programas en Java tienen al menos 5 renglones.
b. Cualquier argumento válido con premisas verdaderas tiene una conclusión verdadera.

23. Reescriba cada uno de los siguientes enunciados en las dos formas "$\forall x$, si ____ entonces ____ " y "$\forall$ ____ x, ____ " (sin un si-entonces).

a. Todos los triángulos equiláteros son isósceles.
b. Cada estudiante de ciencia computacional necesita tomar estructuras de datos.

24. Reescriba los siguientes enunciados en las dos formas "$\exists$ ____ x tal que ____ " y "$\exists x$ tal que ____ y ____".

a. Algunos sombrereros están locos.
b. Algunas preguntas son fáciles.

25. El enunciado "El cuadrado de cualquier número racional es racional" se puede escribir formalmente como "Para todos los números racionales x, x^2 es racional" o como "Para toda x, si x es racional entonces x^2 es racional". Reescriba cada uno de los siguientes enunciados en las dos formas "$\forall$ ____ x, ____" y "$\forall x$, si ____ , entonces ____" o en las dos formas de "$\forall$ ____ x y y, ____ " y "$\forall x$ y y si ____, entonces ____".

a. El recíproco de cualquier fracción distinta de cero es una fracción.
b. La derivada de cualquier función polinomial es una función polinomial.
c. La suma de los ángulos de cualquier triángulo es 180°.
d. El negativo de cualquier número irracional es irracional.
e. La suma de dos enteros pares es par.
f. El producto de dos fracciones es una fracción.

26. Considere el enunciado "Todos los números enteros son números racionales, pero algunos números racionales no son enteros".

a. Escriba este enunciado en la forma "$\forall x$, si ____ entonces ____, pero $\exists$ ____ x tal que ____ ".
b. Sea Ratl(x) "x es un número racional" y sea Int(x) "x es un número entero". Escriba el enunciado dado formalmente usando solamente los símbolos Ratl(x), Int(x), $\forall$, $\exists$, $\wedge$, $\vee$, $\sim$ y $\rightarrow$.

27. Consulte la imagen de El mundo de Tarski dada en el ejemplo 3.1.13. Sea que Arriba(x, y) signifique que x está arriba de y

(aunque posiblemente en otra columna). Determine la verdad o falsedad de cada uno de los siguientes enunciados. Justifique sus respuestas.
a. $\forall x$, Círculo(u) $\rightarrow$ Gris(u).
b. $\forall u$, Gris(u) $\rightarrow$ Círculo(u).
c. $\exists y$ tal que Cuadrado(y) $\wedge$ Arriba(y, d).
d. $\exists z$ tal que Triángulo(z) $\wedge$ Arriba(f, z).

En los ejercicios del 28 al 30, reescriba cada enunciado sin utilizar cuantificadores o variables. Indique cuáles son verdaderos y cuáles son falsos y justifique sus respuestas lo mejor que pueda.

28. Sea el dominio de x el conjunto D de objetos analizados en los cursos de matemáticas y sea Real(x) "x es un número real", Pos(x) es "x es un número real positivo", Neg(x) es "x es un número real negativo" e Int(x) es "x es un número entero".
a. Pos(0)
b. $\forall x$, Real(x) $\wedge$ Neg(x) $\rightarrow$ Pos($-x$).
c. $\forall x$, Int(x) $\rightarrow$ Real(x).
d. $\exists x$ tales que Real(x) $\wedge \sim$Int(x).

29. Sea el dominio de x el conjunto de figuras geométricas en el plano y Cuadrado(x) es "x es un cuadrado" y Rect(x) es "x es un rectángulo".
a. $\exists x$ tal que Rect(x) $\wedge$ Cuadrado(x).
b. $\exists x$ tal que Rect(x) $\wedge \sim$Cuadrado(x).
c. $\forall x$, Cuadrado(x) $\rightarrow$ Rect(x).

30. Sea el dominio de x el conjunto **Z** de enteros y sea Impar(x) "x es impar", Primo(x) es "x es primo" y Cuadrado(x) es "x es un cuadrado perfecto". (Un entero n se dice que es un **cuadrado perfecto** si y sólo si, es igual al cuadrado de un número entero. Por ejemplo, 25 es un cuadrado perfecto porque $25 = 5^2$.)
a. $\exists x$ tal que Primo(x) $\wedge \sim$Impar(x).
b. $\forall x$, Primo(x) $\rightarrow \sim$Cuadrado(x).
c. $\exists x$ tal que Impar(x) $\wedge$ Cuadrado(x).

H 31. En cualquier libro de matemáticas o ciencias de la computación que no sea este libro, encontramos un ejemplo de un enunciado que es universal, pero está cuantificado implícitamente. Copie el enunciado tal y como aparece, reescríbalo haciendo explicita la cuantificación. Dé una cita completa para su ejemplo, que incluya título, autor, editorial, año y número de página.

32. Sea **R** el dominio de la variable del predicado x. ¿Cuáles de los siguientes son verdaderos y cuáles son falsos? Presente contraejemplos para los enunciados que son falsos.
a. $x > 2 \Rightarrow x > 1$
b. $x > 2 \Rightarrow x^2 > 4$
c. $x^2 > 4 \Rightarrow x > 2$
d. $x^2 > 4 \Leftrightarrow |x| > 2$

33. Sea **R** el dominio de la variables del predicado a, b, c y d. ¿Cuáles de los siguientes enunciados son verdaderos y cuáles son falsos? Presente contraejemplos para los enunciados que son falsos.
a. $a > 0$ y $b > 0 \Rightarrow ab > 0$
b. $a < 0$ y $b < 0 \Rightarrow ab < 0$
c. $ab = 0 \Rightarrow$ a $= 0$ o $b = 0$
d. $a < b$ y $c < d \Rightarrow ac < bd$

Respuestas del autoexamen

1. $\{x \in D \mid P(x)\}$, el conjunto de todas las x en D tal que $P(x)$ 2. *Posibles respuestas*: para todo, para cada, para cualquier, para cada uno, para un arbitrario, para cualquier dado. 3. *Posibles respuestas*: existen, existe, existe al menos un, para algún, al menos un, podemos encontrar un 4. verdadero, cada x en D (*respuesta alternativa:* toda x en D, cada una de las x en D) 5. verdadero, al menos una x en D (*respuesta alternativa:* alguna x en D)

3.2 Predicados y enunciados cuantificados II

PARRAGÓN: *Adelantaos, acariciaos el mentón y jurad por vuestras barbas que soy un granuja.*
CELIA: *Por nuestras barbas —si las tuviéramos— que lo eres.*
PARRAGÓN: *Por mi granujería —si la tuviera— entonces lo sería. Pero quien jura por lo que no hay, no jura en falso.* —William Shakespeare, *Como les guste*

En esta sección se continúa el análisis de los predicados y de los enunciados cuantificados que se inició en la Sección 3.1. Contiene las reglas de negación de los enunciados cuantificados, una exploración de la relación entre $\forall$, $\exists$, $\wedge$ y $\vee$, una introducción al concepto de la verdad vacía de los enunciados universales; ejemplos de variantes de los enunciados condicionales universales y una extensión del significado de *necesario*, *suficiente* y *sólo si* de los enunciados cuantificados.

Negaciones de enunciados cuantificados

Considere el enunciado "Todos los matemáticos usan lentes". Mucha gente diría que su negación es "Ningún matemático usa lentes", pero si aún un matemático no usa lentes, entonces, el arrollador enunciado que *todos* los matemáticos usan lentes es falso. Por tanto una negación correcta es "Hay al menos un matemático que no usa lentes".

La forma general de la negación de un enunciado universal es consecuencia inmediata de las definiciones de negación y de los valores de verdad de los enunciados universal y existencial.

Teorema 3.2.1 Negación de un enunciado universal

La negación de un enunciado de la forma

$$\forall x \text{ en } D,\ Q(x)$$

es lógicamente equivalente a un enunciado de la forma:

$$\exists x \text{ en } D \text{ tal que } \sim Q(x).$$

Simbólicamente, $\sim(\forall x \in D,\ Q(x)) \equiv \exists x \in D \text{ tal que } \sim Q(x)$.

Por tanto

> **La negación de un enunciado universal ("todos son") es lógicamente equivalente a un enunciado existencial ("algunos no son" o "hay al menos uno que no es").**

Observe que cuando hablamos de la **equivalencia lógica de los enunciados cuantificados**, queremos decir que los enunciados siempre tienen idénticos valores de verdad sin importar qué predicados se sustituyan por los símbolos de predicado y no importando qué conjuntos se utilicen para los dominios de las variables del predicado.

Consideremos ahora el enunciado "Algunos copos de nieve son iguales". ¿Cuál es su negación? Que este enunciado sea falso significa que ni un solo copo de nieve es igual a cualquier otro. En otras palabras, "Los copos de nieve no son iguales" o "Todos los copos de nieve son diferentes".

La forma general para la negación de un enunciado existencial se deduce inmediatamente de las definiciones de la negación y de los valores de verdad para enunciados existenciales y universales.

Teorema 3.2.2 Negación de un enunciado existencial

La negación de un enunciado de la forma

$$\exists x \text{ en } D \text{ tal que } Q(x)$$

es lógicamente equivalente a un enunciado de la forma

$$\forall x \text{ en } D,\ \sim Q(x).$$

Simbólicamente, $\sim(\exists x \in D \text{ tal que } Q(x)) \equiv \forall x \in D,\ \sim Q(x)$.

Por tanto

> **La negación de un enunciado existencial ("algunos están") es lógicamente equivalente a un enunciado universal ("ninguno está" o "no todos están").**

Ejemplo 3.2.1 Negación de enunciados cuantificados

Escriba negaciones formales de los siguientes enunciados:

a. ∀ primo p, p es impar.

b. ∃ un triángulo T tal que la suma de los ángulos de T es igual a 200°.

Solución

a. Aplicando la regla de la negación de un enunciado ∀, puede ver que la respuesta es

∃ un primo p tal que p no es impar.

b. Aplicando la regla de la negación de un enunciado ∃, se puede ver que la respuesta es

∀ triángulo T, la suma de los ángulos de T no es igual a 200°. ■

Se necesita tener especial cuidado para evitar errores al escribir negaciones de los enunciados que se dan de manera informal. Una forma de evitar el error es reescribir el enunciado formal y tomar la negación usando la regla formal.

Ejemplo 3.2.2 Más negaciones

Reescriba el siguiente enunciado formal. Después, escriba negaciones formales e informales.

Ningún político es honesto.

Solución

Versión formal: ∀ político x, x no es honesto.

Negación formal: ∃ un político x tal que x es honesto.

Negación informal: Algunos políticos son honestos. ■

Otra forma de evitar errores al tomar las negaciones de los enunciados que se presentan en lenguaje informal es preguntarse, "¿Qué significa *exactamente* que el enunciado dado es falso?" "¿Qué enunciado, si es verdadero, sería equivalente a decir que el enunciado dado es falso?"

Ejemplo 3.2.3 Aún más negaciones

Escribe negaciones informales para los enunciados siguientes:

a. Todos los programas de computadora son finitos.

b. Algunos hackers son mayores de 40.

c. El número 1 357 es divisible por un número entero entre 1 y 37.

Solución

a. ¿Qué significa exactamente que este enunciado es falso? El enunciado asegura que todos los programas de computadora satisfacen una determinada propiedad. Así que para que sea falso, tendría que haber al menos un programa de computadora que no cumpla la propiedad. Así, la respuesta es

Hay un programa de computadora que no es finito.

O: Algunos programas de computadora son infinitos.

b. Este enunciado es equivalente a decir que hay al menos un hacker con la propiedad dada. Así que para que sea falso, no hay un solo hacker que pueda tener esa propiedad. Así pues, la negación es

No hay hackers informáticos de más de 40.

O: Todos los hackers tienen 40 o menos.

Nota ¿Cuál es verdadero: el enunciado en el inciso *c*) o su negación? ¿Es 1 357 divisible entre algún entero entre 1 y 37? ¿O es 1 357 no divisible entre cualquier entero entre 1 y 37?

c. Este enunciado tiene un cuantificador de seguimiento. Escrito formalmente se convierte en:

∃ un número entero n entre 1 y 37 tal que 1 357 es divisible entre n.

Su negación es por tanto

∀ entero n entre 1 y 37; 1 357 no es divisible entre n.

Una versión informal de la negación es

El número 1 357 no es divisible por cualquier número entero entre 1 y 37. ■

¡Precaución! Insertar sólo la palabra *no* para negar un enunciado cuantificado puede dar como resultado un enunciado ambiguo.

Se pueden construir negaciones informales de muchos enunciados universales con sólo insertar la palabra *no* o las palabras *no es* en un lugar adecuado. Sin embargo, los enunciados resultantes pueden ser ambiguos. Por ejemplo, una posible negación de "Todos los matemáticos usan lentes" es "Todos los matemáticos no usan lentes". El problema es que esta frase tiene dos significados. Haciendo énfasis en la palabra *no*, se puede interpretar como negación lógica. (¡Qué! ¿Usted dice que todos los matemáticos usan lentes? ¡No tiene sentido! Todos los matemáticos *no* usan lentes). Por otra parte, si habla en tono monótono de voz (¡inténtelo!), esto significaría que todos los matemáticos no son usuarios de lentes; es decir, ni un solo matemático usa lentes. Este es un enunciado mucho más fuerte que la negación lógica: Implica la negación, pero no equivale a lo mismo.

Negaciones de enunciados condicionales universales

Las negaciones de enunciados condicionales universales son de especial importancia en matemáticas. La forma de dichas negaciones se puede deducir de hechos que ya se han establecido.

Por definición de la negación de un enunciado *para todos*,

$$\sim(\forall x,\ P(x) \to Q(x)) \equiv \exists x \text{ tal que } \sim(P(x) \to Q(x)). \qquad 3.2.1$$

Pero la negación de un enunciado si-entonces es lógicamente equivalente a un enunciado y. Más precisamente,

$$\sim(P(x) \to Q(x)) \equiv P(x) \wedge \sim Q(x). \qquad 3.2.2$$

Sustituyendo (3.2.2) en (3.2.1) se obtiene

$$\sim(\forall x,\ P(x) \to Q(x)) \equiv \exists x \text{ tal que } (P(x) \wedge \sim Q(x)).$$

Escrito menos simbólicamente, se convierte en

Negación de un enunciado condicional universal

$\sim(\forall x,$ si $P(x)$ entonces $Q(x)) \equiv \exists x$ tal que $P(x)$ y $\sim Q(x)$.

Ejemplo 3.2.4 Negación de enunciados condicionales universales

Escriba una negación formal del enunciado *a*) y una negación informal del enunciado *b*).

a. ∀ persona p, si p es rubio entonces p tiene los ojos azules.

b. Si un programa de computadora tiene más de 100 000 líneas, entonces tiene un error.

Solución

a. ∃ una persona p tal que p es rubio y p no tiene ojos azules.

b. Hay al menos un programa de computadora que tiene más de 100 000 líneas y no tiene un error. ■

La relación entre ∀, ∃, ∧ y ∨

La negación de un enunciado *para todo* es un enunciado *existe* y la negación de un enunciado *existe* es un enunciado *para todo*. Estos hechos son análogos a las leyes de De Morgan, que establecen que la negación de un enunciado y es un enunciado o y que la negación de un enunciado o es un enunciado y. Esta similitud no es casual. En cierto sentido, los enunciados universales son generalizaciones de enunciados y y los enunciados existenciales son generalizaciones de enunciados o.

Si $Q(x)$ es un predicado y el dominio D de x es el conjunto $\{x_1, x_2, \ldots, x_n\}$, entonces los enunciados

$$\forall x \in D,\ Q(x)$$

y

$$Q(x_1) \wedge Q(x_2) \wedge \cdots \wedge Q(x_n)$$

son lógicamente equivalentes. Por ejemplo, sea $Q(x)$ "$x \cdot x = x$" y supongamos $D = \{0,1\}$. Entonces,

$$\forall x \in D,\ Q(x)$$

Se puede reescribir como $\forall$ dígito binario x, $x \cdot x = x$.

Esto es equivalente a

$$0 \cdot 0 = 0 \quad \text{y} \quad 1 \cdot 1 = 1,$$

que se pueden reescribir simbólicamente como

$$Q(0) \wedge Q(1).$$

De manera similar, si $Q(x)$ es un predicado y $D = \{x_1, x_2, \ldots, x_n\}$, entonces los enunciados

$$\exists x \in D \text{ tal que } Q(x)$$

y

$$Q(x_1) \vee Q(x_2) \vee \cdots \vee Q(x_n)$$

son lógicamente equivalentes. Por ejemplo, sea $Q(x)$ "$x + x = x$" y supongamos $D = \{0,1\}$. Entonces,

$$\exists x \in D \text{ tal que } Q(x)$$

se puede reescribir como $\exists$ un dígito binario x tal que $x + x = x$.
Esto es equivalente a

$$0 + 0 = 0 \quad \text{o} \quad 1 + 1 = 1,$$

que se pueden reescribir simbólicamente como

$$Q(0) \vee Q(1).$$

Verdad vacía de los enunciados universales

Supongamos que se coloca un recipiente en una mesa y junto al recipiente está un montón de cinco bolas azules y cinco bolas de color gris, cualquiera de las cuales se pueden colocar en el recipiente. Si se colocan tres bolas azules y una bola gris en el recipiente, como se muestra en la figura 3.2.1*a*), el enunciado "Todas las bolas en el recipiente son de color azul" sería falso (puesto que una de las bolas en el recipiente es gris).

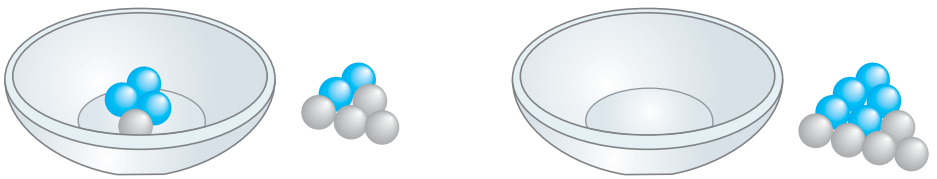
Ahora supongamos que no se colocan todas las bolas en el recipiente, como se muestra en la figura 3.2.1*b*). Considere el enunciado

Todas las bolas en el recipiente son de color azul.

¿Es este enunciado verdadero o falso? El enunciado es falso si y sólo si, su negación es verdadera. Y su negación es

Existe una bola en el recipiente que no es azul

Pero la única manera de que esta negación pueda ser verdadera es que de hecho haya una bola que no es azul en el recipiente. ¡Y no hay! Por tanto la negación es falsa, por lo que el enunciado es verdadero "por defecto".



a) *b)*

Figura 3.2.1

En general, un enunciado de la forma

$$\forall x \text{ en } D, \text{ si } P(x) \text{ entonces } Q(x)$$

se llama **vacíamente verdadero** o **verdadero por defecto** si y sólo si $P(x)$ es falso para toda x en D.

Por la forma, en el lenguaje común las palabras, *en general*, significan algo que regularmente es, aunque no siempre, el caso. (En general, yo tomo el autobús a casa, pero hoy caminé). En matemáticas, las palabras *en general* se utilizan de manera muy diferente. Cuando se presentan justo después del análisis de un ejemplo en particular (como en el párrafo anterior), son una señal de que lo que sigue es una generalización de algún aspecto del ejemplo que siempre es verdadero.

Variantes de los enunciados condicionales universales

Recordemos de la sección 2.2 que un enunciado condicional tiene un contrapositivo, un converso y un contrario. Las definiciones de estos términos se pueden extender a los enunciados condicionales universales.

• Definición

Considere un enunciado de la forma: $\forall x \in D$, si $P(x)$ entonces $Q(x)$.

1. Su **contrapositivo** es el enunciado: $\forall x \in D$, si $\sim Q(x)$, entonces $\sim P(x)$.
2. Su **converso** es el enunciado: $\forall x \in D$, si $Q(x)$, entonces $P(x)$.
3. Su **contrario** es el enunciado: $\forall x \in D$, si $\sim P(x)$, entonces $\sim Q(x)$.

Ejemplo 3.2.5 Contrapositivo, converso y contrario de un enunciado condicional universal

Escriba un enunciado formal y uno contrapositivo informal, converso e contrario del siguiente enunciado:

Si un número real es mayor que 2, entonces su cuadrado es mayor que 4.

Solución La versión formal de este enunciado es $\forall x \in \mathbf{R}$, si $x > 2$ entonces $x^2 > 4$.

Contrapositivo: $\forall x \in \mathbf{R}$, si $x^2 \leq 4$ entonces $x \leq 2$.
O: Si el cuadrado de un número real es menor o igual a 4, entonces el número es menor o igual a 2.

Converso: $\forall x \in \mathbf{R}$, si $x^2 > 4$ entonces $x > 2$.
O: Si el cuadrado de un número real es mayor que 4, entonces el número es mayor que 2.

Contrario: $\forall x \in \mathbf{R}$, si $x \leq 2$ entonces $x^2 \leq 4$.
O: Si un número real es menor o igual a 2, entonces el cuadrado del número es menor o igual a 4.

Observe que en la solución de este ejemplo, hemos utilizado la equivalencia de "$x \not> a$" y "$x \leq a$" para todos los números reales x y a. (Véase la página 33.) ■

En la sección 2.2, hemos demostrado que un enunciado condicional es lógicamente equivalente a su contrapositivo y que no es lógicamente equivalente a cualquiera de su converso o su contrario. El siguiente análisis muestra que estos hechos generalizan el caso de los enunciados condicionales universales y sus contrapositivos, conversos y sus contrarios.

Sea $P(x)$ y $Q(x)$ predicados cualesquiera, sea D el dominio de x y considere el enunciado

$$\forall x \in D, \text{ si } P(x) \text{ entonces } Q(x)$$

y su contrapositivo

$$\forall x \in D, \text{ si } \sim Q(x) \text{ entonces } \sim P(x).$$

Cualquier x dada en D que hace "si $P(x)$, entonces $Q(x)$" verdadero también hace verdadero a "si $\sim Q(x)$, entonces $\sim P(x)$" (por la equivalencia lógica entre $p \to q$ y $\sim q \to \sim p$). De lo que se deduce que la frase "Si $P(x)$, entonces $Q(x)$" es verdadera para toda x en D si y sólo si, la frase "Si $\sim Q(x)$, entonces $\sim P(x)$" es verdadera para toda x en D.

Por lo que se escribe lo siguiente y se dice que un enunciado condicional universal es lógicamente equivalente a su contrapositivo:

$$\forall x \in D, \text{ si } P(x), \text{ entonces } Q(x) \equiv \forall x \in D, \text{ si } \sim Q(x), \text{ entonces } \sim P(x)$$

En el ejemplo 3.2.5 se indicó que el enunciado

$$\forall x \in \mathbf{R}, \text{ si } x > 2 \text{ entonces } x^2 > 4$$

tiene el converso

$$\forall x \in \mathbf{R}, \text{ si } x^2 > 4 \text{ entonces } x > 2.$$

Observe que el enunciado es verdadero, mientras que su contrario es falso (ya que, por ejemplo $(-3)^2 = 9 > 4$, pero $-3 \not> 2$). Esto demuestra que un enunciado condicional universal puede tener un valor de verdad diferente de su converso. En consecuencia, un enunciado condicional universal no es lógicamente equivalente a su converso. Esto se escribe simbólicamente de la siguiente manera:

$$\forall x \in D, \text{ si } P(x), \text{ entonces } Q(x) \not\equiv \forall x \in D, \text{ si } Q(x), \text{ entonces } P(x).$$

En los ejercicios al final de esta sección, se le pide demostrar de manera similar que un enunciado condicional universal no es lógicamente equivalente a su contrario.

$$\forall x \in D, \text{ si } P(x), \text{ entonces } Q(x) \not\equiv \forall x \in D, \text{ si } \sim P(x), \text{ entonces } \sim Q(x).$$

Condiciones necesarias y suficientes, sólo si

Las definiciones de *necesario*, *suficiente* y *sólo si* se pueden también extender para aplicarse a los enunciados condicionales universales.

• Definición

- "$\forall x$, $r(x)$ es una **condición suficiente** para $s(x)$" significa "$\forall x$, si $r(x)$, entonces $s(x)$".
- "$\forall x$, $r(x)$ es una **condición necesaria** para $s(x)$" significa "$\forall x$, si $\sim r(x)$, entonces $\sim s(x)$" o, equivalentemente "$\forall x$, si $s(x)$, entonces $r(x)$".
- "$\forall x$, $s(x)$ **sólo si** $s(x)$" significa "$\forall x$, si $\sim s(x)$, entonces $\sim r(x)$" o, equivalentemente, "$\forall x$, si $r(x)$ entonces $s(x)$".

Ejemplo 3.2.6 Condiciones necesarias y suficientes

Reescriba los siguientes enunciados, como enunciados condicionales cuantificados. No utilice la palabra *necesario* o *suficiente*.

a. La forma cuadrada es una condición suficiente para la forma rectangular.

b. Tener al menos 35 años de edad es una condición necesaria para ser presidente de Estados Unidos.

Solución

a. Una versión formal del enunciado es

$\forall x$, si x es un cuadrado, entonces x es un rectángulo.

O, en lenguaje informal:

Si una figura es un cuadrado, entonces es un rectángulo.

b. Con un lenguaje formal, podría escribir la respuesta como

$\forall$ persona x, si x es menor de 35, entonces x no puede ser Presidente de Estados Unidos.

O, por la equivalencia entre un enunciado y su contrapositivo:

$\forall$ persona x, si x es el Presidente de Estados Unidos, entonces x tiene al menos 35 años de edad. ■

Ejemplo 3.2.7 Sólo si

Reescriba el siguiente enunciado como un enunciado universal condicional:

Un producto de dos números es 0 sólo si uno de los números es 0.

Solución Utilizando un lenguaje informal, podría escribir la respuesta como

Si ninguno de los dos números es 0, entonces el producto de los números no es 0.

O, por la equivalencia entre un enunciado y su contrapositivo,

Si un producto de dos números es 0, entonces uno de los números es 0. ■

Autoexamen

1. Una negación de "Toda R tiene la propiedad S" es "Existe____R que____".
2. Una negación de "Algún R tienen la propiedad S" es "____".
3. Una negación de "Para toda x, si x tiene la propiedad P, entonces x tiene la propiedad Q" es "____".
4. El converso de "Para toda x, si x tiene la propiedad P, entonces x tiene la propiedad Q" es "____".
5. El contrapositivo de "Para toda x, si x tiene la propiedad P, entonces x tiene la propiedad Q" es "____".
6. El contrario de "Para toda x, si x tiene la propiedad P, entonces x tiene la propiedad Q" es "____".

Conjunto de ejercicios 3.2

1. ¿Cuáles de los siguientes enunciados es una negación de "Todos los estudiantes de matemáticas discretas son atléticos"? Más de una respuesta puede ser correcta.

a. Hay un estudiante de matemáticas discretas que es no atlético.
b. Todos los estudiantes de matemáticas discretas son no atléticos.
c. Hay una persona atlética, que es un estudiante de matemáticas discretas.
d. Ningún estudiante de matemáticas discretas es atlético.
e. Algunos estudiantes de matemáticas discretas no son atléticos.
f. Ninguna persona atlética es estudiante de matemáticas discretas.

2. Cuáles de los siguientes enunciados es una negación para ¿"Todos los perros son leales"? Más de una respuesta puede ser correcta.
   a. Todos los perros son desleales. b. Ningún perro es leal.
   c. Algunos perros son desleales.
   d. Algunos perros son leales.
   e. Hay un animal desleal que no es un perro.
   f. Hay un perro que es desleal.
   g. Ningún animal que no sea perro es leal.
   h. Algunos animales que no son perros son leales.

3. Escriba una negación formal de cada uno de los siguientes enunciados:
   a. ∀ pez x, x tiene agallas.
   b. ∀ computadora c, c tiene una CPU.
   c. ∃ una película m tal que m es de más de 6 horas de duración.
   d. ∃ una banda b tal que b ha ganado al menos 10 premios Grammy.

4. Escriba una negación informal para cada uno de los siguientes enunciados. Tenga cuidado para evitar negaciones ambiguas.
   a. Todos los perros son amigables.
   b. Todas las personas son felices.
   c. Algunas sospechas eran fundadas.
   d. Algunas estimaciones son exactas.

5. Escriba una negación de cada uno de los siguientes enunciados.
   a. Cualquier argumento válido tiene una conclusión verdadera.
   b. Cada número real es positivo, negativo o cero.

6. Escriba una negación de cada uno de los enunciados siguientes.
   a. Los conjuntos A y B no tienen ningún punto en común.
   b. Los pueblos P y Q no están conectados por una carretera en el mapa.

7. El lenguaje informal es en realidad más complejo que el lenguaje formal. Por ejemplo, la frase "No hay pedidos de la tienda A del artículo B" contiene la palabra *hay*. ¿Es un enunciado existencial? Escriba una negación informal del enunciado y después escriba el enunciado formal usando cuantificadores y variables.

8. Considere el enunciado "No hay soluciones simples para los problemas de la vida". Escriba una negación informal del enunciado y después escriba el enunciado formalmente usando cuantificadores y variables.

Escriba una negación para cada uno de los enunciados 9 y 10.

9. ∀ número real x, si $x > 3$, entonces $x^2 > 9$.

10. ∀ programa de computadora P, si P se compila sin mensajes de error, entonces P es correcto.

En cada uno de los ejercicios del 11 al 14 determine si la negación propuesta es correcta. Si no lo es, escriba una negación correcta.

11. *Enunciado:* La suma de dos números irracionales es irracional.
Negación propuesta: La suma de dos números irracionales es racional.

12. *Enunciado:* El producto de cualquier número irracional y cualquier número racional es irracional.
Negación propuesta: El producto de cualquier número irracional y cualquier racional es un número racional.

13. *Enunciado:* Para todo entero n, si n^2 es par entonces n es par.
Negación propuesta: Para todos los enteros n, si n^2 es par entonces n no es par.

14. *Enunciado:* Para todos los números reales x_1 y x_2, si $x_1^2 = x_2^2$ entonces $x_1 = x_2$.
Negación propuesta: Para todos los números reales x_1 y x_1, si $x_1^2 = x_2^2$ entonces $x_1 \neq x_2$.

15. Sea $D = \{-48, -14, -8, 0, 1, 3, 16, 23, 26, 32, 36\}$. Determine cuáles de los siguientes enunciados son verdaderos y cuáles son falsos. Proporcione contraejemplos para los enunciados que son falsos.
   a. $\forall x \in D$, si x es impar, entonces $x > 0$.
   b. $\forall x \in D$, si x es menor que 0 entonces x es par.
   c. $\forall x \in D$, si x es par, entonces $x \leq 0$.
   d. $\forall x \in D$, si el dígito de las unidades de x es 2, entonces el dígito de las decenas es 3 o 4.
   e. $\forall x \in D$, si el dígito de las unidades de x es 6, entonces el dígito de las decenas es 1 o 2.

En los ejercicios del 16 al 23, escriba una negación de cada enunciado.

16. ∀ número real x, si $x^2 \geq 1$ entonces $x > 0$.

17. ∀ entero d, si $6/d$ es un entero entonces $d = 3$.

18. $\forall x \in \mathbf{R}$, si $x(x+1) > 0$ entonces $x > 0$ o $x < -1$.

19. $\forall n \in \mathbf{Z}$, si n es primo entonces n es impar o $n = 2$.

20. ∀ entero a, b y c, si $a - b$ es par y $b - c$ es par, entonces $a - c$ es par.

21. ∀ entero n, si n es divisible entre 6, entonces n es divisible entre 2 y n es divisible entre 3.

22. Si el cuadrado de un número entero es impar, entonces el entero es impar.

23. Si una función es derivable entonces es continua.

24. Reescriba los enunciados de cada par en la forma si-entonces e indique la relación lógica entre ellos.
   a. Todos los niños en la familia de Tom son mujeres. Todas las mujeres en la familia de Tom son niños.
   b. Todos los números enteros que son mayores de 5 y que terminan en 1, 3, 7 o 9 son primos.
   Todos los números enteros que son mayores de 5 y que son primos terminan en 1, 3, 7 o 9.

25. Cada uno de los siguientes enunciados es verdadero. En cada caso escriba el converso del enunciado y de un contraejemplo que muestre que el converso es falso.
   a. Si n es cualquier número primo mayor que 2, entonces $n + 1$ es par.
   b. Si m es un entero impar, entonces $2m$ es par.
   c. Si dos circunferencias se cortan en exactamente dos puntos, entonces no tienen un centro común.

En los ejercicios del 26 al 33, para cada enunciado en el ejercicio escriba el converso, el contrario y el contrapositivo. Indique lo mejor que pueda cuáles entre el enunciado, su converso, contrario y contrapositivo son verdaderos y cuáles son falsos. Dé un contraejemplo para cada uno, que sea falso.

26. Ejercicio 16 27. Ejercicio 17

28. Ejercicio 18 29. Ejercicio 19

30. Ejercicio 20 31. Ejercicio 21

32. Ejercicio 22 33. Ejercicio 23

34. Escriba el contrapositivo de cada uno de los siguientes enunciados.
   a. Si n es primo, entonces n no es divisible entre cualquier número primo entre 1 y $\sqrt{n}$ en sentido estricto. (Suponga que n es un entero fijo que es mayor que 1.)
   b. Si A y B no tienen elementos en común, entonces son disjuntos. (Suponga que A y B son conjuntos fijos.)

35. Dé un ejemplo para demostrar que un enunciado condicional universal no es lógicamente equivalente a su contrario.

✶36. Si $P(x)$ es un predicado y el dominio de x es el conjunto de todos los números reales, sea R "$\forall x \in \mathbf{Z}$, $P(x)$", sea S "$\forall x \in \boldsymbol{Q}$, $P(x)$" y sea T "$\forall\, x \in \mathbf{R}$, $P(x)$".
   a. Determine una definición de $P(x)$ (pero no use "$x \in \mathbf{Z}$") tal que R es verdadero y tanto S como T son falsos.
   b. Encuentre una definición de $P(x)$ (pero no use "$x \in \mathbf{Q}$") de modo que R y S son verdaderos y T es falso.

37. Considere la siguiente secuencia de dígitos: 0204. Una persona afirma que todos los 1 en la secuencia están a la izquierda de todos los 0 en la secuencia. ¿Es esto verdadero? Justifique su respuesta. (*Sugerencia:* Escriba la afirmación formal y escriba una negación formal de que la negación es verdadera o falsa?)

38. ¿Verdadero o falso? Todas las ocurrencias de la letra u en Matemática Discreta están en minúsculas. Justifique su respuesta.

Reescriba cada enunciado de los ejercicios 39 al 42 en la forma si-entonces.

39. La obtención de una calificación de C en este curso es una condición suficiente para que lo apruebe.

40. El ser divisible entre 8 es una condición suficiente para ser divisible entre 4.

41. Llegar a tiempo cada día es una condición necesaria para conservar este trabajo.

42. Aprobar un examen completo es una condición necesaria para la obtención de un título de maestría.

Utilice los hechos de que la negación de un enunciado $\forall$ es un enunciado $\exists$ y de que la negación de un enunciado si-entonces es un enunciado *y*, para reescribir cada uno de los enunciados de los ejercicios 43 al 46 sin usar la palabra *necesario* o *suficiente*.

43. El ser divisible entre 8 no es una condición necesaria para ser divisible entre 4.

44. Tener un gran ingreso no es una condición necesaria para que una persona sea feliz.

45. Tener un gran ingreso no es una condición suficiente para que una persona sea feliz.

46. Ser un polinomio no es una condición suficiente para que una función tenga una raíz real.

47. Los científicos computacionales Richard Conway y David Gries escribieron una vez:

> La ausencia de mensajes de error en la ejecución de un programa de computadora es sólo una condición necesaria y no una condición suficiente para la corrección razonable [del programa].

Reescriba este enunciado sin usar las palabras *necesario* o *suficiente*.

48. Un folleto de un club de viajeros frecuentes dice: "Usted puede seleccionar entre compañías aéreas sólo si ofrecen lo mismo al precio más bajo". Suponiendo que "sólo si" tiene su significado formal, lógico, ¿este enunciado garantiza de que si dos compañías ofrecen la misma tarifa más baja, el cliente tendrá la libertad de elegir entre ellos? Explique.

Respuestas del autoexamen

1. alguno (*respuestas alternativas*: al menos uno, a), no tiene la propiedad S. 2. Ninguna R tiene la propiedad S. 3. Hay un x tal que x tiene la propiedad P y x no tiene la propiedad Q. 4. Para toda x, si x tiene la propiedad Q, entonces x tiene la propiedad P. 5. Para toda x, si x no tiene la propiedad Q, entonces x no tiene la propiedad P. 6. Para toda x, si x no tiene la propiedad P, entonces x no tiene la propiedad P.

3.3 Enunciados con cuantificadores múltiples

No es suficiente tener una buena mente. Lo principal es usarla bien. —René Descartes

Imagínese que usted está visitando una fábrica que produce microchips. La guía de la fábrica le dice,

> Hay una persona que supervisa todos los detalles del proceso de producción.

Observe que este enunciado contiene versiones informales tanto del cuantificador existencial *hay* como del cuantificador universal *cada*. ¿Cuál de las siguientes opciones describe mejor su significado?

- Hay una sola persona que supervisa todos los detalles del proceso de producción.
- Para cualquier detalle de la producción en particular, hay una persona que supervisa ese detalle, pero podría haber diferentes supervisores de diferentes detalles.

Si esto pasa, su interpretación podría ser como dice la guía. (¡Vuelva a leer la frase para asegurarse de que está de acuerdo!) Dígase a sí mismo, su enunciado es realmente ambiguo, aunque él pudo haber dicho otras cosas que (el contexto de su enunciado) podrían aclarar. En nuestra vida cotidiana, todo el tiempo nos ocupamos de este tipo de ambigüedad. En general, el contexto ayuda a resolverlo, pero a veces simplemente entendemos mal.

Por el contrario, en matemáticas, en lógica formal y en ciencia computacional, es esencial que interpretemos los enunciados exactamente de la misma manera. Por ejemplo, la etapa inicial de desarrollo de software normalmente implica un análisis cuidadoso entre un analista programador y un cliente para convertir descripciones vagas en lo que el cliente quiere, en especificaciones de un programa inequívoco en el que cliente y programador concuerdan mutuamente.

Debido a que muchos enunciados técnicamente importantes contienen tanto a $\exists$ como a $\forall$, se ha desarrollado una convención para su interpretación uniforme. Cuando un enunciado contenga más de un cuantificador, imaginamos que las acciones sugeridas por los cuantificadores que se realizan en el orden en que ocurren los cuantificadores. Por ejemplo, considere una enunciado de la forma

$\forall x$ en el conjunto D, $\exists y$ en el conjunto E tal que x y y satisfacen la propiedad $P(x, y)$.

Para demostrar que tal enunciado es verdadero, debe ser capaz de afrontar el reto siguiente:

- Imagine que a alguien se le permite elegir cualquier elemento que sea del conjunto D e imagine que la persona le da ese elemento. Llámelo x.
- El reto para usted es encontrar un elemento y en E, para que la persona x y su y, en conjunto, satisfagan la propiedad $P(x, y)$.

Observe que ***debido a que no es necesario especificar la y hasta después de que la otra persona ha especificado la x, se le permite encontrar un valor diferente de y para cada x diferente que le den.***

Ejemplo 3.3.1 Verdad de un enunciado ∀∃ en un mundo de Tarski

Considere el mundo de Tarski que se muestra en la figura 3.3.1.

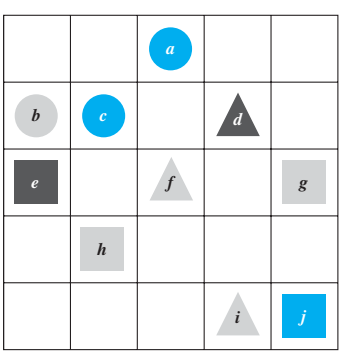


Figura 3.3.1

Demuestre que el siguiente enunciado es verdadero en este mundo:

Para todos los triángulos x, hay una cuadrado y tal que x y y tienen el mismo color.

Solución El enunciado dice que no importa quién le dé el triángulo, podrá encontrar un cuadrado del mismo color. Sólo hay tres triángulos, d, f e i. La siguiente tabla muestra que para cada uno de estos triángulos se puede encontrar un cuadrado del mismo color.

Dado $x =$	elija $y =$	y compruebe que y es del mismo color que x.
d	e	sí ✓
f o i	h o g	sí ✓

Ahora considere un enunciado que contenga tanto a ∀ como a ∃, donde ∃ se coloca antes de ∀:

$$\exists \text{ un } x \text{ en } D \text{ tal que } \forall y \text{ en } E,\ x \text{ y } y \text{ satisfagan la propiedad } P(x, y).$$

Para demostrar que un enunciado de esta forma es verdadero:

Usted debe encontrar un solo elemento (llámelo x) en D, con la siguiente propiedad:

- Después de haber encontrado su x, se le permite a alguien elegir cualquier elemento de E. La persona que lo reta le da ese elemento. Llámelo y.
- Su trabajo es mostrar que su x junto con la y de la persona satisfacen la propiedad $P(x, y)$.

Observe que x tiene que trabajar para cualquier y que la persona le da: ***no se le permite cambiar la x una vez que la haya especificado inicialmente***.

Ejemplo 3.3.2 Verdad de un enunciado ∃∀ en un mundo de Tarski

Consideremos de nuevo el mundo de Tarski en la figura 3.3.1. Demuestre que el enunciado siguiente es verdadero: Hay un triángulo x tal que para todos los círculos y, x está a la derecha de y.

Solución El enunciado dice que usted puede encontrar un triángulo que esté a la derecha de todos los círculos. En realidad, ya sea d o i funcionaría para todos los tres círculos, a, b y c, como se puede ver en la siguiente tabla.

Elija $x =$	Entonces, dado, $y =$	compruebe que x está a la derecha de y.
d o i	a	sí ✓
	b	sí ✓
	c	sí ✓

A continuación se presenta un resumen de la convención para interpretar los enunciados de dos cuantificadores diferentes:

Interpretación de enunciados con dos cuantificadores diferentes

Si desea establecer la verdad de un enunciado de la forma

$$\forall x \text{ en } D,\ \exists y \text{ en } E \text{ tal que } P(x, y)$$

su reto es permitir que otra persona elija cualquier elemento x en D que deseen y después usted debe encontrar un elemento y en E que "funcione" para un x dado.

Si desea establecer la verdad de un enunciado de la forma

$$\exists x \text{ en } D \text{ tal que } \forall y \text{ en } E,\ P(x, y)$$

su trabajo es encontrar un x dado en D que va a "funcionar" no importa cuál y en E podrían elegir para retarlo.

Ejemplo 3.3.3 Interpretación de enunciados con cuantificadores múltiples*

Una línea de cafetería de la escuela cuenta con cuatro puestos: ensaladas, platos principales, postres y bebidas. El puesto de ensaladas ofrece una selección de ensaladas verdes o ensaladas de frutas, el puesto de platos principales ofrece espagueti o pescado, el puesto de postres ofrece postre pay o pastel y el puesto de bebidas ofrece la leche, refresco o café. Tres estudiantes, Uta, Tim y Yuen, pasan por la cola y toman las siguientes decisiones:

Uta: ensalada verde, espagueti, pay, leche

Tim: ensalada de frutas, pescado, pay, pastel, leche, café

Yuen: espagueti, pescado, pay, refresco

En la figura 3.3.2 se muestran estas opciones.

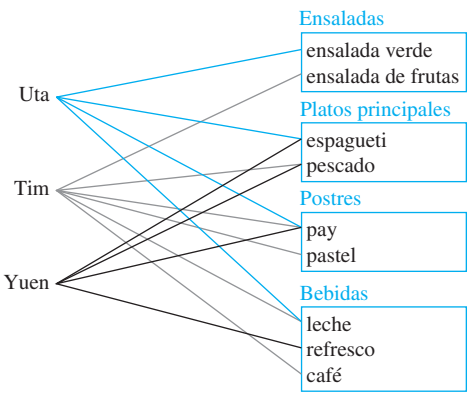


Figura 3.3.2

Escriba cada uno de los siguientes enunciados de manera informal y determine su valor de verdad.

a. $\exists$ un platillo I tal que $\forall$ estudiante S, S eligió I.

b. $\exists$ un estudiante S tal que $\forall$ platillo I, S escogió I.

c. $\exists$ un estudiante S tal que $\forall$ los puestos Z, $\exists$ un platillo I en Z tal que S eligió I.

d. $\forall$ estudiante S y $\forall$ puesto Z, $\exists$ un platillo I en Z tal que S eligió I.

Solución

a. Hay un platillo que fue elegido por cada estudiante. Esto es verdadero, todo alumno eligió pay.

b. Hay un estudiante que eligió todos los platillos disponibles. Esto es falso, ningún alumno eligió los nueve platillos.

c. Hay un estudiante que eligió al menos un platillo de cada puesto. Esto es cierto, tanto Uta como Tim eligieron por lo menos un elemento de cada puesto.

d. Cada estudiante eligió por lo menos un platillo de cada puesto. Esto es falso; Yuen no eligió una ensalada. ■

*El término "cuantificadores múltiples" se pronuncia MÚL-ti-ples CUAN-ti-fi-ca-do-res. Un enunciado con cuantificadores múltiples es un enunciado que contiene más de un cuantificador.

Traducción del lenguaje informal al formal

La mayoría de problemas se expresan en un lenguaje informal, pero la solución de ellos con frecuencia requiere que se traduzca a términos más formales.

Ejemplo 3.3.4 Traducción de enunciados con cuantificadores múltiples del lenguaje informal al formal

El **recíproco** de un número real a es un número real b tal que $ab = 1$. Los siguientes dos enunciados son verdaderos. Reescríbalos formalmente usando cuantificadores y variables:

a. Todo número real distinto de cero tiene un recíproco.

b. Hay un número real, sin recíproco. El número 0 no tiene recíproco.

Solución

a. $\forall$ número real distinto de cero u, $\exists$ un número real tal que $uv = 1$.

b. $\exists$ un número real c tal que $\forall$ número real d, $cd \neq 1$. ■

Ejemplo 3.3.5 Hay un entero positivo más pequeño

Recuerde que todo entero es un número real y que los números reales son de tres tipos: positivos, negativos y cero (cero que ni es positivo ni negativo). Considere el enunciado "Hay un entero positivo más pequeño". Escriba este enunciado formal utilizando los símbolos $\exists$ y $\forall$.

Solución Decir que hay un entero positivo más pequeño significa que existe un entero positivo m con la propiedad que no importa qué entero positivo n podría elegir una persona, m va a ser menor o igual a n:

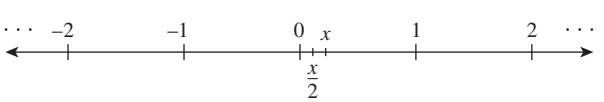
$$\exists \text{ un entero positivo } m \text{ tal que } \forall \text{ entero positivo } n,\ m \leq n.$$

Observe que este enunciado es verdadero ya que 1 es un entero positivo que es menor o igual a cada número entero positivo.

■

Ejemplo 3.3.6 No hay número real positivo más pequeño

Imagine cualquier número real positivo x en la recta numérica real. Estos números corresponden a todos los puntos a la derecha de 0. Observe que no importa lo pequeño que sea x, el número $x/2$ será a la vez positivo y menor que x.*



*Esto se puede deducir de las propiedades de los números reales que se presentan en el apéndice A. Ya que x es positivo, $0 < x$. Sume x en ambos lados para obtener $x < 2x$. Entonces, $0 < x < 2x$. Ahora se multiplican todas las partes de la desigualdad por el número positivo $1/2$. Esto no cambia la dirección de la desigualdad, por lo que $0 < x/2 < x$.

Por lo que el siguiente enunciado es verdadero: "No hay un número real positivo más pequeño". Este enunciado se escribe formalmente utilizando los símbolos ∀ y ∃.

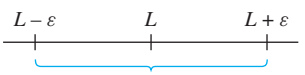
Solución ∀ número real positivo x, ∃ un número real positivo y tal que $y < x$. ■

Ejemplo 3.3.7 La definición de límite de una sucesión

La definición de límite de una sucesión, que se estudia en cálculo, utiliza dos cuantificadores ∀ y ∃ y también si-entonces. Decimos que el límite de la sucesión a_n cuando n tiende a infinito es igual a L y se escribe

$$\lim_{n\to\infty} a_n = L$$

si y sólo si, los valores de a_n están *arbitrariamente* cerca de L conforme n se hace más y más grande sin límite. Más precisamente, esto significa que dado cualquier número positivo ε, podemos encontrar un entero N tal que cuando n es mayor que N, el número a_n se encuentra entre $L - \varepsilon$ y $L + \varepsilon$ en la recta numérica.



a_n se debe encontrar aquí cuando $n > N$

Simbólicamente:

$$\forall \varepsilon > 0, \exists \text{ un entero } N \text{ tal que } \forall \text{ entero } n,$$
$$\text{si } n > N \text{ entonces } L - \varepsilon < a_n < L + \varepsilon.$$

Considerando la complejidad lógica de esta definición, no es de extrañar que a muchos estudiantes les resulta difícil entenderla. ■

Lenguaje ambiguo

El dibujo de la figura 3.3.3 es un famoso ejemplo de ambigüedad visual. Cuando nos fijamos en él por un tiempo, es probable que vea o una silueta de una mujer joven que llevaba un gran sombrero o de una mujer mayor con una gran nariz. Cualquier imagen

Figura 3.3.3

aparecerá primero en su mente, intente ver cómo se puede interpretar el dibujo de otra manera. (*Sugerencia*: La boca de la anciana es el collar de la joven.)

Una vez que la mayoría de la gente ve una de las imágenes, es difícil para ellos percibir la otra. Lo mismo sucede con el lenguaje ambiguo. Una vez que interpretó la frase del principio de esta sección de una manera, puede haber sido difícil para usted ver que se podía entender de otra forma. Tal vez tuvo dificultades a pesar de que se explican los dos posibles significados, al igual que muchas personas tienen dificultad para ver la segunda interpretación en el dibujo, aún cuando se les dice lo que deben buscar.

A pesar de que los enunciados escritos de manera informal pueden estar abiertos a múltiples interpretaciones, no podemos determinar su veracidad o falsedad, sin interpretarlos de una manera u otra. Por tanto, tenemos que usar el contexto para tratar de averiguar su significado lo mejor que podamos.

Negaciones de enunciados con cuantificadores múltiples

Puede utilizar las mismas reglas para negar los enunciados con los cuantificadores múltiples que utilizó para negar los enunciados con cuantificadores más simples. Recuerde que

$$\sim(\forall x \text{ en } D,\ P(x)) \equiv \exists x \text{ en } D \text{ tal que } \sim P(x).$$

y

$$\sim(\exists x \text{ en } D \text{ tal que } P(x)) \equiv \forall x \text{ en } D,\ \sim P(x).$$

Se aplican estas leyes para encontrar

$$\sim(\forall x \text{ en } D,\ \exists y \text{ en } E \text{ tal que } P(x, y))$$

al pasar por etapas de izquierda a derecha a lo largo de la frase.

Primera versión de la negación: $\exists x$ en D tal que $\sim(\exists y$ en E tal que $P(x, y))$.
Versión final de la negación: $\exists x$ en D tal que $\forall y$ en E, $\sim P(x, y)$.

Del mismo modo, para encontrar

$$\sim(\exists x \text{ en } D \text{ tal que } \forall y \text{ en } E,\ P(x, y)),$$

tenemos

Primera versión de la negación: $\forall x$ en D, $\sim(\forall y$ en E, $P(x, y))$.
Versión final de la negación: $\forall x$ en D, $\exists y$ en E tal que $\sim P(x, y)$.

Estos hechos se pueden resumir de la siguiente manera:

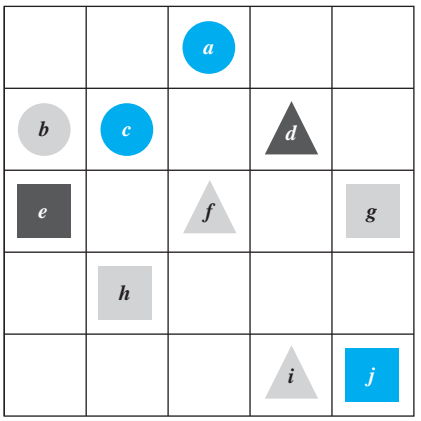
Negaciones de enunciados con cuantificadores múltiples

$\sim(\forall x \text{ en } D,\ \exists y \text{ en } E \text{ tal que } P(x, y)) \equiv \exists x \text{ en } D \text{ tal que } \forall y \text{ en } E,\ \sim P(x, y).$

$\sim(\exists x \text{ en } D \text{ tal que } \forall y \text{ en } E,\ P(x, y)) \equiv \forall x \text{ en } D,\ \exists y \text{ en } E \text{ tal que } \sim P(x, y).$

Ejemplo 3.3.8 Negación de enunciados en un mundo de Tarski

Consulte la figura 3.3.1 del mundo de Tarski, que se reimprime aquí para referencia.



Escriba una negación de cada uno de los siguientes enunciados y determine cuál es verdadero, el enunciado dado o su negación.

a. Para todos los cuadrados x, hay un círculo y tal que x y y tienen el mismo color.

b. Hay un triángulo x tal que para todos los cuadrados y, x está a la derecha de y.

Solución

a. *Primera versión de la negación:* ∃ un cuadrado x tal que ∼(∃ un círculo y tal que x y y tienen el mismo color).

Versión final de la negación: ∃ un cuadrado x tal que ∀ círculo y, x y y no tienen el mismo color.

La negación es verdadera. El cuadrado e es de color negro y el no círculo es de color negro, por lo que es un cuadrado que no tiene el mismo color que cualquier círculo.

b. *Primera versión de la negación:* ∀ triángulo x, ∼(∀ cuadrado y, x está a la derecha de y).

Versión final de la negación: ∀ triángulo x, ∃ un cuadrado y tal que x no está a la derecha de y.

La negación es verdadera porque no importa qué triángulo se elija, no está a la derecha del cuadrado g (o un cuadrado j). ■

Orden de cuantificadores

Considere los siguientes dos enunciados:

∀ gente x, ∃ una persona y tal que x ama y.

∃ una persona y tal que ∀ gente x, x ama y.

Note que excepto por el orden de los cuantificadores, estos enunciados son idénticos. Sin embargo, el primero significa que, dada cualquier persona, es posible encontrar a alguien a quien esa persona ama, mientras que el segundo significa que hay una persona asombrosa que es amada por todas las personas. (¡Vuelve a leer los enunciados con cuidado para comprobar estas interpretaciones!) Las dos frases muestran una propiedad muy importante de los enunciados con cuantificadores múltiples:

¡Precaución! Si un enunciado tiene dos cuantificadores diferentes, al invertir su orden podemos cambiar el valor de verdad del enunciado en su opuesto.

En un enunciado que contiene tanto a ∀ como a ∃, al cambiar el orden de los cuantificadores generalmente se cambia el significado del enunciado.

Sin embargo, curiosamente, si un cuantificador se encuentra inmediatamente después de otro cuantificador *del mismo tipo*, entonces el orden de los cuantificadores no afecta el significado. Considere la propiedad conmutativa de la suma de números reales, por ejemplo:

$$\forall \text{ número real } x \text{ y } \forall \text{ número real } y,\ x + y = y + x.$$

Esto significa lo mismo que

$$\forall \text{ número real } y \text{ y } \forall \text{ número real } x,\ x + y = y + x.$$

Así, la propiedad se puede expresar más brevemente como

$$\forall \text{ números reales } x \text{ y } y,\ x + y = y + x.$$

Ejemplo 3.3.9 Cuantificador de orden en un mundo de Tarski

Observe de nuevo la figura 3.3.1 del mundo de Tarski. ¿Los siguientes dos enunciados tienen el mismo valor de verdad?

a. Por cada cuadrado x hay un triángulo y tal que x y y tienen colores diferentes.

b. Existe un triángulo y tal que para cada cuadrado x, x y y tienen colores diferentes.

Solución El enunciado *a*) dice que si alguien le da uno de los cuadrados del mundo de Tarski, usted puede encontrar un triángulo que tenga un color diferente. Esto es verdadero. Si alguien le da un cuadrado g o h (que son de color gris), puede utilizar el triángulo d (que es negro), si alguien le da un cuadrado e (que es negro), puede utilizar cualquier triángulo el f o el i (que son grises ambos) y si alguien le da un cuadrado j (que es de color azul), puede utilizar un triángulo d (que es negro) o un triángulo f o i (que son grises).

El enunciado *b*) dice que hay un triángulo particular en el mundo de Tarski que tiene un color diferente en cada uno de los cuadrados del mundo. Esto es falso. Dos de los triángulos son de color gris, pero no se pueden utilizar para mostrar la verdad del enunciado porque el mundo de Tarski tiene cuadrados grises. El único otro triángulo es negro, pero no se puede utilizar porque hay un cuadrado negro en el mundo de Tarski.

Así, uno de los enunciados es verdadero y el otro es falso; por lo que tienen valores de verdad opuestos. ■

Notación lógica formal

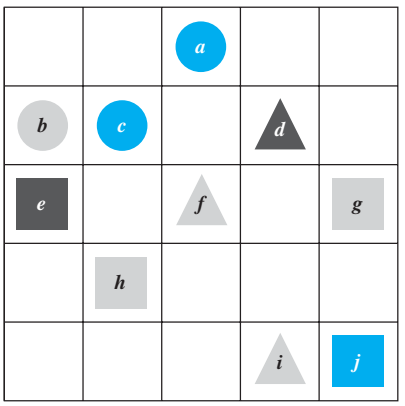
En algunas áreas de la ciencia computacional, los enunciados lógicos se expresan en notación puramente simbólica. La notación implica el uso de predicados para describir todas las propiedades de las variables y omitir las palabras *tal que* en los enunciados existenciales. (Sin embargo, cuando trate de averiguar el significado de un enunciado formal, es útil que piense en las palabras *tal que* cada vez que sean adecuadas.) El formalismo también depende de los siguientes hechos:

"$\forall x$ en D, $P(x)$" se puede escribir como "$\forall x(x \text{ en } D \rightarrow P(x))$" y
"$\exists x$ en D tal que $P(x)$" se puede escribir como "$\exists x(x \text{ en D} \wedge P(x))$".

El uso de estos hechos se ilustra en el ejemplo 3.3.10.

Ejemplo 3.3.10 Formalización de enunciados en un mundo de Tarski

Considere una vez más el mundo de Tarski de la figura 3.3.1:



Sea Triángulo(x), Círculo(x) y Cuadrado(x) significa "x es un triángulo", "x es un círculo" y "x es un cuadrado", sean Azul(x), Gris(x) y Negro(x) que signifiquen "x es azul", "x es gris" y "x es negro", sean DerechaDe(x, y), Arriba(x, y) y MismoColorQue(x, y) que signifiquen "x está a la derecha de y", "x está arriba de y" y "x tiene el mismo color que y" y utilice de la notación $x = y$ para denotar el predicado "x es igual a y". Sea el dominio común D de todas las variables como el conjunto de todos los objetos en el mundo de Tarski. Utilice notación formal y lógica para escribir cada uno de los enunciados siguientes y escriba una negación formal de cada enunciado.

a. Para todos los círculos x, x está arriba de f.

b. Hay un cuadrado x tal que x es negro.

c. Para todos los círculos x, hay un cuadrado y tal que x y y tienen el mismo color.

d. Hay un cuadrado x tal que para todos los triángulos y, x está a la derecha de y.

Solución

a. *Enunciado*: $\forall x(\text{Círculo}(x) \rightarrow \text{Arriba}(x, f))$.
Negación: $\sim(\forall x(\text{Círculo}(x) \rightarrow \text{Arriba}(x, f)))$

$$\equiv \exists x \sim (\text{Círculo}(x) \rightarrow \text{Arriba}(x, f))$$
por la ley de negación de un enunciado $\forall$

$$\equiv \exists x(\text{Círculo}(x) \wedge \sim\text{Arriba}(x, f))$$
por la ley de la negación de un enunciado si-entonces

b. *Enunciado*: $\exists x(\text{Cuadrado}(x) \wedge \text{Negro}(x))$.
Negación: $\sim(\exists x(\text{Cuadrado}(x) \wedge \text{Negro}(x)))$

$$\equiv \forall x \sim (\text{Cuadrado}(x) \wedge \text{Negro}(x))$$
por la ley de la negación de un enunciado $\exists$

$$\equiv \forall x\ (\sim\text{Cuadrado}(x) \vee \sim\text{Negro}(x))$$
por la ley de De Morgan

c. *Enunciado:* $\forall x(\text{Círculo}(x) \rightarrow \exists y(\text{Cuadrado}(y) \wedge \text{MismoColor}(x, y)))$.
Negación: $\sim(\forall x(\text{Círculo}(x) \rightarrow \exists y(\text{Cuadrado}(y) \wedge \text{MismoColor}(x, y))))$

$$\equiv \exists x \sim (\text{Círculo}(x) \rightarrow \exists y(\text{Cuadrado}(y) \wedge \text{MismoColor}(x, y)))$$
por la ley de negación de un enunciado $\forall$

$$\equiv \exists x(\text{Círculo}(x) \wedge \sim(\exists y(\text{Cuadrado}(y) \wedge \text{MismoColor}(x, y))))$$
por la ley de negación de un enunciado si-entonces

$$\equiv \exists x(\text{Círculo}(x) \wedge \forall y(\sim(\text{Cuadrado}(y) \wedge \text{MismoColor}(x, y))))$$
por la ley de negación de un enunciado ∃

$$\equiv \exists x(\text{Círculo}(x) \wedge \forall y(\sim\text{Cuadrado}(y) \vee \sim\text{MismoColor}(x, y)))$$
por la ley de De Morgan

d. *Enunciado:* $\exists x(\text{Cuadrado}(x) \wedge \forall y(\text{Triángulo}(y) \rightarrow \text{DerechaDe}(x, y)))$.
Negación: $\sim(\exists x(\text{Cuadrado}(x) \wedge \forall y(\text{Triángulo}(y) \rightarrow \text{DerechaDe}(x, y))))$.

$$\equiv \forall x \sim (\text{Cuadrado}(x) \wedge \forall y(\text{Triángulo}(x) \rightarrow \text{DerechaDe}(x, y)))$$
por la ley de negación de un enunciado ∃

$$\equiv \forall x(\sim\text{Cuadrado}(x) \vee \sim(\forall y(\text{Triángulo}(y) \rightarrow \text{DerechaDe}(x, y))))$$
por la ley de De Morgan

$$\equiv \forall x(\sim\text{Cuadrado}(x) \vee \exists y(\sim(\text{Triángulo}(y) \rightarrow \text{DerechaDe}(x, y))))$$
por la ley de negación de un enunciado ∀

$$\equiv \forall x(\sim\text{Cuadrado}(x) \vee \exists y(\text{Triángulo}(y) \wedge \sim\text{DerechaDe}(x, y)))$$
por la ley de negación de un enunciado si-entonces

■

La desventaja de la notación totalmente formal es que debido a que es complicada y está un tanto alejada de la comprensión intuitiva, cuando la usamos, podemos cometer errores que pasan desapercibidos. Sin embargo, la ventaja, es que operaciones, tales como hacer negaciones, pueden ser completamente mecánicas y programadas en una computadora. Además, cuando nos acostumbremos a manipulaciones formales, podemos utilizarlas para comprobar nuestras intuiciones y entonces, podemos usar nuestra intuición para ver nuestras manipulaciones formales. La notación lógica formal se utiliza en ramas de ciencias de la computación, tales como la inteligencia artificial, la comprobación del programa y la teoría de autómatas y en los lenguajes formales.

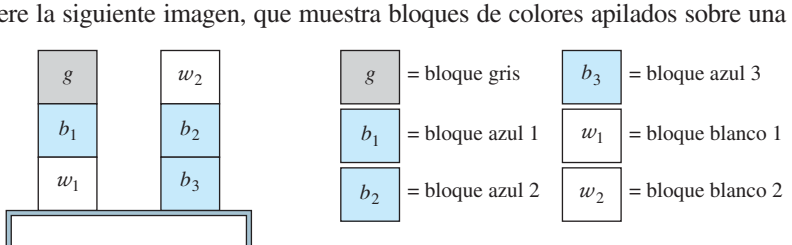
En conjunto, los símbolos de los cuantificadores, variables, predicados y conectores lógicos constituyen lo que se conoce como el **lenguaje lógico de primer orden**. A pesar de que este lenguaje es más simple en muchos aspectos comparado con el lenguaje que usamos todos los días, aprenderlo requiere del mismo tipo de práctica necesaria que para aprender cualquier lengua extranjera.

Prolog

El lenguaje de programación Prolog (nombre corto para *pro*gramación en *ló*gica) se desarrolló en Francia en la década de 1970 por A. Colmerauer y P. Roussel para ayudar a los programadores que trabajaban en el campo de la inteligencia artificial. Un simple programa Prolog se compone de un conjunto de enunciados que describen una situación, junto con preguntas acerca de la situación. Para construirlo en el lenguaje se requieren técnicas de búsqueda e inferencia para responder las preguntas que se deducen de las respuestas de los enunciados dados. Esto libera al programador de la necesidad de tener que escribir programas distintos para responder a cada tipo de pregunta. El ejemplo 3.3.11 es un ejemplo muy simple de un programa Prolog.

Ejemplo 3.3.11 Un programa Prolog

Considere la siguiente imagen, que muestra bloques de colores apilados sobre una mesa.



Nota Diferentes implementaciones de Prolog siguen diferentes convenciones como son cómo representar una constante, una variable, los nombres del predicado y las formas de las preguntas y respuestas. Las convenciones que se usan en este libro son similares a las usadas por el Prolog de Edimburgo.

Los siguientes son enunciados en Prolog que describen esta imagen y hace dos preguntas al respecto.

esarriba(g, b_1) color(g, gris), color(b_3, azul)
esarriba(b_1, w_1) color(b_1, azul) color(w_1, blanco)
esarriba(w_2, b_2) color(b_2, azul) color(w_2, blanco)
esarriba(b_2, b_3) esarriba(X, Z) si esarriba (X, Y) y esarriba (Y, Z)
?color(b_1, azul) ?esarriba(X, w_1)

Los enunciados "esarriba(g, b_1)" y "color(g, gris)" se interpretan como "g está arriba de b_1" y "g es de color gris". El enunciado "esarriba (X, Z) si esarriba (X, Y) y esarriba (Y, Z)" se debe interpretar como "Para todos X, Y y Z, si X está arriba de Y y Y está arriba de Z, entonces X está arriba de Z". El enunciado del programa

?color(b_1, azul)

es una pregunta acerca de si el bloque b_1 es de color azul. Prolog responde ésta al escribir

Sí.

El enunciado

?esarriba (X, w_1)

es una pregunta que cuestiona para cuál bloque X el predicado "X está arriba de w_1" es verdadero. Prolog responde dando una lista de todos esos bloques. En este caso, la respuesta es

$$X = b_1, X = g.$$

Observe que Prolog puede encontrar la solución $X = b_1$ simplemente buscando en el conjunto original de hechos dados. Sin embargo, Prolog debe *inferir* la solución $X = g$ a partir de los siguientes enunciados:

esarriba(g, b_1),
esarriba(b_1, w_1),
esarriba(X, Z) si esarriba (X, Y) y esarriba(Y, Z).

Escriba las respuestas que daría Prolog si las siguientes preguntas se agregaran al programa anterior.

a. ?esarriba(b_2, w_1) b. ?color(w_1, X) c. ?color(X, azul)

Solución

a. La pregunta significa "Está b_2 arriba de w_1?; por lo que la respuesta es "No".

b. La pregunta significa "¿Para qué colores X es el predicado 'w_1 es de color X' verdadero?", Por lo que la respuesta es "X = blanco".

c. La pregunta significa "¿Para qué bloques es el predicado 'X es de color azul' verdadero?", Por lo que la respuesta es "$X = b_1$", "$X = b_2$" y "$X = b_3$". ■

Autoexamen

1. Para establecer la verdad de un enunciado de la forma "$\forall x$ en D, $\exists y$ en E tal que $P(x, y)$", imagine que alguien le ha dado un elemento x de D, pero que no tiene control sobre qué elemento es. Entonces necesita encontrar _____ con la propiedad de que la x que la persona le dio junto con la _____ que posteriormente encontró satisfacen _____.

2. Para establecer la verdad de un enunciado de la forma "$\exists x$ en D tal que $\forall y$ en E, $P(x, y)$", necesita encontrar _____ por lo que _____ que pudiera darle posteriormente, _____ sería verdadero.

3. Considere el enunciado "$\forall x$, $\exists y$ tal que $P(x, y)$, una propiedad que implica a x y y, es verdadera". Una negación de este enunciado es "_____".

4. Considere el enunciado "$\exists x$ tal que $\forall y$, $P(x, y)$, una propiedad que implica a x y y, es verdadero". Una negación de este enunciado es "____".

5. Supongamos que $P(x, y)$ es una propiedad que implica a x y y; supongamos que el enunciado "$\forall x$ en D, $\exists y$ en E tal que $P(x, y)$" es verdadero. Entonces, el enunciado "$\exists x$ en D tal que $\forall y$ en E, $P(x, y)$"

   a. es verdadero. b. es falso. c. puede ser verdadero o falso.

Conjunto de ejercicios 3.3

1. Sea C el conjunto de ciudades en el mundo, sea N el conjunto de las naciones en el mundo y sea $P(c, n)$ "c es la ciudad capital de n". Determine los valores de verdad de los siguientes enunciados.
   a. P(Tokio, Japón) **b.** P(Atenas, Egipto)
   c. P(París, Francia) d. P(Miami, Brasil)

2. Sea G(x, y) "$x^2 > y$". Indique cuáles de los siguientes enunciados son verdaderos y cuáles son falsos.
   a. $G(2, 3)$ **b.** $G(1, 1)$
   c. $G\left(\frac{1}{2}, \frac{1}{2}\right)$ d. $G(-2, 2)$

3. El siguiente enunciado es verdadero: "$\forall$ número real x distinto de cero, $\exists$ un número real y tal que $xy = 1$". Para cada x se indican a continuación, determine una y para que haga que el predicado "$xy = 1$" sea verdadero.
   a. $x = 2$ **b.** $x = -1$ c. $x = 3/4$

4. El siguiente enunciado es verdadero: "$\forall$ número real x, $\exists$ un entero n tal que $n > x$".* Para cada x que se indique a continuación, encuentre una n que haga que el predicado "$n > x$" sea verdadero.
   a. $x = 15.83$ b. $x = 108$ c. $x = 10^{10^{10}}$

Los enunciados de los ejercicios del 5 al 8 se refieren al mundo de Tarski presentado en el ejemplo 3.3.1. Explique por qué cada uno es verdadero.

5. Para todos los círculos x hay un cuadrado y tal que x y y tienen el mismo color.

6. Para todos los cuadrados x hay un círculo y tal que x y y tienen diferentes colores y y está arriba de x.

7. Hay un triángulo x tal que para todos los cuadrados y, x está arriba de y.

8. Hay un triángulo x tal que para todos los círculos y, y está arriba de x.

9. Sea $D = E = \{-2, -1, 0, 1, 2\}$. Explique por qué los siguientes enunciados son verdaderos.
   a. $\forall x$ en D, $\exists y$ en E tal que $x + y = 0$.
   b. $\exists x$ en D tal que $\forall y$ en E, $x + y = y$.

10. Este ejercicio se refiere al ejemplo 3.3.3. Determine si cada uno de los siguientes enunciados es verdadero o falso.
    a. $\forall$ los estudiantes S, $\exists$ un postre D tal que S elige a D.
    b. $\forall$ los estudiantes S, $\exists$ una ensalada T tal que S elige a T.
    c. $\exists$ un postre D tal que $\forall$ estudiante S, S elige a D.
    d. $\exists$ una bebida B tal que $\forall$ estudiante D, D elige a B.
    e. $\exists$ un artículo I tal que $\forall$ estudiante S, S no elige a I.
    f. $\exists$ un puesto Z tal que $\forall$ estudiante S, $\exists$ un artículo I tal que S elige a I de Z.

11. Sea S el conjunto de estudiantes en su escuela, sea M el conjunto de películas que se han publicado y sea $V(s, m)$ "el estudiante s ha visto la película m". Reescriba cada uno de los siguientes enunciados sin necesidad de utilizar el símbolo $\forall$, el símbolo $\exists$ o variables.
    a. $\exists s \in S$ tal que $V(s,$ Casablanca).
    b. $\forall s \in S$, V$(s,$ Guerra de las galaxias).
    c. $\forall s \in S$, $\exists m \in M$ tal que $V(s, m)$.
    d. $\exists m \in M$ tal que $\forall s \in S$, $V(s, m)$.
    e. $\exists s \in S$, $\exists t \in S$ y $\exists m \in M$ tal que $s \neq t$ y $V(s, m) \wedge V(t, m)$.
    f. $\exists s \in S$ y $\exists t \in S$ tal que $s \neq t$ y $\forall m \in M$, $V(s, m) \rightarrow V(t, m)$.

12. Sea $D = E = \{-2, -1, 0, 1, 2)$. Escriba negaciones para cada uno de los siguientes enunciados y determine cuál es verdadero, el enunciado dado o su negación.
    a. $\forall x$ en D, $\exists y$ en E tales que $x + y = 1$.
    b. $\exists x$ en D tal que $\forall y$ en E, $x + y = -y$.
    c. $\forall x$ en D, $\exists y$ en E tal que $xy \geq y$.
    d. $\exists x$ en D tal que $\forall y$ en E, $x \leq y$.

En cada uno de los enunciados 13 al 19, *a*) escriba el enunciado en español sin utilizar el símbolo $\forall$ o $\exists$ o variables y exprese su respuesta lo más simple posible y *b*) escriba una negación del enunciado.

13. $\forall$ color C, $\exists$ un animal A tal que A es de color C.

14. $\exists$ un libro b tal que $\forall$ persona p, p ha leído b.

15. $\forall$ entero impar n, $\exists$ un entero k tal que $n = 2k + 1$.

16. $\exists$ un número real u tal que $\forall$ número real v, $uv = v$.

17. $\forall r \in \mathbf{Q}$, $\exists$ enteros a y b tales que $r = a/b$.

18. $\forall x \in \mathbf{R}$, $\exists$ un número real y tal que $x + y = 0$.

19. $\exists x \in \mathbf{R}$ tal que para todos los números reales y, $x + y = 0$.

20. Recuerde que invertir el orden de los cuantificadores en un enunciado con dos cuantificadores diferentes puede cambiar el valor de verdad del enunciado, pero no necesariamente lo hace. Todos los enunciados de los pares en la página siguiente se refieren al mundo de Tarski de la figura 3.3.1. En cada par, el orden de los cuantificadores se invierte, pero todo lo demás es igual. Para cada par, determine si los enunciados tienen el mismo valor de verdad u opuesto. Justifique su respuesta.

*Esto se conoce como el principio de Arquímedes, ya que fue formulada por primera vez (en términos geométricos) por el gran matemático griego Arquímedes de Siracusa, que vivió aproximadamente del 287 al 212 a.C.

a. 1) Para todos los cuadrados y hay un triángulo x tal que x y y tienen un color diferente.
2) Existe un triángulo x tal que para todos los cuadrados y, x y y tienen colores diferentes.

b. 1) Para todos los círculos y hay un cuadrado x tal que x y y tienen el mismo color.
2) Hay un cuadrado x tal que para todos los círculos y, x y y tienen el mismo color.

21. En cada una de las siguientes ecuaciones, determine cuáles de los siguientes enunciados son verdaderos:
1) Para todos los números reales x, existe un número real y tal que la ecuación es verdadera.
2) Existe un número real x, tal que para todo número real y, la ecuación es verdadera.
Observe que es posible que ambos enunciados sean verdaderos o falsos.
a. $2x + y = 7$
b. $y + x = x + y$
c. $x^2 - 2xy + y^2 = 0$
d. $(x - 5)(y - 1) = 0$
e. $x^2 + y^2 = -1$

En los ejercicios 22 y 23, reescriba cada frase, sin usar variables o el símbolo $\forall$ o $\exists$. Indique si el enunciado es verdadero o falso.

22. a. $\forall$ número real x, $\exists$ un número real y tal que $x + y = 0$.

b. $\exists$ un número real y tal que $\forall$ número real x, $x + y = 0$.

23. a. $\forall$ número real distinto de cero r, $\exists$ un número real s tal que $rs = 1$.
b. $\exists$ un número real r tal que $\forall$ número real distinto de cero s, $rs = 1$.

24. Utilice las leyes de negación de enunciados existenciales y universales para deducir las siguientes reglas:
a. $\sim(\forall x \in D(\forall y \in E(P(x, y)))) \equiv \exists x \in D(\exists y \in E(\sim P(x, y)))$
b. $\sim(\exists x \in D(\exists y \in E(P(x, y)))) \equiv \forall x \in D(\forall y \in E(\sim P(x, y)))$

Cada enunciado del 25 al 28 se refiere al mundo de Tarski de la figura 3.3.1. Para cada uno, *a*) determine si el enunciado es verdadero o falso y justifique su respuesta, *b*) escriba una negación del enunciado (refiriéndose, si lo desea, al resultado del ejercicio 24).

25. $\forall$ círculo x y $\forall$ cuadrado y, x está arriba de y.

26. $\forall$ círculo x y $\forall$ triángulo y, x está arriba de y.

27. $\exists$ un círculo x y $\exists$ un cuadrado y tal que x está arriba de y y x y y tienen colores diferentes.

28. $\exists$ un triángulo x y $\exists$ un cuadrado y tal que x está arriba de y y x y y tienen el mismo color.

Para cada uno de los enunciados en los ejercicios 29 y 30, *a*) escriba un nuevo enunciado intercambiando los símbolos $\forall$ y $\exists$ y *b*) establezca que es verdadero: el enunciado dado, la versión con cuantificadores intercambiados, ninguno de ellos o ambos.

29. $\forall x \in \mathbf{R}$, $\exists y \in \mathbf{R}$ tal que $x < y$.

30. $\exists x \in \mathbf{R}$ tal que $\forall y \in \mathbf{R}^-$ (el conjunto de los números reales negativos), $x > y$.

31. Considere el enunciado "Todo cuerpo tiene más edad que algún cuerpo". Reescriba este enunciado en la forma "$\forall$ persona x, $\exists$ _____".

32. Considere el enunciado de "Algún cuerpo tiene más edad que todo cuerpo". Reescriba este enunciado en la forma "$\exists$ una persona x tal que $\forall$ _____".

En los ejercicios del 33 al 39, *a*) reescriba el enunciado formalmente con cuantificadores y variables y *b*) escriba una negación del enunciado.

33. Todo el mundo ama a alguien.

34. Alguien ama a todos.

35. Todo el mundo confía en alguien.

36. Alguien confía en todo el mundo.

37. Cualquier entero par es igual al doble de un número entero.

38. Cada acción tiene una reacción igual y opuesta.

39. Hay un programa que da la respuesta correcta a cada pregunta que se plantea él mismo.

40. En el lenguaje informal la mayoría de los enunciados de la forma "Hay _____ cada _____" intentan ser entendidas como que significan "$\forall$ _____ $\exists$ _____", a pesar de que el cuantificador existencial *hay* está antes del cuantificador universal *cada*. Observe que esta interpretación se aplica a las siguientes frases conocidas. Reescríbalas utilizando cuantificadores y variables.
a. Cada minuto nace un tonto.
b. Hay un tiempo para cada cosa bajo el cielo.

41. Indique cuáles de los siguientes enunciados son verdaderos y cuáles son falsos. Justifique su respuesta lo mejor que pueda.
a. $\forall x \in \mathbf{Z}^+$, $\exists y \in \mathbf{Z}^+$ tal que $x = y + 1$.
b. $\forall x \in \mathbf{Z}$, $\exists y \in \mathbf{Z}$ tal que $x = y + 1$.
c. $\exists x \in \mathbf{R}$ tal que $\forall y \in \mathbf{R}$, $x = y + 1$.
d. $\forall x \in \mathbf{R}^+$, $\exists y \in \mathbf{R}^+$ tal que $xy = 1$.
e. $\forall x \in \mathbf{R}$, $\exists y \in \mathbf{R}$ tal que $xy = 1$.
f. $\forall x \in \mathbf{Z}^+$ y $\forall y \in \mathbf{Z}^+$, $\exists z \in \mathbf{Z}^+$ tal que $z = x - y$.
g. $\forall x \in \mathbf{Z}$ y $\forall y \in \mathbf{Z}$, $\exists z \in \mathbf{Z}$ tal que $z = x - y$.
h. $\exists u \in \mathbf{R}^+$ tal que $\forall v \in \mathbf{R}^+$, $uv < v$.

42. Escriba la negación de la definición de límite de una sucesión dada en el ejemplo 3.3.7.

43. La siguiente es la definición de $\lim_{x \to a} f(x) = L$:
Para todo número real $\varepsilon > 0$, existe un número real $\delta > 0$ tal que para todo número real x, si $a - \delta < x < a + \delta$ y $x \neq a$ entonces $L - \varepsilon < f(x) < L + \varepsilon$.
Escriba qué significa $\lim_{x \to a} f(x) \neq L$. En otras palabras, escriba la negación de la definición.

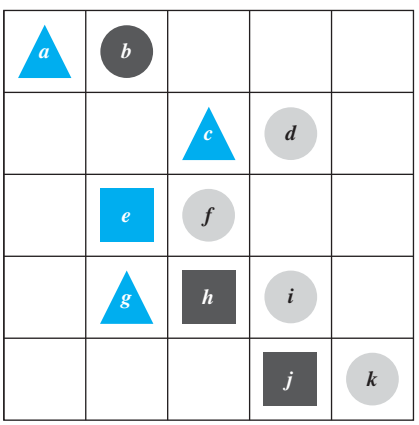
44. La notación de $\exists!$ Se establece para las palabras "existe un único". Por lo que, por ejemplo, "$\exists! x$ tal que x es primo y x es

par" significa que hay uno y sólo un, número primo par. ¿Cuáles de los siguientes enunciados son verdaderos y cuáles son falsos? Explique.

a. ∃! número real x tal que ∀ número real y, $xy = y$.
b. ∃! entero x tal que $1/x$ es un número entero.
c. ∀ número real x, ∃! número real y tal que $x + y = 0$.

✶45. Supongamos que $P(x)$ es un predicado y D es el dominio de x. Reescriba la frase "∃! $x \in D$ tal que $P(x)$" sin necesidad de utilizar el símbolo ∃!. (Vea el ejercicio 44 para el significado de ∃!)

En los ejercicios del 46 al 54, se refieren al mundo de Tarski de la figura 3.1.1, que se imprime de nuevo aquí como referencia. Los dominios de todas las variables consisten de todos los objetos en el mundo de Tarski. Para cada enunciado, *a*) indique si el enunciado es verdadero o falso y justifique su respuesta, *b*) escriba el enunciado dado usando la notación lógico-formal que se muestra en el ejemplo 3.3.10 y *c*) escriba la negación del enunciado dado usando la notación lógico-formal del ejemplo 3.3.10.



46. Hay un triángulo x tal que para todos los cuadrados y, x está arriba de y.

47. Hay un triángulo x tal que para todos los círculos y, x está arriba de y.

48. Para todos los círculos x, hay un cuadrado y tal que y está a la derecha de x.

49. Para cada objeto x, hay un objeto y tal que $x \neq y$ y x y y tienen colores diferentes.

50. Para cada objeto x, hay un objeto y tal que si $x \neq y$ entonces x y y tienen colores diferentes.

51. Hay un objeto y tal que todos los objetos x, si $x \neq y$, entonces x y y tienen colores diferentes.

52. Para todos los círculos x y para todos los triángulos y, x está a la derecha de y.

53. Hay un círculo x y hay un cuadrado y tal que x y y tienen el mismo color.

54. Hay un círculo x y hay un triángulo y tal que x y y tienen el mismo color.

Sean $P(x)$ y $Q(x)$ predicados y supongamos que D es el dominio de x. En los ejercicios 55 al 58, por las formas del enunciado de cada par, determine si *a*) tienen el mismo valor de verdad para cada elección de $P(x)$, $Q(x)$ y D, o *b*) hay una elección de $P(x)$, $Q(x)$ y D para la que tienen valores de verdad opuestos.

55. $\forall x \in D, (P(x) \wedge Q(x))$ y
$(\forall x \in D, P(x)) \wedge (\forall x \in D, Q(x))$

56. $\exists x \in D, (P(x) \wedge Q(x))$ y
$(\exists x \in D, P(x)) \wedge (\exists x \in D, Q(x))$

57. $\forall x \in D, (P(x) \vee Q(x))$ y
$(\forall x \in D, P(x)) \vee (\forall x \in D, Q(x))$

58. $\exists x \in D, (P(x) \vee Q(x))$ y
$(\exists x \in D, P(x)) \vee (\exists x \in D, Q(x))$

En los ejercicios 59 al 61, encuentre las respuestas que Prolog daría si se agregaran las siguientes preguntas al programa dado en el ejemplo 3.3.1 1.

59. a. ?esarriba(b_1, w_1)
b. ?color(X, blanco)
c. ?esarriba(X, b_3)

60. a. ?esarriba(w_1, g)
b. ?color(w_2, azul)
c. ?esarriba(X, b_1)

61. a. ?esarriba(w_2, b_3)
b. ?color(X, gris)
c. ?esarriba(g, X)

Respuestas del autoexamen

1. un elemento y en E; y; $P(x, y)$ 2. Un elemento x en D; y en E; $P(x, y)$ 3. ∃x de tal manera que ∀y, la propiedad $P(x, y)$ es falsa. 4. ∀x, ∃y tal que la propiedad $P(x, y)$ es falsa. 5. La respuesta es *c*): la veracidad o falsedad de un enunciado en el que los cuantificadores se invierten depende de la naturaleza de la propiedad que implique a x y y.

3.4 Argumentos con enunciados cuantificados

La única salvaguardia de los malos razonamientos es el hábito de razonar bien, la familiarización con los principios del razonamiento exacto y la aplicación práctica de estos principios. —John Stuart Mill

La regla de la *instanciación universal* (in-stan-AY-shun) dice lo siguiente:

> Si alguna propiedad es verdadera *de todas las cosas* en un conjunto, entonces es verdadera *cualquier particular* cosa en el conjunto.

El uso de las palabras *instanciación universal* indica que la verdad de una propiedad en un caso particular es como un caso especial de una verdad más general o universal. La validez de esta forma de argumento se deduce inmediatamente de la definición de los valores de verdad de un enunciado universal. Uno de los ejemplos más famosos de la instanciación universal es el siguiente:

Todos los hombres son mortales.
Sócrates es un hombre.
$\therefore$ Sócrates es mortal.

La instanciación universal es *la* herramienta fundamental del razonamiento deductivo. Las fórmulas matemáticas, definiciones y teoremas son como plantillas generales que se utilizan una y otra vez en una gran variedad de situaciones particulares. Un teorema dado dice que tal o cual es cierto para todas las cosas de un cierto tipo. Si, en una situación dada, tiene un objeto en particular de ese tipo y luego por la instanciación universal, concluye que tal y tal cosa son verdaderas para ese objeto en particular. Puede repetir este proceso 10, 20 o más veces en una sola demostración o solución del problema.

Como un ejemplo de instanciación universal, supongamos que está haciendo un problema que requiere que simplifique $r^{k+1} \cdot r$,

donde r es un número real en particular y k es un entero en particular. Sabe de su estudio del álgebra que los siguientes enunciados universales son verdaderos:

1. Para todo número real x y todos los enteros m y n, $x^m \cdot x^n = x^{m+n}$.
2. Para todo número real x, $x^1 = x$.

Por lo que hacemos lo siguiente:

$$\begin{aligned} r^{k+1} \cdot r &= r^{k+1} \cdot r^1 && \text{Paso 1} \\ &= r^{(k+1)+1} && \text{Paso 2} \\ &= r^{k+2} && \text{por algebra básica.} \end{aligned}$$

El razonamiento detrás de los pasos 1 y 2 se resume de la siguiente manera.

Paso 1:
Para todos los números reales x, $x^1 = x$. — verdad universal
r es un número real dado. — caso particular
$\therefore r^1 = r$. — conclusión

Paso 2:
Para todos los números reales x números y para todos los enteros m y n, $x^m \cdot x^n = x^{m+n}$. — verdad universal
r es un número real dado y $k+1$ y 1 son enteros dados. — caso particular
$\therefore r^{k+1} \cdot r^1 = r^{(k+1)+1}$. — conclusión

Ambos argumentos son ejemplos de instanciación universal.

Modus ponens universal

La regla de la instanciación universal puede combinarse con el *modus ponens* para obtener la forma válida de argumento llamado *modus ponens universal*.

Modus ponens universal

Versión formal	*Versión informal*
$\forall x$, si $P(x)$, entonces $Q(x)$.	Si x hace a $P(x)$ verdadero, entonces x hace a $Q(x)$ verdadero.
$P(a)$ para una a dada.	a hace a $P(x)$ verdadero.
$\therefore Q(a)$	$\therefore a$ hace a $Q(x)$ verdadero.

Observe que la primera, o mayor, premisa del *modus ponens* universal se podría escribir "Todas las cosas que hacen a $P(x)$ verdadero hacen a $Q(x)$ verdadero", en cuyo caso la conclusión que se deduce sólo de la instanciación universal. Sin embargo, la forma si-entonces es más natural para usarse en la mayoría de las situaciones matemáticas.

Ejemplo 3.4.1 Reconocimiento del *modus ponens* universal

Reescriba el siguiente argumento usando cuantificadores, variables y símbolos de predicado. ¿Es este argumento válido? ¿Por qué?

Si un número entero es par, entonces su cuadrado es par.
k es un entero dado, que es par.
$\therefore k^2$ es par.

Solución La mayor premisa de este argumento se puede reescribir como

$\forall x$, si x es un entero par entonces x^2 es par.

Sea $E(x)$ "x es un entero par", sea $S(x)$ "x^2 es par" y sea que k se establezca para un entero particular que es par. Entonces el argumento tiene la forma siguiente:

$\forall x$, si $E(x)$ entonces $S(x)$.
$E(k)$, para una k dada.
$\therefore S(x)$.

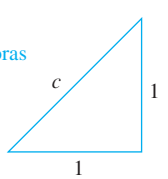
Este argumento tiene la forma de *modus ponens* universal y por tanto, es válido. ■

Ejemplo 3.4.2 Esbozo de conclusiones usando el *modus ponens* universal

Escriba la conclusión que se puede deducir utilizando el *modus ponens* universal.

Si T es cualquier triángulo rectángulo con hipotenusa c y los catetos a y b, entonces $c^2 = a^2 + b^2$.
El triángulo que se muestra a la derecha es un triángulo rectángulo con ambos catetos iguales a 1 y la hipotenusa c.
$\therefore$ _____

Teorema de Pitágoras



Solución $c^2 = 1^2 + 1^2 = 2$

Observe que si usted toma la raíz cuadrada no negativa de ambos lados de esta ecuación, se obtiene $c = \sqrt{2}$. Esto demuestra que hay un segmento de recta, cuya longitud es $\sqrt{2}$. La sección 4.7 tiene una demostración de que $\sqrt{2}$ no es un número racional. ■

Uso del modus ponens universal en una demostración

En el capítulo 4 se analizan los métodos de demostración de enunciados cuantificados. Aquí se presenta una demostración de que la suma de dos enteros pares es par. Hace uso de la definición de entero par, es decir, que un número entero es *par* si y sólo si, es igual a dos veces un número entero. (O, más formalmente: ∀ entero x, x es par si y sólo si, ∃ un entero k tal que $x = 2k$.)

> Supongamos que m y n son particulares, pero se eligen arbitrariamente, números pares enteros. Entonces $m = 2r$ para algún entero r,(1) y $n = 2s$ para algún entero s.(2) Por tanto
>
> $$m + n = 2r + 2s \quad \text{por sustitución}$$
> $$= 2(r + s)^{(3)} \quad \text{al factorizar el 2.}$$
>
> Ahora $r + s$ es un número entero(4) y por tanto $2(r + s)$ es par(5). Así $m + n$ es par.

El desarrollo siguiente de la demostración muestra cómo cada uno de los pasos numerados se justifica con argumentos que son válidos por el *modus ponens* universal.

Nota El principio lógico de la **instanciación existencial** dice que si sabemos que algo existe, podemos darle un nombre. Este principio, se analizará con más detalle en la sección 4.1 ya que nos permite dar a los enteros los nombres r y s.

1. Si un número entero es par, entonces es igual a dos veces un número entero.
   m es un entero par dado.
   ∴ m es igual a dos veces algún entero r.
2. Si un número entero es par, entonces es igual al doble de algún número entero.
   n es un entero par dado.
   ∴ n es igual a dos veces algún entero s.
3. Si la cantidad es un número entero, entonces es un número real.
   r y s son enteros dados.
   ∴ r y s son números reales.

   Para todo a, b y c, si a, b y c son números reales, entonces $ab + ac = a(b + c)$.
   2, r, s son números reales dados.
   ∴ $2r + 2s = 2(r + s)$.
4. Para todo u y v, si u y v son enteros, entonces $u + v$ es un número entero.
   r y s son dos números enteros dados.
   ∴ $r + s$ es un número entero.
5. Si un número es igual al doble de un número entero, entonces ese número es par.
   $2(r + s)$ es igual al doble del número entero $r + s$.
   ∴ $2(r + s)$ es par.

Por supuesto, la demostración real de que la suma de números enteros pares es par, no tiene explícitamente la secuencia de los argumentos dados antes. (¡Dios no lo quiera!) Y, de hecho, aún las personas que son buenas en el pensamiento analítico normalmente no son conscientes de su razonamiento de esta manera. Esto se debe a que han absorbido el método de manera tan completa que se ha convertido casi tan automático como respirar.

Modus tollens universal

Otra regla de suma importancia de la inferencia es el *modus tollens universal*. Los resultados de la combinación de la *instanciación universal* con el *modus tollens*. El *modus tollens* universal es el corazón de la demostración por contradicción, que es uno de los métodos más importantes de la argumentación matemática.

***Modus tollens* universal**

Versión formal	*Versión informal*
$\forall x$, si $P(x)$, entonces $Q(x)$.	Si x hace que $P(x)$ sea verdadero, entonces x hace que $Q(x)$ sea verdadero.
$\sim Q(a)$, para una a dada.	a no hace que $Q(x)$ sea verdadero.
$\therefore \sim P(a)$.	$\therefore a$ no hace que $P(x)$ sea verdadero.

Ejemplo 3.4.3 Reconociendo la forma de *modus tollens* universal

Reescriba el siguiente argumento usando cuantificadores, variables y símbolos de predicado. Escriba la premisa mayor en forma condicional. ¿Es este argumento válido? ¿Por qué?

Todos los seres humanos son mortales.
Zeus no es mortal.
$\therefore$ Zeus no es humano.

Solución La mayor premisa se puede reescribir como

$\forall x$, si x es humano entonces x es mortal.

Sea $H(x)$ "x es humano", sea $M(x)$ "x es mortal" y se establece a Z para Zeus. El argumento se convierte en

$\forall x$, si $H(x)$, entonces $M(x)$
$\sim M(Z)$
$\therefore \sim H(Z)$.

Este argumento tiene la forma de *modus tollens* universal y por tanto, es válido. ■

Ejemplo 3.4.4 Esbozo de conclusiones usando *modus tollens* universal

Escriba la conclusión que se puede deducir utilizando *modus tollens* universal

Todos los profesores son distraídos.
Tom Hutchins no es distraído.
$\therefore$ _____.

Solución Tom Hutchins no es un profesor. ■

Prueba de validez de argumentos con enunciados cuantificados

La definición intuitiva de validez de argumentos con enunciados cuantificados es la misma que para los argumentos con enunciados compuestos. Un argumento es válido si y sólo si, la verdad de su conclusión se deduce *necesariamente* de la verdad de sus premisas. La definición formal es la siguiente:

• Definición

Decir que una *forma de argumento* es **válida** significa lo siguiente: No importa que predicados particulares se sustituyan por los símbolos del predicado en sus premisas, si los enunciados resultantes de las premisas son todos verdaderos, entonces la conclusión también es verdadera. Un *argumento* se llama **válido** si y sólo si, su forma es válida.

Como ya se ha indicado, la validez de la instanciación universal se deduce inmediatamente de la definición del valor de verdad de un enunciado universal. Demostraciones generales formales de validez de los argumentos en el cálculo de predicados están fuera del alcance de este libro. Le presentamos la demostración de la validez del *modus ponens* universal como un ejemplo para mostrar que tales demostraciones son posibles y para dar una idea de cómo se ven.

El *modus ponens* universal afirma que

$$\begin{aligned} &\forall x, \text{ si } P(x) \text{ entonces } Q(x). \\ &P(a) \text{ para una } a \text{ dada.} \\ \therefore\ &Q(a). \end{aligned}$$

Para demostrar que esta forma de argumento es válida, supongamos que las premisas mayores y menores son verdaderas. [*Debemos demostrar que la conclusión de "Q(a)" también es verdadera*]. Por la premisa menor, $P(a)$ es verdadera para un valor de a dado. Por la premisa mayor y la instanciación universal el enunciado "Si $P(a)$, entonces $Q(a)$" es verdadero para una a dada. Pero por el *modus ponens*, puesto que los enunciados "Si $P(a)$ entonces $Q(a)$" y "$P(a)$" son verdaderos, se deduce que $Q(a)$ es también verdadero. *[Esto es lo que se iba demostrar.]*

La demostración de validez dada anteriormente es abstracta y un tanto sutil. Incluimos la demostración no porque no creamos que sea capaz de realizar estas demostraciones por sí mismo en esta etapa de su estudio. Sino más bien, pretende ser una visión de un tratamiento más avanzado del tema, que puede intentar manejar en los ejercicios 35 y 36 al final de esta sección si lo desea.

Una de las paradojas del estudio formal de la lógica es que las leyes de la lógica se utilizan para demostrar que ¡las leyes de la lógica son válidas!

En la siguiente parte de esta sección se muestra cómo se pueden utilizar los diagramas para analizar la validez o no validez de los argumentos que contienen enunciados cuantificados. Los diagramas no proporcionan demostraciones totalmente rigurosas de la validez y la no validez y en algunos entornos complejos incluso pueden ser confusos, pero en muchas situaciones son útiles y convincentes.

Uso de diagramas para probar validez

Considere el enunciado

Todos los números enteros son números racionales.

O, formalmente,

$\forall$ entero n, n es un número racional.

Imagine el conjunto de todos los enteros y el conjunto de todos los números racionales como discos. La verdad del enunciado dado se representa colocando el disco de los enteros completo dentro del disco de los racionales, como se muestra en la figura 3.4.1.

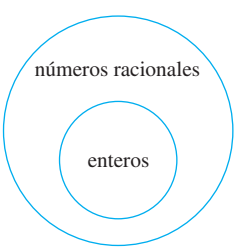


Figura 3.4.1

Debido a que los dos enunciados "$\forall x \in D$, $Q(x)$" y "$\forall x$, si x está en D, entonces $Q(x)$", son lógicamente equivalentes, ambos se pueden representar con diagramas como el anterior.


Culver Pictures

G. W. Leibniz
(1646-1716)

Tal vez la primera persona en utilizar diagramas como éstos para analizar argumentos fue el matemático y filósofo alemán Gottfried Wilhelm Leibniz. Leibniz (que se pronuncia en inglés LIPE-nits) que estaba muy adelantado para su tiempo anticipándose a la lógica simbólica moderna. También desarrolló las ideas principales del cálculo diferencial e integral aproximadamente al mismo tiempo que (e independientemente de) Isaac Newton (1642-1727).

Para probar con diagramas la validez de un argumento, represente la verdad de ambas premisas con diagramas. Después analice los diagramas para ver si necesariamente representan la verdad de la conclusión.

Ejemplo 3.4.5 Uso de un diagrama para mostrar la validez

Utilice diagramas para mostrar la validez del siguiente silogismo:

Todos los seres humanos son mortales.
Zeus no es mortal.
$\therefore$ Zeus no es un ser humano.

Solución La premisa mayor es la imagen de la izquierda en la figura 3.4.2 colocando un disco con la etiqueta "seres humanos" dentro de un disco con la etiqueta "mortales". La premisa menor es la imagen de la derecha en la figura 3.4.2 colocando un punto llamado "Zeus" fuera de la disco con la etiqueta "mortales".

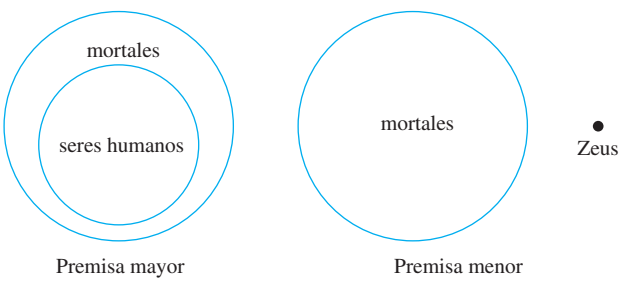


Figura 3.4.2

Los dos diagramas se ajustan de una sola manera, como se muestra en la figura 3.4.3.

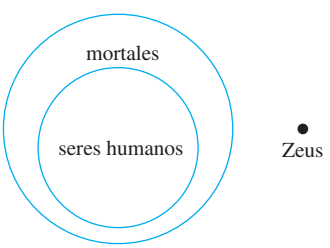


Figura 3.4.3

Ya que el punto Zeus se encuentra fuera del disco de los mortales, está necesariamente fuera del disco de los seres humanos. Por lo que, la verdad de la conclusión se desprende necesariamente de la verdad de las premisas. Es imposible que las premisas de este argumento sean verdaderas y la conclusión falsa, por lo que el argumento es válido. ■

Ejemplo 3.4.6 Uso de diagramas para mostrar *no* validez

Utilice un diagrama para mostrar la no validez de los argumentos siguientes:

Todos los seres humanos son mortales.
Félix es mortal.
$\therefore$ Félix es un ser humano.

Solución Las premisas mayores y menores están representadas esquemáticamente en la figura 3.4.4.

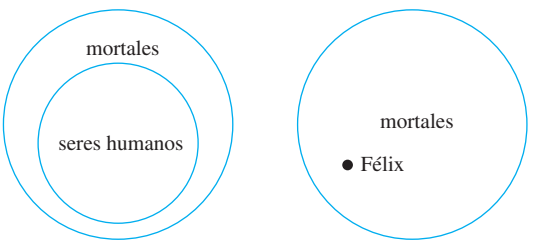


Figura 3.4.4

Todo lo que se sabe es que Félix se encuentra en *algún* punto dentro del disco de mortales. Cuando se encuentra con respecto al disco seres humanos no se puede determinar. Cualquiera de las situaciones que se muestran en la figura 3.4.5 puede ser el caso.

¡Precaución! ¡Tenga cuidado cuando use diagramas para probar la validez! Por ejemplo, en este ejemplo si pone los diagramas de las premisas juntos para obtener sólo la figura 3.4.5*a*) y no la figura 3.4.5*b*), concluirá erróneamente que el argumento era válido.

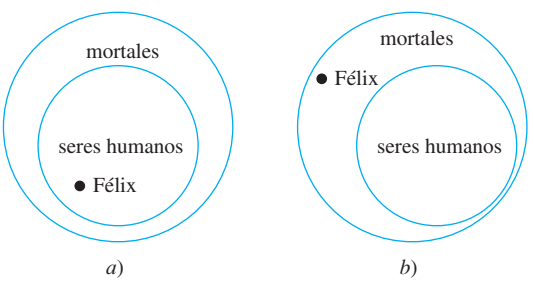


Figura 3.4.5

La conclusión "Félix es un ser humano" es verdadera en el primer caso pero no en el segundo (Félix podría, por ejemplo, ser un gato). Debido a que la conclusión no necesariamente se deduce de las premisas, el argumento es no válido. ■

El argumento del ejemplo 3.4.6 sería válido si la premisa mayor se sustituye por su converso. Pero puesto que un enunciado condicional universal no es lógicamente equivalente a su converso, esa sustitución no puede, en general, hacerse. Decimos que este argumento presenta el error converso.

Error converso (Forma cuantificada)

Versión formal	*Versión informal*
$\forall x$, si $P(x)$, entonces $Q(x)$.	Si x hace que $P(x)$ sea verdadero, entonces x hace que $Q(x)$ sea verdadero.
$Q(a)$ para una a dada.	a hace que $Q(x)$ sea verdadero.
$\therefore P(a)$ ← conclusión no válida	$\therefore a$ hace que $P(x)$ sea verdadero. ← conclusión no válida

La siguiente forma de argumento sería válido si un enunciado condicional fuera lógicamente equivalente a su contraria. Pero no lo es y la forma de argumento no es válido. Decimos que presenta el error contrario. Se le pide el argumento para mostrar la no validez de esta forma en los ejercicios al final de esta sección.

Error contrario (Forma cuantificada)

Versión formal	*Versión informal*
$\forall x$, si $P(x)$, entonces $Q(x)$.	Si x hace a $P(x)$ verdadero, entonces x hace a $Q(x)$ verdadero.
$\sim P(a)$, para una a dada.	a no hace a $P(x)$ verdadero.
$\therefore \sim Q(a)$ ← conclusión no válida	$\therefore$ a no hace a $Q(x)$ verdadero. ← conclusión no válida

Ejemplo 3.4.7 Un argumento con "no"

Utilice los diagramas para demostrar la validez del siguiente argumento:

Ninguna función polinomial tienen asíntotas horizontales.
Esta función tiene una asíntota horizontal.
$\therefore$ Esta función no es una función polinomial.

Solución En la figura 3.4.6, se muestra una buena manera de representar la premisa mayor en forma de diagrama, dos discos, un disco de funciones polinomiales y un disco para funciones con asíntotas horizontales, que no se superponen para nada. La premisa menor se representa con el punto etiquetado "esta función" dentro del disco para funciones con asíntotas horizontales.

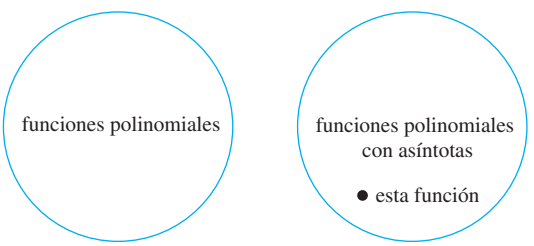


Figura 3.4.6

El diagrama muestra que "esta función" debe estar fuera del disco de funciones polinomiales, por lo que la verdad de la conclusión se deduce necesariamente de la verdad de las premisas. Por tanto el argumento es válido. ■

Un enfoque alternativo a este ejemplo es transformar el enunciado "ninguna función polinomial tiene asíntotas horizontales" en la forma equivalente "$\forall x$, si x es una función polinomial, entonces x no tiene una asíntota horizontal". Si se hace esto, el argumento se puede ver que tienen la forma

$\forall x$, si $P(x)$ entonces $Q(x)$.
$\sim Q(a)$, para una a dada.
$\therefore \sim P(a)$

donde $P(x)$ es "x es una función polinomial" y $Q(x)$ es "x no tiene una asíntota horizontal". Esto es válido por el *modus tollens* universal.

Creación de formas adicionales del argumento

El *modus ponens* universal y *modus tollens* se obtuvieron mediante la combinación de instancias universales con *modus ponens* y *modus tollens*. De la misma manera, formas adicionales de los argumentos que implican enunciados cuantificados universales se pueden obtener mediante la combinación de la instanciación universal con otras formas de argumento válido dadas en la sección 2.3. Por ejemplo, en la sección 2.3 se introdujo la forma del argumento llamada transitividad:

$$\begin{array}{l} p \to q \\ q \to r \\ \therefore\ p \to r \end{array}$$

Esta forma de argumentación se puede combinar con la creación de instancias universales para obtener la forma siguiente de argumento válido.

Transitividad Universal

Versión formal	*Versión informal*
$\forall x\ P(x) \to Q(x).$	Cualquier x que hace que $P(x)$ sea verdadero hace que $Q(x)$ sea verdadero.
$\forall x\ Q(x) \to R(x).$	Cualquier x que hace que $Q(x)$ sea verdadero hace que $R(x)$ sea verdadero.
$\therefore \forall x\ P(x) \to R(x).$	$\therefore$ Cualquier x que hace que $P(x)$ sea verdadero hace que $R(x)$ sea verdadero.

Ejemplo 3.4.8 Evaluación de un argumento para el mundo de Tarski

El siguiente argumento se refiere al tipo de presentación de objetos de diversos tipos y colores descritos en los ejemplos 3.1.13 y 3.3.1. Reordene y reescriba las premisas para mostrar que la conclusión se deduce como consecuencia válida de las premisas.

1. Todos los triángulos son de color azul.
2. Si un objeto está a la derecha de todos los cuadrados, entonces, está arriba de todos los círculos.
3. Si un objeto no está a la derecha de todos los cuadrados, entonces no es de color azul.

$\therefore$ Todos los triángulos están arriba de todos los círculos.

Solución Es útil comenzar por reescribir las premisas y la conclusión en la forma si-entonces:

1. $\forall x$, si x es un triángulo, entonces x es azul.
2. $\forall x$, si x está a la derecha de todos los cuadrados, entonces x está arriba de todos los círculos.
3. $\forall x$, si x no está a la derecha de todos los cuadrados, entonces x no es azul.

$\therefore$ $\forall x$, si x es un triángulo, entonces x está arriba de todos los círculos.

El objetivo es reordenar las premisas, para que la conclusión de cada una sea la misma que la hipótesis de la siguiente. También, la hipótesis de la conclusión del argumento debe ser la misma que la hipótesis de la primera premisa y la conclusión del argumento de la conclusión debe ser la misma que la conclusión de la última premisa. Para lograr este objetivo, puede ser necesario volver a escribir algunos de los enunciados en forma de contraposición.

En este ejemplo se puede ver que la primera premisa debe permanecer donde está, pero la segunda y tercera premisa se deben intercambiar. Entonces la hipótesis del argumento es la misma que la hipótesis de la primera premisa y la conclusión del argumento de la conclusión debe ser igual que la conclusión de la tercera premisa. Sin embargo, las hipótesis

y conclusiones de las premisas no están muy ordenadas. Esto se soluciona reescribiendo la tercera premisa en forma contrapositiva.

Así, las premisas y la conclusión del argumento se puede reescribir de la siguiente manera:

1. $\forall x$, si x es un triángulo, entonces x es azul.
3. $\forall x$, si x es azul, entonces x está a la derecha de todos los cuadrados.
2. $\forall x$, si x está a la derecha de todos los cuadrados, entonces x está arriba de todos los círculos.

$\therefore$ $\forall x$, si x es un triángulo, entonces x está arriba de todos los círculos.

La validez de este argumento se deduce fácilmente de la validez de la transitividad universal. Al poner 1 y 3 juntas y usar la transitividad universal se obtiene que

4. $\forall x$, si x es un triángulo, entonces x está a la derecha de todos los cuadrados.

Y poniendo 4, junto con 2 y con la transitividad universal se tiene que

$\forall x$, si x es un triángulo, entonces x está arriba de todos los círculos,

que es la conclusión del argumento. ■

Observación acerca de los errores converso y contrario

Una de las razones del porqué tantas personas cometen errores conversos y contrarios es que las formas de los argumentos resultantes sería válida si la premisa mayor fuera un bicondicional más que un simple condicional. Y, como indicamos en la sección 2.2, muchas personas tienden a confundir bicondicionales y condicionales.

Considere, por ejemplo, el siguiente argumento:

Todos los criminales de la ciudad frecuentan la guarida del bar de la maldad.

John frecuenta la guarida del bar de la maldad.

$\therefore$ John es uno de los criminales de la ciudad.

La conclusión de este argumento no válida, es el resultado de cometer el error converso. Por tanto, puede ser falsa, aún cuando las premisas del argumento son verdaderas. Este tipo de argumento intenta injustamente establecer la culpabilidad por asociación.

Sin embargo, entre más cerca, la premisa mayor llega a ser un bicondicional y lo más probable es que la conclusión sea verdadera. Si casi nadie más, sino sólo los delincuentes frecuentan el bar y John también frecuenta el bar, entonces es probable (aunque no seguro) que John es un criminal. En base a las premisas dadas, podría ser razonable sospechar de John, pero sería un error condenarlo.

Una variación del error converso es una herramienta de razonamiento muy útil, siempre y cuando se utilice con precaución. Es el tipo de razonamiento que utilizan los médicos para hacer diagnósticos médicos y los mecánicos para reparar automóviles. Es el tipo de razonamiento que se utiliza para generar explicaciones de los fenómenos. Dice así: si un enunciado de la forma

Para toda x, si $P(x)$ entonces $Q(x)$

es verdadero y si

$Q(a)$ es verdadero, para una a dada,

entonces analice el enunciado $P(a)$; éste sólo podría ser verdadero. Por ejemplo, supongamos que un médico sabe que

Para toda x, si x tiene neumonía, entonces x tiene fiebre y escalofríos, tos profunda y se siente excepcionalmente cansado y triste.

Y supongamos que el médico también sabe que

John tiene fiebre y escalofríos, tos profunda
y se siente excepcionalmente cansado y triste.

Con base en estos datos, el médico concluye que el diagnóstico de la neumonía es una fuerte posibilidad, aunque no una certeza. El médico probablemente tratará de lograr mayor apoyo para el diagnóstico mediante pruebas de laboratorio que están específicamente diseñadas para detectar neumonía. Observe que la cercanía con un conjunto de síntomas de una enfermedad llega a ser una condición necesaria y suficiente, para que el diagnóstico del médico sea más seguro.

Esta forma de razonamiento se ha llamado **abducción** por los investigadores que trabajan en inteligencia artificial. Se utiliza en ciertos programas de computadora, en los llamados sistemas de expertos, que tratan de duplicar el funcionamiento de un experto en algún campo del conocimiento.

Autoexamen

1. La regla de la instanciación universal dice que si una propiedad es verdadera para _____ en un dominio, entonces es verdadera para _____ .
2. Si las dos primeras premisas del *modus ponens* universal se escriben como "Si x hace a $P(x)$ verdadero, entonces x hace a $Q(x)$ verdadero" y "Para un valor dado de a _____", entonces la conclusión se puede escribir como "_____".
3. Si las dos primeras premisas del *modus tollens* universal se escriben como "Si x hace a $P(x)$ verdadero, entonces x hace a $Q(x)$ verdadero" y "Para un valor dado de a _____", entonces la conclusión se puede escribir como "_____".
4. Si las dos primeras premisas de transitividad universal se escriben como "Cualquier x que hace a $P(x)$ verdadero hace a $Q(x)$ verdadero" y "Cualquier x que hace a $Q(x)$ verdadero hace a $R(x)$ verdadero", entonces se puede escribir la conclusión como "_____".
5. Los diagramas pueden ser útiles para probar un argumento para la validez. Sin embargo, si no se hacen algunas configuraciones posibles de las premisas, una persona podría concluir que un argumento era _____ cuando en realidad era _____ .

Conjunto de ejercicios 3.4

1. Sea la siguiente ley del álgebra el primer enunciado de un argumento: Para todos los números reales a y b,

$$(a + b)^2 = a^2 + 2ab + b^2.$$

Supongamos que cada uno de los siguientes enunciados es, a su vez, el segundo enunciado del argumento. Utilice la instanciación universal o el *modus ponens* universal para escribir la conclusión que se deduce de cada caso.

a. $a = x$ y $b = y$ son números reales dados.
b. $a = f_i$ y $b = f_j$ son números reales dados.
c. $a = 3u$ y $b = 5v$ son números reales dados.
d. $a = g(r)$ y $b = g(s)$ son números reales dados.
e. $a = \log(t_1)$ y $b = \log(t_2)$ son números reales dados.

Use la instanciación universal o el *modus ponens* universal para completar los espacios en blanco en las conclusiones válidas para los argumentos del 2 al 4.

2. Si un número entero n es igual a $2 \cdot k$ y k es un número entero, entonces n es par.
0 es igual a $2 \cdot 0$ y 0 es un número entero.
$\therefore$ _____

3. Para todos los números reales a, b, c y d, si $b \neq 0$ y $d \neq 0$, entonces $a/b + c/d = (ad + bc)/bd$.
$a = 2$, $b = 3$, $c = 4$ y $d = 5$ son números reales dados tales que $b \neq 0$ y $d \neq 0$.
$\therefore$ _____

4. $\forall$ números reales r, a y b, si r es positivo, entonces $(r^a)^b = r^{ab}$.
$r = 3$, $a = 1/2$ y $b = 6$ son números reales dados tales que r es positivo.
$\therefore$ _____

Utilice el *modus tollens* universal para completar los espacios en blanco en las conclusiones válidas para los argumentos 5 y 6.

5. Todos los números irracionales son números reales
$\frac{1}{0}$ no es un número real.
$\therefore$ _____

6. Si un programa de computadora es correcta, entonces la compilación del programa no produce mensajes de error.
La compilación de este programa produce mensajes de error.
$\therefore$ _____

Algunos de los argumentos son válidos en los ejercicios del 7 al 18 por el *modus ponens* universal o por el *modus tollens* universal, mientras que otros son no válidos y presentan error converso o contrario. Establezca cuáles son válidos y cuáles son no válidos. Justifique su respuesta.

7. Todas las personas sanas comen una manzana al día.
Keisha come una manzana al día.
$\therefore$ Keisha es una persona sana.

8. Todos los estudiantes deben tomar escritura.
Carolina es una estudiante de primer año.
$\therefore$ Carolina debe tomar escritura.

9. Todas las personas sanas comen una manzana al día.
Herbert no es una persona sana.
$\therefore$ Herbert no come una manzana al día.

10. Si un producto de dos números es 0, al menos uno de los números es 0.
Para un número x dado, ni $(2x + 1)$ ni $(x - 7)$ son igual a 0.
$\therefore$ El producto $(2x + 1)(x - 7)$ no es 0.

11. Todos los tramposos se sientan en la fila de atrás.
Monty se sienta en la fila de atrás.
$\therefore$ Monty es un tramposo.

12. Todas las personas honestas pagan sus impuestos.
Darth no es honesto.
$\therefore$ Darth no paga sus impuestos.

13. Para todo estudiante x, si x estudia matemáticas discretas, entonces x es bueno en lógica.
Tarik estudia matemáticas discretas.
$\therefore$ Tarik es bueno en lógica.

14. Si la compilación de un programa de computadora produce mensajes de error, entonces el programa no está correcto.
La compilación de este programa no produce mensajes de error.
$\therefore$ Este programa está correcto.

15. Cualquier suma de dos números racionales es racional.
La suma $r + s$ es racional.
$\therefore$ Los números r y s son racionales.

16. Si un número es par, entonces el doble de ese número es par.
El número $2n$ es par, para un número n dado.
$\therefore$ El número dado n, es par.

17. Si una serie infinita converge, los términos se van a 0.
Los términos de la serie infinita $\sum_{n=1}^{\infty} \frac{1}{n}$ se van a 0.
$\therefore$ La serie infinita $\sum_{n=1}^{\infty} \frac{1}{n}$ converge.

18. Si una serie infinita converge, entonces sus términos se van a 0.
Los términos de la serie infinita $\sum_{n=1}^{\infty} \frac{n}{n+1}$ no se van a 0.
$\therefore$ La serie infinita $\sum_{n=1}^{\infty} \frac{n}{n+1}$ no converge.

19. Reescriba la frase "Ningún buen coche es barato" en forma "$\forall x$, si $P(x)$, entonces $\sim Q(x)$". Indique si cada uno de los siguientes argumentos es válido o no válido y justifique sus respuestas.

a. Ningún buen coche es barato.
Un Rimbaud es un buen coche.
$\therefore$ Un Rimbaud no es barato.

b. Ningún buen coche es barato.
Un Simbaru no es barato.
$\therefore$ Un Simbaru es un buen coche.

c. Ningún buen coche es barato.
Un roadster VX es barato.
$\therefore$ Un roadster VX no es bueno.

d. Ningún buen coche es barato.
Un Omnex no es un buen coche.
$\therefore$ Un Omnex es barato.

20. a. Utilice un diagrama para mostrar que el siguiente argumento puede tener premisas verdaderas y una conclusión falsa.

Todos los perros son carnívoros.
Aaron no es un perro.
$\therefore$ Aaron no es carnívoro.

b. ¿Qué puede concluir acerca de la validez o no validez de la forma del siguiente argumento? Explique cómo el resultado del inciso *a*) conduce a esta conclusión.

$\forall x$, si $P(x)$, entonces $Q(x)$.
$\sim P(a)$ para una a dada.
$\therefore$ $\sim Q(a)$.

Indique si los argumentos del 21 al 27 son válidos o no válidos. Apoye sus respuestas con diagramas.

21. Todas las personas son ratones.
Todos los ratones son mortales.
$\therefore$ Todas las personas son mortales.

22. Todos los estudiantes de matemáticas discretas pueden llamar a un argumento válido de un no válido.
Todas las personas inteligentes pueden decir un argumento válido de un no válido.
$\therefore$ Todos los estudiantes de matemáticas discretas son inteligentes.

23. Todos los maestros a veces cometen errores.
Los dioses nunca cometen errores.
$\therefore$ Los profesores no son dioses.

24. Ningún vegetariano comen carne.
Todos los veganos son vegetarianos.
$\therefore$ Ningún vegano come carne.

25. Ninguna comida de la cafetería universitaria es buena.
Ninguna comida buena se desperdicia.
$\therefore$ Ninguna comida de la cafetería universitaria se desperdicia.

26. Todas las funciones polinomiales son derivables.
Todas las funciones derivables son continuas.
$\therefore$ Todas las funciones polinomiales son continuas.

27. [Adaptado de Lewis Carroll.]
Nada que no sea razonable nunca *me* ha sorprendido.
La lógica me sorprende.
$\therefore$ La lógica no es razonable.

En los ejercicios del 28 al 32, reordene las premisas en cada uno de los argumentos para demostrar que la conclusión se desprende como un contexto de secuencia válida de las premisas. Puede ser útil volver a escribir los enunciados en la forma si-entonces y reemplace algunas declaraciones de sus contrapositivos. Los ejercicios del 28 al 30 se refieren a los tipos de mundos de Tarski analizados en el ejemplo 3.1.13 y 3.3.1. Los ejercicios 31 y 32 se han adaptado de *Lógica simbólica* de Lewis Carrol.*

28. 1. Cada objeto que está a la derecha de todos los objetos azules está arriba de todos los triángulos.
2. Si un objeto es un círculo, entonces, está a la derecha de todos los objetos de color azul.
3. Si un objeto no es un círculo, entonces no es de color gris.
∴ Todos los objetos grises están arriba de todos los triángulos.

29. 1. Todos los objetos que están a la derecha de todos los triángulos están arriba de todos los círculos.
2. Si un objeto no está arriba de todos los objetos en negro, entonces no es un cuadrado.
3. Todos los objetos que están arriba de todos los objetos en negro están a la derecha de todos los triángulos.
∴ Todos los cuadrados están arriba de todos los círculos.

30. 1. Si un objeto está arriba de todos los triángulos, entonces está arriba de todos los objetos de color azul.
2. Si un objeto no está arriba de todos los objetos grises, entonces no es un cuadrado.
3. Cada objeto negro es un cuadrado.
4. Cada objeto que está arriba de todos los objetos grises está arriba de todos los triángulos.
∴ Si un objeto es negro, entonces está arriba de todos los objetos de color azul.

31. 1. Confío en todos los animales que me pertenecen.
2. Los perros muerden huesos.
3. No admito animales en mi estudio, a menos que se los indique.
4. Todos los animales del patio son míos.
5. Admito a todos los animales en quienes confío en mi estudio.
6. Los únicos animales que están realmente dispuestos a venir cuando se les indica son los perros.
∴ Todos los animales del patio muerden huesos.

32. 1. Cuando trabajo un ejemplo de lógica, sin quejarme, puede estar seguro de que lo entiendo.
2. Los argumentos en estos ejemplos no están arreglados en orden regular como a los que estoy acostumbrado.
3. Ningún ejemplo fácil hace que me duela la cabeza.
4. No puedo entender ejemplos si los argumentos no están arreglados en orden regular como al que estoy acostumbrado.
5. Nunca me quejo en un ejemplo a no ser que me dé un dolor de cabeza.
∴ Estos ejemplos no son fáciles.

En los ejercicios 33 y 34 se deduce la única conclusión siguiente cuando se consideran todas las premisas dadas, pero es difícil ver porque las premisas están mezcladas. Reordene las premisas para dejar claro que la conclusión es consecuencia lógica y establezca la conclusión válida que se puede sacar. (Puede ser útil reescribir algunos de los enunciados en la forma si-entonces y sustituya algunos enunciados por sus contrapositivos.)

33. 1. No hay pájaros, excepto avestruces que son al menos de 9 pies de altura.
2. No hay pájaros en la pajarera que pertenezcan a nadie más que a mí.
3. Ningún avestruz vive de pastelillos de fruta.
4. No tengo aves de menos de 9 pies de altura.

34. 1. Todos los escritores que entienden la naturaleza humana son inteligentes.
2. Nadie es un verdadero poeta, a menos que pueda conmocionar al corazón humano.
3. Shakespeare escribió *Hamlet*.
4. Ningún escritor que no entienda la naturaleza humana puede conmocionar el corazón humano.
5. Nadie más que un verdadero poeta podría haber escrito *Hamlet*.

✶35. Deduzca la validez del *modus tollens* universal de la instanciación universal y del *modus tollens*.

✶36. Deduzca la validez de la forma universal del inciso *a*) de la regla eliminación de la validez de las instanciación universal y del argumento válido llamado eliminación en la sección 2.3.

* Lewis Carroll, *Simbolic Logic* (Nueva York: Dover, 1958), pp 118, 120, 123.

Respuestas del autoexamen

1. todos los elementos; un elemento dado en el dominio (*O*: cada elemento individual del dominio) 2. $P(a)$ es verdadero; $Q(a)$ es verdadero 3. $Q(a)$ es falso; $P(a)$ es falso 4. cualquier x que hace a $P(x)$ verdadero hace a $R(x)$ verdadero. 5. válido; no válida (*O*: no válido; válido).

CAPÍTULO 4

TEORÍA ELEMENTAL DE NÚMEROS Y MÉTODOS DE DEMOSTRACIÓN

El contenido fundamental de este capítulo probablemente le sea conocido. Se trata de las propiedades de los enteros (números enteros), los racionales (fracciones de enteros) y números reales. El tema de fondo de este capítulo es la cuestión de cómo determinar la verdad o falsedad de un enunciado matemático.

A continuación se presenta un ejemplo que implica un concepto usado con frecuencia en la ciencia computacional. Dado cualquier número real x, el piso de x, o el mayor entero en x, que se denota $\lfloor x \rfloor$, es el mayor entero que es menor o igual a x. En la recta numérica, $\lfloor x \rfloor$ es el número entero inmediatamente a la izquierda de x (o igual a x si x es un número entero). Por tanto $\lfloor 2.3 \rfloor = 2$, $\lfloor 12.99999 \rfloor = 12$ y $\lfloor -1.5 \rfloor = -2$. Considere las siguientes dos preguntas:

1. ¿Para cualquier número real x, es $\lfloor x - 1 \rfloor = \lfloor x \rfloor - 1$?
2. ¿Para cualesquiera números reales x y y, es $\lfloor x - y \rfloor = \lfloor x \rfloor - \lfloor y \rfloor$?

Tómese unos minutos para tratar de responder estas preguntas por sí mismo.

Resulta que la respuesta a 1) es sí, mientras que la respuesta a 2) es no. ¿Obtuvo estas respuestas? Si no, no se preocupe. En la sección 4.5 aprenderá las técnicas necesarias para responder a estas preguntas y más. Si obtuvo la respuesta correcta, ¡felicitaciones! Tiene una excelente intuición matemática. Ahora pregúntese, ¿qué tan seguro estoy de mis respuestas? ¿Eran suposiciones concebibles o certezas absolutas? ¿Existe alguna diferencia en la certeza entre mis respuestas de 1) y 2)? ¿Podría haber apostado una gran suma de dinero por la exactitud de mis respuestas?

Una de las mejores maneras de pensar una demostración matemática es con un argumento cuidadosamente razonado para convencer a un oyente escéptico (con frecuencia usted) que un enunciado es verdadero. Imagine al difícil oyente ante su razonamiento en cada paso del camino, siempre preguntando: ¿Por qué es así? Si puede contrarrestar todos los desafíos posibles, entonces la demostración en su conjunto será la correcta.

Como ejemplo, imagine demostrar a alguien no muy familiarizado con la notación matemática que si x es un número que cumple que $5x + 3 = 33$, entonces $x = 6$. Se podría argumentar como sigue:

> Si $5x + 3 = 33$, entonces $5x + 3$ menos 3 será igual a $33 - 3$ ya que restar el mismo número de dos cantidades iguales da los mismos resultados. Pero $5x + 3$ menos 3 es igual a $5x$ al sumar 3 a $5x$ y después restando 3 sólo queda $5x$. También, $33 - 3 = 30$. Por tanto $5x = 30$. Esto significa que x es un número que, multiplicado por 5 es igual a 30. Pero el único número con esta propiedad es 6. Por tanto, si $5x + 3 = 33$ entonces $x = 6$.

Por supuesto que hay otras formas de expresar esta demostración, dependiendo del nivel previsto de sofisticación matemática del lector. En la práctica, los matemáticos con frecuencia

omiten razones en ciertos pasos de un argumento cuando se confía en que el lector pueda proporcionarlas. Sin embargo, cuando está aprendiendo a escribir demostraciones, es mejor errar por el lado de dar demasiadas razones más que pocas. Con demasiada frecuencia, cuando ni siquiera los mejores matemáticos examinan cuidadosamente algunos "detalles" en sus argumentos, descubren que esos detalles son en realidad falsos. Una de las razones más importantes para exigir la demostración matemática es que escribir una demostración nos obliga a tomar conciencia de las debilidades de nuestros argumentos y en las suposiciones inconscientes que hemos hecho.

A veces la corrección de un argumento matemático puede ser un asunto de vida o muerte. Supongamos, por ejemplo, que un matemático es parte de un equipo encargado de diseñar un nuevo tipo de motor de avión y supongamos que al matemático se le ha dado la tarea de determinar si el impulso entregado por diversos tipos de motores es el adecuado. Si supiera que sólo el matemático estaba bastante seguro, pero no positivo, de la exactitud de su análisis, probablemente usted no querría subirse en el avión resultante.

En cierto momento en *Alicia en el País de las Maravillas* de Lewis Carroll (ver ejercicio 28 de la sección 2.2), la Liebre de Marzo le dice a Alicia "di lo que quieres decir". En otras palabras, ella debía ser precisa en su uso del lenguaje. Si ella quería decir una cosa, entonces eso es exactamente lo que debía decir. En este capítulo, quizá más que en cualquier curso de matemáticas que usted ha tomado alguna vez, encuentra que es necesario decir lo que quiere decir. Precisión de pensamiento y del lenguaje es esencial para lograr la certeza matemática que se necesita si va a tener plena confianza en sus soluciones a los problemas matemáticos.

4.1 Demostración directa y contraejemplo I: introducción

Las Matemáticas, como ciencia, comenzaron cuando alguien por primera vez, probablemente un griego, demostró proposiciones acerca de "cualquier" cosa o acerca de "algunas" cosas sin especificar las cosas particulares definitivas. —Alfred North Whitehead, 1861-1947

Tanto el descubrimiento como la demostración son partes integrales de la solución de problemas. Cuando usted piensa que ha descubierto que un determinado enunciado es verdadero, trate de averiguar por qué es verdadero. Si tiene éxito, usted sabrá que su descubrimiento es genuino. Incluso si no, el proceso de intentar le dará idea de la naturaleza del problema y puede conducir al descubrimiento de que el enunciado es falso. En caso de problemas complejos, la interacción entre el descubrimiento y la demostración no se reserva hasta el final del proceso de solución del problema, sino más bien es una parte importante de cada paso.

Suposiciones

- En este texto se supone que está familiarizado con las leyes del álgebra básica, que se enumeran en el apéndice A.
- También utilizamos las tres propiedades de la igualdad: Para todos los objetos A, B y C, 1) $A = A$, 2) si $A = B$, entonces $B = A$ y 3) si $A = B$ y $B = C$, entonces $A = C$.
- Además, suponemos que no hay números enteros entre 0 y 1 y que el conjunto de todos los enteros es cerrado bajo suma, resta y multiplicación. Esto significa que las sumas, restas y productos de los números enteros son números enteros.
- Por supuesto, la mayoría de los cocientes de enteros no son números enteros. Por ejemplo, $3 \div 2$, que es igual a $3/2$, no es un número entero y $3 \div 0$ no es ni siquiera un número.

El contenido matemático de esta sección se refiere principalmente a los números enteros pares e impares y a los números primos y compuestos.

Definiciones

Con el fin de evaluar la veracidad o falsedad de un enunciado, debe entender lo que el enunciado trata. En otras palabras, debe conocer el significado de los términos que se presentan en el enunciado. Los matemáticos definen términos con mucho cuidado y precisión y consideramos que es importante aprender las definiciones casi palabra por palabra.

• Definiciones

Un entero n es **par** si y sólo si, n es igual a dos veces un número entero. Un entero n es **impar** si y sólo si, n es igual a dos veces un número entero más 1.

Simbólicamente, si n es un entero, entonces

$$n \text{ es par} \Leftrightarrow \exists \text{ un entero } k \text{ tal que } n = 2k.$$
$$n \text{ es impar} \Leftrightarrow \exists \text{ un entero } k \text{ tal que } n = 2k + 1.$$

De lo que se deduce de la definición que si usted está haciendo un problema en el que por casualidad usted sabe que un número entero dado es par, se puede deducir que tiene la forma 2 · (algún entero). Por el contrario, si usted sabe de alguna situación en la que un número entero es igual a 2 · (algún entero), entonces se puede deducir que el número entero es par.

Sabiendo que un entero n dado, es par. $\xrightarrow{\text{se deduce}}$ n tiene la forma 2 · (algún entero).

Sabiendo que n tiene la forma 2 · (algún entero). $\xrightarrow{\text{se deduce}}$ n es par.

Ejemplo 4.1.1 Enteros pares e impares

Utilice las definiciones de pares e impares para justificar sus respuestas a las siguientes preguntas.

a. ¿Es 0 par?

b. ¿Es −301 impar?

c. Si a y b son números enteros, ¿es $6a^2b$ par?

d. Si a y b son números enteros, ¿es $10a + 8b + 1$ impar?

e. ¿Es todo entero par o impar?

Solución

a. Sí, $0 = 2 \cdot 0$.

b. Sí, $-301 = 2(-151) + 1$.

c. Sí, $6a^2b = 2(3a^2b)$ y puesto que a y b son números enteros, por lo que es $3a^2b$ (es un producto de números enteros).

d. Sí, $10a + 8b + 1 = 2(5a + 4b) + 1$ y puesto que a y b son números enteros, por lo que $5a + 4b$ (es una suma de productos de números enteros).

e. La respuesta es sí, aunque la demostración no es obvia. (Trate de dar una razón usted.) Vamos a mostrar en la sección 4.4 que este hecho es resultado de otro hecho conocido como el teorema del cociente-residuo. ■

El entero 6, es igual a 2 · 3, es un producto de dos números más pequeños enteros positivos. Por otra parte, 7 no se puede escribir como un producto de dos más pequeños números

enteros positivos, sus únicos factores positivos sólo son 1 y 7. Un número entero positivo, como 7, que no se puede escribir como un producto de dos números enteros positivos más pequeños se llama *primo*.

• Definición

Un entero n es **primo** si y sólo si, $n > 1$ y para todos los enteros positivos r y s, si $n = rs$, entonces ya sea r o s es igual a n. Un entero n es **compuesto** si y sólo si, $n > 1$ y $n = rs$ para algunos enteros r y s con $1 < r < n$ y $1 < s < n$.

Simbólicamente:

$$n \text{ es primo} \Leftrightarrow \forall \text{ entero positivo } r \text{ y } s, \text{ si } n = rs \text{ entonces ya sea } r = 1 \text{ y } s = n \text{ o } r = n \text{ y } s = 1.$$

$$n \text{ es compuesto} \Leftrightarrow \exists \text{ enteros positivos } r \text{ y } s \text{ tales que } n = rs \text{ y } 1 < r < n \text{ y } 1 < s < n.$$

Ejemplo 4.1.2 Números primos y compuestos

a. ¿Es 1 primo?

b. ¿Cada número entero mayor que 1 es ya sea primo o compuesto?

c. Escriba los seis primeros números primos.

d. Escriba los seis primeros números compuestos.

Solución

Nota La razón para no permitir que 1 sea primo se analiza en la sección 4.3.

a. No. Para que sea un número primo es necesario que sea mayor que 1.

b. Sí. Sea n un número entero mayor que 1. Considere todos los pares de números enteros positivos r y s tales que $n = rs$. Existen al menos dos de estos pares, por ejemplo, $r = n$ y $s = 1$ y $r = 1$ y $s = n$. Además, ya que $n = rs$, todos los pares cumplen las desigualdades $1 \leq r \leq n$ y $1 \leq s \leq n$. Si n es primo, entonces los dos pares que aparecen son las únicas formas de escribir a n como rs. De lo contrario, existe un par de números enteros positivos r y s tales que $n = rs$ y ni r ni s es igual a 1 o n. Por tanto, en este caso $1 < r < n$ y $1 < s < n$ y por tanto n es compuesto.

c. 2, 3, 5, 7, 11, 13

d. 4, 6, 8, 9, 10, 12

■

Prueba de enunciados existenciales

De acuerdo con la definición dada en la sección 3.1, un enunciado de la forma

$$\exists x \in D \text{ tal que } Q(x)$$

es verdadero si y sólo si,

$$Q(x) \text{ es verdadera para al menos una } x \text{ en } D.$$

Una forma de probar esto es encontrar una x en D que haga a $Q(x)$ verdadero. Otra forma es dar un conjunto de instrucciones para encontrar tal x. Ambos métodos se llaman **demostraciones constructivas de existencia**.

Ejemplo 4.1.3 Demostraciones constructivas de existencia

a. Demuestre lo siguiente: ∃ un entero n par que se puede escribir de dos maneras, como una suma de dos números primos.

b. Supongamos que r y s son números enteros. Demuestre lo siguiente: ∃ un entero k tal que $22r + 18s = 2k$.

Solución

a. Sea $n = 10$. Entonces, $10 = 5 + 5 = 3 + 7$ y 3, 5 y 7 son números primos.

b. Sea $k = 11r + 9s$. Entonces k es un número entero, ya que es una suma de productos de números enteros y por sustitución, $2k = 2(11r + 9s)$, que es igual a $22r + 18s$ por la ley distributiva del álgebra. ■

Una **demostración no constructiva de existencia** implica demostrar, *a*) que la existencia de un valor de x que hace a $Q(x)$ verdadero está garantizada por un axioma o por un teorema previamente demostrado o *b*) que la suposición de que no existe tal x conduce a una contradicción. La desventaja de una demostración no constructiva es que no puede dar prácticamente ninguna pista sobre dónde o cómo se puede encontrar a x. El uso generalizado de las computadoras digitales en los últimos años ha dado lugar a cierto descontento con este aspecto de las demostraciones no constructivas y se ha aumentado el esfuerzo para producir demostraciones constructivas que tengan instrucciones para el cálculo con computadora de la cantidad en cuestión.

Refutación de un enunciado universal con un contraejemplo

Refutar un enunciado significa demostrar que es falso. Considere el tema de refutar un enunciado de la forma

$$\forall x \in D, \text{ si } P(x), \text{ entonces } Q(x).$$

Demostrar que este enunciado es falso es equivalente a demostrar que su negación es verdadera. La negación del enunciado es existencial:

$$\exists x \text{ en } D \text{ tal que } P(x) \text{ y no } Q(x).$$

Pero para demostrar que un enunciado existencial es verdadero, en general se da un ejemplo y ya que el ejemplo se utiliza para demostrar que el enunciado original es falso, lo llamamos un *contraejemplo*. Así, el método de refutación con un *contraejemplo* se puede escribir de la siguiente manera:

Refutación con un contraejemplo

Para refutar un enunciado de la forma "$\forall x \in D$, si $P(x)$, entonces $Q(x)$", determine un valor de x en D para que la hipótesis $P(x)$ es verdadera y la conclusión de $Q(x)$ es falsa. Dicha x se llama un **contraejemplo**.

Ejemplo 4.1.4 Refutación con un contraejemplo

Refute el siguiente enunciado encontrando un contraejemplo:

$$\forall \text{ números reales } a \text{ y } b, \text{ si } a^2 = b^2 \text{ entonces } a = b.$$

Solución Para refutar esta afirmación, se necesitan encontrar los números reales a y b tales que la hipótesis $a^2 = b^2$ es verdadera y la conclusión $a = b$ es falsa. El hecho de que tanto

enteros positivos como negativos tienen cuadrados positivos ayuda en la búsqueda. Si piensa en algunas posibilidades, verá rápidamente que 1 y -1 funcionarán (o 2 y -2, o el 0.5 y -0.5 y así sucesivamente).

Enunciado: $\forall$ números reales a y b, si $a^2 = b^2$, entonces $a = b$.

Contraejemplo: Sea $a = 1$ y $b = -1$. Entonces $a^2 = 1^2 = 1$ y $b^2 = (-1)^2 = 1$ y así $a^2 = b^2$. Pero $a \neq b$ ya que $1 \neq -1$.

■

Es un signo de inteligencia hacer generalizaciones. Con frecuencia, después de observar una propiedad que se mantiene en un gran número de casos, es posible suponer que se mantiene en todos los casos. Sin embargo, puede, tener problemas al intentar demostrar su conjetura. Tal vez simplemente no han descubierto la clave de la demostración. Pero tal vez su suposición es falsa. Por tanto, cuando usted está teniendo serias dificultades para demostrar un enunciado general, debe interrumpir sus esfuerzos para buscar un contraejemplo. Analizar los tipos de problemas que está encontrando en sus esfuerzos por demostrar puede ayudar en la búsqueda. Incluso puede suceder que si usted encuentra un contraejemplo y por tanto demostrar que el enunciado es falso, su comprensión puede ser lo suficientemente clara que se puede formular una versión más limitada, pero verdadera del enunciado. Por ejemplo, el ejemplo 4.1.4 muestra que no siempre es verdad que si los cuadrados de dos números son iguales, entonces los números son iguales. Sin embargo, es verdad que si los cuadrados de dos números *positivos* son iguales, entonces los números son iguales.

Prueba de enunciados universales

La gran mayoría de los enunciados matemáticos que deben probarse son universales. Al analizar cómo demostrar dichos enunciados, es útil imaginarlos en una forma estándar:

$$\forall x \in D, \text{ si } P(x) \text{ entonces } Q(x)$$

Las secciones 1.1 y 3.1 presentan ejemplos que muestran cómo escribir un enunciado universal en esta forma. Cuando D es finito o cuando sólo un número finito de elementos que satisfacen $P(x)$, dicho enunciado se puede probar con el método de agotamiento.

Ejemplo 4.1.5 El método de agotamiento

Utilice el método de agotamiento para probar el siguiente enunciado:

> $\forall n \in \mathbf{Z}$, si n es par y $4 \leq n \leq 26$, entonces n se puede escribir como una suma de dos números primos.

Solución

$$4 = 2 + 2 \qquad 6 = 3 + 3 \qquad 8 = 3 + 5 \qquad 10 = 5 + 5$$
$$12 = 5 + 7 \qquad 14 = 11 + 3 \qquad 16 = 5 + 11 \qquad 18 = 7 + 11$$
$$20 = 7 + 13 \qquad 22 = 5 + 17 \qquad 24 = 5 + 19 \qquad 26 = 7 + 19$$

■

En la mayoría de los casos en matemáticas, sin embargo, el método del agotamiento no se puede utilizar. Por ejemplo, ¿puede probar por agotamiento que *cada* entero par mayor que 2 puede escribirse como la suma de dos números primos? No. Para hacer eso tendría que revisar cada entero par y puesto que hay un infinito de dichos números, ésta es una tarea imposible.

Aun cuando el dominio es finito, puede ser no factible utilizar el método de agotamiento. Imagine, por ejemplo, que está tratando de comprobar por agotamiento que el circuito de multiplicación de una computadora dada, da el resultado correcto para cada par de números en el rango de la computadora. Ya que en una computadora típica se requerirían de miles de años sólo para calcular todos los productos posibles de todos los números en su rango (por no mencionar el tiempo que se tardaría en comprobar la exactitud de las respuestas), comprobar la corrección por el método de agotamiento es, obviamente, poco práctico.

La técnica más poderosa para demostrar que un enunciado universal es uno que funciona independientemente del tamaño del dominio sobre el cual se cuantifica el enunciado. Se llama *el método de generalización a partir de lo particular*. Esta es la idea que subyace en el método:

Método de generalización a partir de lo particular

Para mostrar que cada elemento de un conjunto cumple una determinada propiedad, supongamos que x es un elemento *particular*, pero que se *eligió arbitrariamente* del conjunto y se demuestra que x satisface la propiedad.

Ejemplo 4.1.6 Generalización a partir de lo particular

En algún momento puede haber mostrado un "truco matemático" como el siguiente. Le pide a una persona que elija cualquier número, le suma 5, lo multiplica por 4, le resta 6, lo divide entre 2 y le resta el doble del número original. Después sorprenderá a la persona presentando que su resultado final fue 7. ¿Cómo funciona este "truco"? Deje una caja vacía □ o establezca el símbolo x para el número que la persona eligió. A continuación se presenta lo que sucede cuando la persona sigue sus instrucciones:

Paso	Resultado visual	Resultado algebraico
Elija un número.	□	x
Sume 5.	□ | | | | |	$x + 5$
Multiplique por 4.	□ | | | | | □ | | | | | □ | | | | | □ | | | | |	$(x + 5) \cdot 4 = 4x + 20$
Reste 6.	□ | | □ | | □ | | | | | □ | | | | |	$(4x + 20) - 6 = 4x + 14$
Divida entre 2.	□ | | □ | | | | |	$\frac{4x + 14}{2} = 2x + 7$
Reste dos veces el número original.	| | | | | | |	$(2x + 7) - 2x = 7$

Por tanto no importa con qué número inicie la persona, el resultado siempre será 7. Observe que la x en el análisis anterior es particular (ya que representa una cantidad individual), pero también es elegido arbitrariamente o genérico (ya que cualquier número que sea se puede poner en su lugar). Esto muestra el proceso de sacar una conclusión general de un objeto genérico particular. ■

El punto de tener que elegir arbitrariamente a x (o genérico) es para hacer una demostración que se pueda generalizar a todos los elementos del dominio. Al elegir x arbitrariamente, no está haciendo ninguna suposición especial acerca de x que no sea verdad para todos los demás elementos del dominio. La palabra *genérico* significa "compartir todas las características comunes con un grupo o clase". Por tanto todo lo que deducimos de un elemento genérico x del dominio es igualmente verdadero para cualquier otro elemento del dominio.

Cuando se aplica el método de la generalización de lo particular a lo general a una propiedad de la forma "Si $P(x)$, entonces $Q(x)$", el resultado es el método de *demostración directa*. Recuerde que la única forma en que un enunciado si-entonces pueda ser falso es que la hipótesis es verdadera y la conclusión es falsa. Por tanto, dado el enunciado "Si $P(x)$ entonces $Q(x)$", puede demostrar que la verdad de $P(x)$ obliga a la verdad de $Q(x)$, entonces se habrá demostrado el enunciado. Lo que se deduce por el método de la generalización de lo particular a lo general para demostrar que "$\forall x$, si $P(x)$, entonces $Q(x)$" es verdadero para *todos* los elementos x en un conjunto D, suponga que x es un elemento particular, pero elegido arbitrariamente de D que hace que a $P(x)$ verdadero y después demuestre que x hace a $Q(x)$ verdadero.

Método de demostración directa

1. Exprese el enunciado a demostrar en la forma "$\forall x \in D$, si $P(x)$, entonces $Q(x)$". (Con frecuencia este paso se hace mentalmente.)
2. Inicie la demostración, suponiendo que x es un elemento particular pero que se elige arbitrariamente de D para que la hipótesis de $P(x)$ sea verdadera. (Este paso con frecuencia se abrevia como "Supongamos $x \in D$ y $P(x)$".)
3. Demuestre que la conclusión $Q(x)$ es verdadera usando las definiciones, previamente establecidos y las reglas de inferencia lógica.

Ejemplo 4.1.7 Una demostración directa de un teorema

¡Precaución! La palabra *dos* en este enunciado no se refiere necesariamente a dos enteros distintos. Si se hace una selección arbitraria de números enteros, los enteros son muy probablemente distintos, pero podrían ser iguales.

Demuestre que la suma de dos enteros pares es par.

Solución Cada vez que se le presenta un enunciado a demostrar es una buena idea preguntarle si usted cree que es verdadero. En este caso se puede imaginar algunos pares de enteros pares, por ejemplo $2 + 4$, $6 + 10$, $12 + 12$, $28 + 54$ y comprobar mentalmente que sus sumas son pares. Sin embargo, ya que no puede comprobar todos los pares de números pares, no se puede saber a ciencia cierta que el enunciado es verdadero, en general al comprobar su veracidad en estos casos en particular. Muchas propiedades son válidas para un gran número de ejemplos y, sin embargo no son verdaderas en general.

Para demostrar este enunciado, en general, se tiene que demostrar que no importa qué enteros pares se den, su suma es par. Sin embargo, dados dos números enteros pares, es posible representarlos como $2r$ y $2s$ para algunos enteros r y s. Y por la ley distributiva del álgebra, $2r + 2s = 2(r + s)$, que es par. Así, el enunciado es verdadero en general.

Supongamos que el enunciado que demostró era mucho más complicado que este. ¿Qué método podría utilizar para obtener una demostración?

Reexpresión formal: $\forall$ enteros m y n, si m y n son pares entonces $m + n$ es par.

Este enunciado es universalmente cuantificado sobre un dominio infinito. Así, para demostrarlo en general, necesita demostrar que no importa qué par de números enteros le den, si ambos son pares entonces su suma también será par.

A continuación se pregunta: ¿de dónde estoy partiendo? o ¿qué estoy suponiendo? La respuesta a esa pregunta le da el punto de partida o la primera frase de la demostración.

Punto de partida: Supongamos que m y n son números enteros en particular, pero arbitrariamente elegidos que son pares.

O, en forma abreviada:

Supongamos que m y n son cualesquier enteros pares.

Entonces se pregunta, ¿qué conclusión necesito mostrar para terminar la demostración?

Para demostrar que: $m + n$ es par.

En este punto es necesario preguntarse, ¿cómo puedo llegar a la conclusión desde el punto de partida? Dado que ambas implican el término *entero par*, debemos utilizar la definición de este término y por tanto usted debe saber lo que significa que un número entero sea par. Se deduce de la definición que ya que m y n son pares, cada uno es igual al doble de un número entero. Una de las leyes básicas de la lógica, llamada *instanciación existencial*, dice, en efecto, que si usted sabe que algo existe, puede darle un nombre. Sin embargo, no se puede utilizar el mismo nombre para referirse a dos cosas diferentes, los que están actualmente bajo análisis.

Instanciación existencial

Si se supone la existencia de un cierto tipo de objeto o se ha deducido entonces se le puede dar un nombre, siempre y cuando ese nombre no esté siendo utilizado actualmente para designar a otra cosa.

¡Precaución! Ya que m y n son elegidos arbitrariamente, podrían ser cualquier par de números enteros pares. Una vez que se introduce r para satisfacer $m = 2r$, entonces r no está disponible para representar otra cosa. Si se ha establecido que $m = 2r$ y $n = 2r$, entonces m será igual a n, que no tiene por qué ser el caso.

Así, ya que m es igual al doble de un número entero, se puede dar ese entero un nombre y puesto que n es igual a dos veces un número entero, también puede dar ese entero un nombre:

$$m = 2r, \text{ para algún entero } r \qquad \text{y} \qquad n = 2s, \text{ para algún entero } s.$$

Ahora lo que quiere demostrar es que $m + n$ es par. En otras palabras, desea demostrar que $m + n$ es igual a $2 \cdot$ (algún entero). Después de haber encontrado representaciones alternativas para m (como $2r$) y para n (como $2s$), parece razonable sustituir estas representaciones en lugar de m y s:

$$m + n = 2r + 2s.$$

Su objetivo es demostrar que $m + n$ es par. Por definición de par, esto significa que $m + n$ se puede escribir en la forma

$$2 \cdot (\text{algún entero}).$$

Este análisis estrecha la brecha entre el punto de partida y lo que se verifica al demostrar que

$$2r + 2s = 2 \cdot (\text{algún entero}).$$

¿Por qué es esto cierto? En primer lugar, debido a la ley distributiva del álgebra, que dice que

$$2r + 2s = 2(r + s)$$

y, segundo, ya que la suma de dos números enteros es un número entero, lo que implica que $r + s$ es un número entero.

Este análisis se resume al reescribir el enunciado como un teorema y dar una demostración formal del mismo. (En matemáticas, la palabra *teorema* se refiere a un enunciado que se sabe que es verdadero porque se ha demostrado.) La demostración formal, así como muchas otras en este libro, incluye notas explicativas para hacer su flujo lógico aparente. Estos comentarios son simplemente una conveniencia para el lector y pueden ser omitidos por completo. Por esta razón, están en cursiva y encerrado en cursiva entre corchetes: *[ ]*.

Donald Knuth, uno de los pioneros de la ciencia computacional, ha comparado la construcción de un programa de computadora de un conjunto de especificaciones con la escritura de una demostración matemática basada en un conjunto de axiomas.* De acuerdo con esta analogía, los comentarios entre paréntesis se pueden pensar como parecidos a la documentación explicativa presentada por un buen programador. La documentación no es necesaria para que un programa se ejecute, pero ayuda a que un lector humano entienda lo que está pasando.

Teorema 4.1.1

La suma de dos números enteros pares es par.

Demostración:

Supongamos que m y n son *[particulares, pero arbitrariamente elegidos]*, números enteros pares. *[Debemos demostrar que $m + n$ es par.]* Por definición de par, $m = 2r$ y $n = 2s$ para algunos enteros r y s. Entonces,

$$\begin{aligned} m + n &= 2r + 2s && \text{por sustitución} \\ &= 2(r + s) && \text{factorizando a 2.} \end{aligned}$$

Nota Introducir t igual a $r + s$ es otro uso de la instanciación existencial.

Sea $t = r + s$. Observe que t es un número entero, porque es una suma de números enteros. Por tanto

$$m + n = 2t \quad \text{donde } t \text{ es un número entero.}$$

De lo que se deduce, por definición de par ya que $m + n$ es par. *[Esto es lo que necesita para demostrar.]*†

■

La mayoría de los teoremas, como el anterior, se pueden analizar en un punto donde se dé cuenta de que tan pronto como una determinada cosa sea demostrada, el teorema se demostrará. Cuando esa cosa se ha demostrado, es natural para poner finalizar la prueba con las palabras "esto es lo que quería demostrar". Las palabras en latín de esto son *quod erat demonstrandum* o Q.E.D. para abreviar. Las demostraciones en la mayoría de los libros viejos de matemáticas finalizan con estas iniciales.

Observe que tanto las partes *si* como *sólo si* de la definición de par fueron utilizadas en la demostración del teorema 4.1.1. Ya que se sabe que m y n son pares, la parte *sólo si* ($\Rightarrow$) de la definición se utilizaron para deducir que m y n tenían cierta forma general. Entonces, después de cierta sustitución y manejo algebraico, la parte *si* ($\Leftarrow$) de la definición se utiliza para deducir que $m + n$ era par.

Instrucciones para escribir demostraciones de enunciados universales

Piense en una demostración como una manera de comunicar un argumento convincente de la veracidad de un enunciado matemático. Cuando se escribe una demostración, imagine que usted se lo envía a un compañero capaz que ha tenido que perder la última o dos semanas de su curso. Trate de ser claro y completo. Tenga en cuenta que su compañero de clase sólo verá lo que realmente está escrito, no los pensamientos no expresados detrás de él. Idealmente, la demostración conducirá a su compañero de clase para entender por qué el enunciado es verdadero.

*Donald E. Knuth, *The Art of Computer Programing* 2*a*. ed., Vol. I (Reading, Massachusetts: Addison-Wesley, 1973), p. ix.

† Consulte la página 134 para un análisis sobre el papel de *modus ponens* universal en esta prueba.

Con los años, las siguientes reglas de estilo se han convertido en bastante comunes para la escritura de las versiones finales de las demostraciones:

1. **Copie el enunciado del teorema que demostrará en su papel.**
2. **Marque con claridad el comienzo de la demostración con la palabra Demostración.**
3. **Haga su demostración autocontenida.**

   Esto significa que debe explicar el significado de cada variable utilizada en la prueba en el cuerpo de la demostración. Así comenzará las demostraciones presentando las variables iniciales e indicando qué tipo de objetos que son. La primera frase de su demostración sería algo así como "Supongamos que m y n son cualesquier enteros pares" o "Sea x un número real tal que x es mayor que 2". Esto es similar a declarar variables y sus tipos de datos al inicio de un programa de computadora.

   En un punto más adelante en la demostración, es posible introducir una nueva variable para representar una cantidad que se sabe que existe en ese momento. Por ejemplo, si usted ha supuesto que un entero dado n, es par, entonces usted sabe que n es igual a 2 veces algún entero y puede dar a este número entero un nombre, para que pueda trabajar con él en concreto más adelante en la demostración. Así, si decide llamar al número entero, por ejemplo, s, usted escribiría: "Ya que n es par, $n = 2s$ para algunos entero s", o "ya que n es par, existe un entero s tal que $n = 2s$".
4. **Escriba su demostración completa, con oraciones gramaticalmente correctas.**

   Esto no significa que debe evitar el uso de símbolos y abreviaturas, sólo que debe incorporarlas en las oraciones. Por ejemplo, la demostración del teorema 4.1.1 contiene la frase

   $$\begin{aligned} \text{Entonces } m + n &= 2r + 2\text{s} \\ &= 2(r + s). \end{aligned}$$

   Para leer el texto como una oración, lea el primer signo de igualdad como "igual a" y cada signo de igualdad posterior como "lo que es igual a".
5. **Mantenga a su lector informado sobre el estado de cada enunciado en su demostración.**

   Su lector nunca debe dudar acerca de si algo en su demostración que se ha supuesto o establecido o aún no se ha deducido. Si hay algo que se supone, escriba una introducción de la palabra como *Suponga* o *Asuma*. Si aún no se ha demostrado, escriba esto con palabras como, *Debemos demostrar que* o *En otras palabras, debemos demostrar que*. Esto es especialmente importante si se introduce una variable para reformular lo que necesita para demostrar. (Vea Errores comunes en la siguiente página.)
6. **Dé una razón para cada afirmación en su demostración.**

   Cada afirmación en una demostración debe venir directamente de la hipótesis del teorema; deducirse de la definición de uno de los términos del teorema; ser un resultado obtenido anteriormente en la demostración; ser un resultado matemático que ha sido previamente establecido o que se acuerda suponer. Indique el motivo de cada paso de la demostración usando frases como, *por hipótesis*, *por definición de* . . . y *por el teorema* . . . .
7. **Incluya las "pequeñas palabras y frases" que hacen la lógica de sus argumentos clara.**

   Cuando se escribe un argumento matemático, sobre todo una demostración, indique cómo cada frase está relacionada con la anterior. ¿Se deduce de la frase anterior o de una combinación de la frase anterior y las anteriores? Si es así, inicie la frase estableciendo la razón por la que se deduce o escribiendo *Entonces*, *Por tanto*, *Así*, *Por consiguiente*, *Por tanto*, *En consecuencia, De lo que se deduce que* e incluya la razón al final de la frase. Por ejemplo, en la demostración del teorema 4.1.1, una vez que sabe que m es par, se puede escribir: "Por definición de par, $m = 2r$ para alguno entero r", o puede escribir, "Entonces, $m = 2r$ para alguno entero r por definición de par".

Si una frase expresa un nuevo pensamiento o de hecho que no se deduce como consecuencia inmediata del enunciado anterior, pero es necesario para una parte posterior de una demostración, presentar por escrito *Observe que*, *Note que*, *Pero* o *Ahora*.

A veces, en una demostración es conveniente definir una nueva variable en términos de las variables anteriores. En tal caso, introduzca la nueva variable con la palabra *Sea*. Por ejemplo, en la demostración del teorema 4.1.1, una vez que se sabe que $m + n = 2(r + s)$, donde r y s son números enteros, se introduce una nueva variable t para representar a $r + s$. La demostración continúa diciendo, "Sea $t = r + s$. Entonces t es un entero ya que es una suma de dos números enteros".

8. **Presente ecuaciones y desigualdades.**

La convención es presentar ecuaciones y desigualdades en renglones separados para aumentar la legibilidad, tanto para los demás, como para nosotros mismos así con facilidad podemos comprobar la exactitud de nuestro trabajo. Seguimos la convención en el texto de este libro, pero con el fin de ahorrar espacio, la violamos en algunos de los ejercicios y en muchas de las soluciones contenidas en el apéndice B. Así puede necesitar copiar algunas partes de las soluciones en papel borrador para comprenderla plenamente. Por favor, siga la convención en su propio trabajo. Deje suficiente espacio vacío y ¡no sea tacaño con el papel!

Variación entre demostraciones

Es raro que dos demostraciones de un enunciado dado, escrito por dos personas diferentes, sean idénticos. Aun cuando los pasos matemáticos básicos sean los mismos, las dos personas pueden usar diferentes notaciones o pueden dar distintas cantidades de explicación para sus pasos o pueden elegir diferentes palabras para vincular los pasos juntos en forma de párrafo. Una cuestión importante es el grado de detalle de las explicaciones de los pasos de una demostración. En última instancia, esto debe ser resuelto entre el escritor de una demostración y el lector previsto, ya sea que se trate de estudiantes y profesores, maestro y estudiante, estudiante y compañero de estudios o matemático y colega. Su profesor puede proporcionar directrices explícitas para que usted las utilice en su curso. O puede seguir el ejemplo de las demostraciones en este libro (que generalmente se explica totalmente con el fin de ser comprendidos por los estudiantes en las diversas etapas de desarrollo matemático). Recuerde que las frases escritas entre corchetes *[ ]* tienen por objeto dilucidar el flujo lógico o suposiciones subyacentes de la demostración y no se necesita escribir debajo de todo. Es enteramente su decisión si se debe incluir frases en sus propias demostraciones.

Errores comunes

Los siguientes son algunos de los errores más comunes que se cometen al escribir demostraciones matemáticas.

1. **Argumentar a partir de ejemplos.**

Revisar ejemplos es una de las prácticas más útiles en las que un solucionador de problemas puede participar y se sienta motivado por todos los buenos profesores de matemáticas. Sin embargo, es un error pensar que un enunciado general se puede demostrar al enseñar que es verdadero para algunos casos especiales. Una propiedad a la que se refiere en un enunciado universal puede ser verdadera en muchos casos sin ser verdadera en general.

A continuación se presenta un ejemplo de este error. Se trata de una "demostración" incorrecta del hecho de que la suma de dos enteros pares es par. (Teorema 4.1.1.)

> Esto es verdad porque si $m = 14$ y $n = 6$, que son a la vez, pares, entonces $m + n = 20$, que también es par.

Algunas personas encuentran este tipo de argumentos convincentes, ya que, después de todo, consisten en pruebas en apoyo de una conclusión verdadera. Pero recuerde

que cuando hablamos de argumentos válidos, indicamos que un argumento puede ser inválido y, sin embargo, tener una conclusión verdadera. De la misma manera, un argumento a partir de ejemplos se puede utilizar erróneamente para "demostrar" un enunciado verdadero. En el ejemplo anterior, no es suficiente demostrar que la conclusión "$m + n$ es par" es verdadera para $m = 14$ y $n = 6$. Debe dar un argumento para demostrar que la conclusión es verdadera para cualesquier enteros pares m y n.

2. **Usar la misma letra para significar dos cosas diferentes.**

   Algunos demostradores principiantes dan a una nueva cantidad variable el nombre de la misma letra introducida antes como una variable. Considere el siguiente fragmento de "demostración":

   > Supongamos que m y n son cualesquier enteros impares. Entonces, por definición, de impar, $m = 2k + 1$ y $n = 2k + 1$ para algún entero k.

   Esto es incorrecto. Usar el mismo símbolo, k, en las expresiones para m y n implica que $m = 2k + 1 = n$. De lo que se deduce que el resto de la demostración se aplica sólo a los enteros m y n que son iguales entre sí. Esto es inconsistente con la suposición de que m y n son algunos enteros impares arbitrariamente elegidos. Por ejemplo, la demostración no demuestra que la suma de 3 y 5 es par.

3. **Saltar a una conclusión.**

   Saltar a una conclusión significa alejar la verdad de algo sin dar una razón adecuada. Considere la siguiente "demostración" de que la suma de dos enteros pares es par.

   > Supongamos que m y n son cualesquier enteros pares. Por definición de par, $m = 2r$ y $n = 2s$ para algunos enteros r y s. Entonces $m + n = 2r + 2s$. Así $m + n$ es par.

   El problema con esta "demostración" es que falta el cálculo crucial

   $$2r + 2s = 2(r + s)$$

   está omitido. El autor de la "demostración" ha saltado antes de tiempo a una conclusión.

4. **Razonamiento circular.**

   Participar en el razonamiento circular, significa asumir que lo que se ha demostrado, es una variación de saltar a una conclusión. Como ejemplo, considere la siguiente "demostración" de que el producto de dos enteros impares es impar:

   > Supongamos que m y n son cualesquier enteros impares. Cuando cualesquier enteros impares se multiplican, su producto es impar. Por tanto mn es impar.

5. **Confusión entre lo que se sabe y lo que aún no se ha demostrado.**

   Una forma más sutil de participar en un razonamiento circular se produce cuando la conclusión que se muestra se actualiza utilizando una variable. A continuación se presenta un ejemplo en una "demostración" de que el producto de dos enteros impares es impar:

   > Supongamos que m y n son cualesquier enteros impares. Debemos demostrar que mn es impar. Esto significa que existe un entero s tal que
   >
   > $$mn = 2s + 1.$$
   >
   > También, por definición de impar, existen números enteros a y b tal que
   >
   > $$m = 2a + 1 \text{ y } n = 2b + 1.$$
   >
   > Entonces,
   >
   > $$mn = (2a + 1)(2b + 1) = 2s + 1.$$
   >
   > Por tanto, ya que s es un número entero, mn es impar, por definición, de impar.

   En este ejemplo, cuando el autor recapituló la conclusión que se muestra (que mn es impar), el autor escribió "existe un entero s tal que $mn = 2s + 1$". Más tarde el autor saltó a una conclusión injustificada al suponer la existencia de este s cuando, de hecho,

no se había establecido. Este error podría haberse evitado si el autor hubiese escrito "Esto significa que debemos demostrar que existe un entero s tal que

$$mn = 2s + 1".$$

Una manera mejor de evitar este tipo de error no es introducir una variable en una demostración a menos que sea parte de la hipótesis o que se deduzca de ella.

6. **Uso de *cualquier* más que de *alguno*.**

Hay algunas situaciones en las que las palabras *cualquier* y *alguno* se pueden usar indistintamente. Por ejemplo, al iniciar una demostración de que el cuadrado de cualquier número entero impar es impar, uno podría correctamente escribir "Supongamos que m es un entero impar" o "Supongamos que m es un entero impar". Sin embargo, en la mayoría de situaciones, las palabras *cualquier* y *alguno* no son intercambiables. Aquí está el comienzo de una "demostración" de que el cuadrado de cualquier número entero impar es impar, que utiliza *cualquier* cuando la palabra correcta es *alguno*:

> Supongamos que m es un entero impar dado, pero elegido arbitrariamente.
> Por definición de impar $m = 2a + 1$ para cualquier entero a.

En la segunda frase es incorrecto decir que "$m = 2a + 1$ para cualquier entero a" porque a no puede ser "cualquier" entero, de hecho, al resolver $m = 2a + 1$ para a se muestra que el único valor posible para a es $(m - 1)/2$. La forma correcta para terminar la frase es, "$m = 2a + 1$ para algún entero a" o "existe un número entero a tal que $m = 2a + 1$".

7. **Mal uso de la palabra *si*.**

Otro error común no es grave en sí mismo, sino que refleja el pensamiento impreciso que a veces conduce problemas más adelante en una demostración. Este error implica el uso de la palabra *si* cuando la palabra, *porque* es realmente significativa. Considere el siguiente fragmento de demostración:

> Supongamos que p es un número primo. Si p es primo, entonces p no se puede escribir como producto de dos números enteros positivos más pequeños.

El uso de la palabra *si* en la segunda frase es inapropiado. Se sugiere que lo primo de p está en duda. Pero se sabe que p es primo en la primera frase. No se puede escribir como un producto de dos números enteros positivos menores *debido* a que es primo. En seguida se presenta una versión correcta del fragmento:

> Supongamos que p es un número primo. Dado que p es primo, p no se puede escribir como el producto de dos números enteros positivos menores.

Obtención del inicio de demostraciones

Lo crea o no, una vez que comprende la idea de la generalización de lo particular a lo general y del método de la demostración directa, se puede escribir el inicio de las demostraciones, aún para teoremas que no entienda. La razón es que el punto de partida y lo que se muestra en una demostración depende sólo de la forma lingüística del enunciado a demostrar, no del contenido del enunciado.

Ejemplo 4.1.8 Identificación del "punto de partida" y de la "conclusión que se demostrará"

Escriba la primera frase de una demostración (el "punto de partida") y la última frase de una demostración (la "conclusión que se demuestra") del siguiente enunciado:

Nota No espere saber nada de gráficos bipartidos completos.

Cada grafo completo, bipartido es conexo.

Solución Es útil reescribir la instrucción formal con un cuantificador y una variable:

Reexpresión formal: $\forall$ grafo G (dominio), si G es completo y bipartido (hipótesis), entonces G es conexo (conclusión).

La primera frase, o punto de partida, de una demostración supone la existencia de un objeto (en este caso, G) en el dominio (en este caso el conjunto de todos los grafos) que satisfacen la hipótesis de la parte si-entonces del enunciado (en este caso que G es completo y bipartido). La conclusión que se muestra es sólo la conclusión de la parte si-entonces del enunciado (en este caso que G es conexo).

Punto de partida: Supongamos que G es un grafo *[particular, pero elegido arbitrariamente]* tal que G es completo y bipartido.

Conclusión que se muestra: G es conexo.

Así, la demostración tiene la forma siguiente:

Demostración:

Supongamos que G es un grafo *[particular, pero elegido arbitrariamente]* tal que G es completo y bipartido.
⋮
Por tanto, G es conexo. ■

Mostrando que un enunciado existencial es falso

Recordemos que la negación de un enunciado existencial es universal. De lo que se deduce que para demostrar un enunciado existencial que es falso, tiene que demostrar un enunciado universal (su negación) que es verdadero.

Ejemplo 4.1.9 Refutación de un enunciado existencial

Demuestre que el siguiente enunciado es falso:

Hay un entero positivo n tal que $n^2 + 3n + 2$ es primo.

Solución Demostrar que el enunciado dado es falso es equivalente a demostrar que su negación es verdadera. La negación es

Para todos los enteros positivos n, $n^2 + 3n + 2$ no es primo.

Ya que la negación es universal, si se demuestra mediante la generalización a partir de lo particular.

Afirmación: El enunciado "Hay un entero positivo n tal que $n^2 + 3n + 2$ es primo" es falso.

Demostración:

Supongamos que n es cualquier *[particular, pero arbitrariamente elegido]* entero positivo. *[Vamos a demostrar que $n^2 + 3n + 2$ no es primo.]* Podemos factorizar $n^2 + 3n + 2$ como $n^2 + 3n + 2 = (n + 1)(n + 2)$. También observamos que $n + 1$ y $n + 2$ son enteros (ya que son sumas de enteros) y que tanto $n + 1 > 1$ como $n + 2 > 1$ (ya que $n \geq 1$). Así $n^2 + 3n + 2$ es un producto de dos enteros cada uno mayor que 1 y así $n^2 + 3n + 2$ no es primo. ■

Conjetura, demostración y refutación

Hace más de 350 años, el matemático francés Pierre de Fermat afirmó que es imposible encontrar números enteros positivos x, y y z con $x^n + y^n = z^n$ si n es un entero que es al menos 3. (Para $n = 2$, la ecuación tiene muchas soluciones enteras, como $3^2 + 4^2 = 5^2$ y $5^2 + 12^2 = 13^2$.) Fermat escribió su afirmación en la margen de un libro, junto con el comentario de "he descubierto una DEMOSTRACIÓN verdaderamente notable de este teorema que este margen es demasiado pequeño para contenerla". Sin embargo, no se encontró ninguna demostración, entre sus papeles y durante años algunas de las mentes matemáticas

Bettmann/CORBIS

Pierre de Fermat (1601-1665)

Andrew Wiles/Princeton University

Andrew Wiles (nació en 1953)

más brillantes intentaron sin éxito descubrir una demostración o un contraejemplo, por lo que llegó a ser conocido como el último teorema de Fermat.

En 1986 Kenneth Ribet, de la Universidad de California en Berkeley demostró que si un enunciado dado diferente, la conjetura de Taniyama-Shimura, se podía comprobar, entonces se deduciría el teorema de Fermat. Andrew Wiles, un matemático inglés y miembro de la facultad en la Universidad de Princeton, estaba intrigado con la afirmación de Fermat, desde que era un niño y como adulto, había estado trabajando en la rama de las matemáticas a la que pertenecía la conjetura de Taniyama-Shimura. Tan pronto como se enteró del resultado de Ribet, Wiles de inmediato se puso a trabajar para demostrar la conjetura. En junio de 1993, después de 7 años de un concentrado esfuerzo, presentó una demostración con gran éxito a todo el mundo.

Sin embargo, durante el verano de 1993, mientras que cada parte de la demostración estaba siendo cuidadosa y totalmente comprobada para preparar su publicación formal, Wiles descubrió que no podía justificar un paso y ese paso mostraría que en realidad podría estar equivocado. Trabajó sin descanso por un año para resolver el problema, dándose cuenta de que la brecha en la demostración era un error involuntario, pero que un método con el que había trabajado en años anteriores y lo había abandonado siempre que de alguna forma evitaba la dificultad. A finales de 1994, la demostración había sido revisada cuidadosamente comprobada y escrita correctamente en cada detalle por expertos en la materia. Se publicó en la revista *Annals of Mathematics* en 1995. Varios libros y un excelente documental de televisión han sido producidos para comunicar el drama y la emoción del descubrimiento de Wiles.*

Uno de los problemas más antiguos en matemáticas que sigue sin resolverse es la conjetura de Goldbach. En el ejemplo 4.1.5 se demostró que todo entero par del 4 al 26 se puede representar como una suma de dos números primos. Hace más de 250 años, Christian Goldbach (1690-1764) conjeturó que todo entero par mayor que 2 se puede representar así. Los cálculos explícitos asistidos por computadora han demostrado la conjetura de que es verdad por lo menos hasta 10^{18}. Pero hay un abismo enorme entre 10^{18} y el infinito. Como ha indicado James Gleick del *New York Times*, muchas otras conjeturas plausibles en la teoría de números han resultado ser falsas. Por ejemplo, Leonhard Euler (1707-1783), propuso en el siglo XVIII que $a^4 + b^4 + c^4 = d^4$ tenía soluciones no triviales de números enteros. En otras palabras, no hay tres potencia a la cuarta perfectas que sumadas den otra cuarta potencia perfecta. Para números pequeños, la conjetura de Euler se veía bien. Pero en 1987 un matemático de Harvard, Noam Elkies, demostró que estaba mal. Un contraejemplo, encontrado por Roger Frye de Thinking Machines Corporation en una gran computadora de búsqueda, es $95\,800^4 + 217\,519^4 + 414\,560^4 = 422\,481^4$.†

En mayo de 2000, "para celebrar las matemáticas en el nuevo milenio", anunció el Instituto Clay de Matemáticas de Cambridge, Massachusetts, que se otorgarían premios de $1 millón para cada una de las soluciones a siete preguntas de grandes datos, matemática clásica. Uno de ellos, "P vs. NP", pregunta si los problemas que pertenecen a una determinada clase se pueden resolver en una computadora usando métodos más eficaces que los métodos muy ineficientes con los que actualmente trabajan ellos. Esta cuestión se analiza brevemente al final del capítulo 11.

Autoexamen

Las respuestas a las preguntas del autoexamen se encuentran al final de cada sección.

1. Un entero es par si y sólo si, _____.
2. Un entero es impar si y sólo si, _____.
3. Un entero n es primo si y sólo si, _____.
4. La manera más común de refutar un enunciado universal es encontrar _____.

*"The Proof", producida en 1997, para la serie *Nova* del Sistema Público de Radiodifusión; *Fermat's Enigma: The Epic Quest to Solve the World's Greatest Mathemathical Problem*, de Simon Singh y John Lynch (New York: Bantam Books, 1998); *Fermat's Last Theorem: Unlocking The Secret of an Ancient Mathematical Problem* de Amir D. Aczel (Nueva York: Delacorte Press, 1997).

†James Gleick, "Fermat's Last Theorem Still Has Zero Solutions", New York Times, 17 de abril de 1988.

5. De acuerdo con el método de la generalización a partir de lo particular, para demostrar que cada elemento de un conjunto cumple una determinada propiedad, supongamos que x es un _____ y demostremos que _____.

6. Utilice el método de demostración directa para demostrar un enunciado de la forma, "Para toda x en un conjunto D, si $P(x)$, entonces $Q(x)$" se supone que _____ y uno muestra que _____.

Conjuntos de ejercicios 4.1*

En los ejercicios del 1 al 3, utilice las definiciones de los pares, impares, primos y compuestos para justificar cada una de sus respuestas.

1. Supongamos que k es un entero dado.
   a. ¿Es -17 un entero impar? b. ¿Es 0 un entero par?
   c. ¿Es $2k - 1$ un impar?

2. Suponga que m y n son enteros dados.
   a. ¿Es $6m + 8n$ par?
   b. ¿Es $10mn + 7$ impar?
   c. Si $m > n > 0$, es $m^2 - n^2$ compuesto?

3. Suponga que r y s son enteros dados.
   a. ¿Es $4rs$ par?
   b. ¿Es $6r + 4s^2 + 3$ impar?
   c. Si r y s son ambos positivos, ¿es $r^2 + 2rs + s^2$ compuesto?

Demuestre los enunciados de los ejercicios del 4 al 10.

4. Hay números enteros m y n tales que $m > 1$ y $n > 1$ y $\frac{1}{m} + \frac{1}{n}$ es un número entero.

5. Hay m y n enteros distintos tal que $\frac{1}{m} + \frac{1}{n}$ es un entero.

6. Hay números reales a y b tal que
$$\sqrt{a+b} = \sqrt{a} + \sqrt{b}.$$

7. Hay un número entero $n > 5$ tal que $2^n - 1$ es primo.

8. Hay un número real x tal que $x > 1$ y $2^x > x^{10}$.

> **Definición:** Un entero n se llama **cuadrado perfecto** si y sólo si, $n = k^2$ para algún entero k.

9. Hay un cuadrado perfecto que se puede escribir como una suma de otros dos cuadrados perfectos.

10. Hay un entero n tal que $2n^2 - 5n + 2$ es primo.

Refute los enunciados del 11 al 13, dando un contraejemplo.

11. Para todos los números reales a y b, si $a < b$ entonces $a^2 < b^2$.

12. Para todos los enteros n, si n es impar, entonces $\frac{n-1}{2}$ es impar.

13. Para todos los números enteros m y n, si $2m + n$ es impar, entonces m y n son ambos impares.

En los ejercicios del 14 al 16, determine si la propiedad es verdadera para todos los enteros, verdadera para ningún entero o verdadera para algunos enteros y falsa para otros enteros. Justifique su respuesta.

14. $(a + b)^2 = a^2 + b^2$ **H** 15. $-a^n = (-a)^n$

16. El promedio de cualesquiera dos enteros impares es impar.

Demuestre los enunciados en 17 y 18 por el método de agotamiento.

17. Cada número entero positivo par menor de 26 se puede expresar como la suma de tres o menos cuadrados perfectos. (Por ejemplo, $10 = 1^2 + 3^2$ y $16 = 4^2$.)

18. Para cada entero n con $1 \le n \le 10$, $n^2 - n + 11$ es un número primo.

19. a. Reescriba el siguiente teorema de tres maneras diferentes: como ∀ _____, si _____ entonces _____, como ∀ _____, _____ (sin utilizar las palabras *si* o *entonces*) y como Si _____, entonces _____ (sin usar un cuantificador universal explícito).
   b. Complete los espacios en blanco en la prueba del teorema.

   Teorema: La suma de cualquier entero par y cualquier entero impar es impar.

   Demostración: Supongamos que m es cualquier número entero par y n es __(a)__. Por definición de par, $m = 2r$ para algún __(b)__ y por definición de impar, $n = 2s + 1$ para algún entero s. Por sustitución y álgebra,
$$m + n = \text{__(c)__} = 2(r + s) + 1.$$
   Ya que r y s son números enteros, por lo que su suma es $r + s$. Por tanto $m + n$ tiene la forma doble de un número entero más uno y así __(d)__, por definición, de impar.

Cada uno de los enunciados del 20 al 23 es verdadero. Para cada uno, *a*) reescriba el enunciado con la cuantificación implícita como Si _____, entonces, _____ y *b*) escriba la primera frase de una demostración (el "punto de partida") y la última frase de una demostración (la conclusión "que se demuestra"). Observe que no es necesario entender los enunciados para poder hacer estos ejercicios.

20. Para todos los números enteros m, si $m > 1$ entonces $0 < \frac{1}{m} < 1$.

21. Para todos los números reales x, si $x > 1$, entonces $x^2 > x$.

22. Para todos los números enteros m y n, si $mn = 1$, entonces $m = n = 1$ o $m = n = -1$.

23. Para todos los números reales x, si $0 < x < 1$ entonces $x^2 < x$.

*Para los ejercicios con números o letras azules, las soluciones están dadas en el apéndice B. El símbolo **H** indica que sólo se da una sugerencia o una solución parcial. El símbolo ✶ indica que el ejercicio es más difícil de lo normal.

Demuestre los enunciados del 24 al 34. En cada caso use sólo las definiciones de los términos y las suposiciones que se enumeran en la página 146, no todas las propiedades previamente establecidas de enteros pares e impares. Siga las instrucciones que se dan en esta sección para escribir las demostraciones de las enunciados universales.

24. El negativo de cualquier entero par es par.

25. La diferencia de cualquier entero par menos cualquier entero impar es impar.

***H* 26.** La diferencia entre cualquier entero impar y cualquier entero par es impar. (*Nota*: La "demostración" que se muestra en el ejercicio 39 contiene un error ¿Puedes ver qué?).

27. La suma de dos números enteros impares es par.

28. Para todos los enteros n, si n es impar, entonces n^2 es impar.

29. Para todos los enteros n, si n es impar, entonces $3n + 5$ es par.

30. Para todos los números enteros m, si m es par entonces $3m + 5$ es impar.

31. Si k es cualquier entero impar y m es un entero par, entonces, $k^2 + m^2$ es impar.

32. Si a es cualquier entero impar y b es cualquier número entero par, entonces, $2a + 3b$ es par.

33. Si n es un entero par, entonces $(-1)^n = 1$.

34. Si n es un entero impar, entonces $(-1)^n = -1$.

Demuestre que los enunciados del 35 al 37 son falsos.

35. Existe un entero $m \geq 3$ tales que $m^2 - 1$ es primo.

36. Existe un entero n tal que $6n^2 + 27$ es primo.

37. Existe un entero $k \geq 4$ tal que $2k^2 - 5k + 2$ es primo.

Encuentre los errores en las "demostraciones" que se muestran en los ejercicios del 38 al 42.

38. **Teorema:** Para todos los enteros k, si $k > 0$ entonces $k^2 + 2k + 1$ es compuesto.

"**Demostración:** Para $k = 2$, $k^2 + 2k + 1 = 2^2 + 2 \cdot 2 + 1 = 9$. Pero $9 = 3 \cdot 3$ y así 9 es compuesto. Por tanto el teorema es verdadero".

39. **Teorema:** La diferencia entre cualquier número entero impar y cualquier entero par es impar.

"**Demostración:** Supongamos que n es un entero impar y m es cualquier entero par, por definición de impar, $n = 2k + 1$ donde k es un número entero y por definición de par, $m = 2k$, donde k es un entero. Entonces

$$n - m = (2k + 1) - 2k = 1.$$

Pero 1 es impar. Por tanto, la diferencia entre cualquier número entero impar y cualquier entero par es impar".

40. **Teorema:** Para todos los enteros k, si $k > 0$ entonces $k^2 + 2k + 1$ es compuesto.

"**Demostración:** Supongamos que k es cualquier entero tal que $k > 0$. Si $k^2 + 2k + 1$ es compuesto, entonces $k^2 + 2k + 1 = rs$ para algunos enteros r y s tales que

$$1 < r < (k^2 + 2k + 1)$$

y

$$1 < s < (k^2 + 2k + 1).$$

Ya que

$$k^2 + 2k + 1 = rs$$

y tanto r como s están estrictamente entre 1 y $k^2 + 2k + 1$, entonces $k^2 + 2k + 1$ no es primo. Por tanto $k^2 + 2k + 1$ es compuesto como se quería demostrar".

41. **Teorema:** El producto de un entero par y un entero impar es par.

"**Demostración:** Supongamos que m es un entero par y n es un entero impar. Si $m \cdot n$ es par, entonces, por definición de par existe un entero r tal que $m \cdot n = 2r$. También, puesto que m es par, existe un número entero p tal que $m = 2p$ y puesto que n es impar existe un entero q tal que $n = 2q + 1$. Por tanto

$$mn = (2p)(2q + 1) = 2r,$$

donde r es un número entero. Por definición de par, entonces, $n \cdot m$ es par, como se quería demostrar".

42. **Teorema:** La suma de dos enteros pares es igual a $4k$ para algún entero k.

"**Demostración:** Supongamos que m y n son cualesquiera dos números enteros. Por definición de par, $m = 2k$ para algún entero k y $n = 2k$ para algún entero k. Por sustitución,

$$m + n = 2k + 2k = 4k.$$

Esto es lo que se quería demostrar".

En los ejercicios 43 al 60 determine si el enunciado es verdadero o falso. Justifique su respuesta con una demostración o un contraejemplo, según corresponda. En cada caso use sólo las definiciones de los términos y las suposiciones que se enumeran en la página 146 y no todas las propiedades previamente establecidas.

43. El producto de dos enteros impares es impar.

44. El negativo de cualquier entero impar es impar.

45. La diferencia de cualesquiera dos enteros impares es impar.

46. El producto de cualquier número entero par y cualquier número entero es par.

47. Si la suma de dos números enteros es par, entonces uno de los sumandos es par. (En la expresión $a + b$, a y b se llaman **sumandos**.)

48. La diferencia de cualesquiera dos enteros pares es par.

49. La diferencia de cualesquiera dos enteros impares es par.

50. Para todos los enteros n y m, si $n - m$ es par entonces $n^3 - m^3$ es par.

51. Para todos los enteros n, si n es primo entonces $(-1)^n = -1$.

52. Para todos los números enteros m, si $m > 2$ entonces $m^2 - 4$ es compuesto.

53. Para todos los enteros n, $n^2 - n + 11$ es un número primo.

54. Para todos los enteros n, $4(n^2 + n + 1) - 3n^2$ es un cuadrado perfecto.

55. Cada entero positivo puede expresarse como la suma de tres o menos cuadrados perfectos.

H ∗ 56. (Dos números enteros son **consecutivos**, si y sólo si, uno es uno más que el otro.) Cualquier producto de cuatro enteros consecutivos es uno menos que un cuadrado perfecto.

57. Si m y n son números enteros positivos y mn es un cuadrado perfecto, entonces m y n son cuadrados perfectos.

58. La diferencia de los cuadrados de cualesquiera dos números enteros consecutivos es impar.

59. Para todos los números reales no negativos a y b, $\sqrt{ab} = \sqrt{a}\sqrt{b}$. (Observe que si x es un número real no negativo, entonces hay un único número real no negativo y, denotado por $\sqrt{x}$, tal que $y^2 = x$).

60. Para todos los números reales no negativos a y b,

$$\sqrt{a+b} = \sqrt{a} + \sqrt{b}.$$

61. Supongamos que m y n enteros son cuadrados perfectos. Entonces, $m + n + 2\sqrt{mn}$ también es un cuadrado perfecto. ¿Por qué?

H ∗ 62. Si p es un número primo, ¿$2^p - 1$ también debe ser primo? Demuestre o dé un contraejemplo.

∗ 63. Si n es un entero no negativo, ¿debe $2^{2^n} + 1$ ser primo? Demuestre o dé un contraejemplo.

Respuestas del autoexamen

1. es igual a dos veces un número entero 2. es igual al doble de un número entero más 1 3. n es mayor que 1 y si n es igual al producto de dos números enteros positivos, entonces uno de los números enteros es igual a 1 y el otro es igual a n. 4. un contraejemplo 5. elemento particular, pero que se eligió arbitrariamente del conjunto; x satisface la propiedad dada 6. x es un elemento particular, pero arbitrariamente elegido del conjunto D que hace a la hipótesis $P(x)$ verdadera; x hace que la conclusión $Q(x)$ sea verdadera.

4.2 Demostración directa y contraejemplo II: números racionales

Tal es, entonces, todo el arte de convencer. Está contenido en dos principios: en definir todas las notaciones utilizadas y en demostrar siempre sustituyendo mentalmente los términos definidos por sus descripciones. —Blaise Pascal, 1623-1662

Las sumas, diferencias y productos de los números enteros son números enteros. Pero la mayoría de los cocientes de enteros no son números enteros. Sin embargo, es importante saber que los cocientes de enteros, se conocen como *números racionales*.

• Definición

Un número r es **racional** si y sólo si, se puede expresar como un cociente de dos números enteros con un denominador distinto de cero. Un número real que no es racional es **irracional**. Más formalmente, si r es un número real, entonces

$$r \text{ es racional} \Leftrightarrow \exists \text{ enteros } a \text{ y } b \text{ tales que } r = \frac{a}{b} \text{ y } b \neq 0.$$

La palabra *racional* contiene la palabra *razón*, que es otra palabra para el cociente. Un número racional se puede escribir como una razón de números enteros.

Ejemplo 4.2.1 Determinación de si los números son racionales o irracionales

a. ¿Es 10/3 un número racional?

b. ¿Es $-\frac{5}{39}$ un número racional?

c. ¿Es 0.281 un número racional?

d. ¿Es 7 un número racional?

e. ¿Es 0 un número racional?

f. ¿Es 2/0 un número racional?

g. ¿Es 2/0 un número irracional?

h. ¿Es 0.12121212 . . . un número racional (donde se supone que los dígitos 12 se repiten siempre)?

i. ¿Si m y n son números enteros y ni m ni n son cero, es $(m + n)/mn$ un número racional?

Solución

a. Sí, 10/3 es un cociente de los enteros 10 y 3 y por tanto, es racional.

b. Sí, $-\frac{5}{39} = \frac{-5}{39}$, que es un cociente de los enteros -5 y 39 y por tanto, es racional.

c. Sí, $0.281 = 281/1000$. Observe que los números reales representados en una pantalla de la calculadora típica son decimales finitos. Una explicación similar a la de este ejemplo muestra que cualquier número es racional. De lo que se deduce que una calculadora con una pantalla tan sólo puede representar números racionales.

d. Sí, $7 = 7/1$.

e. Sí, $0 = 0/1$.

f. No, 2/0 no es un número (la división entre 0 no está permitida).

g. No, ya que cada número irracional es un número y 2/0 no es un número. En las secciones 4.6, 4.7 y 9.4, se analizan técnicas adicionales para determinar si los números son irracionales.

h. Sí. Sea $x = 0.12121212 \ldots$. Entonces $100x = 12.12121212 \ldots$. Así

$$100x - x = 12.12121212 \ldots - 0.12121212 \ldots = 12.$$

Pero también $100x - x = 99x$ por álgebra básica

Por tanto $99x = 12,$

y así $$x = \frac{12}{99}.$$

Por tanto, $0.12121212 \ldots = 12/99$, que es un cociente de dos números enteros distintos de cero y por tanto es un número racional.

Observe que puede utilizar un argumento similar a éste para demostrar que cualquier decimal periódico es un número racional. En la sección 9.4 se muestra que cualquier número racional se puede escribir como una repetición o terminación de decimales.

i. Sí, ya que m y n son números enteros, así lo son $m + n$ y mn (debido a que las sumas y productos de números enteros son números enteros). También $mn \neq 0$ por la *propiedad del producto cero*. Una versión de esta propiedad, dice lo siguiente:

Propiedad del producto cero

Si ninguno de dos números reales es cero, entonces su producto tampoco es cero.

(Vea el teorema de T11 en el apéndice A y el ejercicio 8 al final de esta sección.) De lo que se deduce que $(m + n)/mn$ es un cociente de dos números enteros con un denominador distinto de cero y por tanto es un número racional. ■

Más de la generalización de lo general a lo particular

A algunas personas les gusta pensar en el método de generalización de lo general a lo particular como un proceso de desafío. Si usted afirma que una propiedad vale para todos los elementos en un dominio, entonces alguien puede cuestionar su afirmación tomando cualquier elemento en el dominio y pidiéndole que pruebe que ese elemento satisface la propiedad. Para probar su afirmación, usted debe poder satisfacer todos estos retos. Es decir, debe tener una forma de convencer al rival que la propiedad es verdadera para un elemento *elegido arbitrariamente* en el dominio.

Por ejemplo, supongamos que "A" afirma que todo entero es un número racional. "B" desafía esta afirmación al pedirle a "A" que lo compruebe para $n = 7$. "A" señala que

$$7 = \frac{7}{1} \qquad \text{que es un cociente de números enteros y por tanto racional.}$$

"B" acepta esta explicación, pero lo reta de nuevo con $n = -12$. "A" responde que

$$-12 = \frac{-12}{1} \qquad \text{que es un cociente de números enteros y por tanto racional.}$$

A continuación "B" trata de atrapar a "A", desafiándolo con $n = 0$, pero "A" responde que

$$0 = \frac{0}{1} \qquad \text{que es un cociente de números enteros y por tanto racional.}$$

Como puede ver, "A" es capaz de responder con eficacia todos los retos de "B" porque "A" tiene un procedimiento general para poner enteros en forma de números racionales: "A" sólo divide cualquier número entero "B" entre 1. Es decir, no importa qué número entero n le dé "B" a "A", "A", escribe

$$n = \frac{n}{1} \qquad \text{que es un cociente de números enteros y por tanto racional.}$$

Este análisis demuestra el siguiente teorema.

Teorema 4.2.1

Cada entero es un número racional.

En el ejercicio 11 al final de esta sección se le pide resumir el análisis anterior en una demostración formal.

Demostración de propiedades de números racionales

El siguiente ejemplo muestra cómo utilizar el método de la generalización de lo general a lo particular para demostrar una propiedad de los números racionales.

Ejemplo 4.2.2 Una suma de racionales es racional

Demuestre que la suma de dos números racionales es racional.

Solución Comience mental o explícitamente la reescritura del enunciado que se demostrará en la forma "∀ _____, si _____ entonces _____".

Reexpresión formal: ∀ números reales r y s, si r y s son racionales, entonces $r + s$ es racional. Después se pregunta: ¿De dónde estoy partiendo? o ¿Qué estoy suponiendo? La respuesta le da el punto de partida, o la primera frase de la demostración.

Punto de partida: Supongamos que r y s son números reales particulares, pero arbitrariamente elegidos tales que r y s son racionales, o, más simplemente,

Supongamos que r y s son números racionales.

Entonces se pregunta: ¿Qué tengo que mostrar para completar la demostración?

Mostrar que: $r + s$ es racional.

Por último se pregunta: ¿Cómo puedo llegar desde el punto de partida a la conclusión? o ¿Por qué tiene que $r + s$ ser racional si tanto r como s son racionales? La respuesta depende de manera esencial de la definición de racional.

Los números racionales son cocientes de enteros, por lo que el decir que r y s son racionales significa que

$$r = \frac{a}{b} \quad \text{y} \quad s = \frac{c}{d} \quad \begin{array}{l}\text{para algunos enteros } a, b, c \text{ y } d \\ \text{donde } b \neq 0 \text{ y } d \neq 0.\end{array}$$

De lo que se deduce por sustitución que

$$r + s = \frac{a}{b} + \frac{c}{d}.$$

Necesita demostrar que $r + s$ es racional, lo que significa que $r + s$ se puede escribir como una sola fracción o cociente de dos números enteros con un denominador distinto de cero. Pero el lado derecho de la ecuación (4.2.1) en

$$\begin{aligned} \frac{a}{b} + \frac{c}{d} &= \frac{ad}{bd} + \frac{bc}{bd} && \text{reescribiendo la fracción con un denominador común} \\ &= \frac{ad + bc}{bd} && \text{sumando fracciones con un denominador común.} \end{aligned}$$

¿Es esta fracción un cociente de números enteros? Sí. Ya que los productos y sumas de números enteros son enteros, $ad + bd$ y bd son ambos enteros. ¿Es el denominador $bd \neq 0$? Sí, por la propiedad del producto cero (ya que $b \neq 0$ y $d \neq 0$). Por tanto $r + s$ es un número racional.

Este análisis se resume de la siguiente manera:

Teorema 4.2.2

La suma de dos números racionales es racional.

Demostración:

Supongamos que r y s son números racionales. *[Debemos demostrar que $r + s$ es racional.]* Entonces, por definición de racional, $r = a/b$ y $s = c/d$ para algunos enteros a, b, c y d con $b \neq 0$ y $d \neq 0$. Por tanto

$$\begin{aligned} r + s &= \frac{a}{b} + \frac{c}{d} && \text{por sustitución} \\ &= \frac{ad + bc}{bd} && \text{por álgebra básica.} \end{aligned}$$

Sea $p = ad + bc$ y $q = bd$. Entonces p y q son enteros ya que los productos y sumas de los números enteros son números enteros y ya que a, b, c y d son todos números enteros. También $q \neq 0$ por la propiedad del producto cero. Por tanto

$$r + s = \frac{p}{q} \text{ donde } p \text{ y } q \text{ son enteros y } q \neq 0.$$

Por tanto, $r + s$ es racional por definición de un número racional. *[Esto es lo que se quería demostrar.]*

■

Deducción de nuevas Matemáticas a partir de las viejas

La sección 4.1 se centra en el establecimiento de la verdad y la falsedad de los teoremas matemáticos utilizando sólo el álgebra básica que normalmente se enseña en la escuela secundaria, el hecho de que los números enteros son cerrados bajo la suma, resta y multiplicación y las definiciones de los términos de los propios teoremas. En el futuro, cuando le pidamos que **demuestre algo directamente de las definiciones**, lo que queremos decir es que debe limitarse a este método. Sin embargo, una vez que ha juntado los enunciados que ha demostrado directamente de las definiciones, es posible otro método de demostración. Los enunciados recolectados se pueden utilizar para obtener resultados adicionales.

Ejemplo 4.2.3 Obtención de resultados adicionales de enteros pares e impares

Supongamos que ya ha demostrado las siguientes propiedades de los números enteros pares e impares:

1. La suma, producto y la resta de cualesquiera dos enteros pares son pares.
2. La suma y la resta de cualesquiera dos números enteros impares son pares.
3. El producto de dos enteros impares es impar.
4. El producto de cualquier número entero par y cualquier entero impar es par.
5. La suma de cualquier número entero impar y cualquier entero par es impar.
6. La resta de cualquier entero impar menos cualquier entero par es impar.
7. La diferencia de cualquier número entero par menos cualquier entero impar es impar.

Utilice las propiedades que se acaban de mencionar para demostrar que si a es cualquier número entero par y b es cualquier entero impar, entonces $\frac{a^2 + b^2 + 1}{2}$ es un número entero.

Solución Supongamos que a es cualquier entero par y que b es cualquier entero impar. Por la propiedad 3, b^2 es impar y por la propiedad 1, a^2 es par. Entonces por la propiedad 5, $a^2 + b^2$ es impar y ya que 1 también es impar, la suma $(a^2 + b^2) + 1 = a^2 + b^2 + 1$ es par por la propiedad 2. Por tanto, por definición de par, existe un entero k tal que $a^2 + b^2 + 1 = 2k$. Dividiendo ambos lados entre 2 se obtiene $\frac{a^2 + b^2 + 1}{2} = k$, que es un entero. Así $\frac{a^2 + b^2 + 1}{2}$ es un número entero *[que era lo que se quería demostrar]*. ■

Un **corolario** es un enunciado cuya verdad se puede deducir inmediatamente de un teorema que ya se ha demostrado.

Ejemplo 4.2.4 El doble de un número racional

Deduzca el siguiente corolario del teorema 4.2.2.

Corolario 4.2.3

El doble de un número racional es racional.

Solución El doble de un número es sólo su suma consigo mismo. Pero como la suma de dos números racionales es racional (teorema 4.2.2), la suma de un número racional consigo mismo es racional. Por tanto el doble de un número racional es racional. A continuación se presenta una versión formal de este argumento:

Demostración:
Supongamos que r es un número racional. Entonces $2r = r + r$ es la suma de dos números racionales. Así, por el teorema 4.2.2, $2r$ es racional. ■

Autoexamen

1. Para demostrar que un número real es racional, debemos demostrar que lo podemos escribir como _____.
2. Un número irracional es un _____ que _____.
3. El cero es un número racional ya que _____.

Conjunto de ejercicios 4.2

Los números en los ejercicios del 1 al 7 son racionales. Escriba cada número como un cociente de dos números enteros.

1. $-\frac{35}{6}$ 2. 4.6037 3. $\frac{4}{5} + \frac{2}{9}$

4. 0.37373737 . . .

5. 0.56565656 . . .

6. 320.5492492492 . . .

7. 52.4672167216721 . . .

8. La propiedad del producto cero, dice que si un producto de dos números reales es 0, entonces uno de los números debe ser 0.
   a. Escriba esta propiedad formal usando cuantificadores y variables.
   b. Escriba el contrapositivo de su respuesta del inciso *a*).
   c. Escriba una versión informal (sin símbolos de cuantificadores o variables) para su respuesta del inciso *b*).

9. Supongamos que a y b son números enteros y que $a \neq 0$ y $b \neq 0$. Explique por qué $(b - a)/(ab^2)$ debe ser un número racional.

10. Suponga que m y n son números enteros y que $n \neq 0$. Explique por qué $(5m + 12n)/(4n)$ debe ser un número racional.

11. Demuestre que cada entero es un número racional.

12. Complete los espacios en blanco en la siguiente demostración que el cuadrado de cualquier número racional es racional:
Demostración: Supongamos que r es __(a)__. Por definición del racional, $r = a/b$ para algún __(b)__ con $b \neq 0$. Por sustitución,

$$r^2 = \text{(c)} = a^2/b^2$$

Ya que tanto a como b son números enteros, por lo que los productos a^2 y __(d)__. También $b^2 \neq 0$ por el __(e)__. Por tanto r^2 es un cociente de dos números enteros con un denominador distinto de cero y así __(f)__, por definición, de racional.

13. Considere el siguiente enunciado: El negativo de cualquier número racional es racional.
   a. Escriba el enunciado formalmente usando un cuantificador y una variable.
   b. Determine si el enunciado es verdadero o falso y justifique su respuesta.

14. Considere el enunciado siguiente: El cuadrado de cualquier número racional es un número racional.
   a. Escriba el enunciado formal usando un cuantificador y una variable.
   b. Determine si el enunciado es verdadero o falso y justifique su respuesta.

Determine cuáles de los enunciados en los ejercicios del 15 al 20 son verdaderos y cuáles son falsos. Demuestre cada enunciado verdadero, directamente a partir de las definiciones y dé un contraejemplo para cada enunciado falso.

En el caso de que el enunciado es falso, determine si un pequeño cambio lo haría verdadero. Si es así, haga el cambio y demuestre el nuevo enunciado. Siga las instrucciones para demostraciones escritas de la página 154.

15. El producto de dos números racionales es un número racional.

***H* 16.** El cociente de dos números racionales es un número racional.

***H* 17.** La resta de dos números racionales es un número racional.

***H* 18.** Si r y s son dos números racionales, entonces $\frac{r+s}{2}$ es racional.

***H* 19.** Para todos los números reales a y b, si $a < b$ entonces $a < \frac{a+b}{2} < b$. (Puede usar las propiedades de las desigualdades del T17 al T27 del apéndice A.)

20. Dados cualesquier dos números racionales r y s con $r < s$, existe otro número racional entre r y s. (*Sugerencia*: use los resultados de los ejercicios 18 y 19.)

Utilice las propiedades de los números enteros pares e impares que se enumeran en el ejemplo 4.2.3 para hacer los ejercicios del 21 al 23. Indique qué propiedades se utilizan para justificar su razonamiento.

21. ¿Verdadero o falso? Si m es cualquier entero par y n es cualquier entero impar, entonces $m^2 + 3n$ es impar. Explique.

22. ¿Verdadero o falso? Si a es cualquier entero impar, entonces $a^2 + a$ es par. Explique.

23. ¿Verdadero o falso? Si k es cualquier entero par y m es un entero impar, entonces $(k+2)^2 - (m-1)^2$ es par. Explique.

Deduzca los enunciados en los ejercicios del 24 al 26 como corolarios de los teoremas 4.2.1, 4.2.2 y los resultados de los ejercicios 12, 13, 14, 15 y 17.

24. Para cualesquiera números racionales r y s, $2r + 3s$ es racional.

25. Si r es un número racional, entonces $3r^2 - 2r + 4$ es racional.

26. Para cualquier número racional s, $5s^3 + 8s^2 - 7$ es racional.

27. Es un hecho que si n es un entero no negativo, entonces

$$1 + \frac{1}{2} + \frac{1}{2^2} + \frac{1}{2^3} + \cdots + \frac{1}{2^n} = \frac{1 - (1/2^{n+1})}{1 - (1/2)}.$$

(En la sección 5.2 se demuestra una forma más general de este enunciado.) ¿Es el lado derecho de esta ecuación racional? Si es así, expréselo como un cociente de dos números enteros.

28. Supongamos que a, b, c y d son números enteros y $a \neq c$. Supongamos también que x es un número real que satisface la ecuación

$$\frac{ax + b}{cx + d} = 1.$$

¿x debe ser racional? Si es así, exprese x como una razón de dos números enteros.

✶ 29. Supongamos que a, b y c son números enteros y x, y y z son números reales distintos de cero que satisfacen las siguientes ecuaciones:

$$\frac{xy}{x+y} = a \quad \text{y} \quad \frac{xz}{x+z} = b \quad \text{y} \quad \frac{yz}{y+z} = c.$$

¿x es racional? Si es así, expréselo como un cociente de dos números enteros.

30. Demuestre que si la solución de una ecuación cuadrática de la forma $x^2 + bx + c = 0$ es racional (donde b y c son racionales), entonces la otra solución también es racional. (Utilice el hecho de que si las soluciones de la ecuación son r y s, entonces, $x^2 + bx + c = (x - r)(x - s)$).

31. Demuestre que si un número real c satisface una ecuación polinomial de la forma

$$r_3x^3 + r_2x^2 + r_1x + r_0 = 0,$$

donde r_0, r_1, r_2 y r_3 son números racionales, entonces c satisface una ecuación de la forma

$$n_3x^3 + n_2x^2 + n_1 + n_0 = 0,$$

donde n_0, n_1, n_2 y n_3 son números enteros.

Definición: Un número c que se llama un **cero** de un polinomio $p(x)$ si y sólo si, $p(c) = 0$.

✶ 32. Demuestre que para todo número real c, si c es un cero de un polinomio con coeficientes racionales, entonces c es un cero de un polinomio con coeficientes enteros.

Utilice las propiedades de los números enteros pares e impares que se enumeran en el ejemplo 4.2.3 para hacer los ejercicios 33 y 34.

33. Cuando se multiplican expresiones de la forma $(x - r)(x - s)$, se obtiene un polinomio de segundo grado. Por ejemplo $(x - 2)(x - (-7)) = (x - 2)(x + 7) = x^2 + 5x - 14$.

***H* a.** ¿Qué se puede decir de los coeficientes del polinomio que se obtiene de la multiplicación $(x - r)(x - s)$ cuando tanto r como s son números enteros impares? ¿cuándo tanto r como s son enteros pares? ¿cuando uno de r y s es par y el otro es impar?

b. Se deduce del inciso *a*) que $x^2 - 1253x + 255$ no se puede escribir como un producto de dos polinomios de coeficientes enteros. Explique por qué esto es así.

✶ 34. Observe que $(x - r)(x - s)(x - t)$

$$= x^3 - (r + s + t)x^2 + (rs + rt + st)x - rst.$$

a. Deduzca un resultado para polinomios cúbicos similar al resultado del inciso *a*) del ejercicio 33 para polinomios cuadráticos.

b. ¿Puede $x^3 + 7x^2 - 8x - 27$ escribirse como un producto de tres polinomios de coeficientes enteros? Explique.

En los ejercicios del 35 al 39 encuentre los errores en las "demostraciones" de que la suma de dos números racionales es un número racional.

35. "**Demostración:** Cualquiera dos números racionales producen un número racional cuando se suman. Así que si r y s son particulares pero que se eligen arbitrariamente de los números racionales, entonces $r + s$ es racional".

36. "**Demostración:** Sean los números racionales $r = \frac{1}{4}$ y $s = \frac{1}{2}$ dados. Entonces $r + s = \frac{1}{4} + \frac{1}{2} = \frac{3}{4}$, es un número racional. Esto es lo que se quería demostrar".

37. "**Demostración:** Supongamos que r y s son números racionales. Por definición racional, $r = a/b$ para algunos enteros a y b con $b \neq 0$ y $s = a/b$ para algunos enteros a y b con $b \neq 0$. Entonces

$$r + s = \frac{a}{b} + \frac{a}{b} = \frac{2a}{b}.$$

Sea $p = 2a$. Entonces p es un número entero, ya que es un producto de números enteros. Por lo que $r + s = p/b$, donde p y b son números enteros y $b \neq 0$. Por tanto $r + s$ es un número racional por definición de racional. Esto es lo que se quería demostrar".

38. "**Demostración:** Supongamos que r y s son números racionales. Entonces $r = a/b$ y $s = c/d$ para algunos enteros a, b, c y d con $b \neq 0$ y $d \neq 0$ (por definición de racional). Entonces

$$r + s = \frac{a}{b} + \frac{c}{d}.$$

Pero esta es una suma de dos fracciones, que es una fracción. Así que $r + s$ es un número racional ya que un número racional es una fracción".

39. "**Demostración:** Supongamos que r y s son números racionales. Si $r + s$ es racional, entonces por definición de racional $r + s = a/b$ para algunos enteros a y b con $b \neq 0$. También puesto que r y s son racionales, $r = i/j$ y $s = m/n$ para algunos números enteros i, j, m y n con $j \neq 0$ y $n \neq 0$. De lo que se deduce que

$$r + s = \frac{i}{j} + \frac{m}{n} = \frac{a}{b},$$

que es un cociente de dos números enteros con un denominador distinto de cero. Por tanto es un número racional. Esto es lo que se quería demostrar".

Respuestas del autoexamen

1. un cociente de números enteros con un denominador distinto de cero 2. número real; no racional 3. $0 = \frac{0}{1}$

4.3 Demostración directa y contraejemplo III: divisibilidad

La cualidad esencial de una prueba es forzarla a ser creíble. —Pierre de Fermat

Cuando se introdujo por primera vez al concepto de división en la escuela primaria, probablemente se le enseñó que 12 dividido por 3 es 4, porque si separa 12 objetos en grupos de 3, obtiene 4 grupos y nada más.

También se le enseñó a describir este hecho diciendo que "12 es divisible por 3" o que "3 divide a 12 de manera exacta".

El concepto de divisibilidad es el concepto central de uno de los temas más bellos de las matemáticas avanzadas: **la teoría de números**, el estudio de las propiedades de los números enteros.

• Definición

Si n y d son números enteros y $d \neq 0$ entonces

n es **divisible entre** d, si y sólo si, n es igual a d veces algún entero.

En lugar de "n es divisible por d", podemos decir que

n **es un múltiplo de** d, o
d **es un factor de** n, o
d **es un divisor de** n, o
d **divide a** n.

La notación $\mathbf{d \mid n}$ se lee "d divide a n". Simbólicamente, si n y d son números enteros y $d \neq 0$:

$$d \mid n \quad \Leftrightarrow \quad \exists \text{ un entero } k \text{ tal que } n = dk.$$

Ejemplo 4.3.1 Divisibilidad

a. ¿Es 21 divisible por 3? b. ¿5 divide a 40? c. ¿Es 7 | 42?
d. ¿Es 32 un múltiplo de -16? e. ¿Es 6 un factor de 54? f. ¿Es 7 un factor de -7?

Solución

a. Sí, $21 = 3 \cdot 7$. b. Sí, $40 = 5 \cdot 8$. c. Sí, $42 = 7 \cdot 6$.
d. Sí, $32 = (-16) \cdot (-2)$. e. Sí, $54 = 6 \cdot 9$. f. Sí, $-7 = 7 \cdot (-1)$. ■

Ejemplo 4.3.2 Divisores de cero

Si k es cualquier entero distinto de cero, ¿k divide a 0?

Solución Sí, porque $0 = k \cdot 0$. ■

Dos propiedades útiles de la divisibilidad son: 1) que si un entero positivo divide a un segundo entero positivo, entonces el primero es menor o igual que el segundo y 2) que los únicos divisores de 1 son 1 y -1.

Teorema 4.3.1 Un divisor positivo de un entero positivo

Para todos los números enteros a y b, si a y b son positivos y a divide a b, entonces $a \leq b$.

Demostración:

Supongamos que a y b son números enteros positivos y que a divide a b. *[Debemos demostrar que $a \leq b$.]* Entonces existe un entero k tal que $b = ak$. Por la propiedad T25 del apéndice A, k debe ser positivo, porque tanto a como b son positivos. De lo que se deduce que

$$1 \leq k$$

ya que todo entero positivo es mayor o igual a 1. Multiplicando ambos lados por una a se obtiene

$$a \leq ka = b$$

porque multiplicando ambos lados de una desigualdad por un número positivo se preserva la desigualdad por la propiedad T20 del apéndice A. Así, $a \leq b$ *[como se quería demostrar]*.

■

Teorema 4.3.2 Divisores de 1

Los únicos divisores de 1 son 1 y -1.

Demostración:

Ya que $1 \cdot 1 = 1$ y $(-1)(-1) = 1$, tanto 1 como -1 son divisores de 1. Ahora supongamos que m es cualquier número entero que divide a 1. Entonces existe un entero n tal que $1 = mn$. Por el teorema T25 del apéndice A, ya sea m y n son positivos o m y n son negativos. Si m y n son positivos, entonces m es un divisor entero positivo de 1. Por el teorema 4.3.1, $m \leq 1$ y, ya que el único entero positivo que es menor o igual

continúa en la página 172

a 1 es el 1 mismo, se deduce que $m = 1$. Por otro lado, si m y n son negativos, entonces, por el teorema T12 del apéndice A $(-m)(-n) = mn = 1$. En este caso $-m$ es un divisor entero positivo de 1 y así, con el mismo razonamiento, $-m = 1$ y por tanto $m = -1$. Por tanto sólo hay dos posibilidades: o bien $m = 1$ o $m = -1$. Así los únicos divisores de 1 son 1 y -1.

Ejemplo 4.3.3 Divisibilidad de expresiones algebraicas

a. Si a y b son números enteros, ¿es $3a + 3b$ divisible por 3?

b. Si k y m son números enteros, ¿es $10km$ divisible por 5?

Solución

a. Sí. Por la ley distributiva del álgebra, $3a + 3b = 3(a + b)$ y $a + b$ es un número entero, porque es una suma de dos números enteros.

b. Sí. Por la ley asociativa de álgebra, $10km = 5 \cdot (2km)$ y $2km$ es un número entero, porque es un producto de tres enteros. ■

Cuando la definición se reescribe formalmente con el cuantificador existencial, el resultado es

$$d \mid n \quad \Leftrightarrow \quad \exists \text{ un entero } k \text{ tal que } n = dk.$$

Ya que la negación de un enunciado existencial es universal, se tiene que d no divide a n (que se denota por $d \nmid n$) si y sólo si, $\forall$ entero k, $n \neq dk$, o, en otras palabras, el cociente n/d no es un entero.

Para todos los enteros n y d, $\quad d \nmid n \quad \Leftrightarrow \quad \dfrac{n}{d}$ no es un número entero.

Ejemplo 4.3.4 Comprobación de no divisibilidad

¿Es $4 \mid 15$?

Solución No, $\frac{15}{4} = 3.75$, que no es un número entero. ■

¡Precaución! $a \mid b$ denota la *frase* "a divide a b", mientras que a/b denota el *número* a dividido por b.

Tenga cuidado de distinguir entre la notación $a \mid b$ y la notación a/b. La notación $a \mid b$ significa la frase "a divide a b", que significa que existe un entero k tal que $b = ak$. Dividiendo ambos lados entre a se obtiene $b/a = k$, un número entero. Así, cuando $a \neq 0$, $a \mid b$ si y sólo si, b/a es un número entero. Por otra parte, la notación a/b se establece para el número a/b que es el resultado de dividir a entre b y que puede o no ser un número entero. En particular, asegúrese de evitar escribir cosas como

$$\cancel{4 \mid (3 + 5) = 4 \mid 8.}$$

Si se lee en voz alta, será "4, divide la cantidad de 3 más 5 que es igual a 4 que divide a 8", que no tiene sentido.

Ejemplo 4.3.5 Números primos y divisibilidad

Una forma alternativa de definir un número primo es decir que un entero $n > 1$ es primo si y sólo si, sus únicos divisores enteros positivos son 1 y él mismo. ■

Demostración de propiedades de la divisibilidad

Una de las propiedades más útiles de la divisibilidad es que es transitiva. Si un número divide a un segundo y el segundo número divide a un tercero, entonces el primer número divide al tercero.

Ejemplo 4.3.6 Transitividad de la divisibilidad

Demuestre que para todos los números enteros a, b y c, si $a \mid b$ y $b \mid c$, entonces $a \mid c$.

Solución Puesto que el enunciado que demostrará ya está escrito formalmente, puede seleccionar inmediatamente el punto de partida o la primera frase de demostración y la conclusión que debe ser demostrada.

Punto de partida: Supongamos que a, b y c son números enteros particulares, pero elegidos arbitrariamente tal que $a \mid b$ y $b \mid c$.

Para demostrar: $a \mid c$.
Necesita demostrar que $a \mid c$, o, en otras palabras, que

$$c = a \cdot (\text{algún entero}).$$

Pero ya que $a \mid b$,

$$b = ar \quad \text{para algún entero } r. \tag{4.3.1}$$

Y puesto que $b \mid c$,

$$c = bs \quad \text{para algún entero } s. \tag{4.3.2}$$

La ecuación 4.3.2 expresa a c en términos de b y la ecuación 4.3.1 expresa a b en términos de a. Así, si sustituye 4.3.1 en 4.3.2, tendrá una ecuación que expresa c en términos de a.

$$\begin{aligned} c &= bs && \text{por la ecuación 4.3.2} \\ &= (ar)s && \text{por la ecuación 4.3.1.} \end{aligned}$$

Pero $(ar)s = a(rs)$ por la ley asociativa de la multiplicación. Por tanto

$$c = a(rs).$$

Ahora ya está casi terminado. Ha expresado a c como $a \cdot$ (algo). Sólo queda comprobar que ese algo es un número entero. Pero por supuesto lo es, porque es un producto de dos números enteros.

Este análisis se resume de la siguiente manera:

Teorema 4.3.3 Transitividad de divisibilidad

Para todos los números enteros a, b y c, si a divide a b y b divide a c, entonces a divide a c.

Demostración:

Supongamos que a, b y c son *[particulares, pero arbitrariamente elegidos]* enteros tales que a divide b y b divide a c. *[Debemos demostrar que a divide a c.]* Por definición de divisibilidad,

$$b = ar \quad \text{y} \quad c = bs \quad \text{para algunos enteros } r \text{ y } s.$$

continúa en la página 174

Por sustitución

$$\begin{aligned} c &= bs \\ &= (ar)\text{s} \\ &= a(rs) \qquad \text{por álgebra básica.} \end{aligned}$$

Sea $k = rs$. Entonces k es un número entero, ya que es un producto de números enteros y por tanto

$$c = ak \text{ donde } k \text{ es un número entero.}$$

Así a divide a c por la definición de divisibilidad. *[Esto es lo que se quería demostrar.]*

■

Podría parecer, de la definición de primos, que para demostrar que un número entero es primo se tendría que demostrar que no es divisible entre cualquier número entero mayor que 1 y menor que él mismo. De hecho, sólo tiene que comprobar que es divisible por un número primo menor o igual a sí mismo. Esto se deduce de los teoremas 4.3.1, 4.3.3 y el siguiente teorema, que dice que cualquier número entero mayor que 1 es divisible entre un número primo. La idea de la demostración es muy sencilla. Comienza con un entero positivo. Si es primo ya terminó, si no, se trata de un producto de dos factores positivos más pequeños. Si uno de estos es primo, ya está resuelto, si no, puede escoger uno de los factores y escribirlo como un producto de factores positivos aún más pequeños. Puede continuar de esta manera, factorizando los factores del número con el que comenzó, hasta que uno de ellos resulte ser primo. A la larga esto debe suceder ya que todos los factores se pueden elegir positivos y cada uno es más pequeño que el anterior.

Teorema 4.3.4 Divisibilidad de un primo

Todo entero $n > 1$ es divisible por un número primo.

Demostración:

Supongamos que n *[particular, pero elegido arbitrariamente]* es un entero que es mayor que 1. *[Debemos demostrar que existe un número primo que divide a n.]* Si n es primo, entonces n es divisible por un número primo (es decir, él mismo) y ya está. Si n no es primo, entonces, como se analiza en el ejemplo 4.1.2*b*,

$$n = r_0 s_0 \qquad \text{donde } r_0 \text{ y } s_0 \text{ son números enteros y } 1 < r_0 < n \text{ y } 1 < s_0 < n.$$

Lo que se deduce por la definición de divisibilidad que $r_0 \mid n$.

Si r_0 es primo, entonces r_0 es un número primo que divide a n y ya está. Si r_0 no es primo, entonces

$$r_0 = r_1 s_1 \qquad \text{donde } r_1 \text{ y } s_1 \text{ son números enteros y } 1 < r_1 < r_0 \text{ y } 1 < s_1 < r_0.$$

Lo que se deduce por la definición de divisibilidad que $r_1 \mid r_0$. Pero ya sabemos que $r_0 \mid n$. En consecuencia, por transitividad de la divisibilidad, $r_1 \mid n$.

Si r_1 es primo, entonces r_1 es un número primo que divide a n y ya está. Si r_1 no es primo, entonces

$$r_1 = r_2 s_2 \qquad \text{donde } r_2 \text{ y } s_2 \text{ son números enteros y } 1 < r_2 < r_1 \text{ y } 1 < s_2 < r_1.$$

Lo que se deduce por la definición de divisibilidad que $r_2 \mid r_1$. Pero ya sabemos que $r_1 \mid n$. En consecuencia, por transitividad de la divisibilidad, $r_2 \mid n$.

Si r_2 es primo, entonces r_2 es un número primo que divide a n y ya está. Si r_2 no es primo, entonces podemos repetir el proceso anterior factorizando a r_2 como $r_3 s_3$.

Podemos continuar de esta manera, factorizando los factores sucesivos de n hasta que encontremos un factor primo. Debemos tener éxito en un número finito de pasos, ya que cada nuevo factor es menor que el anterior (que es menor que n) y mayor que 1 y hay pocos enteros n que estrictamente se encuentren entre 1 y n.* Así se obtiene una sucesión

$$r_0, r_1, r_2, \ldots, r_k,$$

donde $k \geq 0$, $1 < r_k < r_{k-1} < \cdots < r_2 < r_1 < r_0 < n$ y $r_i \mid n$ para cada $i = 0, 1, 2, \ldots, k$. La condición de terminación es que r_k debe ser primo. Por tanto r_k es un número primo que divide a n. *[Esto es lo que se quería demostrar.]*

Contraejemplos y divisibilidad

Para demostrar que una propiedad de divisibilidad propuesta no es una verdad universal, sólo es necesario encontrar un par de números enteros para los cuales es falso.

Ejemplo 4.3.7 Comprobación de una propiedad de divisibilidad propuesta

¿Es el siguiente enunciado verdadero o falso? Para todos los números enteros a y b, si $a \mid$ b y $b \mid a$ entonces $a = b$.

Solución Este enunciado es falso. ¿Puede pensar en un solo contraejemplo concentrándose durante un minuto o algo así?

El análisis siguiente describe un proceso mental que puede tomar unos pocos segundos. Sin embargo, es útil poder usarlo conscientemente, para resolver los problemas más difíciles.

Para descubrir la verdad o falsedad de un enunciado como la que se acaba de dar, comience como si estuviera tratando de probarlo.

Punto de partida: Supongamos que a y b son números enteros tales que $a \mid b$ y $b \mid a$. Pregúntese: ¿Debo suponer que $a = b$, o podría suceder que $a \neq b$ para alguna a y b? Concéntrese en la suposición. ¿Qué significa? Por definición de divisibilidad, las condiciones $a \mid b$ y $b \mid a$ significan que

$$b = ka \text{ y } a = lb \text{ para algunos enteros } k \text{ y } l.$$

¿Debe seguir que $a = b$, o se pueden encontrar números enteros a y b que satisfagan estas ecuaciones para las que $a \neq b$? Las ecuaciones implican que

$$b = ka = k(lb) = (kl)b$$

Ya que $b \mid a$, $b \neq 0$ y así usted puede eliminar a b del extremo izquierdo y del lado derecho para obtener

$$1 = kl.$$

En otras palabras, k y l son divisores de 1. Pero, por el teorema 4.3.2, los únicos divisores de 1 son 1 y -1. Así k y l son ambos 1 o ambos -1. Si $k = l = 1$, entonces $b = a$. Pero

*Estrictamente hablando, este enunciado se justifica por un axioma de los números enteros llamado el principio del buen orden, que se analiza en la sección 5.4. El teorema 4.3.4 también se puede probar con inducción matemática fuerte, tal como se muestra en el ejemplo 5.4.1.

si $k = l = -1$, entonces $b = -a$ y así $a \neq b$. Este análisis sugiere que usted puede encontrar un contraejemplo tomando $b = -a$. Presentamos una respuesta formal:

Propuesta de la propiedad de divisibilidad: Para todos los números enteros a y b, si $a \mid b$ y $b \mid a$ entonces $a = b$.

Contraejemplo: Sea $a = 2$ y $b = -2$. Entonces,

$a \mid b$ ya que $2 \mid (-2)$ y $b \mid a$ ya que $(-2) \mid 2$, pero $a \neq b$ ya que $2 \neq -2$.

Por tanto, el enunciado es falso.

■

La búsqueda de una demostración con frecuencia le ayudará a descubrir un contraejemplo (suponiendo que el enunciado que están tratando de demostrar es, de hecho, falso). Por el contrario, al tratar de encontrar un contraejemplo para el enunciado, puede llegar a darse cuenta de para qué razón es verdadero (si es, de hecho, verdadero). Lo importante es mantener una mente abierta hasta que esté convencido por la evidencia de su propio razonamiento cuidadoso.

Teorema de factorización única de enteros

El enunciado más completo sobre divisibilidad de enteros se encuentra en el *teorema de factorización única de enteros*. Debido a su importancia este teorema también se conoce como el *teorema fundamental de la aritmética*. Aunque Euclides, vivió alrededor del 300 a.C., parece haber estado familiarizado con el teorema, el primero en establecerlo precisamente fue el gran matemático alemán Carl Friedrich Gauss (rima con *house*(casa en inglés)) en 1801.

El teorema de factorización única de números enteros, dice que cualquier número entero mayor que 1 es primo o se puede escribir como un producto de números primos de una forma que es única, excepto, quizá, por el orden en que se escriben los primos. Por ejemplo,

$$72 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 = 2 \cdot 3 \cdot 3 \cdot 2 \cdot 2 = 3 \cdot 2 \cdot 2 \cdot 3 \cdot 2$$

y así sucesivamente. Los tres 2 y dos 3 se puede escribir en cualquier orden, pero cualquier factorización de 72 como producto de primos deberá contener exactamente tres 2 y dos 3; ningún otro conjunto de números primos, además de tres 2 y dos 3 multiplicados dan 72.

Nota Este teorema es la razón de por qué no se le permite al número 1 ser primo. Si 1 fuese primo, entonces las factorizaciones no serían únicas. Por ejemplo, $6 = 2 \cdot 3 = 1 \cdot 2 \cdot 3$ y así sucesivamente.

Teorema 4.3.5 Teorema de factorización única de números enteros (teorema fundamental de la aritmética)

Dado cualquier número entero $n > 1$, existe un entero positivo k, de números primos distintos, $p_1, p_2, \ldots\ p_k$ y números enteros positivos $e_1, e_2, \ldots\ e_k$ tal que

$$n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \ldots p_k^{e_k},$$

y cualquier otra expresión para n como producto de números primos es idéntico a éste, excepto, quizás, por el orden en que se escriben los factores.

La demostración del teorema de factorización única se describe en los ejercicios para las secciones 5.4 y 8.4.

Debido al teorema de factorización única, cualquier entero $n > 1$ se puede poner en una *forma factorizada estándar* en la que los factores primos se escriben en orden ascendente de izquierda a derecha.

• Definición

Dado cualquier número entero $n > 1$, la **forma factorizada estándar** de n es una expresión de la forma

$$n = p_1^{e_1} p_2^{e_2} p_3^{e_3} \cdots p_k^{e_k},$$

donde k es un entero positivo, $p_1, p_2, \ldots\ p_k$ son números primos, $e_1, e_2, \ldots\ e_k$ son enteros positivos y $p_1 < p_2 < \cdots < p_k$.

Ejemplo 4.3.8 Escritura de números enteros en la forma factorizada estándar

Escriba 3 300 en la forma factorizada estándar.

Solución Primero encuentre todos los factores de 3 300. Después escriba en orden ascendente:

$$\begin{aligned} 3\,300 &= 100 \cdot 33 = 4 \cdot 25 \cdot 3 \cdot 11 \\ &= 2 \cdot 2 \cdot 5 \cdot 5 \cdot 3 \cdot 11 = 2^2 \cdot 3^1 \cdot 5^2 \cdot 11^1. \end{aligned}$$

■

Ejemplo 4.3.9 Uso de la factorización única para resolver un problema

Supongamos que m es un entero tal que

$$8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot m = 17 \cdot 16 \cdot 15 \cdot 14 \cdot 13 \cdot 12 \cdot 11 \cdot 10.$$

¿Es $17 \mid m$?

Solución Ya que 17 es uno de los factores primos del lado derecho de la ecuación, también es un factor primordial de la izquierda (por el teorema de factorización única de números enteros). Pero 17 no es igual a cualquier factor primo de 8, 7, 6, 5, 4, 3, o 2 (ya que es demasiado grande). Por tanto 17 deben presentarse como uno de los factores primos de m y así $17 \mid m$. ■

Autoexamen

1. Para demostrar que un número entero distinto de cero d divide a un entero n, debemos demostrar que _____.
2. Decir que d divide a n significa lo mismo que decir que _____ es divisible entre _____.
3. Si a y b son números enteros positivos y $a \mid b$, entonces _____ es menor o igual a _____.
4. Para todos los enteros n, d, $d \nmid n$, si y sólo si, _____.
5. Si a y b son números enteros, la notación $a \mid b$ denota _____ y la notación a/b denota _____.
6. La transitividad del teorema de la divisibilidad, dice que para todos los enteros a, b y c, si _____ entonces _____.
7. La divisibilidad por un teorema de primos dice que cada número entero mayor que 1 es _____.
8. El teorema de factorización única de números enteros, dice que cualquier número entero mayor que 1 es ya sea _____ o se puede escribir como _____ en una forma que es única, excepto, posiblemente, en el _____ en que se escriben los números.

Conjunto de ejercicios 4.3

Dé una razón para su respuesta en cada uno de los ejercicios del 1 al 13. Supongamos que todas las variables representan números enteros.

1. ¿Es 52 divisible por 13?

2. ¿Es $7 \mid 56$?

3. ¿Es $5 \mid 0$?

4. ¿3 divide a $(3k + 1)(3k + 2)(3k + 3)$?

5. ¿Es $6m(2m + 10)$ divisible por 4?

6. ¿Es 29 un múltiplo de 3?

7. ¿Es -3 un factor de 66?

8. ¿Es $6a(a + b)$ un múltiplo de $3a$?

9. ¿Es 4 un factor de $2a \cdot 34b$?

10. ¿Es $7 \mid 34$?

11. ¿Es $13 \mid 73$?

12. ¿Si $n = 4k + 1$, 8 divide a $n^2 - 1$?

13. ¿Si $n = 4k + 3$, 8 divide a $n^2 - 1$?

14. Complete los espacios en blanco en la demostración siguiente para todos los números enteros a y b, si $a \mid b$ entonces $a \mid (-b)$.

Demostración: Supongamos que a y b son números enteros tales que cualquier __(a)__. Por definición de divisibilidad, existe un número entero r tal que __(b)__. Sustituyendo.

$$-b = -ar = a(-r).$$

Sea $t =$ __(c)__. Entonces t es un número entero, porque $t = (-1) \cdot r$ y ambos -1 y r son números enteros. Así, por sustitución, $-b = at$, donde r es un número entero y así, por definición, de la divisibilidad, __(d)__. que era lo que se quería demostrar.

Demuestre los enunciados de los ejercicios 15 y 16 directamente de la definición de divisibilidad.

15. Para todos los números enteros a, b y c, si $a \mid b$ y $a \mid c$ entonces $a \mid (b + c)$.

***H* 16.** Para todos los números enteros a, b y c, si $a \mid b$ y $a \mid c$ entonces $a \mid (b - c)$.

17. Considere el enunciado siguiente: El negativo de cualquier múltiplo de 3 es un múltiplo de 3.
   a. Escriba el enunciado formal con un cuantificador y una variable.
   b. Determine si el enunciado es verdadero o falso y justifique su respuesta.

18. Demuestre que el enunciado siguiente es falso: Para todos los números enteros a y b, si $3 \mid (a + b)$, entonces $3 \mid (a - b)$.

Para cada enunciado en los ejercicios del 19 a 31, determine si el enunciado es verdadero o falso. Demuestre el enunciado directamente de las definiciones, si es verdadero y dé un contraejemplo si es falso.

***H* 19.** Para todos los números enteros a, b y c, si a divide a b entonces a divide a bc.

20. La suma de tres enteros consecutivos es divisible por 3. (Dos números enteros son **consecutivos**, si y sólo si, uno es uno más que el otro.)

21. El producto de dos enteros pares es un múltiplo de 4.

***H* 22.** Una condición necesaria para que un número entero sea divisible entre 6 es que sea divisible entre 2.

23. Una condición suficiente para que un número entero sea divisible entre 8 es que sea divisible entre 16.

24. Para todos los números enteros a, b y c, si $a \mid b$ y $a \mid c$ entonces $a \mid (2b - 3c)$.

25. Para todos los números enteros a, b y c, si a es un factor de c entonces ab es un factor de c.

***H* 26.** Para todos los números enteros a, b y c, si $ab \mid c$ entonces $a \mid c$ y $b \mid c$.

***H* 27.** Para todos los números enteros a, b y c, si $a \mid (b + c)$ entonces $a \mid b$ o $a \mid c$.

28. Para todos los números enteros a, b y c, si $a \mid bc$ entonces $a \mid b$ o $a \mid c$.

29. Para todos los números enteros a y b, si $a \mid b$, entonces $a^2 \mid b^2$.

30. Para todos los números enteros a y n, si $a \mid n^2$ y $a \leq n$ entonces $a \mid n$.

31. Para todos los números enteros a y b, si $a \mid 10b$ entonces $a \mid 10$ o $a \mid b$.

32. Una cadena de comida rápida tiene un concurso en el que una tarjeta con números se le da a cada cliente que realiza una compra. Si algunos de los números de la tarjeta suman 100, entonces el cliente gana \$100. Un cliente dado recibe una tarjeta con los números

72, 21, 15, 36, 69, 81, 9, 27, 42 y 63.

¿El cliente gana los \$100? ¿Por qué si o por qué no?

33. ¿Es posible tener una combinación de cinco, diez y veinticinco centavos que sumen 4.72? Explique.

34. ¿Es posible tener 50 monedas, compuestas por monedas de un centavo, monedas de diez centavos y de veinticinco centavos, que sumen 3? Explique.

35. Dos atletas corren en una pista circular con una velocidad constante tal que el primero completa una ronda completa en 8 minutos y el segundo en 10 minutos. Si ambos empiezan desde el mismo lugar a las 4 p.m., ¿cuándo será la primera vez en que se encuentren juntos al inicio?

36. Se puede demostrar (vea los ejercicios 44-48) que un número entero es divisible por 3 si y sólo si, la suma de sus dígitos es divisible por 3. Un entero es divisible por 9 si y sólo si, la suma de sus dígitos es divisible por 9. Un entero es divisible por 5 si y sólo si, su dígito del extremo derecho es un 5 o un 0. Y un número entero es divisible por 4 si y sólo si, el número formado por sus dos dígitos del extremo derecho es divisible por 4. Compruebe con los siguientes enteros la divisibilidad por 3, 4, 5 y 9.
   a. 637 425 403 705 125 b. 12 858 306 120 312
   c. 517 924 440 926 512 d. 14 328 083 360 232

37. Utilice el teorema de factorización única para escribir los números enteros siguientes en su forma factorizada estándar.
   a. 1176 b. 5733 c. 3675

38. Supongamos que en la forma factorizada estándar $a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, donde k es un entero positivo, $p_1, p_2, \ldots, p_k$ son números primos número y $e_1, e_2, \ldots, e_k$ son enteros positivos.
   a. ¿Cuál es la forma factorizada estándar para a^2?
   b. Encuentre el menor entero positivo n tal que $2^5 \cdot 3 \cdot 5^2 \cdot 7^3 \cdot n$ es un cuadrado perfecto. Escriba el producto resultante como un cuadrado perfecto.
   c. Encontrar el menor entero positivo m tal que $2^2 \cdot 3^5 \cdot 7 \cdot 11 \cdot m$ es un cuadrado perfecto. Escriba el producto resultante como un cuadrado perfecto.

39. Supongamos que la forma factorizada estándar de $a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, donde k es un entero positivo, $p_1, p_2, \ldots, p_k$ son números primos número y $e_1, e_2, \ldots, e_k$ son enteros positivos.
   a. ¿Cuál es la forma factorizada estándar para a^3?
   b. Encuentre el menor entero positivo k tal que $2^4 \cdot 3^5 \cdot 7 \cdot 11^2 \cdot k$ es un cubo perfecto (es decir, es igual a un número entero al cubo). Escriba el producto resultante como un cubo perfecto.

40. **a.** Si a y b son números enteros y $12a = 25b$, ¿es 12 | b? ¿es 25 | a? Explique.
    b. Si x y y son números enteros y $10x = 9y$ ¿es 10 | y? ¿es 9 | x? Explique.

***H* 41.** ¿Cuántos ceros se encuentran al final de $45^8 \cdot 88^5$? Explique cómo se puede responder a esta pregunta sin realmente calcular el número. (*Sugerencia*: $10 = 2 \cdot 5$.)

42. Si n es un entero y $n > 1$, entonces $n!$ es el producto de n y los enteros positivos menores que n. Por ejemplo, $5! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$.
    a. Escriba 6! en forma factorizada estándar.
    b. Escriba 20! en forma factorizada estándar.
    c. Sin calcular el valor de $(20!)^2$ determine cuántos ceros se encuentran al final de este número cuando se escribe en forma decimal. Justifique su respuesta.

✶ 43. En cierta ciudad 2/3 de los hombres adultos están casados con 3/5 de las mujeres adultas. Supongamos que todos los matrimonios son monógamos (nadie está casado con más de una persona de otro tipo). Suponga también que hay por lo menos 100 hombres adultos en la ciudad. ¿Cuál es el menor número posible de hombres adultos en la ciudad? ¿y de mujeres adultas en la ciudad?

Definición: Dado un entero n no negativo, la **representación decimal** de n es una expresión de la forma

$$d_k d_{k-1} \cdots d_2 d_1 d_0,$$

donde k es un entero no negativo, d_0, d_1, d_2, …, d_k (llamados los **dígitos decimales** de n) son enteros del 0 a 9 inclusive; $d_k \neq 0$ a menos que $n = 0$ y $k = 0$ y

$$n = d_k \cdot 10^k + d_{k-1} \cdot 10^{k-1} + \cdots + d_2 \cdot 10^2 + d_1 \cdot 10 + d_0.$$

(Por ejemplo, $2503 = 2 \cdot 10^3 + 5 \cdot 10^2 + 0 \cdot 10 + 3$.)

44. Demuestre que si n es un entero no negativo cuya representación decimal termina en 0, entonces 5 | n. (*Sugerencia*: Si la representación decimal de un entero no negativo n termina en d_0, entonces $n = 10m + d_0$ para algún entero m.)

45. Demuestre que si n es un entero no negativo cuya representación decimal termina en 5, entonces 5 | n.

46. Demuestre que si la representación decimal de un entero no negativo n termina en $d_1 d_0$ y si 4 | $(10d_1 + d_0)$, entonces 4 | n. (*Sugerencia*: Si la representación decimal de un entero no negativo termina en $d_1 d_0$, entonces hay un número entero s tal que $n = 100s + 10d_1 + d_0$.)

***H* ✶ 47.** Observe que

$$\begin{aligned} 7524 &= 7 \cdot 1000 + 5 \cdot 100 + 2 \cdot 10 + 4 \\ &= 7(999 + 1) + 5(99 + 1) + 2(9 + 1) + 4 \\ &= (7 \cdot 999 + 7) + (5 \cdot 99 + 5) + (2 \cdot 9 + 2) + 4 \\ &= (7 \cdot 999 + 5 \cdot 99 + 2 \cdot 9) + (7 + 5 + 2 + 4) \\ &= (7 \cdot 111 \cdot 9 + 5 \cdot 11 \cdot 9 + 2 \cdot 9) + (7 + 5 + 2 + 4) \\ &= (7 \cdot 111 + 5 \cdot 11 + 2) \cdot 9 + (7 + 5 + 2 + 4) \\ &= (\text{un entero divisible por 9}) \\ &\qquad + (\text{la suma de los dígitos de 7524}). \end{aligned}$$

Puesto que la suma de los dígitos de 7524 es divisible por 9, 7524 se puede escribir como la suma de dos enteros cada uno de ellos es divisible por 9. Lo que se deduce del ejercicio 15, que 7524 es divisible por 9.

Generalice el argumento dado en este ejemplo para cualquier número entero no negativo n. En otras palabras, demuestre que para cualquier entero n no negativo, si la suma de los dígitos de n es divisible por 9, entonces n es divisible por 9.

✶ 48. Demuestre que para cualquier entero n no negativo, si la suma de los dígitos de n es divisible por 3, entonces n es divisible por 3.

✶ 49. Dado un entero positivo n escrito en forma decimal, la suma alterna de los dígitos de n se obtiene comenzando con el dígito del extremo derecho, restando el dígito inmediato a su izquierda, sumando el siguiente dígito a su izquierda, restando el siguiente dígito y así sucesivamente. Por ejemplo, la suma alterna de los dígitos de 180 928 es $8 - 2 + 9 - 0 + 8 - 1 = 22$. Justifique el hecho de que para cualquier entero n no negativo, si la suma alterna de los dígitos de n es divisible por 11, entonces n es divisible por 11.

Respuestas del autoexamen

1. n es igual d veces un número entero (O: existe un entero r tal que $n = dr$) 2. n; d 3. a; b 4. $\frac{n}{d}$ no es un número entero 5. la frase "a divide a b"; el número que se obtiene cuando a está dividida por b 6. a divide b y b divide a c; a divide a c 7. divisible por algún número primo 8. primo; un producto de números primos; orden

4.4 Demostración directa y contraejemplo IV: división en casos y el teorema del cociente-residuo

Sea especialmente crítico de cualquier enunciado que se encuentre enseguida de la palabra "obviamente". —Anna Pell Wheeler 1883-1966

Cuando divide 11 por 4, se obtiene un cociente de 2 y un residuo de 3.

$$\begin{array}{r} 2 \leftarrow \text{cociente} \\ 4\overline{)\,11} \\ \underline{8} \\ 3 \leftarrow \text{residuo} \end{array}$$

Otra forma de decir esto es que 11 es igual a 2 grupos de 4 y que sobran 3:

$$\underbrace{\boxed{xxxx}\ \boxed{xxxx}}_{\text{2 grupos de 4}}\ \underbrace{xxx}_{\text{sobran 3}}$$

O

$$11 = \underbrace{2}_{\text{2 grupos de 4}} \cdot 4 + \underbrace{3}_{\text{sobran 3}}.$$

Por supuesto, el número que queda (3) es menor que el tamaño de los grupos (4) ya que si sobraran 4 o más, se podría formar otro grupo de 4.

El teorema del cociente-residuo dice que cuando cualquier entero n se divide por un número entero positivo d, el resultado es un cociente q y un residuo r no negativo menor que d.

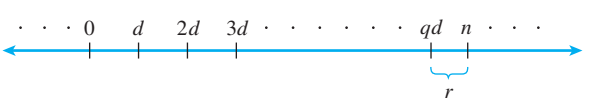
Teorema 4.4.1 Teorema del cociente-residuo

Dado cualquier número entero n y un entero positivo d, existen enteros únicos q y r tales que:

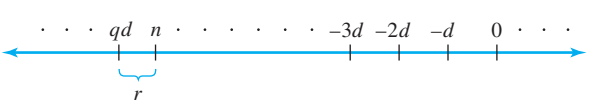
$$n = dq + r \quad \text{y} \quad 0 \leq r < d.$$

La demostración de que existen enteros q y r con las propiedades dadas se encuentra en la sección 5.4, la demostración de que q y r son únicos se describe en el ejercicio 18 en la sección 4.7.

Si n es positivo, el teorema del cociente-residuo se puede ilustrar en la recta numérica de la siguiente manera:



Si n es negativo, cambia la figura. Puesto que $n = dq + r$, donde r es negativo, d se debe multiplicar por un número entero negativo q que va debajo de n. Entonces el entero no negativo r se suma a n. Esto se ilustra de la siguiente manera:



Ejemplo 4.4.1 Teorema del cociente-residuo

Para cada uno de los siguientes valores de n y d, encuentre los enteros q y r tales que $n = dq + r$ y $0 \leq r < d$.

a. $n = 54, d = 4$ b. $n = -54, d = 4$ c. $n = 54, d = 70$

Solución

a. $54 = 4 \cdot 13 + 2$; por tanto $q = 13$ y $r = 2$.

b. $-54 = 4 \cdot (-14) + 2$; por tanto $q = -14$ y $r = 2$.

c. $54 = 70 \cdot 0 + 54$; por tanto $q = 0$ y $r = 54$. ■

div y mod

Un número de lenguajes de programación tienen funciones incorporadas que le permiten calcular muchos valores de q y r para el teorema del cociente-residuo. Estas funciones se llaman **div** y **mod** en Pascal, se llaman / y % en C y en C++, se llaman / y % en Java y se llaman / (o \) y **mod** en .NET. Las funciones dan los valores que satisfacen el teorema del cociente-residuo cuando un entero *no negativo* n se divide entre un número entero positivo d y el resultado se asigna a una variable entera. Sin embargo, no dan los valores que satisfacen el teorema del cociente-residuo cuando un entero negativo n se divide por un número entero positivo d.

• Definición

Dado un entero n y un entero positivo d,

$$\textbf{\textit{n div d}} = \text{el cociente entero que se obtiene cuando } n \text{ se divide por } d, \text{ y}$$

$$\textbf{\textit{n mod d}} = \text{el residuo entero no negativo que se obtiene cuando } n \text{ se divide por } d.$$

Simbólicamente, si n y d son números enteros y $d > 0$, entonces

$$n \; div \; d = q \quad \text{y} \quad n \; mod \; d = r \quad \Leftrightarrow \quad n = dq + r$$

donde q y r son números enteros y $0 \leq r < d$.

Observe que se tiene del teorema del cociente-residuo que $n \; mod \; d$ es igual a uno de los enteros de 0 a $d - 1$ (ya que el residuo de la división de n entre d, debe ser uno de estos números enteros). Observe también que una condición necesaria y suficiente para un entero n es que sea divisible por un número entero que es $n \; mod \; d = 0$. Se le pide que lo demuestre en los ejercicios al final de esta sección.

También puede utilizar una calculadora para suponer los valores de *div* y *mod*. Por ejemplo, para calcular $n \; div \; d$ para un entero n no negativo y un entero positivo d, divida n entre d y desprecie la parte de la respuesta a la derecha del punto decimal. Para encontrar $n \; mod \; d$, puede utilizar el hecho de que si $n = dq + r$, entonces $r = n - dq$. Así $n = d \cdot (n \text{ div } d) + n \; mod \; d$ y así

$$n \; mod \; d = n - d \cdot (n \; div \; d).$$

Por tanto, para encontrar $n \; mod \; d$ *se* calcula $n \; div \; d$, se multiplica por d y se resta el resultado de n.

Ejemplo 4.4.2 Cálculo de *div* y *mod*

Calcule 32 *div* 9 y 32 *mod* 9 a mano y con una calculadora.

Solución Cuando se realice a mano la división se obtienen los siguientes resultados:

$$\begin{array}{r} 3 \quad \leftarrow 32 \text{ div } 9 \\ 9\overline{)\,32} \\ \underline{27} \\ 5 \quad \leftarrow 32 \text{ mod } 9 \end{array}$$

Si utiliza una calculadora de cuatro funciones para dividir 32 entre 9, se obtiene una expresión como 3.555555556. Descartando la parte fraccionaria da $32 \; div \; 9 = 3$ y así

$$32 \; mod \; 9 = 32 - 9 \cdot (32 \; div \; 9) = 32 - 27 = 5.$$

Una calculadora con una función de parte entera integrada iPart permite introducir una sola expresión para cada cálculo:

$$32 \; div \; 9 = \text{iPart}(32/9)$$

y $\quad 32 \; mod \; 9 = 32 - 9 \cdot \text{iPart}\,(32/9) = 5.$ ■

Ejemplo 4.4.3 Cálculo del día de la semana

Suponga que hoy es martes y ni este año ni el próximo es un año bisiesto. ¿Qué día de la semana va a ser en 1 año a partir de hoy?

Solución Hay 365 días en un año que no es un año bisiesto y cada semana tiene 7 días. Ahora

$$365 \; div \; 7 = 52 \quad \text{y} \quad 365 \; mod \; 7 = 1$$

ya que $365 = 52 \cdot 7 + 1$. Así, 52 semanas, o 364 días, a partir de hoy será un martes y 365 días para que a partir de hoy será un día más tarde, es decir, miércoles.

En términos más generales, si *DíaT* es el día de la semana de hoy y *DíaN* hoy es el día de la semana en *N* días, entonces

$$DíaN = (DíaT + N) \; mod \; 7, \tag{4.4.1}$$

donde domingo = 0, lunes = 1, . . . , sábado = 6. ■

Ejemplo 4.4.4 Solución de un problema acerca de *mod*

Supongamos que *m* es un número entero. Si $m \; mod \; 11 = 6$, ¿que es $4m \; mod \; 11$?

Solución Debido a que $m \; mod \; 11 = 6$, se obtiene el residuo cuando *m* dividido entre 11 es 6. Esto significa que hay algún entero *q*, tal que

$$m = 11q + 6.$$

Así $$4m = 44q + 24 = 44q + 22 + 2 = 11(4q + 2) + 2.$$

Ya que $4q + 2$ es un número entero (porque los productos y las sumas de los números enteros son números enteros) y ya que $2 < 11$, el residuo que se obtiene cuando $4m$ se divide por 11 es 2. Por tanto,

$$4m \; mod \; 11 = 2$$ ■

Representaciones de enteros

En la sección 4.1 hemos definido un entero que tiene la forma del doble de un número entero. En ese momento se podría haber definido un número entero impar como uno que no fuera par. En lugar de eso, ya que era más útil para demostrar teoremas, especificamos que un número entero impar tiene la forma del doble de un número entero más uno. El teorema del cociente-residuo estas dos formas juntas de describir enteros impares, al garantizar que cualquier número entero es par o impar. Para ver por qué, sea n cualquier número entero y considere lo que sucede cuando n se divide por 2. Por el teorema del cociente-residuo (con $d = 2$), existen enteros únicos q y r tales que

$$n = 2q + r \quad \text{y} \quad 0 \leq r < 2.$$

Pero los únicos enteros que satisfacen $0 \leq r < 2$ son $r = 0$ y $r = 1$. De lo que se deduce que para cualquier número entero dado n, existe un entero q con

$$n = 2q + 0 \quad \text{o} \quad n = 2q + 1.$$

En el caso que $n = 2q + 0 = 2q$, n es par. En el caso que $n = 2q + 1$, n es impar. Por tanto n es par o impar y, debido a la unicidad de q y r, n no pueden ser ambos pares e impares.

La *paridad* de un entero se refiere a si el entero es par o impar. Por ejemplo, 5 tiene paridad impar y 28 tiene paridad par. Llamamos al hecho de que cualquier número entero es par o impar la **propiedad de paridad**.

Ejemplo 4.4.5 Enteros consecutivos tienen paridad opuesta

Demuestre que dados dos números enteros consecutivos, uno es par y el otro es impar.

Solución Dos números enteros son llamados *consecutivos*, si y sólo si, uno es uno más el otro. Así que si un número entero es m, el entero consecutivo siguiente es $m + 1$.

Para demostrar el enunciado dado, empiece por suponer que usted tiene dos números enteros consecutivos dados, pero elegidos arbitrariamente. Si el menor es m, entonces el más grande será $m + 1$. ¿Cómo se puede saber con certeza que uno de ellos es par y el otro es impar? Puede imaginar algunos ejemplos: 4, 5; 12, 13; 1 073, 1 074. En los dos primeros ejemplos, el menor de los dos números enteros es par y el más grande es impar, en el último ejemplo, es al revés. Estas observaciones sugieren dividir el análisis en dos casos.

***Caso 1*:** El menor de los dos números enteros es par.

***Caso 2*:** El menor de los dos números enteros es impar.

En el primer caso, cuando m es par, parece que el entero consecutivo siguiente es impar. ¿Es esto siempre así? Si un entero m es par, $m + 1$ debe necesariamente ser impar? Por supuesto la respuesta es sí. Porque si m es par, entonces $m = 2k$ para algún entero k y así $m + 1 = 2k + 1$, que es impar.

En el segundo caso, cuando m es impar, el número entero consecutivo siguiente es par. ¿Es esto siempre verdadero? ¿Si un número m es impar, $m + 1$ debe necesariamente ser par? Una vez más, la respuesta es sí. Ya que si m es impar, entonces $m = 2k + 1$ para algún entero k y así $m + 1 = (2k + 1) + 1 = 2k + 2 = 2(k + 1)$, que es par.

Este análisis se resume en la siguiente página.

Teorema 4.4.2 La propiedad de paridad

Cualquiera de los dos números enteros consecutivos tienen paridad opuesta.

Demostración:

Supongamos que se dan dos *[particulares, pero elegidos arbitrariamente]* enteros consecutivos; los llamamos m y $m + 1$. *[Debemos demostrar que uno de m y m + 1 es par y que el otro es impar.]* Por la propiedad de paridad, ya sea m par o m impar. *[Partimos la demostración en dos casos, dependiendo de si m es par o impar.]*

***Caso 1* (*m es par*):** En este caso, $m = 2k$ para algún entero k y así $m + 1 = 2k + 1$, que es impar *[por la definición de impar]*. De ahí que en este caso, uno de m y $m + 1$ es par y el otro es impar.

***Caso 2* (*m es impar*):** En este caso, $m = 2k + 1$ para algún entero k y así $m + 1 = (2k + 1) + 1 = 2k + 2 = 2(k + 1)$. Pero $k + 1$ es un número entero, ya que es una suma de dos números enteros. Por tanto, $m + 1$ es igual a dos veces un número entero y por tanto $m + 1$ es par. De ahí que en este caso también, uno de m y $m + 1$ es par y la otra es impar.

De lo que se deduce que, independientemente de lo que en este caso sucede, para dados m y $m + 1$, que son elegidos, uno de m y $m + 1$ es par y el otro es impar. *[Esto es lo que se quería demostrar.]*

■

La división en casos de una demostración es como la transferencia del control de un enunciado **if-then-else** en un programa de computadora. Si m es par, transfiere el control al caso 1, si no, transfiere el control al caso 2. Para cualquier entero dado, sólo se aplicará uno de los casos. Sin embargo, se deben considerar ambos casos, para obtener una demostración que sea válida para un número entero dado arbitrariamente par o no.

Hay veces en que se pide la división en más de dos casos. Supongamos que en alguna etapa del desarrollo de una demostración, usted sabe que un enunciado de la forma

$$A_1 \text{ o } A_2 \text{ o } A_3 \text{ o } \ldots \text{ o } A_n$$

es verdadero y supongamos que desea deducir una conclusión C. Por definición de *o*, usted sabe que al menos uno de los enunciados A_i es verdadero (aunque no puede saber cuál). En esta situación, debe utilizar el método de división en casos. Primero suponga que A_1 es verdadero y deduzca C; después suponga que A_2 es verdadero y deduzca C y así sucesivamente hasta que haya supuesto que A_n es verdadero y deduzca C. En ese momento, se puede concluir que, independientemente de cuál enunciado sea verdadero, se deduce la veracidad de C.

Método de demostración por división en casos

Para demostrar un enunciado de la forma "Si A_1 o A_2 o $\ldots$, o A_n, entonces C", se demuestran todos los enunciados siguientes:

Si A_1, entonces C,
Si A_2, entonces C,
$\vdots$
Si A_n, entonces C,

Este proceso demuestra que C es verdadero independientemente de cuál de $A_1, A_2, \ldots, A_n$ sea el caso.

La demostración de la división en casos es una generalización de la forma del argumento que se muestra en el ejemplo 2.3.7, cuya validez se le pidió establecer en el ejercicio 21 de la sección 2.3. Este método de demostración se combinó con el teorema del cociente-residuo para $d = 2$ para demostrar el teorema 4.4.2. Permitir que d tome valores adicionales permite obtener una variedad de otros resultados. Comenzamos mostrando lo que sucede cuando $a = 4$.

Ejemplo 4.4.6 Representaciones de enteros de módulo 4

Demuestre que cualquier entero puede ser escrito en una de las cuatro formas

$$n = 4q \quad \text{o} \quad n = 4q + 1 \quad \text{o} \quad n = 4q + 2 \quad \text{o} \quad n = 4q + 3$$

para algún entero q.

Solución Dado cualquier número entero n, aplique el teorema del cociente-residuo a n con $d = 4$. Esto implica que existe un cociente entero q y un residuo r tal que

$$n = 4q + r \quad \text{y} \quad 0 \leq r < 4.$$

Pero los únicos residuos no negativos r que son menores de 4 son 0, 1, 2 y 3. Por tanto

$$n = 4q \quad \text{o} \quad n = 4q + 1 \quad \text{o} \quad n = 4q + 2 \quad \text{o} \quad n = 4q + 3$$

para algún entero q. ■

El siguiente ejemplo ilustra cómo las representaciones alternativas de enteros de módulo 4 pueden ayudar a establecer un resultado en la teoría de números. La solución se divide en dos partes: un análisis y una demostración formal. Estas corresponden a las etapas de desarrollo de la demostración real. Muy pocas personas, cuando se le pide demostrar un teorema desconocido, inmediatamente escriben la clase de demostración formal que se encuentra en un libro de matemáticas. La mayoría necesita experimentar con varios métodos posibles antes de encontrar uno que funcione. Una demostración formal es muy similar a la finalización de una novela de misterio —la parte en la que la acción de la historia es sistemáticamente revisada y todos los cabos sueltos son cuidadosamente atados.

Ejemplo 4.4.7 El cuadrado de un entero impar

Nota Otra forma de establecer este hecho es que si eleva al cuadrado un número entero impar y se divide por 8, siempre obtendrá un residuo de 1. ¡Pruebe con algunos ejemplos!

Demostración: El cuadrado de cualquier número entero impar tiene la forma de $8m + 1$ para algún entero m.

Solución Empiece por preguntarse: ¿De dónde voy a partir? y ¿Qué necesito para demostrar? Para ayudar a responder estas preguntas, introduzca variables para representar las cantidades en el enunciado que demostrará.

Reexpresión Formal: $\forall$ enteros impares n, $\exists$ un entero m tal que $n^2 = 8m + 1$. A partir de éste, inmediatamente puede identificar el punto de partida y lo que se demostrará.

Punto de partida: Supongamos que n es un entero impar dado, pero elegido arbitrariamente.

Para demostrar: $\exists$ un entero m tal que $n^2 = 8m - 1$.

Parece difícil. ¿Por qué debería ser un entero m con la propiedad de que $n^2 = 8m + 1$? ¿Diría que $(n^2 - 1)/8$ es un número entero, o que 8 divide a $n^2 - 1$. Quizás usted podría hacer uso del hecho de que $n^2 - 1 = (n - 1)(n + 1)$. ¿8 divide a $(n - 1)(n + 1)$? Ya que n es impar, tanto $(n - 1)$ como $(n + 1)$ son pares. Eso significa que su producto es divisible entre 4. Pero eso no es suficiente. Necesita demostrar que el producto es divisible por 8. Esto parece ser un callejón sin salida.

Podría intentar otra táctica. Dado que n es impar, se puede representar a n como $2q + 1$ para algún entero q. Entonces, $n^2 = (2q + 1)^2 = 4q^2 + 4q + 1 = 4(q^2 + q) + 1$. De este

análisis se deduce que n^2 se puede escribir en la forma $4m + 1$, pero puede que no sea claro que se puede escribir como $8m + 1$. Esto también parece ser un callejón sin salida.*

Sin embargo, otra posibilidad es utilizar el resultado del ejemplo 4.4.6. Este ejemplo muestra que cualquier número entero se puede escribir en una de las cuatro formas $4q$, $4q + 1$, $4q + 2$ o $4q + 3$. Dos de estas, $4q + 1$ y $4q + 3$, son impares. Así, cualquier número entero impar se puede escribir en la forma $4q + 1$ o $4q + 3$ para algún entero q. Podría intentar partir en casos en base de estas dos formas diferentes.

Nota La desesperación puede estimular la creatividad. Cuando ha intentado sin éxito todos los métodos obvios y realmente se preocupa por resolver un problema, le llega de los rincones de su memoria *cualquier cosa* que pueda ayudar.

Resulta que esta última posibilidad ¡funciona! En cada uno de los dos casos, la conclusión se deduce fácilmente del cálculo directo. Los detalles se muestran en la siguiente demostración formal:

Teorema 4.4.3

El cuadrado de cualquier número entero impar tiene la forma de $8m + 1$ para algún entero m.

Demostración:

Supongamos que n es un *[dado, pero elegido arbitrariamente]* entero impar. Por el teorema del cociente-residuo, n se puede escribir en una de las formas

$$4q \quad \text{o} \quad 4q + 1 \quad \text{o} \quad 4q + 2 \quad \text{o} \quad 4q + 3$$

para algún entero q. De hecho, ya que n es impar y $4q$ y $4q + 2$ son pares, n debe tener una de las formas

$$4q + 1 \quad \text{o} \quad 4q + 3.$$

Caso 1 ($n = 4q + 1$ para algún q entero): *[Debemos encontrar un entero m tal que $n^2 = 8m + 1$.]* Ya que $4q + 1$,

$$\begin{aligned} n^2 &= (4q + 1)^2 && \text{por sustitución} \\ &= (4q + 1)(4q + 1) && \text{por definición de cuadrado} \\ &= 16q^2 + 8q + 1 \\ &= 8(2q^2 + q) + 1 && \text{por las leyes del álgebra.} \end{aligned}$$

Sea $m = 2q^2 + q$. Entonces m es un entero ya que 2 y q son números enteros y las sumas y productos de los números enteros son números enteros. Por tanto, sustituyendo,

$$n^2 = 8m + 1 \quad \text{donde } m \text{ es un número entero.}$$

Caso 2 ($n = 4q + 3$ para algunos entero q): *[Debemos encontrar un entero m tal que $n^2 = 8m + 1$.]* Ya que $n = 4q + 3$,

$$\begin{aligned} n^2 &= (4q + 3)^2 && \text{por sustitución} \\ &= (4q + 3)(4q + 3) && \text{por definición de cuadrado} \\ &= 16q^2 + 24q + 9 \\ &= 16q^2 + 24q + (8 + 1) \\ &= 8(2q^2 + 3q + 1) + 1 && \text{por las leyes del álgebra.} \end{aligned}$$

[La motivación para la elección de los pasos algebraicos fue el deseo de escribir la expresión en la forma $8 \cdot$ (algún entero) $+ 1$.]

*Vea el ejercicio 18 para una perspectiva diferente

Sea $m = 2q^2 + 3q + 1$. Entonces m es un número entero ya que 1, 2, 3 y q son números enteros y las sumas y productos de números enteros son números enteros. Por tanto, sustituyendo,

$$n^2 = 8m + 1 \text{ donde } m \text{ es un número entero.}$$

Los casos 1 y 2 muestran que, dado cualquier número entero impar, ya sea de la forma $4q + 1$ o $4q + 3$, $n^2 = 8m + 1$ para algún entero m. *[Esto es lo que necesitamos demostrar.]*

■

Considere que el resultado del teorema 4.4.3 también se puede escribir: "Para cualquier entero n impar, n^2 *mod* $8 = 1$".

En general, de acuerdo con el teorema del cociente-residuo, si un entero n se divide entre un número entero d, los residuos posibles son 0, 1, 2, . . . , $(d - 1)$. Esto implica que n se puede escribir en una de las formas

$$dq,\ dq + 1,\ dq + 2, \ldots,\ dq + (d - 1) \qquad \text{para algún entero } q.$$

Muchas propiedades de los números enteros se pueden obtener por dar a d una variedad de diferentes valores y analizar los casos que resultan.

Valor absoluto y la desigualdad del triángulo

La desigualdad del triángulo es uno de los resultados más importantes que implican el valor absoluto. Tiene aplicaciones en muchas áreas de las matemáticas.

• Definición

Para cualquier número real x, el **valor absoluto de *x***, que se denota $| x |$, se define de la siguiente manera:

$$|x| = \begin{cases} x & \text{si } x \geq 0 \\ -x & \text{si } x < 0 \end{cases}.$$

La desigualdad del triángulo dice que el valor absoluto de la suma de dos números es menor o igual a la suma de sus valores absolutos. Le damos una demostración basada en los siguientes dos hechos, los cuales se obtienen a partir de la división de casos. Los establecemos como lemas. Un **lema** es un enunciado que no tiene mucho interés intrínseco, pero que es útil para deducir otros resultados.

Lema 4.4.4

Para todos los números reales r, $- | r | \leq r \leq | r |$.

Demostración:

Supongamos que r es cualquier número real. Dividimos en casos de acuerdo si $r \geq 0$ o $r < 0$.

Caso 1 (r ≥ 0): En este caso, por la definición de valor absoluto, $|r| = r$. También, ya que r es positivo y $-|r|$ es negativo, $-|r| < r$. Por tanto, es verdadero que

$$-|r| \leq r \leq |r|.$$

continúa en la página 188

Caso 2 (r < 0): En este caso, por definición de valor absoluto, $|r| = -r$. Multiplicando ambos lados por -1 se obtiene que $-|r| = r$. También, puesto que r es negativo y $|r|$ es positivo, $r < |r|$. Por tanto, también es cierto que en este caso

$$-|r| \leq r \leq |r|.$$

Por tanto, en cualquier caso,

$$-|r| \leq r \leq |r|$$

[que era lo que se quería demostrar].

Lema 4.4.5

Para todos los números reales r, $|-r| = |r|$.

Demostración:

Supongamos que r es cualquier número real. De acuerdo con el teorema T23 en el apéndice A, si $r > 0$, entonces $-r < 0$ y si $r < 0$ entonces $-r > 0$. Por tanto

$$|-r| = \begin{cases} -r & \text{si } -r > 0 \\ 0 & \text{si } -r = 0 \\ -(-r) & \text{si } -r < 0 \end{cases} \quad \text{por definición de valor absoluto}$$

$$= \begin{cases} -r & \text{si } -r > 0 \\ 0 & \text{si } -r = 0 \\ r & \text{si } -r < 0 \end{cases} \quad \text{ya que } -(-r) = r, \text{ por el teorema de T4 del apéndice A}$$

$$= \begin{cases} -r & \text{si } r < 0 \\ 0 & \text{si } -r = 0 \\ r & \text{si } r > 0 \end{cases} \quad \text{ya que, de acuerdo con el teorema T24 del apéndice A, cuando } -r > 0, \text{ entonces } r < 0, \text{ cuando } -r < 0, \text{ entonces } r > 0 \text{ y cuando } -r = 0, \text{ entonces } r = 0,$$

$$= \begin{cases} r & \text{si } r \geq 0 \\ -r & \text{si } r < 0 \end{cases} \quad \text{rearreglando el resultado anterior}$$

$$= |r| \quad \text{por la definición de valor absoluto.}$$

Los lemas 4.4.4 y 4.4.5 proporcionan una base para demostrar la desigualdad del triángulo.

Teorema 4.4.6 La desigualdad del triángulo

Para todos los números reales x y y, $|x + y| \leq |x| + |y|$.

Demostración:

Supongamos que x y y, son números reales.

Caso 1 (x + y ≥ 0): En este caso, $|x + y| = x + y$, por lo que, por el lema 4.4.4,

$$x \leq |x| \quad \text{y} \quad y \leq |y|.$$

Por tanto, por el teorema T26 del apéndice A,

$$|x + y| = x + y \leq |x| + |y|.$$

Caso 2 ($x + y < 0$): En este caso, $|x + y| = -(x + y) = (-x) + (-y)$ y así, por lemas 4.4.4 y 4.4.5,

$$-x \leq |-x| = |x| \quad \text{y} \quad -y \leq |-y| = |y|.$$

Se tiene por el teorema T26 del apéndice A, que

$$|x + y| = (-x) + (-y) \leq |x| + |y|.$$

De ahí que en ambos casos $|x + y| \leq |x| + |y|$ *[que era lo que se quería demostrar]*.

Autoexamen

1. El teorema del cociente-residuo dice que para todos los enteros n y d con $d > 0$, existen _____ q y r tal que _____ y_____.
2. Si n y d son números enteros con $d > 0$, n *div* d es _____ y n *mod* d es _____.
3. La paridad de un entero indica si el entero es _____.
4. De acuerdo con el teorema del cociente-residuo, si un entero n se divide entre un número entero positivo d, los posibles residuos son _____. Esto implica que n se puede escribir en una de las formas _____ para algún entero q.
5. Para demostrar que un enunciado de la forma "Si A_1 o A_2 o A_3, entonces C", pruebe _____ y _____ y _____.
6. La desigualdad del triángulo dice que para todos los números reales x y y, _____.

Conjunto de ejercicios 4.4

Para cada uno de los valores de n y d dados en los ejercicios del 1 al 6 y encuentre los enteros q y r tales que $n = dq + r$ y $0 \leq r < d$.

1. $n = 70$, $d = 9$

2. $n = 62$, $d = 7$

3. $n = 36$, $d = 40$

4. $n = 3$, $d = 11$

5. $n = -45$, $d = 11$

6. $n = -27$, $d = 8$

Evalúe las expresiones de los ejercicios del 7 al 10.

7. a. 43 *div* 9 b. 43 *mod* 9

8. a. 50 *div* 7 b. 50 *mod* 7

9. a. 28 *div* 5 b. 28 *mod* 5

10. a. 30 *div* 2 b. 30 *mod* 2

11. Compruebe la exactitud de la fórmula (4.4.1) que se presenta en el ejemplo 4.4.3 para los siguientes valores de *DíaT* y *N*.
    a. *DíaT* = 6 (sábado) y *N* = 15
    b. *DíaT* = 0 (domingo) y *N* = 7
    c. *DíaT* = 4 (jueves) y *N* = 12

✶ 12. Justifique la fórmula (4.4.1) para los valores generales de *DíaT* y *N*.

13. El lunes un amigo le dice que se reunirá con usted de nuevo en 30 días. ¿Qué día de la semana que va a ser?

***H* 14.** Si hoy es martes, ¿qué día de la semana va a ser en 1 000 días a partir de hoy?

15. El 1 de enero 2000, fue un sábado y 2000 fue un año bisiesto. ¿Qué día de la semana será el 1 de enero 2050?

16. Supongamos que d es un entero positivo y n es un entero. Si $d \mid n$, ¿a qué es igual el residuo obtenido cuando el teorema del cociente-residuo se aplica a n con el divisor d?

17. Demuestre que el producto de dos números enteros consecutivos es par.

18. El resultado del ejercicio 17 sugiere que el segundo aparente callejón sin salida en el análisis del ejemplo 4.4.7 no puede ser un callejón sin salida después de todo. Escriba una nueva demostración del teorema 4.4.3 con base en esta observación.

19. Demuestre que para todo entero n, $n^2 - n + 3$ es impar.

20. Supongamos que a es un número entero. Si a *mod* 7 = 4, ¿qué es 5a *mod* 7? En otras palabras, si la división de a por 7 da un residuo de 4, ¿cuál es el residuo cuando 5a se divide por 7?

21. Supongamos que b es un número entero. Si b *mod* 12 = 5, ¿qué es 8b *mod* 12? En otras palabras, si la división de b entre 12 da un residuo de 5, ¿cuál es el residuo cuando 8b se divide por 12?

22. Supongamos que c es un número entero. Si c *mod* 15 = 3, ¿qué es 10c *mod* 15? En otras palabras, si la división de c por 15 se obtiene un residuo de 3, ¿cuál es el residuo cuando 10c se divide por 15?

23. Demuestre que para todo entero n, si n *mod* 5 = 3 entonces n^2 *mod* 5 = 4.

24. Demuestre que para todos los números enteros m y n, si m *mod* 5 = 2 y n *mod* 3 = 6 entonces mn *mod* 5 = 1.

25. Demuestre que para todos los números enteros a y b, si a *mod* 7 = 5 y b *mod* 7 = 6 entonces ab *mod* 7 = 2.

***H* 26.** Demuestre que una condición necesaria y suficiente para un entero no negativo n será divisible por un número entero positivo d es que n *mod* d = 0.

27. Demuestre que cualquier entero n se puede escribir en una de las tres formas

$$n = 3q \quad \text{o} \quad n = 3q + 1 \quad \text{o} \quad n = 3q + 2$$

para algún entero q.

28. a. Utilice el teorema del cociente-residuo con $d = 3$ para demostrar que el producto de cualesquiera tres números enteros consecutivos es divisible por 3.
b. Utilice la notación *mod* para reescribir el resultado del inciso *a*).

H 29. a. Utilice el teorema de cociente-residuo con $d = 3$ para demostrar que el cuadrado de cualquier número entero tiene la forma $3k$ o $3k + 1$ para algún entero k.
b. Utilice la notación *mod* para reescribir el resultado del inciso *a*).

30. a. Utilice el teorema de cociente-residuo con $d = 3$ para demostrar que el producto de dos números enteros consecutivos, tiene la forma $3k$ o $3k + 2$ para algún entero k.
b. Utilice la notación *mod* para reescribir el resultado del inciso *a*).

En los ejercicios del 31 al 33, puede utilizar las propiedades que se presentan en el ejemplo 4.2.3.

31. a. Demostrar que para todos los números enteros m y n, $m + n$ y $m - n$ son ya sean dos pares o dos impares.
b. Encuentre todas las soluciones a la ecuación $m^2 - n^2 = 56$ en la que tanto m como n son números enteros positivos.
c. Encuentre todas las soluciones a la ecuación $m^2 - n^2 = 88$ en la que tanto m como n son enteros positivos.

32. Dados los números enteros cualesquiera a, b y c, si $a - b$ es par y $b - c$ es par, ¿qué puede decir acerca de la paridad de $2a - (b + c)$? Demuestre su respuesta.

33. Dados los números enteros cualesquiera a, b y c, si $a - b$ es impar y $b - c$ es par, ¿qué puede decir acerca de la paridad de $a - c$? Demuestre su respuesta.

H 34. Dado cualquier número entero n, si $n > 3$, podría n, $n + 2$ y $n + 4$ ser primo? Demuestre o dé un contraejemplo.

Demuestre cada uno de los enunciados en los ejercicios del 35 al 46.

35. La cuarta potencia de cualquier número entero tiene la forma $8m$ o $8m + 1$ para algún entero m.

H 36. El producto de cuatro números enteros consecutivos cualesquiera es divisible por 8.

37. El cuadrado de cualquier número entero tiene la forma $4k$ o $4k + 1$ para algún entero k.

H 38. Para cualquier entero n, $n^2 + 5$ no es divisible por 4.

H 39. La suma de cuatro enteros consecutivos, tiene la forma $4k + 2$ para algún entero k.

40. Para cualquier entero n, $n(n^2 - 1)(n + 2)$ es divisible por 4.

41. Para todos los números enteros m, $m^2 = 5k$ o $m^2 = 5k + 1$ o $m^2 = 5k + 4$ para algún entero k.

H 42. Todos los números primos, excepto 2 y 3 tiene la forma $6q + 1$ o $6q + 5$ para algún entero q.

43. Si n es un entero impar, entonces n^4 *mod* $16 = 1$.

H 44. Para todos los números reales x y y, $|x| \cdot |y| - |xy|$.

45. Para todos los números reales r y c con $c \geq 0$, si $-c \leq r \leq c$, entonces $|r| \leq c$.

46. Para todos los números reales r y c con $c \geq 0$, si $|r| \leq c$, entonces $-c \leq r \leq c$.

47. Una matriz $\mathbf{M}$ tiene 3 renglones y 4 columnas.

$$\begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \end{bmatrix}$$

Las 12 entradas en la matriz se almacenan en forma de un renglón principal en las posiciones de la 7609 a la 7620 en la memoria de una computadora. Esto significa que las entradas del primer renglón (leyendo de izquierda a derecha) se almacenan en primer lugar, después, las entradas del segundo renglón y finalmente las entradas del tercer renglón.
a. ¿En qué posición se almacena a_{22}?
b. Escriba una fórmula (en i y en j) que dé el entero n para que a_{ij} se almacene en la posición $7609 + n$.
c. Encuentre fórmulas (en n) para r y s de modo que a_{rs} se almacene en la posición $7609 + n$.

48. Sea $\mathbf{M}$ una matriz con m renglones y n columnas y supongamos que las entradas de $\mathbf{M}$ se almacenan en la memoria de una computadora en forma de renglón principal (vea el ejercicio 47) en las posiciones $N, N + 1, N + 2, \ldots, N + mn - 1$. Determine fórmulas en k para r y s, tal que a_{rs} se almacene en la posición $N + k$.

✶ 49. Si m, n y d son números enteros, $d > 0$ y m *mod* $d = n$ *mod* d, ¿se deduce necesariamente que $m = n$?, ¿que $m - n$ es divisible por d? Demuestre sus respuestas.

✶ 50. Si m, n y d son números enteros, $d > 0$ y $d \mid (m - n)$, ¿cuál es la relación entre m *mod* d y n *mod* d? Demuestre su respuesta.

✶ 51. Si m, n, a, b y d son números enteros, $d > 0$ y m *mod* $d = a$ y n *mod* $d = b$, es $(m + n)$ *mod* $d = a + b$? ¿Es $(m + n)$ *mod* $d = (a + b)$ *mod* d? Demuestre sus respuestas.

✶ 52. Si m, n, a, b y d son números enteros, $d > 0$ y m *mod* $d = a$ y n *mod* $d = b$, ¿es (mn) *mod* $d = ab$?, ¿es (mn) *mod* $d = ab$ *mod* d? Demuestre sus respuestas.

53. Demuestre que si m, d y k son enteros y $d > 0$, entonces $(m + dk)$ *mod* $d = m$ *mod* d.

Respuestas del autoexamen

1. enteros; $n = dq + r$; $0 \leq r < d$ 2. el cociente que se obtiene cuando n se divide entre d; y el residuo no negativo que se obtiene cuando n se divide por d 3. par o impar 4. 0, 1, 2, …, $(d - 1)$; dq, $dq + 1$, $dq + 2$, …, $dq + (d - 1)$ 5. Si A_1, entonces C; Si A_2, entonces C; Si A_3, entonces C 6. $|x + y| \leq |x| + |y|$

4.5 Demostración directa y contraejemplo V: piso y techo

La demostración sirve para muchos propósitos al mismo tiempo. Para ser expuestas al escrutinio y juicio de un público nuevo, [a] la demostración está sujeta a un proceso constante de crítica y revalidación. Los errores, ambigüedades y malentendidos se aclaran con la exposición constante. Prueba de ello es la respetabilidad. La demostración es el sello de la autoridad.

La demostración, en el mejor de los casos, aumenta la comprensión al revelar el corazón de la materia. La demostración sugiere nuevas matemáticas. El novicio que estudia demostraciones se acerca a la creación de nuevas matemáticas. La demostración es poder matemático, el voltaje eléctrico de la materia que vitaliza las afirmaciones estáticas de los teoremas.

Por último, la demostración es un ritual y una celebración del poder de la razón pura.

—Philip J. Davis y Reuben Hersh, *La experiencia matemática*, 1981

Imagine un número real colocado en una recta numérica. El *piso* y el *techo* del número son los números enteros a la izquierda inmediata y a la derecha del número (a menos que el número sea, en sí, un número entero, en cuyo caso el piso y el techo son iguales al mismo número). Muchos lenguajes de computadora han incorporado funciones que calculan el piso y el techo de forma automática. Estas funciones son muy convenientes para usarse al escribir ciertos tipos de programas de computadora. Además, los conceptos de piso y el techo son importantes en el análisis de la eficiencia de los algoritmos de computadoras.

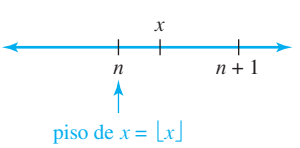
• Definición

Dado cualquier número real x, el **piso de x**, que se denota por $\lfloor x \rfloor$, se define de la siguiente manera:

$$\lfloor x \rfloor = n \text{ es el único entero tal que } n \leq x < n + 1.$$

Simbólicamente, si x es un número real y n es un entero, entonces

$$\lfloor x \rfloor = n \quad \Leftrightarrow \quad n \leq x < n + 1.$$



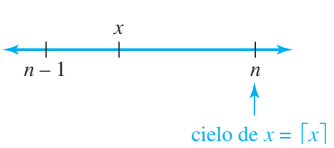
• Definición

Dado cualquier número real x, el **techo de x**, que se denota por $\lceil x \rceil$, se define de la siguiente manera:

$$\lceil x \rceil = n \text{ es el único entero tal que } n - 1 < x \leq n.$$

Simbólicamente, si x es un número real y n es un entero, entonces

$$\lceil x \rceil = n \quad \Leftrightarrow \quad n - 1 < x \leq n.$$



Ejemplo 4.5.1 Cálculo de suelos y techos

Calcule $\lfloor x \rfloor$ y $\lceil x \rceil$ para cada uno de los siguientes valores de x:

a. $25/4$ b. 0.999 c. -2.01

Solución

a. $25/4 = 6.25$ y $6 < 6.25 < 7$; por tanto $\lfloor 25/4 \rfloor = 6$ y $\lceil 25/4 \rceil = 7$.

b. $0 < 0.999 < 1$; por tanto $\lfloor 0.999 \rfloor = 0$ y $\lceil 0.999 \rceil = 1$.

c. $-3 < -2.01 < -2$; por tanto $\lfloor -2.01 \rfloor = -3$ y $\lceil -2.01 \rceil = -2$.

Considere que en algunas calculadoras $\lfloor x \rfloor$ se denota INT (x). ■

Ejemplo 4.5.2 Una aplicación

A los 1 370 estudiantes de un colegio se les da la oportunidad de tomar autobuses para un juego fuera de la ciudad. Cada autobús tiene un máximo de 40 pasajeros.

a. Por razones de economía, el director de atletismo enviará sólo autobuses llenos. ¿Cuál es el número máximo de autobuses que el director deportivo enviará?

b. Si el director deportivo está dispuesto a enviar un autobús parcialmente lleno, ¿cómo cuántos autobuses serán necesarios para permitir que todos los estudiantes tomen el viaje?

Solución

a. $\lfloor 1370/40 \rfloor = \lfloor 34.25 \rfloor = 34$ b. $\lceil 1370/40 \rceil = \lceil 34.25 \rceil = 35$ ■

Ejemplo 4.5.3 Algunos valores generales de piso

Si k es un número entero, ¿qué son $\lfloor k \rfloor$ y $\lfloor k + 1/2 \rfloor$? ¿Por qué?

Solución Supongamos que k es un número entero. Entonces,

$$\lfloor k \rfloor = k \text{ porque } k \text{ es un número entero y } k \le k \le k + 1,$$

y

$$\left\lfloor k + \frac{1}{2} \right\rfloor = k \text{ porque } k \text{ es un entero y } k \le k + \frac{1}{2} < k + 1.$$ ■

Ejemplo 4.5.4 Refutación de una supuesta propiedad de piso

¿Es el siguiente enunciado verdadero o falso?

Para todos los números reales x y y, $\lfloor x + y \rfloor = \lfloor x \rfloor + \lfloor y \rfloor$.

Solución El enunciado es falso. Como un contraejemplo, tome $x = y = \frac{1}{2}$. Entonces

$$\lfloor x \rfloor + \lfloor y \rfloor = \left\lfloor \frac{1}{2} \right\rfloor + \left\lfloor \frac{1}{2} \right\rfloor = 0 + 0 = 0,$$

mientras que

$$\lfloor x + y \rfloor = \left\lfloor \frac{1}{2} + \frac{1}{2} \right\rfloor = \lfloor 1 \rfloor = 1.$$

Por tanto $\lfloor x + y \rfloor \neq \lfloor x \rfloor + \lfloor y \rfloor$.

Para llegar a este contraejemplo, se podría haber razonado de la siguiente manera: Supongamos que x y y son números reales. ¿Debe necesariamente ser el caso de que $\lfloor x + y \rfloor = \lfloor x \rfloor + \lfloor y \rfloor$ o podrían x y y ser tales que $\lfloor x + y \rfloor \neq \lfloor x \rfloor + \lfloor y \rfloor$? Imagínese valores que las distintas cantidades podrían tomar. Por ejemplo, si tanto x como y son positivos, entonces $\lfloor x \rfloor$ y $\lfloor y \rfloor$ son las partes enteras de $\lfloor x \rfloor$ y $\lfloor y \rfloor$, respectivamente, del mismo modo que

$$2\frac{3}{5} = 2 + \frac{3}{5}$$

parte entera parte fraccionaria

así es

$$x = \lfloor x \rfloor + \text{parte fraccionaria de } x$$

y

$$y = \lfloor y \rfloor + \text{parte fraccionaria de } y$$

donde el término *parte fraccionaria* se entiende aquí como la parte del número a la derecha del punto decimal cuando el número está escrito en notación decimal. Así, si x y y son positivos,

$$x + y = \lfloor x \rfloor + \lfloor y \rfloor + \textit{la suma de las partes fraccionarias de } x \textit{ y } y.$$

Pero también

$$x + y = \lfloor x + y \rfloor + \textit{la parte fraccionaria de } (x + y).$$

Estas ecuaciones muestran que sí existen números x y y tales que la suma de las partes fraccionarias de x y y es al menos 1, entonces se puede encontrar un contraejemplo. Pero sí existen dichas x y y, por ejemplo, $x = \frac{1}{2}$ y $y = \frac{1}{2}$ como antes. ■

El análisis del ejemplo 4.5.4 indica que si x y y son positivas y la suma de sus partes fraccionarias es menor que 1, entonces $\lfloor x + y \rfloor = \lfloor x \rfloor + \lfloor y \rfloor$. En particular, si x es positivo y m es un entero positivo, entonces $\lfloor x + m \rfloor = \lfloor x \rfloor + \lfloor m \rfloor = \lfloor x \rfloor + m$. (La parte fraccionaria de m es 0, por lo que la suma de las partes fraccionarias de x y m es igual a la parte fraccionaria de x, que es menor que 1). Resulta que puede utilizar la definición de la palabra para demostrar que esta ecuación es válida para todos los números reales x y para todos los enteros m.

Ejemplo 4.5.5 Demostración de la propiedad de piso

Demostrar que para todos los números reales x y para todos los enteros m, $\lfloor x + m \rfloor = \lfloor x \rfloor + m$.

Solución Comience suponiendo que x es un número real particular, pero elegido arbitrariamente y que m es un entero particular, pero elegido arbitrariamente. Debe demostrar que $\lfloor x + m \rfloor = \lfloor x \rfloor + m$. Ya que se trata de una ecuación que implica a $\lfloor x \rfloor$ y $\lfloor x + m \rfloor$, es razonable dar a una de estas cantidades un nombre: Sea $n = \lfloor x \rfloor$. Por definición de piso,

$$n \text{ es un número entero} \quad \text{y} \quad n \leq x < n + 1.$$

Esta desigualdad doble le permite calcular el valor de $\lfloor x + m \rfloor$ en términos de n al sumar m a ambos lados:

$$n + m \leq x + m < n + m + 1.$$

Así, el lado izquierdo de la ecuación que se muestra es

$$\lfloor x + m \rfloor = n + m.$$

Por otra parte, puesto que $n = \lfloor x \rfloor$, el lado derecho de la ecuación que se muestra es

$$\lfloor x \rfloor + m = n + m$$

también. Por tanto $\lfloor x + m \rfloor = \lfloor x \rfloor + m$. Este análisis se resume de la siguiente manera:

Teorema 4.5.1

Para todos los números reales x y todos los números enteros m, $\lfloor x + m \rfloor = \lfloor x \rfloor + m$.

Demostración:

Supongamos que se dan un número real x y un entero m. *[Debemos demostrar que* $\lfloor x + m \rfloor = \lfloor x \rfloor + m$*.]* Sea $n = \lfloor x \rfloor$. Por definición de piso, n es un entero y

$$n \leq x < n + 1.$$

Al sumar m a las tres partes se obtiene

$$n + m \leq x + m < n + m + 1.$$

[ya que la suma de un número a ambos lados de una desigualdad no cambia la dirección de la desigualdad].

Ahora $n + m$ es un número entero *[ya que n y m son números enteros y la suma de números enteros es un número entero]* y así, por definición de piso, el lado izquierdo de la ecuación que se muestra es

$$\lfloor x + m \rfloor = n + m.$$

Pero $n = \lfloor x \rfloor$. Por tanto, por sustitución,

$$n + m = \lfloor x \rfloor + m,$$

que está en el lado derecho de la ecuación que se muestra. Por tanto $\lfloor x + m \rfloor = \lfloor x \rfloor + m$ *[que era lo que se quería demostrar]*.

■

El análisis de una serie de algoritmos de computadora, tales como la búsqueda binaria y algoritmos de ordenamiento por mezcla, requiere que conozca el valor de $\lfloor n/2 \rfloor$, donde n es un entero. La fórmula para calcular este valor depende de si n es par o impar.

Teorema 4.5.2 El piso de $n/2$

Para cualquier entero n,

$$\left\lfloor \frac{n}{2} \right\rfloor = \begin{cases} \dfrac{n}{2} & \text{si } n \text{ es par} \\ \dfrac{n-1}{2} & \text{si } n \text{ es impar.} \end{cases}$$

Demostración:

Supongamos que n es un entero *[particular, pero elegido arbitrariamente]*. Por el teorema del cociente-residuo, ya sea n es impar o n es par.

Caso 1 (n es impar): En este caso, $n = 2k + 1$ para algún entero k. *[Debemos demostrar que* $\lfloor n/2 \rfloor = (n-1)/2$.*]* Pero el lado izquierdo de la ecuación que se muestra es

$$\left\lfloor \frac{n}{2} \right\rfloor = \left\lfloor \frac{2k+1}{2} \right\rfloor = \left\lfloor \frac{2k}{2} + \frac{1}{2} \right\rfloor = \left\lfloor k + \frac{1}{2} \right\rfloor = k$$

ya que k es un número entero y $k \leq k + 1/2 < k + 1$. Y el lado derecho de la ecuación que se muestra también es

$$\frac{n-1}{2} = \frac{(2k+1)-1}{2} = \frac{2k}{2} = k$$

así. Ya que tanto el lado izquierdo como el lado derecho de la igualdad son iguales a k, son iguales entre sí. Es decir, $\left\lfloor \dfrac{n}{2} \right\rfloor = \dfrac{n-1}{2}$ *[que era lo que se quería demostrar]*.

Caso 2 (n es par): En este caso, $n = 2k$ para algún entero k. *[Debemos demostrar que* $\lfloor n/2 \rfloor = n/2$.*]* El resto de la demostración de este caso se deja como ejercicio.

Dado cualquier número entero n y un entero positivo d, el teorema del cociente-residuo garantiza la existencia de números enteros únicos q y r tales que

$$n = dq + r \quad \text{y} \quad 0 \leq r < d.$$

El siguiente teorema establece que la notación de piso se puede utilizar para describir a q y a r de la siguiente manera:

$$q = \left\lfloor \frac{n}{d} \right\rfloor \quad \text{y} \quad r = n - d\left\lfloor \frac{n}{d} \right\rfloor.$$

Así si, en una calculadora o en un lenguaje de programación, el piso está preconstruido como *div* y *mod*, pero no son, se pueden definir a *div* y *mod* de la siguiente manera: para un entero no negativo n y un entero positivo d,

$$n \; div \; d = \left\lfloor \frac{n}{d} \right\rfloor \quad \text{y} \quad n \; mod \; d = n - d\left\lfloor \frac{n}{d} \right\rfloor. \tag{4.5.1}$$

Observe que d divide a n si y sólo si, $n \; mod \; d = 0$, o, en otras palabras, $n = d \lfloor n/d \rfloor$. Se le pide que lo demuestre en el ejercicio 13.

Teorema 4.5.3

Si n es un entero y d es un entero positivo y si $q = \lfloor n/d \rfloor$ y $r = n - d\lfloor n/d \rfloor$, entonces

$$n = dq + r \quad \text{y} \quad 0 \leq r < d.$$

Demostración:

Supongamos que n es cualquier número entero, d es un entero positivo, $q = \lfloor n/d \rfloor$ y $r = n - d\lfloor n/d \rfloor$. *[Debemos demostrar que $n = dq + r$ y $0 \leq r < d$.]* Sustituyendo,

$$dq + r = d\left\lfloor \frac{n}{d} \right\rfloor + \left(n - d\left\lfloor \frac{n}{d} \right\rfloor\right) = n.$$

Por tanto, sólo queda demostrar que $0 \leq r < d$. Pero $q = \lfloor n/d \rfloor$. Por tanto, por definición de piso,

$$q \leq \frac{n}{d} < q + 1.$$

Entonces,

$$dq \leq n < dq + d \qquad \text{multiplicando todas las partes por } d$$

y así

$$0 \leq n - dq < d \qquad \text{restando } dq \text{ de todas las partes}$$

Pero,

$$r = n - d\left\lfloor \frac{n}{d} \right\rfloor = n - dq.$$

Por tanto

$$0 \leq r < d \qquad \text{por sustitución.}$$

[Esto es lo que se quería demostrar.]

Ejemplo 4.5.6 Cálculo de *div* y *mod*

Utilice la notación de piso para calcular 3 850 *div* 17 y 3 850 *mod* 17.

Solución Por la fórmula (4.5.1),

$$\begin{aligned} 3\,850 \,div\, 17 &= \lfloor 3\,850)\,17 \rfloor = \lfloor 226(4705882\ldots \rfloor = 226 \\ 3\,850 \,mod\, 17 &= 3\,850 - 17 \cdot \lfloor 3\,850)\,17 \rfloor \\ &= 3\,850 - 17 \cdot 226 \\ &= 3\,850 - 3\,842 = 8. \end{aligned}$$

Autoexamen

1. Dado cualquier número real x, el piso de x es el único número entero n tal que ____.
2. Dado cualquier número real x, el techo de x es el único entero n tal que ____.

Conjunto de ejercicios 4.5

Calcule $\lfloor x \rfloor$ y $\lceil x \rceil$ para cada uno de los valores de x en

1. 37.999 2. 17/4

3. −14.00001 4. −32/5

5. Use la palabra piso para expresar la notación 259 *div* 11 y 259 *mod* 11.

6. Si k es un entero, ¿qué es $\lceil k \rceil$? ¿Por qué?

7. Si k es un entero, ¿qué es $\lceil k + \frac{1}{2} \rceil$? ¿Por qué?

8. Se necesitan siete libras de materia prima para fabricar cada unidad de un determinado producto. Exprese el número de unidades que pueden producidos de n libras materia prima utilizando la notación de piso o techo. ¿Cuál notación es más apropiada?

9. Se utilizan cajas, cada una con capacidad de 36 unidades, para enviar un producto del fabricante al mayorista. Exprese el número de cajas que se deben enviar n unidades del producto utilizando la notación de piso o techo. ¿Cuál notación es más apropiada?

10. Si 0 = domingo, 1 = lunes, 2 = martes, . . . , 6 = sábado, entonces el 1 de enero del año n ocurre en el día de la semana dado por la siguiente fórmula:

$$\left(n + \left\lfloor \frac{n-1}{4} \right\rfloor - \left\lfloor \frac{n-1}{100} \right\rfloor + \left\lfloor \frac{n-1}{400} \right\rfloor\right) \textit{mod } 7.$$

a. Utilice esta fórmula para encontrar el 1 de enero de
i. 2050 ii. 2100 iii. el año de su nacimiento.

H **b.** Interprete los diferentes componentes de esta fórmula.

11. Establezca una condición necesaria y suficiente para que el piso de un número real sea igual a este número.

12. Demuestre que si n es un entero par, entonces $\lfloor n/2 \rfloor = n/2$.

13. Supongamos que n y d son números enteros y $d \neq 0$. Demuestre cada uno de los siguientes enunciados.
a. Si $d \mid n$, entonces $n = \lfloor n/d \rfloor \cdot d$.
b. Si $n = \lfloor n/d \rfloor \cdot d$ entonces $d \mid n$.
c. Utilice la notación de piso para establecer una condición necesaria y suficiente para que un entero n sea ser divisible por un número entero d.

Algunos de los enunciados de los ejercicios 14 a 22 son verdaderos y algunos son falsos. Demuestre cada enunciado verdadero y encuentre un contraejemplo para cada enunciado falso, pero no use el teorema 4.5.1. en sus demostraciones.

14. Para todos los números reales x y y, $\lfloor x - y \rfloor = \lfloor x \rfloor - \lfloor y \rfloor$.

15. Para todos los números reales x, $\lfloor x - 1 \rfloor = \lfloor x \rfloor - 1$.

16. Para todos los números reales x, $\lfloor x^2 \rfloor = \lfloor x \rfloor^2$.

H **17.** Para todos los enteros n,

$$\lfloor n/3 \rfloor = \begin{cases} n/3 & \text{si } n \textit{ mod } 3 = 0 \\ (n-1)/3 & \text{si } n \textit{ mod } 3 = 1 \\ (n-2)/3 & \text{si } n \textit{ mod } 3 = 2 \end{cases}.$$

H **18.** Para todos los números reales x y y, $\lceil x + y \rceil = \lceil x \rceil + \lceil y \rceil$.

H **19.** Para todos los números reales x, $\lceil x - 1 \rceil = \lceil x \rceil - 1$.

20. Para todos los números reales x y y, $\lceil xy \rceil = \lceil x \rceil \cdot \lceil y \rceil$.

21. Para todos los enteros impares n, $\lceil n/2 \rceil = (n+1)/2$.

22. Para todos los números reales x y y, $\lceil xy \rceil = \lceil x \rceil \cdot \lfloor y \rfloor$.

Demuestre cada uno de los enunciados en los ejercicios 23 al 29.

23. Para cualquier número real x, si x no es un número entero, entonces $\lfloor x \rfloor + \lfloor -x \rfloor = -1$.

24. Para cualquier entero m y cualquier número real x, si x no es un número entero, entonces $\lfloor x \rfloor + \lfloor m - x \rfloor = m - 1$.

H **25.** Para todos los números reales x, $\lfloor \lfloor x/2 \rfloor /2 \rfloor = \lfloor x/4 \rfloor$.

26. Para todos los números reales x, si $x - \lfloor x \rfloor < 1/2$ entonces $\lfloor 2x \rfloor = 2\lfloor x \rfloor$.

27. Para todos los números reales x, si $x - \lfloor x \rfloor \geq 1/2$ entonces $\lfloor 2x \rfloor = 2\lfloor x \rfloor + 1$.

28. Para cualquier entero impar n,

$$\left\lfloor \frac{n^2}{4} \right\rfloor = \left(\frac{n-1}{2}\right)\left(\frac{n+1}{2}\right).$$

29. Para cualquier entero impar n,

$$\left\lceil \frac{n^2}{4} \right\rceil = \frac{n^2+3}{4}.$$

30. Encuentre el error en la siguiente "demostración" de que $\lfloor n/2 \rfloor = (n-1)/2$ si n es un entero impar.

"**Demostración:** Supongamos que n es un entero impar. Entonces $n = 2k + 1$ para algún entero k. Por tanto,

$$\left\lfloor \frac{2k+1}{2} \right\rfloor = \frac{(2k+1)-1}{2} = \frac{2k}{2} = k.$$

Pero $n = 2k + 1$. Resolviendo para k se obtiene $k = (n-1)/2$. Por tanto, por sustitución, $\lfloor n/2 \rfloor = (n-1)/2$".

Respuestas del autoexamen

1. $n \leq x < n + 1$ 2. $n - 1 < x \leq n$

4.6 Argumento indirecto: contradicción y contraposición

La reducción al absurdo es una de las mejores armas de un matemático. Es una táctica mucho más fina que cualquier jugada de ajedrez: un jugador de ajedrez puede ofrecer el sacrificio de un peón o incluso de una pieza, pero el matemático ofrece el juego. —G. H. Hardy, 1877-1947

Una demostración directa comienza con la hipótesis de un enunciado y hace una deducción tras otra hasta llegar a la conclusión. Las demostraciones indirectas no siguen un camino definido. Un tipo de demostración indirecta, el *argumento por contradicción*, se basa en el hecho de que un enunciado es verdadero o falso, pero no ambos. Así que si puede demostrar que la suposición de un enunciado dado no es verdadera le conduce lógicamente a una contradicción, imposibilidad o absurdo, entonces esa suposición debe ser falsa y, por tanto, el enunciado dado debe ser verdadero. Este método de demostración también se conoce como *reducción al absurdo* o *reducción a un imposible* porque se basa en la reducción de una suposición dada a una imposibilidad o un absurdo.

El argumento por contradicción se produce en muchos entornos diferentes. Por ejemplo, si un hombre que es acusado de haber asaltado un banco puede demostrar que él estaba en otro lugar en el momento en que se cometió el delito, sin duda será absuelto. La lógica de su defensa es la siguiente:

> Supongamos que yo cometí el delito. Entonces en el momento del delito, tendría que haber estado en la escena del delito. De hecho, en el momento del delito estaba en una reunión con 20 personas lejos de la escena del delito, como lo testificarán. Esto contradice la suposición de que he cometido el delito, ya que es imposible estar en dos lugares al mismo tiempo. Por tanto esa suposición es falsa.

Otro ejemplo se produce en el análisis. Una de las técnicas de análisis, es decir, "Supongamos por un momento que lo que dice mi oponente es correcto". Partiendo de esta suposición, el polemista entonces deduce un enunciado tras otro hasta llegar finalmente a un enunciado que es totalmente ridículo e inaceptable para el público. De esta manera el polemista muestra que el enunciado del oponente es falso.

El punto de partida para una demostración por reducción al absurdo es la suposición de que el enunciado a demostrar es falso. El objetivo es razonar a una contradicción. Por tanto la demostración por contradicción sigue el siguiente esquema:

Método de la demostración por contradicción

1. Supongamos que el enunciado a demostrar es falso. Es decir, supongamos que la negación del enunciado es verdadera.
2. Demuestre que esta suposición conduce lógicamente a una contradicción.
3. Concluya que el enunciado a demostrar es verdadero.

Nota ¡Tenga mucho cuidado al escribir la negación!

No hay reglas claras sobre cuándo hacer una demostración directa y cuándo hacer una demostración por reducción al absurdo, pero hay algunos lineamientos generales. La demostración por contradicción se indica si queremos demostrar que no hay un objeto con cierta propiedad, o si se quiere demostrar que un determinado objeto no tiene determinada propiedad. Los dos ejemplos siguientes muestran estos casos.

Ejemplo 4.6.1 No hay un entero mayor

Utilice la demostración por contradicción para mostrar que no hay un entero mayor.

Solución La mayoría de los niños pequeños creen que hay un número mayor que todos que con frecuencia llaman "trillón". Pero con la edad y la experiencia, cambia su creencia. En algún momento se dan cuenta de que si hubiera un número entero mayor, se podría sumar 1 a él y obtener un entero que fuera aún mayor. Dado que es una contradicción, no puede existir un entero mayor. Esta línea de razonamiento es el corazón de la demostración formal.

Para la demostración, de "cierta propiedad" es la propiedad de ser el mayor entero. Para demostrar que no hay ningún objeto con esta propiedad, se comienza por suponer la negación: que hay un objeto con la propiedad.

Punto de partida: Supongamos que no. Supongamos que hay un número entero mayor; lo llamamos N.

Esto significa que $N \geq n$ para todo entero n.

Para demostrar: Esta suposición conduce lógicamente a una contradicción.

Teorema 4.6.1

No hay mayor entero.

Demostración:

[Tomamos la negación del teorema y supongamos que es verdad.] Supongamos que no. Es decir, supongamos que hay un mayor número entero N. *[Debemos deducir una contradicción.]* Entonces $N \geq n$ para todo entero n. Sea $M = N + 1$. Ahora M es un número entero, ya que es una suma de números enteros. También $M > N$ ya que $M = N + 1$. Por tanto M es un número entero que es mayor que N. Así N es el mayor entero y N no es el mayor entero, lo que es una contradicción. *[Esta contradicción muestra que la suposición es falsa y, por tanto, que el teorema es verdadero.]*

■

Después de que se ha obtenido una contradicción, la lógica del argumento siempre es la misma: "Esto es una contradicción. Por tanto la suposición es falsa y el teorema es verdadero". Por esta razón, la mayoría de los libros de matemáticas finalizan las demostraciones por contradicción en el punto en que se ha llegado a la contradicción.

La contradicción en el siguiente ejemplo se basa en el hecho de que $1/2$ no es un número entero.

Ejemplo 4.6.2 No hay enteros que puedan ser pares e impares

El hecho de que un entero pueda ser a la vez par e impar se deduce de la parte de unicidad del teorema del cociente-residuo. Una demostración completa de esta parte del teorema se describe en el ejercicio 18 de la sección 4.7. Este ejemplo muestra cómo utilizar la demostración por contradicción para demostrar un caso concreto.

Teorema 4.6.2

No hay un número entero que sea a la vez par e impar.

Demostración:

[Tomamos la negación del teorema y supongamos que es verdad.] Supongamos que no. Es decir, supongamos que hay por lo menos un entero n que es a la vez par e impar. *[Debemos deducir una contradicción.]* Por definición de par, $n = 2a$ para algún entero a y por definición de impar $n = 2b + 1$ para algún entero b. En consecuencia,

$$2a = 2b + 1 \qquad \text{igualando las dos expresiones para } n$$

continúa en la página 200

y así

$$\begin{aligned} 2a - 2b &= 1 \\ 2(a - b) &= 1 \\ a - b &= 1/2 \quad \text{por el álgebra.} \end{aligned}$$

Ahora bien, como a y b son números enteros, la diferencia $a - b$ también debe ser un entero. Pero $a - b = 1/2$ y $1/2$ no es un número entero. Así, $a - b$ es un entero y $a - b$ no es un número entero, que es una contradicción. *[Se muestra por contradicción que la suposición es falsa y, por tanto, el teorema es verdadero.]*

■

En el ejemplo siguiente se le pide demostrar que la suma de cualquier número racional y de un número irracional es irracional. Una manera de pensar en esto es en términos de un determinado objeto (la suma de un racional y de un irracional) que no tiene una determinada propiedad (la propiedad de ser racional). Esto sugiere intentar una demostración por contradicción: supongamos que el objeto tiene la propiedad y se deduce una contradicción.

Ejemplo 4.6.3 La suma de un número racional y un número irracional

Utilice la demostración por contradicción para mostrar que la suma de cualquier número racional y de un número irracional es irracional.

Solución Comience por suponer la negación de lo que desea probar. Tenga mucho cuidado al escribir lo que esto significa. Si toma la negación en forma incorrecta, todo el resto de la demostración será erróneo. En este ejemplo, el enunciado por demostrar se puede escribir formalmente como

$$\begin{aligned} &\forall \text{ números reales } s \text{ y } r, \text{ si } r \text{ es racional y} \\ &s \text{ es irracional, entonces } r + s \text{ es irracional.} \end{aligned}$$

A partir de éste se puede ver que la negación es

$$\begin{aligned} &\exists \text{ un número racional } r \text{ y un número} \\ &\text{irracional } s \text{ tal que } r + s \text{ es racional.} \end{aligned}$$

¡Precaución! La negación de "La suma de cualquier número irracional y cualquier número racional es irracional" NO es "La suma de cualquier número irracional y cualquier número racional es racional".

De lo que se deduce que el punto de partida y lo que se demostrará son como sigue:

Punto de partida: Supongamos que no. Es decir, supongamos que hay un número r racional y un número irracional s tal que $r + s$ es racional.

Para demostrar: Esta suposición conduce a una contradicción.

Para deducir una contradicción, es necesario entender lo que está suponiendo: que hay números r y s tal que r es racional, s es irracional y $r + s$ es racional. Por definición de racional e irracional, esto significa que s no se puede escribir como un cociente de dos números enteros, pero que r y $r + s$ pueden:

$$r = \frac{a}{b} \quad \text{para algunos enteros } a \text{ y } b \text{ con } b \neq 0 \text{ y} \qquad 4.6.1$$

$$r + s = \frac{c}{d} \quad \text{para algunos enteros } c \text{ y } d \text{ con } d \neq 0. \qquad 4.6.2$$

Si sustituimos (4.6.1) en (4.6.2), se obtiene

$$\frac{a}{b} + s = \frac{c}{d}.$$

Restando a/b de ambos lados se obtiene

$$\begin{aligned} s &= \frac{c}{d} - \frac{a}{b} \\ &= \frac{bc}{bd} - \frac{ad}{bd} && \text{reescribiendo } c/d \text{ y } a/b \text{ como fracciones equivalentes} \\ &= \frac{bc - ad}{bd} && \text{por la regla de resta de fracciones con el mismo denominador.} \end{aligned}$$

Pero tanto $bc - ad$ como bd son enteros porque los productos y las diferencias de los números enteros son números enteros y $bd \neq 0$ por la propiedad del producto cero. Por tanto s se puede expresar como el cociente de dos números enteros con un denominador distinto de cero, por lo que s es racional, lo que contradice la suposición de que es irracional.

Este análisis se resume en una demostración formal.

Teorema 4.6.3

La suma de cualquier número racional y un número irracional es irracional.

Demostración:

[Tomamos la negación del teorema y supongamos que es verdad.] Supongamos que no. Es decir, suponemos que hay un número racional r y un número irracional s tal que $r + s$ es racional. *[Debemos deducir una contradicción.]* Por definición de racional, $r = a/b$ y $r + s = c/d$ para algunos enteros a, b, c y d con $b \neq 0$ y $d \neq 0$. Por sustitución,

$$\frac{a}{b} + s = \frac{c}{d},$$

y así

$$\begin{aligned} s &= \frac{c}{d} - \frac{a}{b} && \text{restando } a/b \text{ de ambos lados} \\ &= \frac{bc - ad}{bd} && \text{por las leyes del álgebra.} \end{aligned}$$

Ahora $bc - ad$ y bd son números enteros *[ya que a, b, c y d son números enteros y ya que los productos y las diferencias de los números enteros son números enteros]* y $bd \neq 0$ *[por la propiedad del producto cero]*. Por tanto s es un cociente de los dos números enteros $bc - ad$ y bd con $bd \neq 0$. Así, por definición de racional, s es racional, lo cual contradice la suposición de que s es irracional. *[Por tanto la suposición es falsa y el teorema es verdadero.]*

■

Argumentos por contraposición

Una segunda forma de argumentación indirecta, *argumento por contraposición*, se basa en la equivalencia lógica entre un enunciado y su contrapositivo. Para probar un enunciado por contraposición, se toma el contrapositivo del enunciado, se demuestra el contrapositivo en una

demostración directa y se concluye que el enunciado original es verdadero. El razonamiento subyacente es que, dado que un enunciado condicional es lógicamente equivalente a su contrapositivo, si el contrapositivo es verdadero, entonces el enunciado también debe ser verdadero.

Método de demostración por contraposición

1. Exprese el enunciado a demostrar en la forma

   $$\forall x \text{ en } D, \text{ si } P(x), \text{ entonces } Q(x).$$

   (Este paso se puede hacer mentalmente.)
2. Reescriba este enunciado en forma contrapositiva

   $$\forall x \text{ en } D, \text{ si } Q(x) \text{ es falso, entonces } P(x) \text{ es falso.}$$

   (Este paso también se puede hacer mentalmente.)
3. Demuestre el enunciado contrapositivo con una demostración directa,
   a. Supongamos que x es un elemento (particular, pero elegido arbitrariamente) de D tal que $Q(x)$ es falso.
   b. Demuestre que $P(x)$ es falso.

Ejemplo 4.6.4 Si el cuadrado de un número entero es par, entonces el entero es par

Demuestre que para todo entero n, si n^2 es par entonces n es par.

Solución Primero forma que el contrapositivo del enunciado a ser probado.

Contrapositivo: Para todo entero n, si n no es par entonces n^2 no es par.

Por el teorema del cociente-residuo con $d = 2$, cualquier número entero es par o impar, por lo que cualquier número entero que no es par es impar. También por el teorema 4.6.2, ningún entero puede ser a la vez par e impar. Así que si un número entero es impar, entonces no es par. Así, el contrapositivo se puede replantear de la siguiente manera:

Contrapositivo: Para todos los enteros n, si n es impar, entonces n^2 es impar.

Un cálculo sencillo es el corazón de una demostración directa de este enunciado, como se muestra a continuación.

Proposición 4.6.4

Para todos los enteros n, si n^2 es par entonces n es par.

Demostración (por contraposición):

Supongamos que n es un entero impar. *[Debemos demostrar que n^2 es impar.]* Por definición de impar, $n = 2k + 1$ para algún entero k. Por sustitución y álgebra,

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$$

Pero $2k^2 + 2k$ es un número entero, porque los productos y las sumas de los números enteros son números enteros. Así $n^2 = 2 \cdot (\text{un entero}) + 1$ y por tanto, por definición, de impar, n^2 es impar *[que era lo que se quería demostrar]*.

Se utilizó la palabra *proposición* aquí en lugar de *teorema*, porque aunque la palabra *teorema* puede referirse a cualquier enunciado que se ha demostrado, los matemáticos con

frecuencia la limitan a enunciados especialmente importantes que tienen varias y diferentes consecuencias. Entonces ellos usan la palabra **proposición** para referirse a un enunciado de que es algo con menos consecuencias pero no obstante vale la pena escribir. Utilizaremos la proposición 4.6.4 en la sección 4.7 para demostrar que $\sqrt{2}$ es irracional. ■

Relación entre demostración por contradicción y demostración por contraposición

Observe que cualquier demostración por contraposición puede remodelar el lenguaje de la demostración por contradicción. En una demostración por contraposición, el enunciado

$$\forall x \text{ en } D, \text{ si } P(x) \text{ entonces, } Q(x)$$

se demuestra al dar una demostración directa del enunciado equivalente

$$\forall x \text{ en } D, \text{ si } \sim Q(x) \text{ entonces, } \sim P(x)$$

Para hacer esto, supongamos que se le da un elemento arbitrario x de D tal que $\sim Q(x)$. Entonces demuestre que $\sim P(x)$. Esto se ilustra en la figura 4.6.1.

Figura 4.6.1 Demostración por contraposición

Exactamente se puede utilizar la misma secuencia de pasos como el corazón de una demostración por contradicción para el enunciado dado. Lo único que cambia es el contexto en el que están escritos los pasos.

Para reescribir la demostración como una demostración por contradicción, supongamos que hay una x en D tal que $P(x)$ y $\sim Q(x)$. Después siga los pasos de la demostración por contraposición para deducir el enunciado $\sim P(x)$. Pero $\sim P(x)$ es una contradicción a la suposición de que $P(x)$ y $\sim Q(x)$. (Ya que para contradecir una conjunción de dos enunciados, sólo es necesario contradecir uno de ellos.) En la figura 4.6.2, se muestra este proceso.

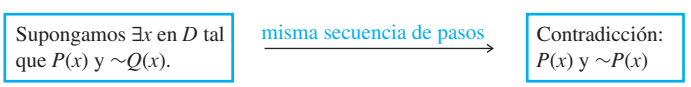


Figura 4.6.2 Demostración por contradicción

Como ejemplo, se presenta una demostración por contradicción de la proposición 4.6.4, es decir, que para cualquier número entero n, si n^2 es par entonces n es par.

Proposición 4.6.4

Para todos los enteros n, si n^2 es par entonces n es par.

Demostración (por contradicción):

[Tomamos la negación del teorema y supongamos que es verdadera.] Supongamos que no. Es decir, supongamos que existe un entero n tal que n^2 es par y n no es par. *[Debemos deducir una contradicción.]* Por el teorema del cociente-residuo con $d = 2$, cualquier número entero es par o impar. Por tanto, ya que n no es par es impar y

continúa en la página 204

por tanto, por definición de impar, $n = 2k + 1$ para algún entero k. Por sustitución y álgebra:

$$n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1.$$

Pero $2k^2 + 2k$ es un número entero, porque los productos y las sumas de números enteros son números enteros. Así $n^2 = 2 \cdot$ (un entero) $+ 1$ y por tanto, por definición de impar, n^2 es impar. Por tanto, n^2 es a la vez par e impar. Esto contradice el teorema 4.6.2, que establece que ningún entero puede ser a la vez par e impar. *[Esta contradicción muestra que la suposición es falsa y, por tanto, que la proposición es verdadera.]*

Observe que cuando se utiliza la demostración por contraposición, sabe exactamente qué conclusión deberá demostrar, a saber, la negación de la hipótesis; mientras que en la demostración de contradicción, puede ser difícil saber qué contradicción debe plantear. Por otro lado, cuando se utiliza la demostración por contradicción, una vez que se ha deducido cualquier contradicción, ya está hecho. La principal ventaja de la contraposición más que de la contradicción es que se evita tener que tomar (posiblemente incorrectamente) la negación de un enunciado complicado. La desventaja de la contraposición con respecto a la contradicción es que puede utilizar la contraposición sólo para una clase específica de enunciados que son universales y condicionales. El análisis anterior muestra que cualquier enunciado que se pueda demostrar por contraposición se puede demostrar por contradicción. Pero el converso no es verdadero. Enunciados tales como "$\sqrt{2}$ es irracional" (que se examinan en la sección siguiente) se puede demostrar por contradicción, pero no por contraposición.

La demostración como herramienta para resolver problemas

La demostración directa, refutación por contraejemplo, la demostración por contradicción y la demostración por contraposición son todas herramientas que pueden utilizarse para ayudar a determinar si los enunciados son verdaderos o falsos. Dado un enunciado de la forma

Para todos los elementos en un dominio, si (hipótesis), entonces (conclusión),

imagine elementos en el dominio que satisfacen la hipótesis. Pregúntese: ¿Deben satisfacer la conclusión? Si usted puede ver que la respuesta es "sí" en todos los casos, el enunciado es verdadero y su conocimiento será la base para una demostración directa. Si después de pensar no es claro que la respuesta es "sí", se pregunta si hay elementos del dominio que satisfacen las hipótesis y *no* la conclusión. Si tienen éxito en la búsqueda de algunos, entonces el enunciado es falso y tiene un contraejemplo. Por otra parte, si no tienen éxito en determinar dichos elementos, tal vez no existan. Quizá puede demostrar que suponer la existencia de elementos en el dominio que satisfacen la hipótesis y la conclusión no conduce lógicamente a una contradicción. Si es así, entonces el enunciado es verdadero y usted tiene la base para una demostración por contradicción. Alternativamente, usted podría imaginarse elementos del dominio para los que la conclusión es falsa y se preguntan si tales elementos tampoco cumplen la hipótesis. Si la respuesta en todos los casos es "sí", entonces tiene una base para una demostración por contraposición.

La solución de problemas, especialmente de problemas difíciles, no suele ser un proceso sencillo. En cualquier etapa si sigue las recomendaciones anteriores, es posible que desee probar de nuevo el método de una etapa anterior. Si, por ejemplo, usted no puede encontrar un contraejemplo para un cierto enunciado, su experiencia en tratar de encontrar le podría ayudar a decidir volver a intentar un argumento directo y más que tratar con un indirecto. Los psicólogos que han estudiado la resolución de problemas han encontrado que los solucionadores de problemas de mayor éxito son aquellos que son flexibles y que están dispuestos

a usar una variedad de métodos, sin quedarse atorados en uno de ellos por mucho tiempo. Los matemáticos trabajan a veces durante meses (o más) con los problemas difíciles. No se desanime si algunos problemas en este libro le toman un buen tiempo para resolverlos.

Aprender las habilidades de comprobación y refutación es muy parecido a aprender otras habilidades, como las utilizadas en la natación, el tenis o para tocar un instrumento musical. Cuando empieza, puede sentirse confundido por todas las reglas y no puede confiar en intentar cosas nuevas. Pero con la práctica se interiorizan las reglas y se pueden usar en conjunción con otras potencialidades de equilibrio, coordinación, juicio estético de los sentidos para concentrarse en ganar un encuentro, ganando un partido o tocando un concierto con éxito.

Ahora que ha trabajado en las cinco primeras secciones de este capítulo, retome la idea de que, sobre todo, una demostración o refutación debe ser un argumento convincente. Necesita conocer cómo se estructuran las demostraciones directas e indirectas y contraejemplos. Sin embargo, para utilizar este conocimiento con eficacia, lo debe utilizar en conjunción con sus potencialidades de imaginación, intuición y sobre todo de sentido común.

Autoexamen

1. Para demostrar un enunciado por contradicción, suponga que _____ y demuestre que _____.
2. Una demostración por contraposición de un enunciado de la forma "$\forall x \in D$, si $P(x)$, entonces $Q(x)$" es una demostración directa de _____.
3. Para demostrar que un enunciado de la forma "$\forall x \in D$, si $P(x)$, entonces $Q(x)$" por contraposición, suponga que _____ y demuestre que _____.

Conjunto de ejercicios 4.6

1. Complete los espacios en blanco en la siguiente demostración por contradicción que no existe un número real positivo menor.

Demostración: Supongamos que no. Es decir, supongamos que hay al menos un número real positivo x. *[Debemos deducir* __(a)__ *.]* Considere el número $x/2$. Puesto que x es un número real positivo, $x/2$ también es __(b)__. Además, podemos deducir que $x/2 < x$ multiplicando ambos lados de la desigualdad $1 < 2$ por __(c)__ y dividiendo entre __(d)__. Por tanto $x/2$ es un número real positivo que es menor que el menor número real positivo. Esto es una __(e)__. *[Así, la suposición es falsa, por lo que no existe ningún número real positivo menor.]*

2. ¿Es $\dfrac{1}{0}$ un número irracional? Explique.

3. Utilice la demostración por contradicción para mostrar que para todo entero n, $3n + 2$ no es divisible entre 3.

4. Utilice la demostración por contradicción para mostrar que para todo entero m, $7m + 4$ no es divisible entre 7.

Con cuidado, formule negaciones de cada uno de los enunciados en los ejercicios del 5 al 7. Después, demuestre cada enunciado por contradicción.

5. No existe un entero par mayor.

6. No hay número real no negativo mayor.

7. No Hay un ningún número racional positivo menor.

8. Complete los espacios en blanco para la siguiente demostración de que la diferencia de cualquier número racional y de un número irracional es irracional.

Demostración: Supongamos que no. Es decir, supongamos que existen __(a)__ x y __(b)__ y tal que $x - y$ es racional. Por definición de racional, existen números enteros a, b, c, d con $b \neq 0$ y $d \neq 0$ tal que $x =$ __(c)__ y $x - y =$ __(d)__. Sustituyendo

$$\frac{a}{b} - y = \frac{c}{d}$$

Sumando y restando $\dfrac{c}{d}$ en ambos lados se obtiene

$$\begin{aligned} y &= \text{(e)} \\ &= \frac{ad}{bd} - \frac{bc}{bd} \\ &= \frac{ad - bc}{bd} \qquad \text{por álgebra.} \end{aligned}$$

Ahora, tanto $ad - bc$ como bd son enteros porque los productos y las diferencias de __(f)__ son __(g)__. Y $bd \neq 0$ por el __(h)__: Por tanto y es un cociente de números enteros con un denominador distinto de cero y por tanto y es __(i)__, por definición, de racional. Por tanto, se tiene tanto que y es irracional como que y es racional, que es una contradicción. *[Así, la suposición es falsa y el enunciado a demostrar es verdadero.]*

9. **a.** Cuando se le pidió demostrar que la diferencia de cualquier número irracional y cualquier número racional es irracional, un estudiante empezó, "Supongamos que no. Es decir, supongamos que la diferencia de cualquier número irracional y cualquier número racional es racional". ¿Qué está mal en comenzar la prueba de esta manera? (*Sugerencia:* Revise la respuesta del ejercicio 11 en la sección 3.2.)
   b. Demuestre que la diferencia de cualquier número irracional y cualquier número racional es irracional.

Demuestre cada enunciado de los ejercicios 10 al 17 por contradicción.

10. La raíz cuadrada de un número irracional es irracional.

11. El producto de cualquier número racional distinto de cero y cualquier número irracional es irracional.

12. Si a y b son números racionales, $b \neq 0$ y r es un número irracional, entonces $a + br$ es irracional.

H 13. Para cualquier entero n, $n^2 - 2$ no es divisible por 4.

H 14. Para todos los números primos a, b y c, $a^2 + b^2 \neq c^2$.

H 15. Si a, b y c son números enteros y $a^2 + b^2 = c^2$, al menos uno de a y b es par.

H ∗ 16. Para todos los enteros impares a, b y c, si z es una solución de $ax^2 + bx + c = 0$ entonces z es irracional. (En la demostración, utilice las propiedades de los números enteros pares e impares que se enumeran en el ejemplo 4.2.3.)

17. Para todos los números enteros a, si $a \bmod 6 = 3$, entonces $a \bmod 3 \neq 2$.

18. Complete los espacios en blanco en la siguiente demostración por contraposición de que para todo entero n, si $5 \nmid n^2$ entonces $5 \nmid n$.

Demostración (por contraposición): *[El contrapositivo es: Para todos los enteros n, si 5 | n entonces 5 | n^2.]* Supongamos que n es cualquier entero tal que __(a)__. *[Debemos demostrar que* __(b)__*.]* Por definición de divisibilidad, $n =$ __(c)__ para algún entero k. Sustituyendo, $n^2 =$ __(d)__ $= 5(5k^2)$. Pero $5k^2$ es un número entero, ya que es un producto de enteros. Por tanto $n^2 = 5 \cdot$ (un entero) y así __(e)__ *[que era lo que se quería demostrar].*

Demuestre por contraposición los enunciados en los ejercicios 19 y 20.

19. Si un producto de dos números reales positivos es mayor que 100, entonces al menos uno de los números es mayor que 10.

20. Si la suma de dos números reales es menor de 50, al menos uno de los números es menor de 25.

21. Considere el enunciado de "Para todos los enteros n, si n^2 es impar, entonces n es impar".
   a. Escriba lo que supondría y lo que tendría que demostrar para probar que este enunciado es una contradicción.
   b. Escriba lo que supondría y lo que tendría que demostrar para probar este enunciado por contraposición.

22. Considere el enunciado "Para todos los números reales r, si r^2 es irracional entonces r es irracional."
   a. Escriba lo que supondría y lo que tendría que demostrar para probar que este enunciado es una contradicción.
   b. Escriba lo que supondría y lo que tendría que demostrar para probar este enunciado por contraposición.

Demuestre cada uno de los enunciados en los ejercicios del 23 al 29 en dos maneras: *a)* por contraposición y *b)* por contradicción.

23. El negativo de cualquier número irracional es irracional.

24. El recíproco de cualquier número irracional es irracional. (El **recíproco** de un número real x distinto de cero es $1/x$).

H 25. Para todos los enteros n, si n^2 es impar, entonces n es impar.

26. Para todos los números enteros a, b y c, si $a \nmid bc$ entonces $a \nmid b$. (Recuerde que el símbolo $\nmid$ significa "no divide").

H 27. Para todos los números enteros m y n, si $m + n$ es par entonces m y n son pares o m y n son impares.

28. Para todos los números enteros m y n, si mn es par entonces m es par o n es par.

29. Para todos los números enteros a, b y c, si $a \mid b$ y $a \nmid c$ entonces $a \nmid (b + c)$. (*Sugerencia:* Para demostrar $p \to q \vee r$, es suficiente demostrar ya sea $p \wedge \sim q \to r$ o $p \wedge \sim r \to q$. Vea el ejercicio 14 en la sección 2.2).

30. La siguiente "demostración" de que todo entero es racional es incorrecta. Encuentre el error.

"**Demostración (por contradicción):** Supongamos que no. Supongamos que cada entero es irracional. Entonces el entero 1 es irracional, pero $1 = 1/1$, que es racional. Esta es una contradicción. *[Por tanto la suposición es falsa y el teorema es verdadero.]*".

31. **a.** Demuestre por contraposición: Para todos los enteros positivos n, r y s, si $rs \leq n$, entonces $r \leq \sqrt{n}$ o $s \leq \sqrt{n}$.
   b. Demuestre: Para todos los enteros $n > 1$, si n no es primo, entonces existe un número primo p tal que $p \leq \sqrt{n}$ y n es divisible entre p. (*Sugerencias:* Utilice el resultado del inciso *a*), los teoremas 4.3.1, 4.3.3 y 4.3.4 y la propiedad transitiva de orden.)
   c. Establezca la contraposición de los resultados del inciso *b*). Los resultados del ejercicio 31 proporcionan una manera de demostrar si un número entero es primo.

Demostración de primalidad

Dado un entero $n > 1$, para demostrar si n es primo compruebe viendo si es divisible por un número primo menor o igual a su raíz cuadrada. Si no es divisible por cualquiera de estos números, entonces es primo.

32. Use la demostración de primalidad para determinar si los números siguientes son primos o no.
   a. 667 **b.** 557 c. 527 d. 613

33. La criba de Eratóstenes, en honor a su inventor, el sabio griego Eratóstenes (276-194 a.C.), proporciona una manera de encontrar todos los números primos menores o iguales a algún número fijo n. Para construirla, escriba todos los números enteros de 2 a n. Tache todos los múltiplos de 2, excepto el 2 mismo, después todos los múltiplos de 3, excepto el 3 mismo, después todos los múltiplos de 5, excepto el 5 mismo y así sucesivamente.

Continuar tachando los múltiplos de cada número primo sucesivo primos hasta $\sqrt{n}$. Los números que no están tachados son todos los números primos del 2 al n. A continuación presentamos una criba de Eratóstenes, que incluye los números del 2 al 27. Los múltiplos de 2 se cruzan con un /, los múltiplos de 3, con un \ y los múltiplos de 5 con una —.

2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13 ~~14~~
~~15~~ ~~16~~ 17 ~~18~~ 19 ~~20~~ 21 ~~22~~ 23 ~~24~~ ~~25~~ ~~26~~ ~~27~~

Use la criba de Eratóstenes para encontrar todos los números primos menores de 100.

34. Use la demostración de primalidad y el resultado del ejercicio 33 para determinar si los siguientes números son primos.
a. 9269 **b.** 9103 c. 8623 d. 7917

***H* ∗ 35.** Utilice la demostración por contradicción para demostrar que todo número entero superior a 11 es una suma de dos números compuestos.

Respuestas del autoexamen

1. el enunciado es falso, esta suposición conduce a una contradicción 2. el contrapositivo del enunciado, es decir, $\forall x \in D$, si $\sim Q(x)$ entonces $\sim Q(x)$ 3. x es cualquier elemento *[dado, pero elegido arbitrariamente]* de D para el que $Q(x)$ es falso, $P(x)$ es falso

4.7 Argumento indirecto: dos teoremas clásicos

Es indigno el nombre de un hombre que no sabe que la diagonal de un cuadrado es incomparable con su lado. —Platón (aproximadamente 428-347 a.C.)

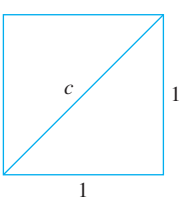
Esta sección tiene las demostraciones de dos de los teoremas más famosos de las matemáticas: que $\sqrt{2}$ es irracional y que hay un infinito de números primos. Ambas demostraciones son ejemplos de argumentos indirectos y eran bien conocidos desde hace más de 2000 años, pero siguen siendo modelos ejemplares de argumentación matemática hasta el día de hoy.

La irracionalidad de $\sqrt{2}$

Cuando las matemáticas florecieron en la época de los antiguos griegos, los matemáticos creyeron que dados dos segmentos de recta, por ejemplo, A: _____ y B: _____, a una cierta unidad de longitud se podía encontrar que el segmento A era exactamente de a unidades de largo y que el segmento era exactamente de b unidades de largo. (Se dice que los segmentos son *comparables* con respecto a esta unidad especial de longitud). Entonces el cociente de longitudes de A y B sería la misma proporción que la razón de los números enteros a y b. Simbólicamente:

$$\frac{\text{longitud } A}{\text{longitud } B} = \frac{a}{b}.$$

Ahora es fácil encontrar un segmento de recta de longitud $\sqrt{2}$, para medir la diagonal del cuadrado unitario:



Por el teorema de Pitágoras, $c^2 = 1^2 + 1^2 = 2$ y así $c = \sqrt{2}$. Si la creencia de los antiguos griegos fuera correcta, habría enteros a y b tal que

$$\frac{\text{longitud (diagonal)}}{\text{longitud (lado)}} = \frac{a}{b}.$$

Y esto implicaría que

$$\frac{c}{1} = \frac{\sqrt{2}}{1} = \sqrt{2} = \frac{a}{b}.$$

Pero entonces $\sqrt{2}$ sería un cociente de dos números enteros, o, en otras palabras, $\sqrt{2}$ sería racional.

En el siglo IV o V a.C., los seguidores del filósofo y matemático griego Pitágoras, descubrieron que $\sqrt{2}$ no es racional. Este descubrimiento fue muy molesto para ellos, por su profundidad, casi religiosa en el poder de los números enteros para describir los fenómenos.

Bettmann/CORBIS

Euclides (aproximadamente 300 a.C.)

La siguiente demostración de la irracionalidad de $\sqrt{2}$ era conocida por Aristóteles y es similar a la que en el libro décimo de los *Elementos de la geometría* de Euclides. El matemático griego Euclides es mejor conocido como un geómetra. De hecho, el conocimiento de la geometría en los primeros seis libros de sus *Elementos* ha sido considerada como una parte esencial de una educación liberal para más de 2000 años. Sin embargo, los libros del 7 al 10 de sus *Elementos*, contienen mucho de lo que ahora llamaríamos la teoría de los números.

La demostración comienza por suponer la negación: $\sqrt{2}$ es racional. Esto significa que existen enteros m y n tales que $\sqrt{2} = m/n$. Ahora bien, si m y n tienen factores comunes, estos pueden factorizarse para obtener una nueva fracción, igual a m/n, en la que el numerador y el denominador no tienen factores comunes. (Por ejemplo, $18/12 = (6 \cdot 3)/(6 \cdot 2) = 3/2$, que es una fracción cuyo numerador y el denominador no tienen factores comunes). Por tanto, sin pérdida de generalidad, podemos suponer que m y n no tenían factores comunes en el primer lugar. Después, se deducirá la contradicción de que m y n *tienen* un factor común de 2. El argumento hace uso de la Proposición 4.6.4. Si el cuadrado de un entero es par, entonces ese número entero es par.

Nota Estrictamente hablando se puede suponer que el hecho de que m y n no tengan factores comunes es una consecuencia del "principio del buen orden para los enteros" que se analiza en la sección 5.4.

Teorema 4.7.1 irracionalidad de $\sqrt{2}$

$\sqrt{2}$ es irracional.

Demostración:

[Tomamos la negación y suponemos que es verdad.] Supongamos que no. Es decir, supongamos que $\sqrt{2}$ es racional. Entonces existen números enteros m y n, sin factores comunes, que

$$\sqrt{2} = \frac{m}{n} \qquad 4.7.1$$

[Dividiendo m y n por los factores comunes si es necesario.] [Debemos deducir una contradicción.] Elevando al cuadrado ambos lados de la ecuación (4.7.1) se obtiene

$$2 = \frac{m^2}{n^2}.$$

O, equivalentemente,

$$m^2 = 2n^2. \qquad 4.7.2$$

Observe que la ecuación (4.7.2) implica que m^2 es par (por definición de par). De lo que se deduce que m es par (por la proposición 4.6.4). Archivamos este hecho para una futura referencia y también para deducir (por definición de par) que

$$m = 2k \quad \text{para algún entero } k. \qquad 4.7.3$$

Sustituyendo la ecuación (4.7.3) en la ecuación (4.7.2), vemos que

$$m^2 = (2k)^2 = 4k^2 = 2n^2.$$

Dividiendo ambos lados de la ecuación del extremo derecho entre 2 se obtiene

$$n^2 = 2k^2.$$

En consecuencia, n^2 es par, por lo que n es par (por la proposición 4.6.4). Pero también sabemos que m es par. *[Este es el hecho que habíamos archivado.]* Por tanto, tanto m y n tienen un factor común de 2. Pero esto contradice la suposición de que m y n no tienen factores comunes. *[Por tanto la suposición es falsa y así que el teorema es verdadero.]*

Ahora que ha visto la demostración de que $\sqrt{2}$ es irracional, puede utilizar la irracionalidad de $\sqrt{2}$ para obtener la irracionalidad de otros números reales.

Ejemplo 4.7.1 Irracionalidad de $1 + 3\sqrt{2}$

Demuestre por contradicción que $1 + 3\sqrt{2}$ es irracional.

Solución La esencia del argumento es la observación de que si $1 + 3\sqrt{2}$ puede ser escrito como un cociente de números enteros, entonces también podría $\sqrt{2}$. Pero por el teorema 4.7.1, sabemos que es imposible.

Proposición 4.7.2

$1 + 3\sqrt{2}$ es irracional.

Demostración:

Supongamos que no. Supongamos que $1 + 3\sqrt{2}$ es racional. *[Debemos deducir una contradicción.]* Entonces, por definición de racional,

$$1 + 3\sqrt{2} = \frac{a}{b} \qquad \text{para algunos enteros } a \text{ y } b \text{ con } b \neq 0.$$

De lo que se deduce

$$\begin{aligned} 3\sqrt{2} &= \frac{a}{b} - 1 && \text{estando 1 a ambos lados} \\ &= \frac{a}{b} - \frac{b}{b} && \text{por sustitución} \\ &= \frac{a-b}{b} && \text{por la regla restar de fracciones con un denominador común.} \end{aligned}$$

Por tanto

$$\sqrt{2} = \frac{a-b}{3b} \qquad \text{dividiendo ambos lados entre 3.}$$

Pero $a - b$ y $3b$ son números enteros (ya que a y b son números enteros y las diferencias y los productos de los números enteros son números enteros) y $3b \neq 0$ por la propiedad del producto cero. Por tanto, $\sqrt{2}$ es un cociente de los dos números enteros $a - b$ y $3b$ con $3b \neq 0$, por lo que $\sqrt{2}$ es racional (por definición de racional). Esto contradice el hecho de que $\sqrt{2}$ es irracional. *[Esta contradicción muestra que la suposición es falsa.]* Por tanto $1 + 3\sqrt{2}$ es irracional.

■

¿Hay un infinito de números primos?

Usted sabe que un número primo es un entero positivo que no se puede factorizar como producto de dos números enteros positivos menores. ¿Es el conjunto de tales números infinito o hay un mayor número primo? La respuesta era conocida por Euclides y una demostración de que el conjunto de todos los números primos es infinito aparece en el libro 9 de sus *Elementos de Geometría*.

La demostración de Euclides requiere un hecho adicional que aún no se ha establecido: Si un número primo divide a un número entero, entonces no divide al siguiente entero sucesivo.

Proposición 4.7.3

Para cualquier número entero y cualquier número primo p, si $p \mid a$ entonces $p \nmid (a + 1)$.

Demostración:

Supongamos que no. Es decir, supongamos que existe un entero a y un número primo p tal que $p \mid a$ y $p \mid (a + 1)$. Entonces, por definición de divisibilidad, existen enteros r y s, tal que $a = pr$ y $a + 1 = ps$. De lo que se deduce que

$$1 = (a + 1) - a = ps - pr = p(s - r),$$

y así (ya que $s - r$ es un número entero) $p \mid 1$. Pero, por el teorema 4.3.2, los únicos divisores enteros de 1 son 1 y -1 y $p > 1$, ya que p es primo. Por tanto $p \leq 1$ y $p > 1$, que es una contradicción. *[Por tanto la suposición es falsa y la proposición es verdadera.]*

La idea de la demostración de Euclides es la siguiente: Supongamos que el conjunto de los números primos fuera finito. Entonces podría tomar el producto de todos los números primos y sumar uno. Por el teorema 4.3.4 este número debe ser divisible por algún número primo. Pero por la proposición 4.7.3, este número no es divisible por ninguno de los números primos en el conjunto. Por tanto debe haber un número primo que no esté en el conjunto de todos los números primos, lo cual es imposible.

La siguiente demostración formal, completa los detalles de este esquema.

Teorema 4.7.4 Infinitud de los primos

El conjunto de números primos es infinito.

Demostración (por contradicción):

Supongamos que no. Es decir, supongamos que el conjunto de números primos es finito. *[Debemos deducir una contradicción.]* Entonces algún número primo p es el mayor de todos los números primos y por tanto, podemos enumerar los números primos en orden ascendente:

$$2, 3, 5, 7, 11, \ldots, p.$$

Sea N el producto de todos los números primos más 1:

$$N = (2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdots p) + 1$$

Entonces $N > 1$ y así, por el teorema 4.3.4, N es divisible por algún número primo q. Ya que q es primo, q debe ser igual a uno de los números primos $2, 3, 5, 7, 11, \ldots, p$.

Por tanto, por definición de divisibilidad, q divide $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdots p$ y así, por la proposición 4.7.3, q no divide a $(2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdots p) + 1$, que es igual a N. Por tanto N es divisible entre q y N no es divisible entre q y hemos llegado a una contradicción. *[Por tanto, la suposición es falsa y el teorema es verdadero.]*

■

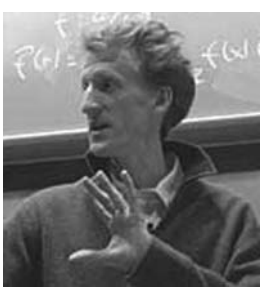
La demostración del teorema 4.7.4 muestra que si se forma el producto de todos los números primos hasta un cierto punto y se suma uno, el resultado, N, no es divisible por un número primo en la lista. La demostración no demuestra que N es, en sí, primo. En los ejercicios al final de esta sección se le pedirá encontrar un ejemplo de un número entero N construido de esta manera que no es primo.

Cuándo usar una demostración indirecta

Los ejemplos en esta sección y de la 4.6 no han dado una respuesta definitiva a la cuestión de cuándo demostrar un enunciado directamente y cuándo demostrar indirectamente. Muchos teoremas se pueden demostrar de cualquier manera. Sin embargo, en general, cuando ambos tipos de demostraciones son posibles, la demostración indirecta es más torpe que una directa. A falta de indicios evidentes que sugieran argumento indirecto, intente primero demostrar un enunciado directamente. Después, si no tiene éxito, busque un contraejemplo. Si la búsqueda de un contraejemplo no tiene éxito, busque una demostración por contradicción o contraposición.

Preguntas abiertas de la Teoría de números

En esta sección hemos demostrado que existen infinitos números primos. No existe una fórmula conocida para la obtención de números primos, pero se ha encontrado que algunas fórmulas tienen más éxito para producirlos que otras fórmulas. Una de ellas se debe a Marin Mersenne, un monje francés que vivió de 1588 hasta 1648. Los *primos de Mersenne* tienen la forma de $2^p - 1$, donde p es primo. No todos los números de esta forma son primos, pero ya que los números primos de Mersenne son más fáciles de probar para la primalidad más que otros números, la mayoría de los números primos más grandes conocidos son los números primos de Mersenne.



Courtesy Ben Joseph Green

Ben Joseph Creen (nacido en 1977)

Una pregunta interesante es si existe un infinito de primos de Mersenne. Hasta la fecha de publicación de este libro, la respuesta no se conoce, pero todos los días se están realizando nuevos descubrimientos matemáticos y al momento de que se lea esto alguien puede haber descubierto la respuesta. Otra fórmula que parece producir un número relativamente grande de números primos se debe a Fermat. Los *primos de Fermat* son números primos de la forma $2^{2^n} + 1$, donde n es un entero positivo. ¿Hay un infinito de números primos de Fermat? Una vez más, hasta ahora, nadie lo sabe. Del mismo modo se desconoce si existe un infinito de números primos de la forma $n^2 + 1$, donde n es un entero positivo y si siempre hay un número primo entre los enteros n^2 y $(n + 1)^2$.

UCLA

Terence Chi-Shen Tao (nacido en 1975)

Otra famosa pregunta abierta que implica a los números primos es la conjetura de los números primos gemelos, que establece que hay infinitos pares de números primos de la forma p y $p + 2$. Al igual que con otros problemas bien conocidos en la teoría de números, esta conjetura ha resistido computadoras de prueba hasta números muy grandes y se han hecho algunos progresos hacia una demostración. En 2004, Ben Green y Terence Tao mostraron que para cualquier entero $m > 1$, hay una sucesión de números enteros m equidistantemente espaciados todos los cuales son primos. En otras palabras, existen los números enteros positivos n y k para los cuales los siguientes números son primos:

$$n,\ n + k,\ n + 2k,\ n + 3k,\ \ \ldots,\ n + (m - 1)k.$$

Relacionada con la conjetura de primos gemelos está una conjetura hecha por Sophie Germain, una matemática francesa nacida en 1776, que hizo un progreso significativo hacia una demostración del Último Teorema de Fermat. Germain conjeturó que existen infinitos


The Art Gallery Collection/Alamy

Marie-Sophie Germain (1776-1831)

pares de números primos de la forma p y $2p + 1$. Los valores iniciales de p con esta propiedad son 2, 3, 5, 11, 23, 29, 41 y 53; pruebas en computadora ha comprobado la conjetura para muchos valores adicionales. De hecho, en el momento en que se escribió este libro, el mayor número primo p para el que $2p + 1$ también es conocido por ser primo es $183\,027 \cdot 2^{265440} - 1$. Este es un número con ¡79 911 dígitos decimales! Pero en comparación con el infinito, cualquier número, no importa que tan grande sea, es menor que una gota en la cubeta.

En 1844, el matemático belga Eugène Catalan conjetura que la única solución a la ecuación $x^n - y^m = 1$, donde x, y, n, m son enteros mayores que 1, es $3^2 - 2^3 = 1$. Esta conjetura sigue sin resolverse hasta hoy.

En 1993, mientras trataba de demostrar el último teorema de Fermat, el aficionado teórico de números, Andrew Beal, empezó a interesarse por la ecuación $x^n + y^m = z^k$, donde no hay dos de x, y o z que tengan algún factor común, más que ± 1. Después de un gran esfuerzo diligente, primero a mano y después en computadora, no encontró ninguna solución, Beal conjeturó que no existen soluciones. Su conjetura se conoce como la *conjetura de Beal* y ha ofrecido un premio de 100 000 dólares a cualquier persona que pueda demostrarla o refutarla.

Estos son sólo algunas de un gran número de cuestiones abiertas en la teoría de números. Muchas personas creen que las matemáticas son un tema fijo que cambia muy poco de un siglo a otro. De hecho, ahora más que nunca antes en la historia se plantean más preguntas matemáticas y se están descubriendo más resultados.

Autoexamen

1. Los antiguos griegos descubrieron que en un triángulo rectángulo donde ambos catetos tienen longitud 1, el cociente de la longitud de la hipotenusa a la longitud de uno de los catetos no es igual a un cociente de _____.
2. Una forma de demostrar que $\sqrt{2}$ es un número irracional es suponer que $\sqrt{2} = a/b$ para algunos enteros a y b que no tienen ningún factor común mayor que 1, utilice el lema dice que si el cuadrado de un entero es par entonces _____ y, finalmente, demuestre que a y b _____.
3. Una forma de demostrar que hay infinitos números primos es suponer que hay un número primo mayor p, construya el número _____ y después, demuestre que este número tiene que ser divisible entre un número primo que es mayor que _____.

Conjunto de ejercicios 4.7

1. Una pantalla de calculadora muestra que $\sqrt{2} = 1.414213562$ y $1.414213562 = \dfrac{1414213562}{1000000000}$. Lo que sugiere que es un número racional, lo que contradice el teorema 4.7.1. Explique la discrepancia.

2. El ejemplo 4.2.1 (h) muestra una técnica para demostrar que cualquier número decimal periódico es racional. Una pantalla de calculadora muestra el resultado de un cálculo determinado como 40.72727272727. ¿Puede usted estar seguro de que el resultado del cálculo es un número racional? Explique.

Determine cuáles enunciados de los ejercicios 3 al 13 son verdaderos y cuáles son falsos. Demuestre los que son verdaderos y refute los que son falsos.

3. $6 - 7\sqrt{2}$ es irracional.

4. $3\sqrt{2} - 7$ es irracional.

5. $\sqrt{4}$ es irracional

6. $\sqrt{2}/6$ es racional.

7. La suma de dos números irracionales es irracional.

8. La diferencia de dos números irracionales es irracional.

9. La raíz cuadrada positiva de un número irracional positivo es irracional.

10. Si r es un número racional y s es un número irracional, entonces r/s es irracional.

11. La suma de dos números irracionales positivos es irracional.

12. El producto de dos números irracionales es irracional.

H 13. Si un entero mayor que 1 es un cuadrado perfecto, entonces su raíz cúbica es irracional.

14. Considere la siguiente frase: Si x es racional entonces $\sqrt{x}$ es irracional. ¿Es esta frase siempre verdadera y es falsa a veces, o siempre es falsa? Justifique su respuesta.

15. a. Demuestre que para todos los enteros a, si es a^3 es par entonces a es par.
    b. Demuestre que $\sqrt[3]{2}$ es irracional.

16. a. Utilice la demostración por contradicción para demostrar que para cualquier entero n, es imposible que n sea igual a tanto a $3q_1 + r_1$ y $3q_2 + r_2$, donde q_1, q_2, r_1 y r_2, son números enteros, $0 \le r_1 < 3$, $0 \le r_2 < 3$ y $r_1 \ne r_2$.

b. Utilice la demostración por contradicción, el teorema del cociente-residuo, la división en casos y el resultado del inciso *a*) para demostrar que para todo entero n, si n^2 es divisible entre 3, entonces n es divisible entre 3.
c. Demuestre que $\sqrt{3}$ es irracional.

17. Dé un ejemplo para mostrar que si d no es primo y n^2 es divisible entre d, entonces n no tiene que ser divisible entre d.

H 18. El teorema del cociente-residuo dice que no sólo existen cocientes y residuos, sino también que el cociente y el residuo de una división son únicos. Demuestre la unicidad. Es decir, demuestre que si a y d son números enteros con $d > 0$ y si q_1, r_1, q_2, r_2 son enteros tales que

$$a = dq_1 + r_1 \quad \text{donde } 0 \le r_1 < d$$

y

$$a = dq_2 + r_2 \quad \text{donde } 0 \le r_2 < d,$$

entonces

$$q_1 = q_2 \quad \text{y} \quad r_1 = r_2.$$

H 19. Demuestre que $\sqrt{5}$ es irracional.

H 20. Demuestre que para cualquier entero a, $9 \not| (a^2 - 3)$.

21. Una demostración alternativa de la irracionalidad de $\sqrt{2}$ cuenta el número de 2 en los dos lados de la ecuación $2n^2 = m^2$ y utiliza el teorema factorización única de números enteros para deducir una contradicción. Escriba una demostración que utilice este método.

22. Utilice la demostración técnica que se muestra en el ejercicio 21 para demostrar que si n es un entero que no es un cuadrado perfecto, entonces $\sqrt{n}$ es irracional.

H 23. Demuestre que $\sqrt{2} + \sqrt{3}$ es irracional.

✶ 24. Demuestre que $\log_5(2)$ es irracional. (*Sugerencia*: Use el teorema de factorización única de números enteros.)

H 25. Sea $N = 2 \cdot 3 \cdot 5 \cdot 7 + 1$. ¿Qué residuo se obtiene cuando N se divide entre 2? 3? 5? 7? ¿N es primo? Justifique su respuesta.

H 26. Supongamos que a es un número entero y p es un número primo tal que $p \mid a$ y $p \mid (a + 3)$. ¿Qué puede deducir acerca de p? ¿Por qué?

27. Sea $p_1, p_2, p_3, \ldots$ una lista de todos los números primos en orden ascendente. En seguida se presenta una tabla de los primeros seis:

p_1	p_2	p_3	p_4	p_5	p_6
2	3	5	7	11	13

H a. Para cada $i = 1, 2, 3, 4, 5, 6$, vamos a $N_i = p_1 p_2 \cdots p_i + 1$. Calcule N_1, N_2, N_3, N_4, N_5 y N_6.

b. Para cada $i = 1, 2, 3, 4, 5, 6$ y encuentra el menor número primo q tal que q_i divide a N_i. (*Sugerencia*: Use la prueba de primalidad del ejercicio 31 en la sección 4.6 para determinar sus respuestas.)

Para los ejercicios 28 y 29, utilice el hecho de que para todo entero positivo n,

$$n! = n(n-1) \ldots 3 \cdot 2 \cdot 1.$$

28. Una demostración alternativa de la infinidad de los números primos comienza de la siguiente manera:

Demostración: Supongamos que hay solamente un número finito de números primos. Entonces uno es el más grande. Llámelo p. Sea $M = p! + 1$. Vamos a demostrar que existe un número primo q tal que $q > p$. Complete esta demostración.

H ✶ 29. Demuestre que para todo entero n, si $n > 2$, entonces hay un número primo p tal que $n < p < n!$.

H ✶ 30. Demostrar que si $p_1, p_2, \ldots, p_n$ y son distintos números primos con $p_1 = 2$ y $n > 1$, entonces, $p_1 p_2 \cdots p_n + 1$ se puede escribir en la forma $4k + 3$ para algún entero k.

H 31. a. El último teorema de Fermat dice que para todo entero $n > 2$, la ecuación $x^n + y^n = z^n$, no tiene solución entera positiva (solución para la que x, y y z son números enteros positivos) Demuestre lo siguiente: Si para todos los números primos $p > 2$, $x^p + y^p = z^p$ no tiene solución entera positiva, entonces para cualquier entero $n > 2$, que no es una potencia de 2, $x^n + y^n = z^n$, no tiene solución entera positiva.
b. Fermat demostró que no existen números enteros x, y y z tales que $x^4 + y^4 = z^4$. Use este resultado para eliminar la restricción del inciso *a*) de que n no es una potencia de 2. Es decir, demuestre que si n es una potencia de 2 y $n > 4$, entonces $x^n + y^n = z^n$, no tiene solución entera positiva.

Para los ejercicios del 32 al 35 observe que para demostrar que hay un objeto único con una cierta propiedad, demuestre que 1) hay un objeto con la propiedad y 2) si los objetos A y B tienen la propiedad, entonces $A = B$.

32. Demuestre que existe un número único primo de la forma $n^2 - 1$, donde n es un entero que es mayor o igual a 2.

33. Demuestre que existe un número único primo de la forma $n^2 + 2n - 3$, donde n es un entero positivo.

34. Demuestre que a lo más hay un número real a con la propiedad de que $a + r = r$ para todos los números reales r. (Este número se llama *identidad aditiva*).

35. Demuestre que existe a lo más un número real b con la propiedad de que $br = r$ para todos los números reales r. (Este número se llama una *identidad multiplicativa*).

Respuestas del autoexamen

1. dos enteros 2. el entero es par; tienen un factor común mayor que 1 3. $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdots p + 1$; p

4.8 Aplicación: algoritmos

Empieza por el principio . . . y sigue hasta llegar al final: luego te detienes.
—Lewis Carroll, *Alicia en el país de las maravillas*, 1865


Hulton Archive/Getty Images

Lady Lovelace (1815-1852)

En esta sección vamos a mostrar cómo los conceptos desarrollados de la teoría de números en este capítulo constituyen la base de algunos algoritmos computacionales útiles.

La palabra *algoritmo* se refiere a un método paso a paso para realizar alguna acción. Algunos ejemplos de algoritmos en la vida cotidiana son las recetas de preparación de alimentos, las instrucciones de montaje de kits de equipos o un pasatiempo, las instrucciones de un patrón de costura y las instrucciones para el llenado de los formularios de impuesto sobre la renta. Gran parte de matemáticas de la escuela primaria se dedica al aprendizaje de algoritmos para realizar cálculos como la suma de varios dígitos y la resta, la multiplicación de varios dígitos (o larga) y la división larga.

La idea de un algoritmo de la computadora se le atribuye a Ada Augusta, Condesa de Lovelace. Formada como matemática, se interesó mucho en el diseño de Charles Babbage de una "máquina analítica", una máquina similar en concepto a una computadora moderna. Lady Lovelace amplió las investigaciones de Babbage de cómo funcionaría una máquina, reconociendo que su importancia radica "en la posibilidad de utilizar una secuencia de instrucciones en varias ocasiones, el número de veces que sea asignada previamente o que depende de los resultados del cálculo". Esta es la esencia de un algoritmo de la computadora moderna.

Un lenguaje algorítmico

El lenguaje algorítmico utilizado en este libro es una especie de seudocódigo, que combina elementos de Pascal, C, Java y VB.NET y el español común, pero bastante preciso. Vamos a utilizar algunas de las construcciones formales de lenguajes de programación, tales como instrucciones de asignación, bucles y así sucesivamente, pero pasaremos por alto los detalles más técnicos, tales como la necesidad de delimitadores explícitos al final de su enunciado, el rango de valores enteros disponibles en una instalación en particular y así sucesivamente. Los algoritmos que se presentan en este texto están destinados a ser lo suficientemente precisos para ser fácilmente traducidos a prácticamente cualquier lenguaje de programación de alto nivel.

En lenguajes de programación de alto nivel, el término **variable** se utiliza para referirse a un lugar de almacenamiento específico en la memoria de una computadora. Decir que la variable x tiene el valor 3 significa que la posición de memoria correspondiente a x contiene el número 3. Una ubicación de almacenamiento dada sólo puede tener un valor a la vez. Así que si a una variable se le asigna un nuevo valor durante la ejecución del programa, entonces se borra el valor anterior. El **tipo de datos** de una variable indica el conjunto en el que la variable toma sus valores, si el conjunto de los enteros, números reales, cadenas de caracteres o el conjunto $\{0,1\}$ (para una variable booleana) y así sucesivamente.

Una **instrucción de asignación** da un valor a una variable. Tiene la forma

$$x := e,$$

donde x es una variable y e es una expresión. Esto se lee "x se le asigna el valor e" o "x sea e". Cuando se ejecuta una instrucción de asignación, la expresión e es evaluada (usando los valores actuales de todas las variables en la expresión) y después su valor se coloca en la posición de memoria correspondiente a x (que sustituye el contenido anterior de este lugar).

Por lo general, los enunciados del algoritmo se ejecutan uno tras otro en el orden en que están escritos. Los **enunciados condicionales** permiten que este orden natural se reemplace con los valores actuales de las variables del programa para determinar el algoritmo de instrucción que se ejecutará a continuación. Los enunciados condicionales se indican ya sea como

a. **if** (*condición*)
then s_1
else s_2

o

b. **if** (*condición*) **then** s_1

donde la *condición* es un predicado que implica variables de algoritmo y donde s_1 y s_2 son enunciados del algoritmo o grupos de enunciados del algoritmo. En general, se usa una sangría para indicar que los enunciados deben ir juntos como una unidad. Sin embargo, cuando la ambigüedad es posible, podemos unir explícitamente a un grupo de enunciados, junto a una unidad anterior a la del grupo con la palabra **do** y finalizar con las palabras **end do**.

La ejecución de un enunciado **if-then-else** se produce de la siguiente manera:

1. Se evalúa la *condición* sustituyendo los valores actuales de todas las variables del algoritmo que se encuentran en éste y se evalúa la veracidad o falsedad del enunciado resultante.
2. Si la *condición* es verdadera, entonces se ejecuta s_1 y se mueve la ejecución al siguiente enunciado del algoritmo al enunciado **if-then-else**.
3. Si la condición es falsa, entonces se ejecuta s_2 y se mueve la ejecución al siguiente enunciado del algoritmo al enunciado **if-then-else**.

La ejecución de un enunciado **if-then** es similar a la ejecución de un enunciado **if-then-else**, excepto que si la *condición* es falsa, la ejecución pasa de inmediato al siguiente enunciado del algoritmo al enunciado **if-then**.

Con frecuencia, la *condición* se llama un **guardia**, ya que se encuentra estacionado antes de s_1 y de s_2 y restringe el acceso a ellos.

Ejemplo 4.8.1 Ejecución de enunciados if-then-else y if-then

Considere el siguiente segmento del algoritmo:

a. **if** $x > 2$
then $y := x + 1$
else do $x := x - 1$
$y := 3 \cdot x$ **end do**

b. $y := 0$
if $x > 2$ **then** $y := 2^x$

¿Cuál es el valor de y después de la ejecución de estos segmentos para los siguientes valores de x?

i. $x = 5$ ii. $x = 2$

Solución

a. (*i*) Dado que el valor de x es 5 antes de la ejecución, la condición de guardia $x > 2$ es verdadera en el momento en que se evalúa. De ahí que se ejecute el siguiente enunciado **then** y así el valor de $x + 1 = 5 + 1$ se calcula y se coloca en la ubicación de almacenamiento correspondiente a y. Así después de su ejecución, $y = 6$.

(ii) Dado que el valor de x es 2 antes de la ejecución, la condición de guardia $x > 2$ es falsa en el momento en que se evalúa. De ahí que se ejecute el siguiente enunciado **else**. Se calcula el valor de $x - 1 = 2 - 1$ y se coloca en el lugar de almacenamiento correspondiente a x y el valor de $3 \cdot x = 3 \cdot 1$ se calcula y se coloca en la ubicación de almacenamiento correspondiente a y. Así que después de su ejecución, $y = 3$.

b. (*i*) Puesto que inicialmente $x = 5$, la condición $x > 2$ es verdadera en el momento en que se evalúa. Así que el siguiente enunciado **then** se ejecuta y se obtiene y el valor $2^5 = 32$.

(*ii*) Puesto que inicialmente $x = 2$, la condición $x > 2$ es falsa en el momento en que se evalúa. Por tanto, la ejecución se mueve al siguiente enunciado después del enunciado if-then y el valor de y no cambia de su valor inicial de 0. ■

Los **enunciados iterativos** se utilizan cuando una secuencia de enunciados del algoritmo se ejecutan una y otra vez. Vamos a utilizar dos tipos de enunciados iterativo: los bucles **while** y los bucles **for-next**.

Un bucle **while** tiene la forma

while (*condición*)
[enunciados que conforman el cuerpo del bucle]
end while

donde *condición* es un predicado con las variables del algoritmo. La palabra **while** marca el inicio del bucle y las palabras **end while** marca su fin. La ejecución de un bucle **while** se produce de la siguiente manera:

1. La *condición* se evalúa mediante la sustitución de los valores actuales de todas las variables del algoritmo de las variables y se evalúa la verdad o falsedad del enunciado resultante.
2. Si la *condición* es verdadera, todos los enunciados en el cuerpo del bucle se ejecutan en orden. Entonces la ejecución se mueve de nuevo al principio del bucle y se repite el proceso.
3. Si la *condición* es falsa, la ejecución pasa al siguiente enunciado del algoritmo del bucle.

El bucle se dice que es **iterada** (i-te-ra-da) cada vez que se ejecuten los enunciados en el cuerpo del bucle. Cada ejecución del cuerpo del bucle se llama una **iteración** (i-te-ra-ción) del bucle.

Ejemplo 4.8.2 Seguimiento de la ejecución de un bucle while

El seguimiento de la ejecución del siguiente segmento del algoritmo de búsqueda de los valores de todas las variables del algoritmo cada vez que se cambian durante la ejecución:

$i := 1, s := 0$
while $(i \leq 2)$
$s := s + i$
$i := i + 1$
end while

Solución Ya que i se le da un valor inicial de 1, la condición $i \leq 2$ es verdadera cuando se introduce el bucle **while**. Así los enunciados dentro del bucle se ejecutan en orden:

$$s = 0 + 1 = 1 \quad \text{y} \quad i = 1 + 1 = 2.$$

Entonces, la ejecución se pasa de nuevo al principio del bucle.

La condición $i \leq 2$, se evalúa al valor actual de i, que es 2. La condición es verdadera, por lo que los enunciados dentro del bucle se ejecutan de nuevo:

$$s = 1 + 2 = 3 \quad \text{y} \quad i = 2 + 1 = 3.$$

La ejecución pasa de nuevo al principio del bucle.

La condición $i \leq 2$, se utiliza dfel valor actual de i, que es 3. Esta vez, la condición es falsa y así la ejecución pasa más allá del bucle al siguiente enunciado del algoritmo.

Este análisis se puede resumir en una tabla, llamada **tabla de seguimiento**, que muestra los valores actuales de las variables del algoritmo en varios puntos durante la ejecución. La tabla de seguimiento para un bucle **while** en general, da todos los valores inmediatamente después de cada iteración del bucle. ("Después de la iteración cero" significa lo mismo que "antes de la primera iteración".)

Tabla de seguimiento

Nombre de la variable	Número de iteración 0	1	2
i	1	2	3
s	0	1	3

La segunda forma de iteración que vamos a utilizar es un bucle **for-next**. Un bucle **for-next** tiene la siguiente forma:

for *variable* := *expresión inicial* **to** *expresión final*
    [enunciados que conforman
    el cuerpo del bucle]
next *(misma) variable*

Un bucle **for-next** se ejecuta de la siguiente manera:

1. La variable de bucle **for-next** se fija igual al valor de la *expresión inicial*.
2. Se realiza una comprobación para determinar si el valor de la *variable* es menor o igual al valor de la *expresión final*.
3. Si el valor de la *variable* es menor o igual al valor de la *expresión final*, entonces los enunciados en el cuerpo del bucle se ejecutan en orden, la *variable* se incrementa en 1 y la ejecución se regresa al paso 2.
4. Si el valor de la *variable* es mayor que el valor de la *expresión final*, entonces la ejecución pasa al siguiente enunciado del algoritmo siguiendo al bucle.

Ejemplo 4.8.3 Tabla de seguimiento para un bucle for-next

Convierta el bucle **for-next** que se muestra a continuación dentro de un bucle **while**. Construya una tabla de seguimiento para el bucle.

for $i := 1$ **to** 4
    $x := i^2$
next i

Solución El bucle **for-next** dado es equivalente al siguiente:

$i := 1$
while $(i \leq 4)$
    $x := i^2$
    $i := i + 1$
end while

Su tabla de seguimiento es la siguiente:

Tabla de seguimiento

Nombre de la variable	Número de iteración 0	1	2	3	4
x		1	4	9	16
i	1	2	3	4	5

Una notación de algoritmos

Expresaremos los algoritmos como subrutinas que pueden ser llamados con otros algoritmos como sea necesario y se utiliza para transformar un conjunto de variables de entrada con los valores dados en un conjunto de variables de salida con valores específicos. Las variables de salida y sus valores asumidos deben regresar a la llamada del algoritmo. Por ejemplo, el algoritmo de la división especifica un procedimiento para tomar cualquiera de los dos números enteros positivos como entrada y produce el cociente y el residuo de la división del número uno por el otro como salida. Siempre que un algoritmo requiere un cálculo, el algoritmo sólo puede "llamar" al algoritmo de la división para hacer el trabajo.

En general, incluya la siguiente información para describir formalmente a los algoritmos:

1. El nombre del algoritmo, junto con una lista de variables de entrada y salida.
2. Una breve descripción de cómo funciona el algoritmo.
3. Los nombres de las variables de entrada, marcada por el tipo de datos (ya sea entero, número real y así sucesivamente).
4. Los enunciados que conforman el cuerpo del algoritmo, posiblemente con comentarios explicativos.
5. Los nombres de las variables de salida, etiquetados con el tipo de datos.

Suleymaniye Kutuphanesi

al-Khowârizmî (aproximadamente 780-850)

Puede preguntarse de dónde proviene la palabra *algoritmo*. Se desarrolló a partir de la última parte del nombre del matemático persa Abu Yafar Mohamed ibn Musa al-Khowârizmî. Durante la Edad Oscura de Europa, el mundo árabe gozó de un periodo de intensa actividad intelectual. Uno de los grandes trabajos matemáticos de la época fue un libro escrito por al-Khowârizmî que contenía las ideas fundamentales de la asignatura de álgebra. La traducción de este libro al latín en el siglo XIII tuvo una profunda influencia en el desarrollo de las matemáticas durante el Renacimiento europeo.

El algoritmo de la división

Para un entero y un entero positivo d, el teorema del cociente-residuo garantiza la existencia de números enteros q y r tales que

$$a = dq + r \quad \text{y} \quad 0 \leq r < d.$$

En esta sección, le damos un algoritmo para calcular q y r para la a y d dada, donde a es no negativo. (La extensión a a negativo se deja en los ejercicios al final de esta sección.) El siguiente ejemplo ilustra la idea detrás del algoritmo. Considere tratar de encontrar el cociente y el residuo de la división de 32 por 9, pero supongo que no recuerda su tabla de multiplicar y tiene que encontrar la respuesta de los principios básicos. El cociente representa ese número, del 9 de los que están contenidos en 32. El residuo es la cantidad cuando todos los grupos posibles de 9 se restan. De este modo se puede calcular el cociente y el residuo en varias ocasiones restando 9 de 32 hasta obtener un número menor de 9:

$$\begin{aligned} 32 - 9 &= 23 \geq 9 \text{ y} \\ 32 - 9 - 9 &= 14 \geq 9 \text{ y} \\ 32 - 9 - 9 - 9 &= 5 < 9. \end{aligned}$$

Esto demuestra que tres grupos de 9 se pueden restar de 32 y sobra 5. Así, el cociente es 3 y el residuo es 5.

Algoritmo 4.8.1 Algoritmo de la división

[Dado un número entero no negativo y un entero positivo d, el objetivo del algoritmo es encontrar enteros q y r que satisfacen las condiciones $a = dq + r$ y $0 \leq r < d$. Esto se hace restando d varias veces de a hasta que el resultado es menor que d, pero sigue siendo negativo.

$$0 \leq a - d - d - d - \cdots - d = a - dq < d.$$

El número total de d que resta es el cociente q. La cantidad $a - dq$ es igual al residuo r.]

Entrada: *un [un entero no negativo], d [un entero positivo]*

Cuerpo del algoritmo:

$r := a, q := 0$
[Repetidamente reste d de r hasta que se obtenga un número menor que d. Sume 1 a q cada vez que se resta d.]

while $(r \geq d)$
  $r := r - d$
  $q := q + 1$
end while

[Después de la ejecución del bucle **while**, $a = dq + r$.*]*

Salida: *q, r [números enteros no negativos]*

Observe que los valores de q y r obtenidos del algoritmo de la división son los mismos que los calculados con las funciones integradas *div* y *mod* en una serie de lenguajes de programación. Es decir, si q y r son el cociente y el residuo obtenido del algoritmo de la división con la entrada a y d, entonces se satisfacen las variables de salida q y r

$$q = a \text{ div } d \quad \text{y} \quad r = a \bmod d.$$

El siguiente ejemplo le pide un seguimiento del algoritmo de división.

Ejemplo 4.8.4 Seguimiento del algoritmo de división

Siga la acción del algoritmo 4.8.1 con las variables de entrada $a = 19$ y $d = 4$.

Solución Haga una tabla de seguimiento como se muestra a continuación. La columna debajo de la k-ésima iteración da los estados de las variables después de la k-ésima iteración del bucle.

Nombre de la variable	Número de iteración 0	1	2	3	4
a	19				
d	4				
r	19	15	11	7	3
q	0	1	2	3	4

■

El algoritmo euclidiano

El máximo común divisor de dos números enteros a y b es el mayor entero que divide a y b. Por ejemplo, el máximo común divisor de 12 y 30 es 6. El algoritmo de Euclides proporciona una manera muy eficiente para calcular el máximo común divisor de dos números enteros.

• Definición

Sean a y b enteros que no son ambos cero. El **máximo común divisor** de a y b, que se denota **mcd(a, b)**, es el entero d con las siguientes propiedades:

1. d es un común divisor de a y b. En otras palabras,
$$d \mid a \quad \text{y} \quad d \mid b$$
2. Para todos los números enteros c, si c es un divisor común de a y b, entonces c es menor o igual a d. En otras palabras,
para todos los enteros c, si $c \mid a$ y $c \mid b$, entonces $c \leq d$.

Ejemplo 4.8.5 Cálculo de algunos mcd

a. Encuentre mcd(72, 63).

b. Determine mcd(10^{20}, 6^{30}).

c. En la definición de máximo común divisor, el mcd(0, 0) no está permitido. ¿Por qué no? ¿A qué es igual mcd(0,0) si se encuentra en la misma forma que el mayor divisor común para otros pares de números?

Solución

a. $72 = 9 \cdot 8$ y $63 = 9 \cdot 7$. Así $9 \mid 72$ y $9 \mid 63$ y no hay entero mayor que 9 que divide a ambos 72 y 63. Por tanto el mcd(72, 63) $= 9$.

b. Por las leyes de los exponentes, $10^{20} = 2^{20} \cdot 5^{20}$ y $6^{30} = 2^{30} \cdot 3^{30} = 2^{20} \cdot 2^{10} \cdot 3^{30}$. De lo que se deduce que
$$2^{20} \mid 10^{20} \quad \text{y} \quad 2^{20} \mid 6^{30},$$
y por el teorema de factorización única de números enteros, no hay entero mayor que 2^{20} que divide a ambos 10^{20} y 6^{30} (ya que no más que veinte 2 dividen 10^{20}, ni 3 divide a 10^{20} y ni 5 divide 6^{30}). Por tanto el mcd(10^{20}, 6^{30}) $= 2^{20}$.

c. Supongamos que mcd(0, 0) se define como el mayor factor común que divide a 0 y 0. El problema es que cada número entero positivo divide 0 y no hay mayor entero. Así que ¡no hay mayor común divisor! ■

Calcular mcd usando el método que se ilustra en el ejemplo 4.8.5 sólo funciona cuando los números se pueden factorizar completamente. Por el teorema de factorización única de números enteros, todos los números, en principio, pueden factorizarse por completo. Pero, en la práctica, incluso con los equipos de mayor velocidad, el proceso es largo para irrealizable para enteros muy grandes. Hace más de 2 000 años, Euclides ideó un método para encontrar más divisores comunes que es fácil de usar y es mucho más eficiente que cualquiera de las pruebas de factorizar números o de división repetida de números para números enteros sucesivamente mayores.

El algoritmo de Euclides se basa en los siguientes dos hechos, que se expresan como lemas.

Lema 4.8.1

Si r es un entero positivo, entonces $\text{mcd}(r, 0) = r$.

Demostración:

Supongamos que r es un entero positivo. *[Debemos demostrar que el máximo común divisor de ambos r y 0 es r.]* Ciertamente, r es un divisor común de ambos r y 0 ya que r se divide a sí mismo y también divide a 0 (ya que cada número entero positivo divide a 0). Tampoco un entero mayor que r puede ser un divisor común de r y 0 (ya que no hay mayor número entero que se puede dividir a r). Por tanto r es el máximo común divisor de r y 0.

La demostración del segundo lema se basa en un modelo inteligente de argumento que se utiliza en diferentes áreas de las matemáticas: Para demostrar que $A = B$, pruebe que $A \leq B$ y que $B \leq A$.

Lema 4.8.2

Si a y b son números enteros diferentes de cero y si q y r son cualesquiera números enteros tales que

$$a = bq + r,$$

entonces

$$\text{mcd}(a, b) = \text{mcd}(b, r)$$

Demostración:

[La demostración se divide en dos secciones: 1) *la demostración de que mcd(a, b) ≤ mcd(b, r) y* 2) *la demostración de que mcd(a, r) < mcd(a, b). Dado que cada mcd es menor o igual que el otro, los dos deben ser iguales.]*

1. **mcd(a, b) ≤ mcd(b, r):**

   a. *[En primer lugar, se mostrará que cualquier común divisor de a y b es también un divisor común de b y r.]*

   Sean a y b enteros, no ambos cero y sea c un divisor común de a y b. Entonces, $c \mid a$ y $c \mid b$ y así, por definición de divisibilidad, un $a = nc$ y $b = mc$, para algunos enteros n y m. Ahora sustituye en la ecuación

   $$a = bq + r$$

   para obtener

   $$nc = (mc)q + r.$$

   Después se resuelve para r:

   $$r = nc - (mc)q = (n - mq)c.$$

   Pero $n - mq$ es un número entero y así, por definición de divisibilidad, $c \mid r$. Porque ya sabemos que $c \mid b$, podemos concluir que c es un divisor común de b y r *[que era lo que se quería demostrar]*.

continúa en la página 222

b. *[A continuación se muestra que* $\text{mcd}(a, b) \leq \text{mcd}(g, r)$*.]*
Por el inciso *a*), cada común divisor de a y b es un divisor común de b y r. De lo que se deduce que el máximo común divisor de a y b se define ya que a y b no son ambos cero y es un divisor común de b y r. Pero entonces $\text{mcd}(a, b)$ (siendo uno de los divisores comunes de b y r) es menor o igual al máximo común divisor de b y r:

$$\text{mcd}(a, b) \leq \text{mcd}(b, r).$$

2. **mcd(b, r) ≤ mcd(a, b):**
La segunda parte de la demostración es muy similar a la primera parte. Se deja como ejercicio.

El algoritmo de Euclides se puede describir de la siguiente manera:

1. Sean A y B enteros con $A > B \geq 0$.
2. Para encontrar el máximo común divisor de A y B, compruebe primero si $B = 0$. Si es así, entonces $\text{mcd}(A, B) = A$ por el lema 4.8.1. Si no es así, entonces $B > 0$ y el teorema del cociente-residuo se puede utilizar para dividir A por B para obtener un cociente q y un residuo r:

$$A = Bq + r \quad \text{donde} \quad 0 \leq r < B.$$

Por el lema 4.8.2, $\text{mcd}(A, B) = \text{mcd}(B, r)$. Por tanto el problema de encontrar el máximo común divisor de A y B se reduce al problema de encontrar el máximo común divisor de B y r.

Lo que hace este tipo de información útil es que B y r son números más pequeños que A y B. Para ver esto, recordemos que hemos supuesto

$$A > B \geq 0.$$

Asimismo, la r que se encuentra por el teorema del cociente-residuo cumple que

$$0 \leq r < B.$$

Poniendo estas dos desigualdades juntas se obtiene

$$0 \leq r < B < A.$$

Así que el número más grande de la pareja (B, r) es menor que el número más grande de la pareja (A, B).

3. Ahora sólo tiene que repetir el proceso, empezando de nuevo en (2), pero el uso de B en lugar de A y r en lugar de B. Las repeticiones están garantizadas para terminar finalmente con $r = 0$, ya que cada nuevo residuo es menor que el anterior y todos son no negativos.

Nota Estrictamente hablando, el hecho de que las repeticiones finalmente terminen se justifica por el principio del buen orden de los números enteros, que se analiza en la sección 5.4.

Por cierto, siempre es el caso de que el número de pasos necesarios en el algoritmo de Euclides es un máximo de cinco veces el número de dígitos en el número entero más pequeño. Esto fue demostrado por el matemático francés Gabriel Lamé (1795 a 1870).

El siguiente ejemplo ilustra cómo utilizar el algoritmo de Euclides.

Ejemplo 4.8.6 Cálculo a mano del mcd usando el algoritmo de Euclides

Utilice el algoritmo de Euclides para encontrar mcd(330, 156).

Solución

1. Divida 330 entre 156:

$$\begin{array}{r} 2 \leftarrow \text{cociente} \\ 156\overline{)\,330} \\ \underline{312} \\ 18 \leftarrow \text{residuo} \end{array}$$

Así, $330 = 156 \cdot 2 + 18$ y por tanto, mcd(330, 156) = mcd(156, 18) por el lema 4.8.2.

2. Divida 156 entre 18:

$$\begin{array}{r} 8 \leftarrow \text{cociente} \\ 18\overline{)\,156} \\ \underline{144} \\ 12 \leftarrow \text{residuo} \end{array}$$

Así, $156 = 18 \cdot 8 + 12$ y por tanto, mcd(156, 18) = mcd(18, 12) por el lema 4.8.2.

3. Divida 18 entre 12:

$$\begin{array}{r} 1 \leftarrow \text{cociente} \\ 12\overline{)\,18} \\ \underline{12} \\ 6 \leftarrow \text{residuo} \end{array}$$

Así, $18 = 1 \cdot 12 + 6$ y por tanto, mcd(18, 12) = mcd(12, 6) por el lema 4.8.2.

4. Divida 12 entre 6:

$$\begin{array}{r} 2 \leftarrow \text{cociente} \\ 6\overline{)\,12} \\ \underline{12} \\ 0 \leftarrow \text{residuo} \end{array}$$

Así, $12 = 6 \cdot 2 + 0$ y, por tanto mcd(12, 6) = mcd(6, 0) por el lema 4.8.2.

Poniendo todas las ecuaciones anteriores juntas se obtiene

$$\begin{aligned} \text{mcd}(330,156) &= \text{mcd}(156, 18) \\ &= \text{mcd}(18, 12) \\ &= \text{mcd}(12, 6) \\ &= \text{mcd}(6, 0) \\ &= 6 \qquad \text{por el lema 4.8.1.} \end{aligned}$$

Por tanto, mcd(330, 156) = 6. ■

La siguiente es una versión del algoritmo de Euclides escrita usando la notación de algoritmo formal.

Algoritmo 4.8.2 Algoritmo euclidiano

[Dados dos números enteros A y B con $A > B \geq 0$, este algoritmo calcula mcd*(A, B). Se basa en dos hechos:*

1. mcd(a, b) = mcd(b, r) *si a, b, q y r son números enteros con* $a = b \cdot q + r$ *y* $0 \leq r < b$.
2. mcd$(a, 0) = a$.*]*

Entrada: *A, B [enteros con* $A > B \geq 0$*]*

Cuerpo del algoritmo:

$a := A$, $b := B$, $r := B$

[Si $b \neq 0$*, calcular a, b mod, el residuo de la división entera de a por b y haga r igual a este valor. Después, repita el proceso usando b en lugar de a y r en lugar de b.]*

while $(b \neq 0)$

$r := a \bmod b$

[El valor de a mod b se puede obtener llamando al algoritmo de la división.]

$a := b$

$b := r$

end while

[Después de la ejecución del bucle **while**, mcd*(A, B)* $= a$*.]*

mcd $:= a$

Salida: mcd *[un entero positivo]*

Autoexamen

1. Cuando un enunciado de algoritmo de la forma $x := e$ se ejecuta, ____.
2. Considere un enunciado del algoritmo de la siguiente forma.

   if (*condición*)
   then s_1
   else s_2

   Cuando se ejecuta dicho enunciado, se evalúa la verdad o falsedad de la *condición*. Si la *condición* es verdadera ____. Si la *condición* es falsa, ____.
3. Considere un enunciado del algoritmo de la siguiente forma.

   while (*condición*)
   [Enunciados que conforman el cuerpo del bucle]
   end while

   Cuando se ejecuta dicho enunciado, se evalúa la verdad o falsedad de la *condición*. Si la *condición* es verdadera, ____. Si la *condición* es falsa, ____.
4. Considere un enunciado del algoritmo de la siguiente forma.

   for *variable* := *expresión inicial* **to** *expresión final*.
   [Enunciados que conforman el cuerpo del bucle]
   next *(same) variable*

   Cuando dicho enunciado se ejecuta, la *variable* es igual al valor de la *expresión inicial* y se realiza una comprobación para determinar si el valor de la *variable* es menor o igual al valor de la *expresión final*. Si es así, ____. Si no, ____.
5. Dado un número entero no negativo y un entero positivo d el algoritmo de la división calcula ____.
6. Dados los números enteros a y b no ambos cero, mcd(a, b) es el entero d que satisface las dos condiciones siguientes: ____ y ____.
7. Si r es un entero positivo, entonces mcd$(r, 0)$ = ____.
8. Si a y b son números enteros no ambos cero y si q y r son números enteros no negativos tales que $a = bq + r$ entonces mcd(a, b) = ____.
9. Dados los números enteros positivos A y B con $A > B$, el algoritmo de Euclides calcula ____.

Conjunto de ejercicios 4.8

Encuentre el valor de z cuando cada uno de los segmentos de algoritmo en los ejercicios 1 y 2 se ejecuta.

1. $i := 2$
if ($i > 3$ o $i \leq 0$)
then $z := 1$
else $z := 0$

2. $i := 3$
if ($i \leq 3$ o $i > 6$)
then $z := 2$
else $z := 0$

3. Considere el segmento siguiente algoritmo:

if $x \cdot y > 0$ **then do** $y := 3 \cdot x$
$x := x + 1$ **end do**
$z := x \cdot y$

Encuentre el valor de z si antes de la ejecución x y y tienen los valores que se dan a continuación.
a. $x = 2, y = 3$ b. $x = 1, y = 1$

Encuentre los valores de a y e después de la ejecución de los bucles en 4 y 5:

4. $a := 2$
for $i := 1$ **to** 2
$a := \frac{a}{2} + \frac{1}{a}$
next i

5. $e := 0, f := 2$
for $j := 1$ **to** 4
$f := f \cdot j$
$e := e + \frac{1}{f}$
next j

Haga una tabla de seguimiento para trazar la acción del algoritmo 4.8.1 de las variables de entrada dadas en los ejercicios 6 y 7.

6. $a = 26, d = 7$ 7. $a = 59, d = 13$

8. El siguiente segmento del algoritmo hace el cambio, de una cantidad de dinero A entre 1¢ y 99¢, determine una división de A en monedas de 25¢ (q), monedas de 10¢ (d), monedas de 5¢ (n) y monedas de 1¢(p).

$q := A \; div \; 25$
$A := A \; mod \; 25$
$d := A \; div \; 10$
$A := A \; mod \; 10$
$n := A \; div \; 5$
$p := A \; mod \; 5$

a. Trace este segmento del algoritmo para $A = 69$.
b. Trace este segmento del algoritmo para $A = 87$.

Encuentre el máximo común divisor de cada uno de los pares de números enteros de los ejercicios del 9 al 12. (Utilice cualquier método que desee).

9. 27 y 72 **10.** 5 y 9

11. 7 y 21 12. 48 y 54

Utilice el algoritmo de Euclides para calcular a mano el máximo común divisor de cada uno de los pares de números enteros de los ejercicios 13 al 16.

13. 1188 y 385 **14.** 509 y 1177

15. 832 y 10933 16. 4131 y 2431

Haga una tabla de seguimiento para trazar la acción del algoritmo 4.8.2 de las variables de entrada dadas en los ejercicios 17 y 18.

17. 1001 y 871 18. 5859 y 1232

H **19.** Demuestre que para todos los enteros positivos a y b, $a \mid b$ si y sólo si, $\text{mcd}(a, b) = a$. (Note que para demostrar "A si y sólo si, B", necesita demostrar "si A, entonces B" y "si B entonces A)".

20. a. Demuestre que si a y b son números enteros, no ambos cero y $d = \text{mcd}(a, b)$, entonces a/d, b/d son enteros sin común divisor que sea mayor que uno.
b. Escriba un algoritmo que acepta el numerador y el denominador de una fracción como entrada y produce como salida el numerador y el denominador de dicha fracción escrita en su mínima expresión. (El algoritmo puede llamar al algoritmo de Euclides, según sea necesario).

21. Complete la demostración del lema 4.8.2, mostrando lo siguiente: Si a y b son números enteros cualesquiera con $b \neq 0$ y q y r son números enteros tales que

$$a = bq + r.$$

entonces

$$\text{mcd}(b, r) \leq \text{mcd}(a, b).$$

H **22.** **a.** Demuestre: Si a y d son números enteros positivos y q y r son números enteros tales que $a = dq + r$ y $0 < r < d$, entonces

$$-a = d(-(q + 1)) + (d - r)$$

y $$0 < d - r < d.$$

b. Indique cómo modificar el algoritmo 4.8.1 para permitir la entrada de a negativo.

23. **a.** Demuestre que si a, d, q y r son números enteros tales que $a = dq + r$ y $0 \leq r < d$, entonces

$$q = \lfloor a/d \rfloor \quad \text{y} \quad r = a - \lfloor a/d \rfloor \cdot d.$$

b. En un lenguaje de programación con una función de piso incorporada, *div* y *mod* se puede calcular de la siguiente manera:

$$a \; div \; d = \lfloor a/d \rfloor \quad \text{y} \quad a \; mod \; d = a - \lfloor a/d \rfloor \cdot d.$$

Reescriba los pasos del algoritmo 4.8.2 para un lenguaje computado con una función integrada de piso, pero sin *div* y *mod*.

24. Una alternativa para el algoritmo de Euclides usar la resta en lugar de la división para calcular máximos divisores comunes. (Después de todo, la división es una resta repetida). Se basa en el siguiente lema:

lema 4.8.3

Si $a \geq b > 0$, entonces $\text{mcd}(a, b) = \text{mcd}(b, a - b)$.

Algoritmo 4.8.3 Cálculo del mcd por sustracción

[Dados dos números enteros positivos A y B, las variables a y b son igual a A y B. Entonces comienza un proceso repetitivo. Si $a \neq 0$ y $b \neq 0$, entonces el mayor de a y b es igual a $a - b$ (si $a > b$) o $b - a$ (si $a < b$) y el más pequeño de a y b permanece sin cambios. Este proceso se repite una y otra vez hasta que finalmente a, b, o se convierte en 0. Por el lema 4.8.3, después de cada repetición del proceso,

$$\text{mcd}(A, B) = \text{mcd}(a, b)$$

Después de la última repetición,

$$\text{mcd}(A, B) = \text{mcd}(a, 0) \text{ o } \text{mcd}(A, B) = \text{mcd}(0, b)$$

depende de si a o b no es cero. Pero con el lema 4.8.1,

$$\text{mcd}(a, 0) = a \text{ y } \text{mcd}(0, b) = b.$$

Por tanto, después de la última repetición,

$\text{mcd}(A, B) = a$ si $a \neq 0$ o $\text{mcd}(A, B) = b$ si $b \neq 0$.*]*

Entrada: *A, B [enteros positivos]*

Cuerpo del algoritmo:

$a := A, b := B$
while $(a \neq 0$ y $b \neq 0)$
  if $a \geq b$ **then** $a := a - b$
    else $b := b - a$
end while
  if $a = 0$ **then** mcd $:= b$
  else mcd $:= a$

[Después de la ejecución de un enunciado **if-then-else**, mcd = mcd(A, B).*]*

Salida: mcd *[un entero positivo]*

a. Demuestre el lema 4.8.3.
b. Siga la ejecución del algoritmo 4.8.3 para $A = 630$ y $B = 336$.
c. Siga la ejecución del algoritmo 4.8.3 para $A = 768$ y $B = 348$.

Los ejercicios del 25 al 29 se refieren a la siguiente definición.

Definición: El **mínimo común múltiplo** de dos enteros diferentes de cero a y b, se denota por mcm(a, b), es el entero positivo c tal que

a. $a \mid c$ y $b \mid c$

b. para todos los enteros positivos m, si $a \mid m$ y $b \mid m$, entonces $c \leq m$.

25. Determine

a. mcm(12, 18) b. mcm($2^2 \cdot 3 \cdot 5$, $2^3 \cdot 3^2$)
c. mcm(2800, 6125)

26. Demostrar que para todos los enteros positivos a y b, mcd(a, b) = mcm(a, b) si y sólo si, $a = b$

27. Demostrar que para todos los enteros positivos a y b, $a \mid b$, si y sólo si, mcm(a, b) = b.

28. Demuestre que para todos los números enteros a y b, mcd(a, b) | mcm(a, b).

29. Demuestre que para todos los enteros positivos a y b, mcd(a, b) $\cdot$ mcm(a, b) = ab.

Respuestas del autoexamen

1. se evalúa la expresión e (utilizando los valores actuales de todas las variables en la expresión) y este valor se coloca en la posición de memoria correspondiente a x (que sustituye el contenido anterior de la posición) 2. El enunciado s_1 se ejecuta; el enunciado s_2 se ejecuta 3. todos los enunciados en el cuerpo del bucle se ejecutan en orden y después la ejecución se mueve de nuevo al principio del bucle y se repite el proceso, la ejecución pasa al siguiente enunciado del algoritmo siguiendo el bucle 4. los enunciados en el cuerpo del bucle se ejecutan en orden, la *variable* se incrementa en 1 y la ejecución regresa a la parte superior del bucle, la ejecución pasa al siguiente enunciado del algoritmo siguiendo el bucle 5. enteros q y r con la propiedad de que $n = dq + r$ y $0 \leq r < d$ 6. d divide tanto a a como b, si c es un divisor común de a y b, entonces $c \leq d$ 7. r 8. mcd(b, r) 9. el máximo común divisor de A y B (O: mcd(A, B))

CAPÍTULO 5

SUCESIONES, INDUCCIÓN MATEMÁTICA Y RECURRENCIA

Una de las tareas más importantes de las matemáticas es descubrir y caracterizar patrones regulares, tales como los relacionados con los procesos que se repiten. La principal estructura matemática que se utiliza en el estudio de los procesos que se repiten es la *sucesión* y la principal herramienta matemática que se usa para comprobar suposiciones acerca de las sucesiones es la *inducción matemática*. En este capítulo se introduce la notación y terminología de las sucesiones, se muestra cómo utilizar tanto la inducción matemática común como la fuerte para demostrar propiedades de las sucesiones, se ilustra cómo surgen diversas formas de sucesiones definidas recursivamente, se describe un método para obtener una fórmula explícita para una sucesión definida de forma recursiva y se explica cómo comprobar la exactitud de esa fórmula. También analizamos un principio, el principio del buen orden de los números enteros que es lógicamente equivalente a las dos formas de inducción matemática y mostramos cómo adaptar la inducción matemática para demostrar la exactitud de los algoritmos de computadora. En la última sección se analizan definiciones recursivas más generales, como la que se utiliza para la formulación cuidadosa del concepto de expresión booleana y de la idea de función recursiva.

5.1 Sucesiones

Un matemático, es como un pintor o poeta, es un fabricante de patrones.
—G. H. Hardy, *A mathematician's Apology*, 1940

Imagine que una persona decide contar sus antepasados. Él tiene dos padres, cuatro abuelos, ocho bisabuelos y así sucesivamente, estos números se pueden escribir en un renglón como

$$2, 4, 8, 16, 32, 64, 128, \ldots$$

El símbolo "..." se llama *puntos suspensivos*. Es la abreviatura de "y así sucesivamente".

Para expresar el patrón de los números, suponga que cada uno está etiquetado por un entero que indica su posición en el renglón.

Posición en el renglón	1	2	3	4	5	6	7...
Número de antepasados	2	4	8	16	32	64	128...

El número correspondiente a la posición 1 es 2, lo que equivale a 2^1. El número correspondiente a la posición 2 es 4, lo que equivale a 2^2. Para las posiciones 3, 4, 5, 6 y 7, los números

correspondientes 8, 16, 32, 64 y 128, son iguales a 2^3, 2^4, 2^5, 2^6 y 2^7, respectivamente. Para un valor general de k, sea A_k el número de antepasados en la k-ésima generación. El patrón de los valores calculados sugiere lo siguiente para cada k:

$$A_k = 2^k.$$

Nota Estrictamente hablando el verdadero valor de A_k es menor que 2^k cuando k es grande ya que los antepasados que provienen de una rama del árbol genealógico pueden presentarse en otras ramas del árbol.

• Definición

Una **sucesión** es una función cuyo dominio es ya sean todos los enteros entre dos enteros dados o todos los enteros mayores o iguales a un entero dado.

En general representamos una sucesión como un conjunto de elementos escritos en un renglón. En la sucesión que se denota por

$$a_m, a_{m+1}, a_{m+2}, \ldots, a_n,$$

cada elemento individual de a_k (que se lee "a subíndice k") se llama un **término**. La k en a_k se llama un **subíndice** o **índice**, m (que puede ser cualquier entero) es el subíndice del **término inicial** y n (que debe ser mayor o igual a m) es el subíndice del **término final**. La notación

$$a_m, a_{m+1}, a_{m+2}, \ldots$$

denota una **sucesión infinita**. Una **fórmula explícita** o **fórmula general** para una sucesión es una regla que muestra cómo los valores de a_k dependen de k.

El siguiente ejemplo muestra que es posible que dos fórmulas diferentes den sucesiones con los mismos términos.

Ejemplo 5.1.1 Determinación de términos de sucesiones dadas con fórmulas explícitas

Defina las sucesiones de $a_1, a_2, a_3, \ldots$ y $b_2, b_3, b_4, \ldots$ con las siguientes fórmulas explícitas:

$$a_k = \frac{k}{k+1} \quad \text{para todo entero } k \geq 1,$$

$$b_i = \frac{i-1}{i} \quad \text{para todo entero } i \geq 2.$$

Calcule los cinco primeros términos de ambas sucesiones.

Solución

$$a_1 = \frac{1}{1+1} = \frac{1}{2} \qquad b_2 = \frac{2-1}{2} = \frac{1}{2}$$

$$a_2 = \frac{2}{2+1} = \frac{2}{3} \qquad b_3 = \frac{3-1}{3} = \frac{2}{3}$$

$$a_3 = \frac{3}{3+1} = \frac{3}{4} \qquad b_4 = \frac{4-1}{4} = \frac{3}{4}$$

$$a_4 = \frac{4}{4+1} = \frac{4}{5} \qquad b_5 = \frac{5-1}{5} = \frac{4}{5}$$

$$a_5 = \frac{5}{5+1} = \frac{5}{6} \qquad b_6 = \frac{6-1}{6} = \frac{5}{6}$$

Como puede ver, los primeros términos de ambas sucesiones son $\frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{5}{6}$; de hecho, se puede demostrar que todos los términos de ambas sucesiones son idénticos. ■

El siguiente ejemplo muestra que una sucesión infinita puede tener un número finito de valores.

Ejemplo 5.1.2 Una sucesión alternante

Calcule los seis primeros términos de la sucesión $c_0, c_1, c_2, \ldots$ que se definen de la siguiente manera:

$$c_j = (-1)^j \quad \text{para todo entero } j \geq 0.$$

Solución

$$\begin{aligned} c_0 &= (-1)^0 = 1 \\ c_1 &= (-1)^1 = -1 \\ c_2 &= (-1)^2 = 1 \\ c_3 &= (-1)^3 = -1 \\ c_4 &= (-1)^4 = 1 \\ c_5 &= (-1)^5 = -1 \end{aligned}$$

Así, los seis primeros términos son $1, -1, 1, -1, 1, -1$. En los ejercicios 33 y 34 de la sección 4.1, las potencias pares de -1 son iguales a 1 y las potencias impares de -1 son iguales a -1. Por lo que se tiene que la sucesión oscila sin fin entre 1 y -1. ■

En los ejemplos 5.1.1 y 5.1.2 la tarea fue calcular los primeros valores de una sucesión dada por una fórmula explícita. El siguiente ejemplo trata la cuestión de cómo encontrar una fórmula explícita para una sucesión con términos iniciales dados. Cualquiera de estas fórmulas es una suposición, pero es muy útil poder hacer tales suposiciones.

Ejemplo 5.1.3 Determinación de una fórmula explícita para ajustar los términos iniciales dados

Encuentre una fórmula explícita para una sucesión que tiene los siguientes términos iniciales:

$$1, \quad -\frac{1}{4}, \quad \frac{1}{9}, \quad -\frac{1}{16}, \quad \frac{1}{25}, \quad -\frac{1}{36}, \ldots.$$

Solución Denote el término general de la sucesión con a_k y suponga que el primer término es a_1. Entonces se observa que el denominador de cada término es un cuadrado perfecto. Así, los términos se pueden reescribir como

$$\begin{array}{cccccc} \dfrac{1}{1^2}, & \dfrac{(-1)}{2^2}, & \dfrac{1}{3^2}, & \dfrac{(-1)}{4^2}, & \dfrac{1}{5^2}, & \dfrac{(-1)}{6^2}. \\ \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \updownarrow \\ a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \end{array}$$

Observe que el denominador de cada término es igual al cuadrado del subíndice de ese término y que el numerador es igual a ± 1. Por tanto

$$a_k = \frac{\pm 1}{k^2}.$$

También el numerador oscila hacia atrás y hacia adelante entre $+1$ y -1; es $+1$ cuando k es impar y -1 cuando k es par. Para lograr esta oscilación, se introduce un factor de $(-1)^{k+1}$ (o $(-1)^{k-1}$) en la fórmula para a_k. *[Cuando k es impar, $k+1$ es par y por tanto $(-1)^{k+1} = 1$ y cuando k es par, $k+1$ es impar y por tanto $(-1)^{k+1} = -1$.]* Por tanto, una fórmula explícita que da los primeros seis términos correctos es

$$a_k = \frac{(-1)^{k+1}}{k^2} \quad \text{para todo entero } k \geq 1.$$

¡Precaución! También es posible que dos sucesiones comiencen con el mismo valor inicial pero que después diverjan. Vea el ejercicio 5 del final de esta sección.

Observe que calcular el primer término a_0 habría conducido a la fórmula alternativa

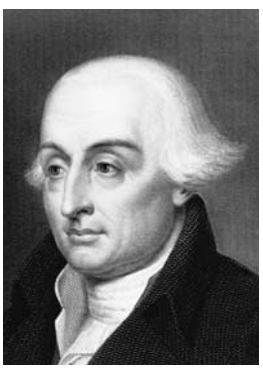
$$a_k = \frac{(-1)^k}{(k+1)^2} \quad \text{para todo entero } k \geq 0.$$

Debe comprobar que esta fórmula también da los primeros seis términos correctos. ■

Notación de suma

Consideremos de nuevo el ejemplo en el que $A_k = 2^k$ representa el número de antepasados que tiene una persona en la k-ésima generación. ¿Cuál es el número total de antepasados de las últimas seis generaciones? La respuesta es

$$A_1 + A_2 + A_3 + A_4 + A_5 + A_6 = 2^1 + 2^2 + 2^3 + 2^4 + 2^5 + 2^6 = 126.$$



CORBIS

Joseph Louis Lagrange (1736-1813)

Es conveniente utilizar una notación abreviada para escribir dichas sumas. En 1772 el matemático francés Joseph Louis Lagrange presentó la letra griega sigma mayúscula, Σ, para denotar la palabra *suma* y definió la notación de suma de la siguiente manera:

• Definición

Si m y n son números enteros y $m \leq n$, el símbolo $\sum_{k=m}^{n} a_k$, se lee como la **suma desde *k* igual a *m* a *n* de *a* subíndice *k***, es la suma de todos los términos de a_m, a_{m+1}, $a_{m+2}, \ldots a_n$. Decimos que $a_m + a_{m+1} + a_{m+2} + \ldots + a_n$ es la **forma desarrollada** de la suma y se escribe como

$$\sum_{k=m}^{n} a_k = a_m + a_{m+1} + a_{m+2} + \cdots + a_n.$$

Llamamos a k al **índice** de la suma, a m al **límite inferior** de la suma y a n el **límite superior** de la suma.

Ejemplo 5.1.4 Cálculo de sumas

Sean $a_1 = -2$, $a_2 = -1$, $a_3 = 0$, $a_4 = 1$ y $a_5 = 2$. Calcule las sumas siguientes:

a. $\sum_{k=1}^{5} a_k$ b. $\sum_{k=2}^{2} a_k$ c. $\sum_{k=1}^{2} a_{2k}$

Solución

a. $\sum_{k=1}^{5} a_k = a_1 + a_2 + a_3 + a_4 + a_5 = (-2) + (-1) + 0 + 1 + 2 = 0$

b. $\sum_{k=2}^{2} a_k = a_2 = -1$

c. $\sum_{k=1}^{2} a_{2k} = a_{2\cdot 1} + a_{2\cdot 2} = a_2 + a_4 = -1 + 1 = 0$ ■

Muchas veces, los términos de una suma se expresan usando una fórmula explícita. Por ejemplo, es común ver a las sumas tales como

$$\sum_{k=1}^{5} k^2 \quad \text{o} \quad \sum_{i=0}^{8} \frac{(-1)^i}{i+1}.$$

Ejemplo 5.1.5 Cuando los términos de la suma están dados por una fórmula

Calcule la suma siguiente:

$$\sum_{k=1}^{5} k^2.$$

Solución

$$\sum_{k=1}^{5} k^2 = 1^2 + 2^2 + 3^2 + 4^2 + 5^2 = 55.$$ ■

Cuando el límite superior de la suma es una variable, se utilizan puntos suspensivos para escribir la suma en forma desarrollada.

Ejemplo 5.1.6 Cambio de la notación de suma a la forma desarrollada

Escriba la siguiente suma en forma desarrollada:

$$\sum_{i=0}^{n} \frac{(-1)^i}{i+1}.$$

Solución

$$\begin{aligned}\sum_{i=0}^{n} \frac{(-1)^i}{i+1} &= \frac{(-1)^0}{0+1} + \frac{(-1)^1}{1+1} + \frac{(-1)^2}{2+1} + \frac{(-1)^3}{3+1} + \cdots + \frac{(-1)^n}{n+1} \\ &= \frac{1}{1} + \frac{(-1)}{2} + \frac{1}{3} + \frac{(-1)}{4} + \cdots + \frac{(-1)^n}{n+1} \\ &= 1 - \frac{1}{2} + \frac{1}{3} - \frac{1}{4} + \cdots + \frac{(-1)^n}{n+1}\end{aligned}$$ ■

Ejemplo 5.1.7 Cambio de la forma desarrollada a la notación de suma

Exprese la siguiente suma usando notación de suma:

$$\frac{1}{n} + \frac{2}{n+1} + \frac{3}{n+2} + \cdots + \frac{n+1}{2n}.$$

Solución El término general de esta suma se puede expresar como $\frac{k+1}{n+k}$ para enteros k de 0 a n. Por tanto

$$\frac{1}{n} + \frac{2}{n+1} + \frac{3}{n+2} + \cdots + \frac{n+1}{2n} = \sum_{k=0}^{n} \frac{k+1}{n+k}.$$ ■

Para valores pequeños de n, la forma desarrollada de una suma puede parecer ambigua. Por ejemplo, considere

$$1^2 + 2^2 + 3^2 + \cdots + n^2.$$

Esta expresión intenta representar la suma de cuadrados de números enteros consecutivos comenzando con 1^2 y terminando con n^2. Por tanto, si $n = 1$ la suma es exactamente 1^2, si $n = 2$, la suma es $1^2 + 2^2$ y si $n = 3$, la suma es $1^2 + 2^2 + 3^2$.

Ejemplo 5.1.8 Evaluación de $a_1, a_2, a_3, \ldots, a_n$ para n pequeñas

¿Cuál es el valor de la expresión $\dfrac{1}{1\cdot 2}+\dfrac{1}{2\cdot 3}+\dfrac{1}{3\cdot 4}+\cdots+\dfrac{1}{n\cdot(n+1)}$ cuando $n=1$? $n=2$? $n=3$?

¡Precaución! No escriba que para $n=1$, la suma es $\dfrac{1}{1\cdot 2}+\dfrac{1}{2\cdot 3}+\dfrac{1}{3\cdot 4}+\cdots+\dfrac{1}{1\cdot 2}$. Esta tachado porque es incorrecto.

Solución

Cuando $n=1$, la expresión es igual a $\dfrac{1}{1\cdot 2}=\dfrac{1}{2}$.

Cuando $n=2$, es igual a $\dfrac{1}{1\cdot 2}+\dfrac{1}{2\cdot 3}=\dfrac{1}{2}+\dfrac{1}{6}=\dfrac{2}{3}$.

Cuando $n=3$, es igual a $\dfrac{1}{1\cdot 2}+\dfrac{1}{2\cdot 3}+\dfrac{1}{3\cdot 4}=\dfrac{1}{2}+\dfrac{1}{6}+\dfrac{1}{12}=\dfrac{3}{4}$. ■

Una definición matemática más precisa de la suma, llamada una *definición recursiva*, es la siguiente:* Si m es cualquier entero, entonces

$$\sum_{k=m}^{m} a_k = a_m \qquad \text{y} \qquad \sum_{k=m}^{n} a_k = \sum_{k=m}^{n-1} a_k + a_n \quad \text{para todo entero } n > m.$$

Cuando se resuelven problemas, con frecuencia es útil reescribir una suma usando la forma recursiva de la definición ya sea separando el término final de una suma o agregando un término final a una suma.

Ejemplo 5.1.9 Separación de un término final y suma de un término final

a. Rescriba $\displaystyle\sum_{i=1}^{n+1}\frac{1}{i^2}$ separando el término final.

b. Escriba $\displaystyle\sum_{k=0}^{n} 2^k + 2^{n+1}$ como una única suma.

Solución

a. $\displaystyle\sum_{i=1}^{n+1}\frac{1}{i^2}=\sum_{i=1}^{n}\frac{1}{i^2}+\frac{1}{(n+1)^2}$ b. $\displaystyle\sum_{k=0}^{n} 2^k + 2^{n+1}=\sum_{k=0}^{n+1} 2^k$ ■

En determinadas sumas cada término es una diferencia de dos cantidades. Cuando escriba tales sumas en forma desarrollada, a veces verá que todos los términos se eliminan excepto el primero y el último. La eliminación sucesiva de términos colapsa a una suma telescópica.

Ejemplo 5.1.10 Una suma telescópica

Algunas cantidades se pueden transformar a sumas telescópicas, que se pueden reescribir como una simple expresión. Por ejemplo, observe que

$$\frac{1}{k}-\frac{1}{k+1}=\frac{(k+1)-k}{k(k+1)}=\frac{1}{k(k+1)}.$$

Use esta identidad para encontrar una expresión simple para $\displaystyle\sum_{k=1}^{n}\frac{1}{k(k+1)}$.

*Otras sucesiones definidas recursivamente se tratan más adelante en esta sección y, con mayor detalle, en la sección 5.6.

Solución

$$\sum_{k=1}^{n} \frac{1}{k(k+1)} = \sum_{k=1}^{n} \left(\frac{1}{k} - \frac{1}{k+1} \right)$$
$$= \left(\frac{1}{1} - \frac{1}{2} \right) + \left(\frac{1}{2} - \frac{1}{3} \right) + \left(\frac{1}{3} - \frac{1}{4} \right) + \cdots + \left(\frac{1}{n-1} - \frac{1}{n} \right) + \left(\frac{1}{n} - \frac{1}{n+1} \right)$$
$$= 1 - \frac{1}{n+1}.$$

■

Notación de producto

La notación del producto de una sucesión de números es análoga a la notación de la suma. La letra mayúscula griega pi, Π, denota un producto. Por ejemplo,

$$\prod_{k=1}^{5} a_k = a_1 a_2 a_3 a_4 a_5.$$

• Definición

Si m y n son enteros y $m \leq n$, el símbolo $\prod_{k=m}^{n} a_k$ se lee como la **forma de producto de *k* es igual a *m* a *n* de *a* subíndice *k***, es el producto de todos los términos, a_m, a_{m+1}, a_{m+2}, ..., a_n. Se escribe

$$\prod_{k=m}^{n} a_k = a_m \cdot a_{m+1} \cdot a_{m+2} \cdots a_n.$$

Una definición recursiva de la notación del producto es la siguiente: Si m es cualquier entero, entonces

$$\prod_{k=m}^{m} a_k = a_m \qquad \text{y} \qquad \prod_{k=m}^{n} a_k = \left(\prod_{k=m}^{n-1} a_k \right) \cdot a_n \quad \text{para todo entero } n > m.$$

Ejemplo 5.1.11 Cálculo de productos

Calcule los siguientes productos:

a. $\prod_{k=1}^{5} k$ b. $\prod_{k=1}^{1} \frac{k}{k+1}$

Solución

a. $\prod_{k=1}^{5} k = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 120$ b. $\prod_{k=1}^{1} \frac{k}{k+1} = \frac{1}{1+1} = \frac{1}{2}$

■

Propiedades de sumas y productos

El teorema siguiente establece las propiedades generales de sumas y productos. En la sección 5.6 se analiza la demostración del teorema.

Teorema 5.1.1

Si $a_m, a_{m+1}, a_{m+2}, \ldots$ y $b_m, b_{m+1}, b_{m+2}, \ldots$, son sucesiones de números reales y c es cualquier número real, entonces las ecuaciones siguientes valen para cualquier entero $n \geq m$:

1. $\displaystyle\sum_{k=m}^{n} a_k + \sum_{k=m}^{n} b_k = \sum_{k=m}^{n} (a_k + b_k)$
2. $\displaystyle c \cdot \sum_{k=m}^{n} a_k = \sum_{k=m}^{n} c \cdot a_k$ ley distributiva generalizada
3. $\displaystyle \left(\prod_{k=m}^{n} a_k\right) \cdot \left(\prod_{k=m}^{n} b_k\right) = \prod_{k=m}^{n} (a_k \cdot b_k).$

Ejemplo 5.1.12 Uso de propiedades de sumas y productos

Sea $a_k = k + 1$ y $b_k = k - 1$ para todo entero k. Escriba cada una de las siguientes expresiones como una suma o un producto:

a. $\displaystyle\sum_{k=m}^{n} a_k + 2 \cdot \sum_{k=m}^{n} b_k$ b. $\displaystyle \left(\prod_{k=m}^{n} a_k\right) \cdot \left(\prod_{k=m}^{n} b_k\right)$

Solución

a.
$$\begin{aligned}
\sum_{k=m}^{n} a_k + 2 \cdot \sum_{k=m}^{n} b_k &= \sum_{k=m}^{n} (k+1) + 2 \cdot \sum_{k=m}^{n} (k-1) && \text{por sustitución} \\
&= \sum_{k=m}^{n} (k+1) + \sum_{k=m}^{n} 2 \cdot (k-1) && \text{por el teorema 5.1.1 (2)} \\
&= \sum_{k=m}^{n} ((k+1) + 2 \cdot (k-1)) && \text{por el teorema 5.1.1 (1)} \\
&= \sum_{k=m}^{n} (3k-1) && \text{por simplificación algebraica}
\end{aligned}$$

b.
$$\begin{aligned}
\left(\prod_{k=m}^{n} a_k\right) \cdot \left(\prod_{k=m}^{n} b_k\right) &= \left(\prod_{k=m}^{n} (k+1)\right) \cdot \left(\prod_{k=m}^{n} (k-1)\right) && \text{por sustitución} \\
&= \prod_{k=m}^{n} (k+1) \cdot (k-1) && \text{por el teorema 5.1.1 (3)} \\
&= \prod_{k=m}^{n} (k^2 - 1) && \text{por simplificación algebraica}
\end{aligned}$$

■

Cambio de variable

Observe que
$$\sum_{k=1}^{3} k^2 = 1^2 + 2^2 + 3^2$$

y también que
$$\sum_{i=1}^{3} i^2 = 1^2 + 2^2 + 3^2.$$

Por tanto $$\sum_{k=1}^{3} k^2 = \sum_{i=1}^{3} i^2.$$

Esta ecuación muestra el hecho de que el símbolo utilizado para representar el índice de una suma se puede sustituir por algún otro símbolo, siempre que la sustitución se haga en cada lugar donde se presente el símbolo. En consecuencia, el índice de una suma se llama una variable muda. Una **variable muda** es un símbolo que deduce su significado completo en su contexto local. Fuera de este contexto (tanto antes como después), el símbolo puede tener otro significado completamente diferente.

La apariencia de una suma también se puede alterar por cambios más complicados de la variable. Por ejemplo, observe que

$$\begin{aligned}\sum_{j=2}^{4}(j-1)^2 &= (2-1)^2 + (3-1)^2 + (4-1)^2 \\ &= 1^2 + 2^2 + 3^2 \\ &= \sum_{k=1}^{3} k^2.\end{aligned}$$

En el ejemplo 5.1.13 se presenta un procedimiento general para transformar la primera suma en la segunda.

Ejemplo 5.1.13 Transformación de una suma con un cambio de variable

Transforme la siguiente suma haciendo el cambio de variable dado.

$$\textit{suma: } \sum_{k=0}^{6} \frac{1}{k+1} \qquad \textit{cambio de variable: } j = k+1$$

Solución Primero calcule los límites inferior y superior de la nueva suma:

$$\begin{aligned}&\text{Cuando } k = 0, \quad j = k+1 = 0+1 = 1.\\ &\text{Cuando } k = 6, \quad j = k+1 = 6+1 = 7.\end{aligned}$$

Así, la nueva suma va de $j = 1$ a $j = 7$.

Después calcule el término general de la nueva suma. Necesita sustituir cada k con una expresión de j:

$$\begin{aligned}&\text{Ya que } j = k+1, \text{ entonces } k = j-1.\\ &\text{Por tanto } \frac{1}{k+1} = \frac{1}{(j-1)+1} = \frac{1}{j}.\end{aligned}$$

Por último, sustituya todos los pasos para obtener

$$\sum_{k=0}^{6} \frac{1}{k+1} = \sum_{j=1}^{7} \frac{1}{j}. \qquad 5.1.1$$

■

La ecuación (5.1.1) puede dar un giro adicional al indicar que, j en la suma de la derecha es una variable muda, que se puede sustituir con cualquier otro nombre de variable,

siempre y cuando se realice la sustitución para todas las j. En particular, es legal sustituir k por j para obtener

$$\sum_{j=1}^{7} \frac{1}{j} = \sum_{k=1}^{7} \frac{1}{k}. \tag{5.1.2}$$

Poniendo juntas las ecuaciones (5.1.1) y (5.1.2) se obtiene

$$\sum_{k=0}^{6} \frac{1}{k+1} = \sum_{k=1}^{7} \frac{1}{k}.$$

A veces es necesario cambiar los límites de una suma sumándoles otro. Un ejemplo es la demostración algebraica del teorema del binomio, que se presenta en la sección 9.7. En el siguiente ejemplo se muestra un procedimiento general para hacer ese corrimiento cuando el límite superior es parte del sumando.

Ejemplo 5.1.14 Cuando el límite superior se presenta en la expresión, que se está sumando

a. Transforme la siguiente suma haciendo el cambio de variable dado.

$$\textit{suma: } \sum_{k=1}^{n+1} \left(\frac{k}{n+k} \right) \qquad \textit{cambio de variable: } j = k - 1$$

b. Transforme la suma obtenida en el inciso *a*) cambiando todas las j por k.

Solución

a. Cuando $k = 1$, entonces $j = k - 1 = 1 - 1 = 0$. (Así el nuevo límite inferior es 0). Cuando $k = n + 1$, entonces $j = k - 1 = (n + 1) - 1 = n$. (Así el nuevo límite superior es n).

Puesto que $j = k - 1$, entonces $k = j + 1$. También observe que n es una constante en todos los términos de la suma. De lo que se deduce que

$$\frac{k}{n+k} = \frac{j+1}{n+(j+1)}$$

por lo que el término general de la nueva suma es

$$\frac{j+1}{n+(j+1)}.$$

Por tanto,

$$\sum_{k=1}^{n+1} \frac{k}{n+k} = \sum_{j=0}^{n} \frac{j+1}{n+(j+1)}. \tag{5.1.3}$$

b. Cambiando todas las j por k en el lado derecho de la ecuación (5.1.3) se obtiene

$$\sum_{j=0}^{n} \frac{j+1}{n+(j+1)} = \sum_{k=0}^{n} \frac{k+1}{n+(k+1)} \tag{5.1.4}$$

Combinando las ecuaciones (5.1.3) y (5.1.4) resulta que

$$\sum_{k=1}^{n+1} \frac{k}{n+k} = \sum_{k=0}^{n} \frac{k+1}{n+(k+1)}.$$

■

Notación factorial y de "n se selecciona r"

El producto de todos los enteros consecutivos hasta un entero dado se produce con tanta frecuencia en las matemáticas que se le da una notación especial: notación *factorial*.

• Definición

Para cada entero positivo n, la cantidad ***n* factorial** que se denota por $\boldsymbol{n!}$, se define como el producto de todos los enteros de 1 a n.

$$n! = n \cdot (n-1) \cdots 3 \cdot 2 \cdot 1.$$

Cero factorial, que se denota por 0!, se define como 1:

$$0! = 1.$$

La definición de cero factorial como 1 puede parecer extraño, pero, como verá cuando lea el capítulo 9, es conveniente para muchas fórmulas matemáticas.

Ejemplo 5.1.15 Los diez primeros factoriales

$$\begin{aligned} 0! &= 1 & 1! &= 1 \\ 2! &= 2 \cdot 1 = 2 & 3! &= 3 \cdot 2 \cdot 1 = 6 \\ 4! &= 4 \cdot 3 \cdot 2 \cdot 1 = 24 & 5! &= 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 120 \\ 6! &= 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 720 & 7! &= 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 5040 \\ 8! &= 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 & 9! &= 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \\ &= 40\,320 & &= 362\,880 \end{aligned}$$

■

Como puede ver en el ejemplo anterior, los valores de $n!$ crecen muy rápidamente. Por ejemplo, $40! \cong 8.16 \times 10^{47}$, que es un número demasiado grande para ser calculado con exactitud utilizando la aritmética común de enteros de las implementaciones específicas de máquina de los lenguajes de computadoras. (El símbolo $\cong$ significa "es aproximadamente igual a").

Una definición recursiva de factorial es la siguiente: Dado un entero no negativo n,

$$n! = \begin{cases} 1 & \text{si } n = 0 \\ n \cdot (n-1)! & \text{si } n \geq 1. \end{cases}$$

¡Precaución! Observe que $n \cdot (n-1)!$ debe interpretarse como $n \cdot [(n-1)!]$.

El siguiente ejemplo muestra la utilidad de la definición recursiva para hacer cálculos.

Ejemplo 5.1.16 Cálculo con factoriales

Simplifique las siguientes expresiones:

a. $\dfrac{8!}{7!}$ b. $\dfrac{5!}{2! \cdot 3!}$ c. $\dfrac{1}{2! \cdot 4!} + \dfrac{1}{3! \cdot 3!}$ d. $\dfrac{(n+1)!}{n!}$ e. $\dfrac{n!}{(n-3)!}$

Solución

a. $\dfrac{8!}{7!} = \dfrac{8 \cdot \cancel{7!}}{\cancel{7!}} = 8$

b. $\dfrac{5!}{2! \cdot 3!} = \dfrac{5 \cdot 4 \cdot \cancel{3!}}{2! \cdot \cancel{3!}} = \dfrac{5 \cdot 4}{2 \cdot 1} = 10$

c. $$\frac{1}{2!\cdot 4!}+\frac{1}{3!\cdot 3!}=\frac{1}{2!\cdot 4!}\cdot\frac{3}{3}+\frac{1}{3!\cdot 3!}\cdot\frac{4}{4}$$ multiplicando cada numerador y cada denominador sólo por lo que es necesario para obtener un denominador común

$$=\frac{3}{3\cdot 2!\cdot 4!}+\frac{4}{3!\cdot 4\cdot 3!}$$ reordenando los factores

$$=\frac{3}{3!\cdot 4!}+\frac{4}{3!\cdot 4!}$$ ya que $3\cdot 2!=3!$ y $4\cdot 3!=4!$

$$=\frac{7}{3!\cdot 4!}$$ por la regla de suma de fracciones con un denominador común

$$=\frac{7}{144}$$

d. $$\frac{(n+1)!}{n!}=\frac{(n+1)\cdot n!}{n!}=n+1$$

e. $$\frac{n!}{(n-3)!}=\frac{n\cdot(n-1)\cdot(n-2)\cdot(n-3)!}{(n-3)!}=n\cdot(n-1)\cdot(n-2)$$
$$=n^3-3n^2+2n$$ ■

Un uso importante para la notación factorial es el cálculo de los valores de las cantidades, llamado *de n se seleccionan r*, que se presentan en muchas ramas de las matemáticas, especialmente en las relacionadas con el estudio de técnicas de conteo y probabilidad.

• Definición

Sean n y r enteros con $0\le r\le n$. El símbolo

$$\binom{n}{r}$$

se lee de **"n se seleccionan r"** y representa el número de subconjuntos de tamaño r que se pueden elegir de un conjunto con n elementos.

Observe que la definición implica que $\binom{n}{r}$ siempre será un número entero ya que es un número de subconjuntos. En la sección 9.5 vamos a explorar muchas aplicaciones de n se seleccionan r para resolver problemas que implican conteo y demostraremos la siguiente fórmula de cálculo:

• Fórmula para calcular $\binom{n}{r}$

Para todo entero n y r con $0\le r\le n$,

$$\binom{n}{r}=\frac{n!}{r!(n-r)!}.$$

Mientras tanto, presentamos algunas experiencias de su uso. Ya que de n se seleccionan r es siempre un número entero, puede estar seguro de que todos los factores en el denominador de la fórmula se eliminaran con factores del numerador. Muchas calculadoras electrónicas tienen teclas para calcular valores de $\binom{n}{r}$. Se denotan de diversas maneras tales como nCr, $C(n, r)$, ${}^nC_r$ y $C_{n,r}$. Se utiliza la letra C ya que las cantidades $\binom{n}{r}$ también se llaman *combinaciones*. A veces se conocen como *coeficientes binomiales* debido a su conexión con el teorema binomial que se analiza en la sección 9.7.

Ejemplo 5.1.17 Cálculo a mano de $\binom{n}{r}$

Use la fórmula para calcular $\binom{n}{r}$ para evaluar las siguientes expresiones:

a. $\binom{8}{5}$ b. $\binom{4}{0}$ c. $\binom{n+1}{n}$

Solución

a. $$\binom{8}{5} = \frac{8!}{5!(8-5)!}$$
$$= \frac{8\cdot 7\cdot \cancel{6}\cdot \cancel{5}\cdot \cancel{4}\cdot \cancel{3}\cdot \cancel{2}\cdot \cancel{1}}{(\cancel{5}\cdot \cancel{4}\cdot \cancel{3}\cdot \cancel{2}\cdot \cancel{1})\cdot(\cancel{3}\cdot \cancel{2}\cdot \cancel{1})}$$
$$= 56.$$

Siempre se eliminan los factores comunes antes de multiplicar

b. $$\binom{4}{4} = \frac{4!}{4!(4-4)!} = \frac{4!}{4!0!} = \frac{\cancel{4\cdot 3\cdot 2\cdot 1}}{\cancel{(4\cdot 3\cdot 2\cdot 1)}(1)} = 1$$

El hecho de que $0! = 1$ hace que esta fórmula sea calculable. Da el valor correcto ya que un conjunto de tamaño 4 tiene exactamente un subconjunto de tamaño 4, o sea el mismo.

c. $$\binom{n+1}{n} = \frac{(n+1)!}{n!((n+1)-n)!} = \frac{(n+1)!}{n!1!} = \frac{(n+1)\cdot \cancel{n!}}{\cancel{n!}} = n+1$$

■

Sucesiones en un programa de cómputo

Un tipo de datos importantes en la programación de la computadora consiste en sucesiones finitas. En contextos de programación de computadoras, éstos se refieren generalmente como *arreglos unidimensionales*. Por ejemplo, considere un programa que analiza los salarios pagados a una muestra de 50 trabajadores. Este programa puede calcular el promedio del salario y la diferencia entre los salarios de cada individuo y el promedio. Para esto sería necesario que cada salario se almacene en la memoria para su posterior recuperación en el cálculo. Para evitar el uso de nombres de variables totalmente independientes de todos los salarios de los 50, se escribe cada uno como un término de un arreglo unidimensional:

$$W[1], W[2], W[3], \ldots, W[50].$$

Observe que las etiquetas de los subíndices están escritas entre corchetes. La razón es que hasta hace relativamente poco, era realmente imposible escribir subíndices en la mayoría de los teclados de computadora.

La principal dificultad que tienen los programadores cuando utilizan arreglos unidimensionales es el mantenimiento correcto de las etiquetas.

Ejemplo 5.1.18 Variable muda en un bucle

La variable índice de un bucle **for-next** es una variable muda. Por ejemplo, todos los tres siguientes segmentos de algoritmo producen el mismo resultado:

1. **for** $i := 1$ **to** n
   print $a[i]$
   next i

2. **for** $j := 0$ **to** $n-1$
   print $a[j+1]$
   next j

3. **for** $k := 2$ **to** $n+1$
   print $a[k-1]$
   next k

■

Las definiciones recursivas para la suma, el producto y el factorial conducen naturalmente a los algoritmos computacionales. Por ejemplo, aquí hay dos conjuntos de pseudocódigo para encontrar la suma de $a[1], a[2], \ldots, a[n]$. El de la izquierda imita exactamente

la definición recursiva al inicializar la suma igual $a[1]$; el de la derecha inicializa la suma igual a 0. En ambos casos el resultado es $\sum_{k=1}^{n} a[k]$.

```
s := a[1]                    s := 0
for k := 2 to n              for k := 1 to n
    s := s + a[k]                s := s + a[k]
next k                       next k
```

Aplicación: algoritmo para convertir de la base 10 a la base 2 usando división repetida por 2

La sección 2.5 contiene algunos ejemplos de conversión de enteros de notación decimal a binaria. Sin embargo, el uso del método que se muestra allí, sólo es conveniente con un número pequeño. Un algoritmo sistemático para convertir cualquier número entero no negativo a la notación binaria utiliza división repetida entre 2.

Supongamos que a es un entero no negativo. Divida a entre 2 usando el teorema de cociente-residuo para obtener un cociente $q[0]$ y un residuo $r[0]$. Si el cociente es diferente de cero, se divide otra vez entre 2 para obtener un cociente $q[1]$ y un residuo $r[1]$. Continúe con este proceso hasta que se obtenga un cociente de 0. En cada etapa, el residuo debe ser menor que el divisor, que es 2. Así, cada residuo es 0 o 1. El proceso se muestra para $a =$ 38. (Lea las divisiones de abajo hacia arriba.)

	0	residuo $= 1 = r[5]$
2	1	residuo $= 0 = r[4]$
2	2	residuo $= 0 = r[3]$
2	4	residuo $= 1 = r[2]$
2	9	residuo $= 1 = r[1]$
2	19	residuo $= 0 = r[0]$
2	38	

Los resultados de todas estas divisiones se puede escribir como una sucesión de ecuaciones:

$$\begin{aligned} 38 &= 19\cdot 2 + 0,\\ 19 &= 9\cdot 2 + 1,\\ 9 &= 4\cdot 2 + 1,\\ 4 &= 2\cdot 2 + 0,\\ 2 &= 1\cdot 2 + 0,\\ 1 &= 0\cdot 2 + 1. \end{aligned}$$

Entonces, por sustitución repetida,

$$\begin{aligned} 38 &= 19\cdot 2 + 0\\ &= (9\cdot 2 + 1)\cdot 2 + 0 \;=\; 9\cdot 2^2 + 1\cdot 2 + 0\\ &= (4\cdot 2 + 1)\cdot 2^2 + 1\cdot 2 + 0 \;=\; 4\cdot 2^3 + 1\cdot 2^2 + 1\cdot 2 + 0\\ &= (2\cdot 2 + 0)\cdot 2^3 + 1\cdot 2^2 + 1\cdot 2 + 0\\ &= 2\cdot 2^4 + 0\cdot 2^3 + 1\cdot 2^2 + 1\cdot 2 + 0\\ &= (1\cdot 2 + 0)\cdot 2^4 + 0\cdot 2^3 + 1\cdot 2^2 + 1\cdot 2 + 0\\ &= 1\cdot 2^5 + 0\cdot 2^4 + 0\cdot 2^3 + 1\cdot 2^2 + 1\cdot 2 + 0. \end{aligned}$$

Observe que cada coeficiente de una potencia de 2 en el lado derecho de la página anterior es uno de los residuos obtenidos en la división repetida de 38 entre 2. Esto es verdadero para la mayoría de 1 de la izquierda, ya que así $1 = 0 \cdot 2 + 1$. Por tanto

$$38_{10} = 100110_2 = (r[5]r[4]r[3]r[2]r[1]r[0])_2.$$

En general, si un entero no negativo a es varias veces dividido entre 2 hasta que se obtiene un cociente de cero y los residuos que se encuentran son $r[0], r[1], \ldots, r[k]$, entonces por el teorema del cociente-residuo cada $r[i]$ es igual a 0 o 1 y por sustitución repetida del teorema,

$$a = 2^k \cdot r[k] + 2^{k-1} \cdot r[k-1] + \cdots + 2^2 \cdot r[2] + 2^1 \cdot r[1] + 2^0 \cdot r[0]. \qquad 5.1.5$$

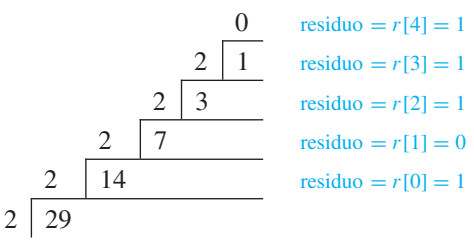
Así, en la ecuación (5.1.5) se puede leer la representación binaria de a:

$$a_{10} = (r[k]r[k-1]\cdots r[2]r[1]r[0])_2.$$

Ejemplo 5.1.19 Conversión de notación decimal a binaria usando división por 2 repetida

Use división repetida entre 2 para escribir el número 29_{10}, en notación binaria.

Solución



Por tanto $29_{10} = (r[4]r[3]r[2]r[1]r[0])_2 = 11101_2$. ■

El procedimiento que hemos descrito para la conversión de base 10 a base 2 se formaliza en el siguiente algoritmo:

Algoritmo 5.1.1 Conversión de decimal a binaria utilizando la división repetida por 2

[En el algoritmo 5.1.1 *la entrada es un entero no negativo n. El objetivo del algoritmo es producir una sucesión de dígitos binarios* $r[0], r[1], r[2], \ldots, r[k]$ *así la representación binaria de a es*

$$(r[k]r[k-1]\cdots r[2]r[1]r[0])_2.$$

Es decir,

$$n = 2^k \cdot r[k] + 2^{k-1} \cdot r[k-1] + \cdots + 2^2 \cdot r[2] + 2^1 \cdot r[1] + 2^0 \cdot r[0].]$$

continúa en la página 242

Entrada: *n[un número no negativo]*
Cuerpo del algoritmo:

$q := n, i := 0$
[Realice repetidamente la división entera de q entre 2 hasta que q se convierta en 0. Almacenando sucesivamente los residuos en un arreglo unidimensional $r[0], r[1], r[2], \ldots, r[k]$. *Aún si el valor inicial de q es igual a 0, el bucle debe ejecutarse una vez (por lo que se calcula* $r[0]$*). Así, la condición de protección para el bucle* **while** *es* $i = 0$ *o* $q \neq 0$.*]*

while ($i = 0$ o $q \neq 0$)
  $r[i] := q \ mod \ 2$
  $q := q \ div \ 2$
  [$r[i]$ *y q se puede obtener al llamar el algoritmo de la división].*
  $i := i + 1$
end while

[Después de la ejecución de este paso, los valores de $r[0], r[1], \ldots, r[i-1]$ *son todos 0 y 1 y* $a = (r[i-1]r[i-2]\cdots r[2]r[1]r[0])_2$.*]*

Salida: $r[0], r[1], r[2], \ldots, r[i-1]$ *[una sucesión de números enteros]*

Autoexamen

Las respuestas a las preguntas del autoexamen se encuentran al final de cada sección.

1. La notación $\sum_{k=m}^{n} a_k$ se lee como "_____".
2. La forma desarrollada de $\sum_{k=m}^{n} a_k$ es _____.
3. El valor de $a_1 + a_2 + a_3 + \cdots + a_n$ cuando $n = 2$ es "_____".
4. La notación $\prod_{k=m}^{n} a_k$ se lee "_____".
5. Si n es un entero positivo, entonces $n! =$ _____.
6. $\sum_{k=m}^{n} a_k + c\sum_{k=m}^{n} b_k =$ _____.
7. $\left(\prod_{k=m}^{n} a_k\right)\left(\prod_{k=m}^{n} b_k\right) =$ _____.

Conjunto de ejercicios 5.1*

Escriba los cuatro primeros términos de las sucesiones definidas por las fórmulas de los ejercicios 1 al 6.

1. $a_k = \dfrac{k}{10+k}$, para todo entero $k \geq 1$.
2. $b_j = \dfrac{5-j}{5+j}$, para todo entero $j \geq 1$.
3. $c_i = \dfrac{(-1)^i}{3^i}$, para todo entero $i \geq 0$.
4. $d_m = 1 + \left(\dfrac{1}{2}\right)^m$, para todo entero $m \geq 0$.
5. $e_n = \left\lfloor \dfrac{n}{2} \right\rfloor \cdot 2$, para todo entero $n \geq 0$.
6. $f_n = \left\lfloor \dfrac{n}{4} \right\rfloor \cdot 4$, para todo entero $n \geq 1$.
7. Sea $a_k = 2k + 1$ y $b_k = (k-1)^3 + k + 2$ para todo entero $k \geq 0$. Demuestre que los tres primeros términos de estas sucesiones son idénticos, pero que difieren en sus primeros cuatro términos.

Calcule los primeros quince términos de cada una de las sucesiones en los ejercicios 8 y 9; describa el comportamiento general de estas sucesiones de palabras. (En la sección 7.1 se da una definición del logaritmo).

8. $g_n = [\log_2 n]$ para todo entero $n \geq 1$.
9. $h_n = [\log_2 n]$ para todo entero $n \geq 1$.

*Para los ejercicios con números o letras azules, las soluciones están dadas en el apéndice B. El símbolo **H** indica que sólo se da una sugerencia o una solución parcial. El símbolo ✶ indica que el ejercicio es más difícil de lo normal.

Determine fórmulas explícitas para las sucesiones de la forma $a_1, a_2, a_3, \ldots$ con los términos iniciales que se dan en los ejercicios del 10 al 16.

10. $-1, 1, -1, 1, -1, 1$ **11.** $0, 1, -2, 3, -4, 5$

12. $\frac{1}{4}, \frac{2}{9}, \frac{3}{16}, \frac{4}{25}, \frac{5}{36}, \frac{6}{49}$

13. $1 - \frac{1}{2}, \frac{1}{2} - \frac{1}{3}, \frac{1}{3} - \frac{1}{4}, \frac{1}{4} - \frac{1}{5}, \frac{1}{5} - \frac{1}{6}, \frac{1}{6} - \frac{1}{7}$

14. $\frac{1}{3}, \frac{4}{9}, \frac{9}{27}, \frac{16}{81}, \frac{25}{243}, \frac{36}{729}$

15. $0, -\frac{1}{2}, \frac{2}{3}, -\frac{3}{4}, \frac{4}{5}, -\frac{5}{6}, \frac{6}{7}$

16. $3, 6, 12, 24, 48, 96$

✶ 17. Considere la sucesión definida por $a_n = \dfrac{2n + (-1)^n - 1}{4}$ para todo entero $n \geq 0$. Determine una fórmula alternativa explícita para a_n que utilice la notación de piso.

18. Sea $a_0 = 2$, $a_1 = 3$, $a_2 = -2$, $a_3 = 1$, $a_4 = 0$, $a_5 = -1$ y $a_6 = -2$. Calcule cada una de las siguientes sumas y productos.

a. $\sum_{i=0}^{6} a_i$ **b.** $\sum_{i=0}^{0} a_i$ **c.** $\sum_{j=1}^{3} a_{2j}$ **d.** $\prod_{k=0}^{6} a_k$ e. $\prod_{k=2}^{2} a_k$

Calcule las sumas y productos de los ejercicios 19 al 28.

19. $\sum_{k=1}^{5}(k+1)$ **20.** $\prod_{k=2}^{4} k^2$ 21. $\sum_{m=0}^{3} \frac{1}{2^m}$

22. $\prod_{j=0}^{4}(-1)^j$ **23.** $\sum_{i=1}^{1} i(i+1)$ 24. $\sum_{j=0}^{0}(j+1)\cdot 2^j$

25. $\prod_{k=2}^{2}\left(1 - \frac{1}{k}\right)$ 26. $\sum_{k=-1}^{1}(k^2+3)$

27. $\sum_{n=1}^{10}\left(\frac{1}{n} - \frac{1}{n+1}\right)$ 28. $\prod_{i=2}^{5} \frac{i(i+2)}{(i-1)\cdot(i+1)}$

Escriba las sumas de los ejercicios 29 al 32 en la forma desarrollada.

29. $\sum_{i=1}^{n}(-2)^i$ 30. $\sum_{j=1}^{n} j(j+1)$ **31.** $\sum_{k=0}^{n+1} \frac{1}{k!}$ 32. $\sum_{i=1}^{k+1} i(i!)$

Evalúe las sumas y productos de los ejercicios 33 al 36 para los valores indicados de la variable.

33. $\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \ldots + \frac{1}{n^2};\ n = 1$

34. $1(1!) + 2(2!) + 3(3!) + \ldots + m(m!);\ m = 2$

35. $\left(\frac{1}{1+1}\right)\left(\frac{2}{2+1}\right)\left(\frac{3}{3+1}\right)\cdots\left(\frac{k}{k+1}\right);\ k = 3$

36. $\left(\frac{1\cdot 2}{3\cdot 4}\right)\left(\frac{4\cdot 5}{6\cdot 7}\right)\left(\frac{6\cdot 7}{8\cdot 9}\right)\cdots\left(\frac{m\cdot(m+1)}{(m+2)\cdot(m+3)}\right);\ m = 1$

Reescriba los ejercicios 37 al 39 separando el término final.

37. $\sum_{i=1}^{k+1} i(i!)$ 38. $\sum_{k=1}^{m+1} k^2$ 39. $\sum_{m=1}^{n+1} m(m+1)$

Escriba cada uno de los ejercicios del 40 al 42 como una única suma.

40. $\sum_{i=1}^{k} i^3 + (k+1)^3$ 41. $\sum_{k=1}^{m} \frac{k}{k+1} + \frac{m+1}{m+2}$

42. $\sum_{m=0}^{n}(m+1)2^m + (n+2)2^{n+1}$

Escriba cada uno de los ejercicios del 43 al 52 usando notación de suma o de producto.

43. $1^2 - 2^2 + 3^2 - 4^2 + 5^2 - 6^2 + 7^2$

44. $(1^3 - 1) - (2^3 - 1) + (3^3 - 1) - (4^3 - 1) + (5^3 - 1)$

45. $(2^2 - 1)\cdot(3^2 - 1)\cdot(4^2 - 1)$

46. $\frac{2}{3\cdot 4} - \frac{3}{4\cdot 5} + \frac{4}{5\cdot 6} - \frac{5}{6\cdot 7} + \frac{6}{7\cdot 8}$

47. $1 - r + r^2 - r^3 + r^4 - r^5$

48. $(1-t)\cdot(1-t^2)\cdot(1-t^3)\cdot(1-t^4)$

49. $1^3 + 2^3 + 3^3 + \cdots + n^3$

50. $\frac{1}{2!} + \frac{2}{3!} + \frac{3}{4!} + \cdots + \frac{n}{(n+1)!}$

51. $n + (n-1) + (n-2) + \cdots + 1$

52. $n + \frac{n-1}{2!} + \frac{n-2}{3!} + \frac{n-3}{4!} + \cdots + \frac{1}{n!}$

Transforme cada uno de los ejercicios 53 y 54 haciendo el cambio de variable $i = k + 1$.

53. $\sum_{k=0}^{5} k(k-1)$ 54. $\prod_{k=1}^{n} \frac{k}{k^2+4}$

Transforme cada uno de los ejercicios 55 a 58, haciendo el cambio de variable

55. $\sum_{i=1}^{n+1} \frac{(i-1)^2}{i\cdot n}$ **56.** $\sum_{i=3}^{n} \frac{i}{i+n-1}$

57. $\sum_{i=1}^{n-1} \frac{i}{(n-i)^2}$ 58. $\prod_{i=n}^{2n} \frac{n-i+1}{n+i}$

Escriba cada uno de los ejercicios 59 al 61 como una suma o producto único.

59. $3\cdot\sum_{k=1}^{n}(2k-3) + \sum_{k=1}^{n}(4-5k)$

60. $2\cdot\sum_{k=1}^{n}(3k^2+4) + 5\cdot\sum_{k=1}^{n}(2k^2-1)$

61. $\left(\prod_{k=1}^{n} \frac{k}{k+1}\right)\cdot\left(\prod_{k=1}^{n} \frac{k+1}{k+2}\right)$

Calcule cada uno de los ejercicios del 62 al 76. Suponga que los valores de las variables están restringidos a que las expresiones estén definidas.

62. $\frac{4!}{3!}$ 63. $\frac{6!}{8!}$ 64. $\frac{4!}{0!}$

65. $\frac{n!}{(n-1)!}$ **66.** $\frac{(n-1)!}{(n+1)!}$ 67. $\frac{n!}{(n-2)!}$

68. $\dfrac{((n+1)!)^2}{(n!)^2}$ **69.** $\dfrac{n!}{(n-k)!}$ 70. $\dfrac{n!}{(n-k+1)!}$

71. $\binom{5}{3}$ 72. $\binom{7}{4}$ **73.** $\binom{3}{0}$

74. $\binom{5}{5}$ **75.** $\binom{n}{n-1}$ 76. $\binom{n+1}{n-1}$

77. **a.** Demuestre que $n! + 2$ es divisible por 2, para todo entero $n \geq 2$.
b. Demuestre que $n! + k$ es divisible por k, para todo entero $n \geq 2$ y $k = 2, 3, \ldots, n$.
H **c.** Dado cualquier entero $m \geq 2$, ¿es posible encontrar una sucesión de $m - 1$ de enteros positivos no consecutivos ninguno de los cuales es primo? Explique su respuesta.

78. Demuestre que para todos los enteros no negativos n y r con $r + 1 \leq n$, $\binom{n}{r+1} = \dfrac{n-r}{r+1}\binom{n}{r}$.

79. Demuestre que si p es un número primo y r es un número entero con $0 < r < p$ entonces $\binom{p}{r}$ es divisible por p.

80. Suponga que $a[1], a[2], a[3], \ldots, a[m]$ es un arreglo unidimensional y considere el siguiente segmento de algoritmo:

```
suma := 0
for k := 1 to m
    suma := suma + a[k]
next k
```

Complete los espacios en blanco para que cada segmento de algoritmo realice el mismo trabajo que el dado previamente.

a.
```
suma := 0
for i := 0 to _____
    suma := _____
next i
```

b.
```
suma := 0
for j := 2 to _____
    suma := _____
next j
```

Use la división repetida entre 2 para convertir (a mano) los enteros en los ejercicios 81 al 83 de la base 10 a base 2.

81. 90 82. 98 83. 205

Haga una tabla de seguimiento para trazar la acción del algoritmo 5.1.1 en la entrada de los ejercicios 84 al 86.

84. 23 85. 28 86. 44

87. Escriba una descripción informal de un algoritmo (usando división repetida entre 16) para convertir un entero no negativo de notación decimal a notación hexadecimal (base 16).

Utilice el algoritmo que desarrolló en el ejercicio 87 para convertir los números enteros en los ejercicios 88 al 90 a la notación hexadecimal.

88. 287 89. 693 90. 2301

91. Escriba una versión formal del algoritmo que desarrolló para el ejercicio 87.

Respuestas del autoexamen

1. la suma de k igual a m a n de a subíndice k 2. $a_m + a_{m+1} + a_{m+2} + \cdots + a_n$ 3. $a_1 + a_2$ 4. el producto de k igual a m a n de a subíndice k 5. $n \cdot (n-1) \cdots 3 \cdot 2 \cdot 1$ (O: $n \cdot (n-1)!$) 6. $\sum_{k=m}^{n} (a_k + cb_k)$ 7. $\prod_{k=m}^{n} a_k b_k$

5.2 Inducción matemática I

[La inducción matemática es] la técnica común de demostración en la ciencia computacional.
—Anthony Ralston, 1984

La inducción matemática es una de las técnicas de demostración de desarrollo más reciente en la historia de las matemáticas. Se utiliza para comprobar suposiciones acerca de los resultados de procesos que ocurren repetidamente y de acuerdo a patrones definidos. Se introduce la técnica con un ejemplo.

Algunas personas afirman que la moneda de un 1¢ en Estados Unidos es una pequeña moneda que debe ser abolida. Indican que, con frecuencia una persona que deja caer una moneda en el suelo ni siquiera se molesta en recogerla. Otras personas argumentan que la supresión de la moneda no daría la flexibilidad suficiente para los precios de las mercancías. ¿Qué precios podrían pagarse con el cambio exacto, si la moneda fuera abolida y se introdujera otra moneda de valor 3¢? La respuesta es que los únicos precios que no se podrían pagar con cambio exacto serían de 1¢, 2¢, 4¢ y 7¢. En otras palabras,

Cualquier número entero de centavos de menos de 8¢
se pueden obtener usando monedas de 3¢ y 5¢.

Más formalmente:

Para todo entero $n \geq 8$, se pueden obtener n centavos con monedas de 3¢ y 5¢.

Aún más formalmente:

> Para todo entero $n \geq 8$, $P(n)$ es verdadera, donde $P(n)$ es la frase de "se pueden obtener n centavos con monedas de $3¢$ y $5¢$".

Puede comprobar que $P(n)$ es verdadera para algunos valores dados de n, como se presenta en la tabla siguiente.

Número de centavos	¿Cómo obtenerlo?
$8¢$	$3¢ + 5¢$
$9¢$	$3¢ + 3¢ + 3¢$
$10¢$	$5¢ + 5¢$
$11¢$	$3¢ + 3¢ + 5¢$
$12¢$	$3¢ + 3¢ + 3¢ + 3¢$
$13¢$	$3¢ + 5¢ + 5¢$
$14¢$	$3¢ + 3¢ + 3¢ + 5¢$
$15¢$	$5¢ + 5¢ + 5¢$
$16¢$	$3¢ + 3¢ + 5¢ + 5¢$
$17¢$	$3¢ + 3¢ + 3¢ + 3¢ + 5¢$

Los casos que se muestran en la tabla proporcionan evidencia inductiva para apoyar la afirmación de que $P(n)$ es verdadera para n general. De hecho, $P(n)$ *es verdadera para* todo $n \geq 8$, *si y sólo si, es posible seguir llenando la tabla para valores arbitrariamente grandes de n.*

El renglón k-ésimo de la tabla proporciona información acerca de cómo obtener $k¢$, usando monedas de $3¢$ y $5¢$. Para continuar el siguiente renglón de la tabla, se deben dar instrucciones respecto a cómo obtener $(k + 1)¢$ usando monedas de $3¢$ y $5¢$. El secreto es observar en primer lugar que si se pueden obtener $k¢$ usando al menos una moneda de $5¢$, entonces se pueden obtener $(k + 1)¢$ sustituyendo la moneda de $5¢$ por dos monedas de $3¢$, como se muestra en la figura 5.2.1.

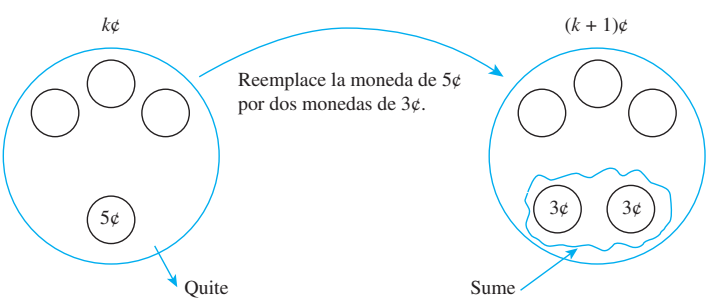


Figura 5.2.1

Si, por el contrario, se obtienen $k¢$ sin necesidad de utilizar una moneda de $5¢$, entonces sólo se utilizan las monedas de $3¢$. Y puesto que el total es de al menos $8¢$, se deben incluir tres o más monedas de $3¢$. Tres de las monedas de $3¢$ se pueden reemplazar con dos monedas de $5¢$ para obtener un total de $(k + 1)¢$, como se muestra en la figura 5.2.2.

La estructura del argumento anterior se puede resumir de la siguiente manera: Para demostrar que $P(n)$ es verdadera para todo entero $n \geq 8$, 1) muestre que $P(8)$ es verdadera y 2) muestre que la veracidad de $P(k + 1)$ es consecuencia necesariamente de la veracidad de $P(k)$ para cada $k \geq 8$.

Cualquier argumento de esta forma es un argumento por *inducción matemática*. En general, la inducción matemática es un método para demostrar que una propiedad definida para enteros n es verdadera para todos los valores de n que son mayores o iguales a algún entero inicial.

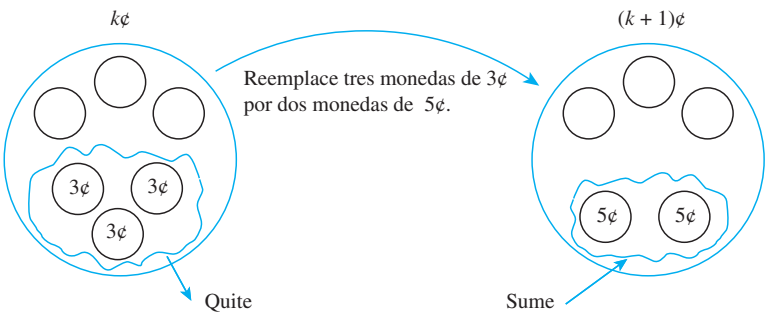


Figura 5.2.2

Principio de inducción matemática

Sea $P(n)$ una propiedad que se define para enteros n y sea a un entero fijo. Suponga que los siguientes dos enunciados son verdaderos:

1. $P(a)$ es verdadera.
2. Para todo entero $k \geq a$, si $P(k)$ es verdadera entonces $P(k + 1)$ es verdadera.

Entonces, el enunciado

$$\text{para todo entero } n \geq a,\ P(n)$$

es verdadero.

El primer uso conocido de la inducción matemática ocurrió en el trabajo del científico italiano Francesco Maurolico en 1575. En el siglo XVII tanto Pierre de Fermat como Blaise Pascal utilizaron la técnica, Fermat la llamó el "método de descenso infinito". En 1883 Augustus De Morgan (mejor conocido por las leyes de De Morgan) describió el proceso cuidadosamente y le dio el nombre de *inducción matemática*.

Para visualizar la idea de inducción matemática, imagine una colección infinita de fichas de dominó colocadas una detrás de la otra de tal manera que si alguna ficha de dominó cae hacia atrás, hace que la que está detrás caiga hacia atrás también. (Vea la figura 5.2.3.) Después imagine que la primera ficha de dominó se cae hacia atrás. ¿Qué sucede? . . . ¡Se caen todas!

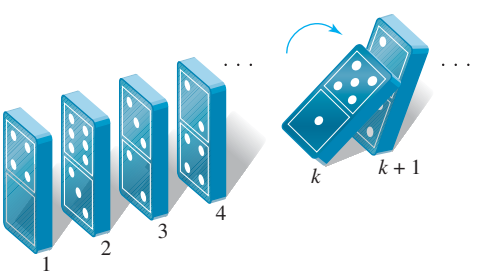


Figura 5.2.3 **Si la k-ésima ficha de dominó cae hacia atrás, también empuja a la $(k + 1)$-ésima ficha de dominó hacia atrás.**

Para ver la conexión entre esta imagen y el principio de inducción matemática, sea $P(n)$ la frase "La enésima ficha de dominó cae hacia atrás". Ésta está dada para cada $k \geq 1$, si $P(k)$ es verdadera (la k-ésima ficha de dominó cae hacia atrás), entonces $P(k + 1)$ también es verdadera (la $(k + 1)$ ficha de dominó cae hacia atrás). También es debido a que $P(1)$ es verdadera (la primera ficha de dominó se cae hacia atrás). Así, con el principio de inducción matemática, $P(n)$ (la enésima ficha de dominó cae hacia atrás) es verdadera para cada entero $n \geq 1$.

La validez de la demostración por inducción matemática generalmente se toma como un axioma. Esto es porque lo que se conoce como el *principio* de inducción matemática y no como un teorema. Es equivalente a la siguiente propiedad de los enteros, que es fácil de aceptar por razones intuitivas:

> Supongamos que S es un conjunto de enteros que satisface 1) $a \in S$, y 2) para todo entero $k \geq a$, si $k \in S$ entonces $k + 1 \in S$. Entonces S debe contener cada número entero mayor o igual que a.

Para entender la equivalencia de esta formulación y la dada anteriormente, sea exactamente S el conjunto de todos los enteros para los que $P(n)$ es verdadera.

Demostrar un enunciado con inducción matemática es un proceso de dos pasos. El primer paso se llama *paso básico* y el segundo paso se llama *paso inductivo*.

Método de demostración por inducción matemática

Considere un enunciado de la forma, "Para todo entero $n \geq a$, una propiedad $P(n)$ es verdadera". Para demostrar este enunciado, realice los siguientes pasos:

Paso 1 (paso básico): Demuestre que $P(a)$ es verdadera.

Paso 2 (paso inductivo): Demuestre que para todo entero $k \geq a$, si $P(k)$ es verdadera entonces $P(k + 1)$ es verdadera. Para realizar este paso,

> **suponga** que $P(k)$ es verdadera, donde k es cualquier entero dado pero elegido arbitrariamente con $k \geq a$.
> *[Esta suposición se llama* **hipótesis inductiva***.]*

Después,

> **demuestre** que $P(k + 1)$ es verdadera.

A continuación se presenta una versión formal de la demostración acerca de las monedas que previamente se desarrolló de manera informal.

Proposición 5.2.1

Para todo entero $n \geq 8$, $n¢$ se pueden obtener usando monedas de 3¢ y 5¢.

Demostración (por inducción matemática):

Sea la propiedad $P(n)$ la frase

$n¢$ se pueden obtener usando monedas de 3¢ y 5¢. ← $P(n)$

Demuestre que P(8) es verdadera:
$P(8)$ es verdadera porque 8¢ se pueden obtener usando una moneda de 3¢ y una moneda de 5¢.

Demuestre que para todo entero $k \geq 8$, si $P(k)$ es verdadera entonces $P(k + 1)$ también es verdadera:
[Suponga que $P(k)$ es verdadera para un entero dado, pero elegido arbitrariamente $k \geq 8$. Es decir:] Suponga que k es un entero con $k \geq 8$ tal que

$k¢$ se puede obtener usando monedas de 3¢ y 5¢. ← $P(k)$ hipótesis inductiva

[Debemos demostrar que $P(k + 1)$ es verdadera. Es decir:] Debemos demostrar que

$(k + 1)¢$ se pueden obtener usando monedas de 3¢ y 5¢. ← $P(k + 1)$

Caso 1 (Hay una moneda de 5¢ entre las que se utilizan para formar los k¢): En este caso, sustituya la moneda de 5¢ por dos monedas de 3¢, el resultado será $(k + 1)¢$.

continúa en la página 248

Caso 2 (No hay una moneda de 5¢ entre las que se utilizan para formar los k¢): En este caso, ya que $k \geq 8$, al menos se deben haber utilizado tres monedas de 3¢. Así al quitar tres monedas de 3¢ y reemplazarlas por dos monedas de 5¢, el resultado será $(k + 1)$¢.

Así, en ambos casos se pueden obtener $(k + 1)$¢ usando monedas de 3¢ y 5¢ *[como se quería demostrar]*.

[Como se ha demostrado el paso básico y el paso inductivo, llegamos a la conclusión de que la proposición es verdadera.]

El siguiente ejemplo muestra cómo utilizar la inducción matemática para demostrar una fórmula para la suma de los primeros n enteros.

Ejemplo 5.2.1 Suma de los *n* primeros enteros

Utilice inducción matemática para demostrar que

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2} \text{ para todo entero } n \geq 1.$$

Solución Para construir una demostración por inducción, primero debe identificar la propiedad $P(n)$. En este caso, $P(n)$ es la ecuación

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}. \quad \leftarrow \text{la propiedad } (P(n))$$

[Para ver que P(n) es una frase, observe que su sujeto es "la suma de los números enteros del 1 al n" y su verbo es "igual"].

En el paso básico de la demostración, debe verificar que la propiedad es verdadera para $n = 1$, o, dicho de otro modo que $P(1)$ es verdadera. Ahora $P(1)$ se obtiene sustituyendo 1 en lugar de n en $P(n)$. El lado izquierdo de $P(1)$ es la suma de todos los enteros sucesivos empezando en 1 y terminando en 1. Este es exactamente 1. Así $P(1)$ es

Nota Para escribir $P(1)$, sólo tienes que copiar $P(n)$ y sustituir cada n por un 1.

$$1 = \frac{1(1+1)}{2}. \quad \leftarrow \text{básico } P(1)$$

Por supuesto, esta ecuación es verdadera ya que el lado derecho es

$$\frac{1(1+1)}{2} = \frac{1 \cdot 2}{2} = 1,$$

que es igual al lado izquierdo.

En el paso inductivo, se supone que $P(k)$ es verdadera, para un entero k dado, pero elegido arbitrariamente con $k \geq 1$. *[Esta suposición es la hipótesis inductiva.]* Entonces, debemos demostrar que $P(k + 1)$ es verdadera. ¿Qué son $P(k)$ y $P(k + 1)$? $P(k)$ se obtiene sustituyendo k para todo n en $P(n)$. Por tanto $P(k)$ es

Nota Para escribir $P(k)$, sólo copie $P(n)$ y sustituya cada n por k.

$$1 + 2 + \cdots + k = \frac{k(k+1)}{2}. \quad \leftarrow \text{hipótesis inductiva } (P(k))$$

Del mismo modo, $P(k+1)$ se obtiene sustituyendo la cantidad $(k+1)$ para todo n que aparece en $P(n)$. Por tanto $P(k+1)$ es

Nota Para escribir $P(k+1)$, sólo copie $P(n)$ y sustituya cada n por $(k+1)$.

$$1+2+\cdots+(k+1)=\frac{(k+1)((k+1)+1)}{2},$$

o, equivalentemente,

$$\boxed{1+2+\cdots+(k+1)=\frac{(k+1)(k+2)}{2}.} \quad \leftarrow \text{para mostrar } (P(k+1))$$

Ahora, la hipótesis inductiva es la suposición de que $P(k)$ es verdadera. ¿Cómo se puede usar esta suposición de demostrar que $P(k+1)$ es verdadera? $P(k+1)$ es una ecuación y la veracidad de una ecuación se puede demostrar de muchas maneras. Una de las más directa es utilizar la hipótesis inductiva junto con el álgebra y otros hechos conocidos para transformar por separado los lados izquierdo y derecho hasta que sea vea que son iguales. En este caso, el lado izquierdo de $P(k+1)$ es

$$1+2+\cdots+(k+1),$$

que es igual a

$$(1+2+\cdots+k)+(k+1)$$

El siguiente al último término es k porque los términos son enteros sucesivos hasta el último término que es $k+1$.

Pero sustituyendo la hipótesis inductiva,

$$(1+2+\cdots+k)+(k+1)$$

$$=\frac{k(k+1)}{2}+(k+1)$$

ya que la hipótesis inductiva dice que $1+2+\cdots+k=\frac{k(k+1)}{2}$

$$=\frac{k(k+1)}{2}+\frac{2(k+1)}{2}$$

multiplicando el numerador y el denominador del segundo término por 2 para obtener un denominador común

$$=\frac{k^2+k}{2}+\frac{2k+2}{2}$$

multiplicando los dos numeradores

$$\frac{k^2+3k+1}{2}$$

sumando fracciones con el mismo denominador y combinando términos semejantes.

Ahora la parte izquierda de $P(k+1)$ es $\frac{k^2+3k+1}{2}$. Ahora el lado derecho de $P(k+1)$ es

$$\frac{(k+1)(k+2)}{2}=\frac{k^2+3k+1}{2}$$

multiplicando el numerador.

Así, los dos lados de $P(k+1)$ son iguales entre sí, por lo que la ecuación $P(k+1)$ es verdadera.

Este análisis se resume de la siguiente manera:

Teorema 5.2.2 Suma de los *n* primeros enteros

Para todo entero $n \geq 1$,

$$1+2+\cdots+n=\frac{n(n+1)}{2}.$$

Demostración (por inducción matemática):

Sea la propiedad $P(n)$ la ecuación

$$1+2+3+\cdots+n=\frac{n(n+1)}{2}.$$

continúa en la página 250

Verifique que P(1) es verdadera:

Para establecer $P(1)$, debemos demostrar que

$$1 = \frac{1(1+1)}{2} \qquad \leftarrow P(1)$$

Pero el lado izquierdo de esta ecuación es 1 y también el lado derecho es

$$\frac{1(1+1)}{2} = \frac{2}{2} = 1$$

Por tanto $P(1)$ es verdadera.

Demuestre que para todo entero $k \geq 1$ si $P(k)$ es verdadera entonces también $P(k+1)$ es verdadera:

[Supongamos que $P(k)$ es verdadera para un entero $k \geq 1$ dado pero elegido arbitrariamente. Es decir:] Supongamos que k es un entero con $k \geq 1$ tal que

$$1 + 2 + 3 + \cdots + k = \frac{k(k+1)}{2} \qquad \leftarrow P(k) \text{ hipótesis inductiva}$$

[Debemos demostrar que $P(k+1)$ es verdadera. Es decir:] Debemos demostrar que

$$1 + 2 + 3 + \cdots + (k+1) = \frac{(k+1)[(k+1)+1]}{2},$$

o, equivalentemente, que

$$1 + 2 + 3 + \cdots + (k+1) = \frac{(k+1)(k+2)}{2}. \qquad \leftarrow P(k+1)$$

[Demostraremos que el lado izquierdo y el lado derecho de $P(k+1)$ son iguales a la misma cantidad y por tanto son iguales entre sí.]

El lado izquierdo de $P(k+1)$ es

$$\begin{aligned} &1 + 2 + 3 + \cdots + (k+1) \\ &\quad = 1 + 2 + 3 + \cdots + k + (k+1) && \text{haciendo explícito el término siguiente al último} \\ &\quad = \frac{k(k+1)}{2} + (k+1) && \text{sustituyendo la hipótesis inductiva} \\ &\quad = \frac{k(k+1)}{2} + \frac{2(k+1)}{2} \\ &\quad = \frac{k^2+k}{2} + \frac{2k+2}{2} \\ &\quad = \frac{k^2+3k+1}{2} && \text{por álgebra.} \end{aligned}$$

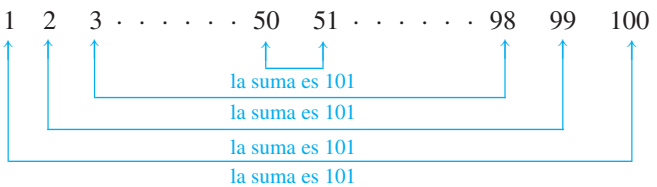
Y el lado derecho de $P(k+1)$ es

$$\frac{(k+1)(k+2)}{2} = \frac{k^2+3k+1}{2}.$$

Así, los dos lados de $P(k+1)$ son iguales a la misma cantidad y así son iguales entre sí. Por tanto la ecuación $P(k+1)$ es verdadera *[como se quería demostrar].* *[Puesto que hemos demostrado tanto el paso básico como el paso inductivo, concluimos que el teorema es verdadero.]*

■

La historia cuenta que uno de los más grandes matemáticos de todos los tiempos, Carl Friedrich Gauss (1777-1855), cuando era un niño pequeño su maestro le dio el problema de la suma de números del 1 al 100. El maestro le pidió a sus alumnos calcular la suma, supuestamente para ganar algo de tiempo con los trabajos del curso. Pero después de unos minutos, Gauss obtuvo la respuesta correcta. Sobra decir que el maestro se quedó estupefacto. ¿Cómo podría el joven Gauss calcular la cantidad tan rápidamente? En sus últimos años, Gauss explicó que él había imaginado a los números apareados de acuerdo con el siguiente esquema.



La suma de los números de cada par es 101 y son sólo 50 pares en total, por lo que la suma total es $50 \cdot 101 = 5\,050$.

• Definición de forma cerrada

Si se demuestra que una suma con un número variable de términos es igual a una fórmula que no contiene ni puntos suspensivos o símbolo de suma, decimos que está escrito **en forma cerrada**.

Por ejemplo, la escritura de $1 + 2 + 3 + \cdots + n = \dfrac{n(n+1)}{2}$ expresa la suma de $1 + 2 + 3 + \cdots + n$ en forma cerrada.

Ejemplo 5.2.2 Aplicación de la fórmula de la suma de los *n* primeros enteros

a. Evalúe $2 + 4 + 6 + \cdots + 500$.

b. Evalúe $5 + 6 + 7 + 8 + \cdots + 50$.

c. Para un número entero $h \geq 2$, escriba $1 + 2 + 3 + \cdots + (h - 1)$ en forma cerrada.

Solución

a. $2 + 4 + 6 + \cdots + 500 = 2 \cdot (1 + 2 + 3 + \cdots + 250)$

$$= 2 \cdot \left(\frac{250 \cdot 251}{2} \right)$$ aplicando la fórmula de la suma de los n primeros enteros con $n = 250$

$$= 62\,750.$$

b. $5 + 6 + 7 + 8 + \cdots + 50 = (1 + 2 + 3 + \cdots + 50) - (1 + 2 + 3 + 4)$

$$= \frac{50 \cdot 51}{2} - 10$$ aplicando la fórmula de la suma de los n primeros enteros con $n = 50$

$$= 1\,265$$

c. $1 + 2 + 3 + \cdots + (h - 1) = \dfrac{(h-1) \cdot [(h-1) + 1]}{2}$ aplicando la fórmula de la suma de los n primeros enteros con $n = h - 1$

$$= \frac{(h-1) \cdot h}{2}$$ ya que $(h - 1) = h$. ■

El siguiente ejemplo pide una demostración de otra fórmula famosa e importante de las matemáticas: la fórmula para la suma de una sucesión geométrica. En una **sucesión geométrica**, cada término se obtiene del anterior multiplicando por un factor constante. Si el primer término es 1 y el factor constante es r, entonces la sucesión es $1, r, r^2, r^3, \ldots, r^n, \ldots$ La suma de los n primeros términos de esta sucesión está dada por la fórmula

$$\sum_{i=0}^{n} r^i = \frac{r^{n+1} - 1}{r - 1}$$

para todo entero $n \geq 0$ y números reales r no igual a 1. La forma desarrollada de la fórmula es

$$r^0 + r^1 + r^2 + \cdots + r^n = \frac{r^{n+1} - 1}{r - 1},$$

y ya que $r^0 = 1$ y $r^1 = r$, la fórmula para $n \geq 1$ se puede reescribir como

$$1 + r + r^2 + \cdots + r^n = \frac{r^{n+1} - 1}{r - 1}.$$

Ejemplo 5.2.3 Suma de una sucesión geométrica

Demuestre que $\displaystyle\sum_{i=0}^{n} r^i = \frac{r^{n+1} - 1}{r - 1}$, para todos enteros $n \geq 0$ y todos los números reales r excepto 1.

Solución En este ejemplo la propiedad $P(n)$ es de nuevo una ecuación, aunque en este caso contiene una variable real r:

$$\sum_{i=0}^{n} r^i = \frac{r^{n+1} - 1}{r - 1}. \quad \leftarrow \text{la propiedad } (P(n))$$

Debido a que r puede ser cualquier número real distinto de 1, la demostración comienza suponiendo que r es un número real particular, pero elegido arbitrariamente que no es igual a 1. Después, la demostración sigue por inducción matemática sobre n, comenzando con $n = 0$. En el paso básico, se debe demostrar que $P(0)$ es verdadera, es decir, verifique que la propiedad es verdadera para $n = 0$. Así sustituyendo 0 para cada n en $P(n)$:

$$\sum_{i=0}^{0} r^i = \frac{r^{0+1} - 1}{r - 1}. \quad \leftarrow \text{básico } (P(0))$$

En el paso inductivo, suponga que k es un entero con $k \geq 0$ para el que $P(k)$ es verdadera, es decir, suponga que la propiedad es verdadera para $n = k$. Así sustituyendo k para cada n en $P(n)$:

$$\sum_{i=0}^{k} r^i = \frac{r^{k+1} - 1}{r - 1}. \quad \leftarrow \text{hipótesis inductiva } (P(k))$$

Después, demuestre que $P(k + 1)$ es verdadera, es decir, demuestre que la propiedad es verdadera para $n = k + 1$. Así sustituyendo $k + 1$ para cada n en $P(n)$:

$$\sum_{i=0}^{k+1} r^i = \frac{r^{(k+1)+1} - 1}{r - 1},$$

o, equivalentemente,

$$\sum_{i=0}^{k+1} r^i = \frac{r^{k+2} - 1}{r - 1}. \quad \leftarrow \text{para demostrar } (P(k+1))$$

En el paso inductivo para esta demostración se utiliza otra técnica común para mostrar que una ecuación es verdadera: Empezamos con el lado izquierdo y transformamos paso a paso el lado derecho con la hipótesis inductiva, junto con álgebra y otros hechos conocidos.

Teorema 5.2.3 Suma de una sucesión geométrica

Para cualquier número real r, excepto 1 y cualquier entero $n \geq 0$,

$$\sum_{i=0}^{n} r^i = \frac{r^{n+1} - 1}{r - 1}.$$

Demostración (por inducción matemática):

Suponga que r es un número real dado, pero elegido arbitrariamente que no es igual a 1 y sea la propiedad $P(n)$ la ecuación

$$\sum_{i=0}^{n} r^i = \frac{r^{i+1} - 1}{r - 1} \quad \leftarrow P(n)$$

Debemos demostrar que $P(n)$ es verdadera para todo entero $n \geq 0$. Lo hacemos por inducción matemática sobre n.

Demostración de que P(0) es verdadera:

Para establecer $P(0)$, debemos verificar

$$\sum_{i=0}^{0} r^i = \frac{r^{0+1} - 1}{r - 1} \quad \leftarrow P(0)$$

El lado izquierdo de esta ecuación es $r^0 = 1$ y es el lado derecho es

$$\frac{r^{0+1} - 1}{r - 1} = \frac{r - 1}{r - 1} = 1$$

también porque $r^1 = r$ y $r \neq 1$. Por tanto $P(0)$ es verdadera.

Demostración de que para todo entero $k \geq 0$, si P(k) es verdadera entonces P(k + 1) también es verdadera:

[*Supongamos que P(k) es verdadera para un entero k dado, pero elegido arbitrariamente* $k \geq 0$. *Es decir:]* Sea k un número entero con $k \geq 0$ y supongamos que

$$\sum_{i=0}^{k} r^i = \frac{r^{k+1} - 1}{r - 1} \quad \leftarrow P(k)$$
hipótesis inductiva

continúa en la página 254

[Debemos demostrar que $P(k+1)$ es verdadera. Es decir:] Debemos demostrar que

$$\sum_{i=0}^{k+1} r^i = \frac{r^{(k+1)+1} - 1}{r - 1},$$

o, equivalentemente, que

$$\sum_{i=0}^{k+1} r^i = \frac{r^{k+2} - 1}{r - 1}. \quad \leftarrow P(k+1)$$

[Demostraremos que el lado izquierdo de $P(k+1)$ es igual al lado derecho.] El lado izquierdo de $P(k+1)$ es

$$\begin{aligned}
\sum_{i=0}^{k+1} r^i &= \sum_{i=0}^{k} r^i + r^{k+1} && \text{escribiendo el } (k+1)\text{-ésimo término por separado de los primeros } k \text{ términos} \\
&= \frac{r^{k+1} - 1}{r - 1} + r^{k+1} && \text{sustituyendo la hipótesis inductiva} \\
&= \frac{r^{k+1} - 1}{r - 1} + \frac{r^{k+1}(r-1)}{r-1} && \text{multiplicando el numerador y el denominador del segundo término por } (r-1) \text{ para obtener un denominador común} \\
&= \frac{(r^{k+1} - 1) + r^{k+1}(r-1)}{r-1} && \text{sumando fracciones} \\
&= \frac{r^{k+1} - 1 + r^{k+2} - r^{k+1}}{r-1} && \text{multiplicando y usando el hecho de que } r^{k+1} \cdot r = r^{k+1} \cdot r^1 = r^{k+2} \\
&= \frac{r^{k+2} - 1}{r-1} && \text{eliminando los } r^{k+1}\text{s.}
\end{aligned}$$

que es el lado derecho de $P(k+1)$ *[como se quería demostrar].*
[Puesto que hemos demostrado el paso básico y el paso inductivo, concluimos que el teorema es verdadero.]

Demostración de una igualdad

Las demostraciones de los pasos básico e inductivo en los ejemplos 5.2.1 y 5.2.3 ilustran dos maneras diferentes de demostrar que una ecuación es verdadera: 1) la transformación del lado izquierdo y del lado derecho de forma independiente hasta que se ve que son iguales y 2) la transformación de un lado de la ecuación hasta que se ve que es igual al otro lado de la ecuación.

A veces la gente utiliza un método que ellos creen que demuestra la igualdad, pero que es realmente no válido. Por ejemplo, para probar el paso básico para el teorema 5.2.3, realizan los siguientes pasos:

¡Precaución! ¡No haga esto!

$$\begin{aligned}
\sum_{i=0}^{0} r^i &= \frac{r^{0+1} - 1}{r - 1} \\
r^0 &= \frac{r^1 - 1}{r - 1} \\
1 &= \frac{r - 1}{r - 1} \\
1 &= 1
\end{aligned}$$

El problema con este método es que el partir de un enunciado y deducir una conclusión verdadera no demuestra que el enunciado es verdadero. Una conclusión verdadera también

puede deducirse de un enunciado falso. Por ejemplo, los pasos siguientes muestran cómo deducir la conclusión verdadera de que $1 = 1$ a partir del enunciado falso de que $1 = 0$:

$$\begin{aligned} 1 &= 0 && \leftarrow \text{falso} \\ 0 &= 1 \\ 1 + 0 &= 0 + 1 \\ 1 &= 1 && \leftarrow \text{verdadero} \end{aligned}$$

Cuando utilice inducción matemática para demostrar fórmulas, asegúrese de usar un método que evite el razonamiento no válido, tanto para el paso básico como para el paso inductivo.

Deducción de fórmulas adicionales

La fórmula para la suma de una sucesión geométrica se puede considerar como una familia de diferentes fórmulas en r, una para cada número real r, excepto 1.

Ejemplo 5.2.4 Aplicación de la fórmula de la suma de una sucesión geométrica

En cada uno de los incisos siguientes *a*) y *b*), suponga que m es un entero que es mayor o igual a 3. Escriba cada una de las sumas en forma cerrada.

a. $1 + 3 + 3^2 + \cdots + 3^{m-2}$

b. $3^2 + 3^3 + 3^4 + \cdots + 3^m$

Solución

a. $$1 + 3 + 3^2 + \cdots + 3^{m-2} = \frac{3^{(m-2)+1} - 1}{3 - 1} = \frac{3^{m-1} - 1}{2}.$$ aplicando la fórmula de la suma de una sucesión geométrica con $r = 3$ y $n = m - 2$

b. $$3^2 + 3^3 + 3^4 + \cdots + 3^m = 3^2 \cdot (1 + 3 + 3^2 + \cdots + 3^{m-2})$$ factorizando 3^2

$$= 9 \cdot \left(\frac{3^{m-1} - 1}{2} \right)$$ por el inciso *a*). ■

Al igual que con la fórmula de la suma de los primeros n números enteros, hay una manera de pensar de la fórmula para la suma de los términos de una sucesión geométrica que la hace parecer sencilla e intuitiva. Sea

$$S_n = 1 + r + r^2 + \cdots + r^n.$$

Entonces,

$$rS_n = r + r^2 + r^3 + \cdots + r^{n+1},$$

y así

$$\begin{aligned} rS_n - S_n &= (r + r^2 + r^3 + \cdots + r^{n+1}) - (1 + r + r^2 + \cdots + r^n) \\ &= r^{n+1} - 1. \end{aligned} \quad 5.2.1$$

Pero,

$$rS_n - S_n = (r - 1)S_n. \quad 5.2.2$$

Igualando los lados derechos de las ecuaciones (5.2.1) y (5.2.2) y dividiendo entre $r - 1$ se obtiene

$$S_n = \frac{r^{n+1} - 1}{r - 1}.$$

Esta deducción de la fórmula es atractiva y bastante convincente. Sin embargo, no es tan lógicamente hermética como la demostración por inducción matemática. Para ir de un paso a otro en los cálculos anteriores, se argumenta que cada término entre los indicados con puntos suspensivos (...) tiene tal o cual aspecto y cuando éstos se eliminan ocurre tal o cual resultado. Pero es imposible en realidad ver cada término y cada cálculo, por lo que la exactitud de estas afirmaciones no se puede comprobar totalmente. Con la inducción matemática es posible enfocar exactamente lo que sucede en el centro de los puntos suspensivos y comprobar sin dudas que los cálculos son correctos.

Autoexamen

1. La inducción matemática es un método para demostrar que una propiedad definida para enteros n es verdadera para todos los valores de n que son ____.
2. Sea $P(n)$ una propiedad definida para enteros n y considere la construcción de una demostración por inducción matemática para el enunciado de "$P(n)$ es verdadera para todo $n \geq a$".
   a) En el paso básico hay que demostrar que ____.
   b) En el paso inductivo se supone que ____ para algún valor entero $k \geq a$ dado, pero elegido arbitrariamente. Esta suposición se llama la ____. Entonces se tiene que demostrar que ____.

Conjunto de ejercicios 5.2

1. Use inducción matemática (y la demostracion de la proposición 5.2.1 como modelo) para demostrar que cualquier cantidad de dinero de al menos 14¢ se pueden formar usando monedas de 3¢ y 8¢.

2. Utilice la inducción matemática para demostrar que de cualquier envío de al menos 12¢ se pueden obtener estampillas de 3¢ y 7¢.

3. Para cada entero positivo n, sea $P(n)$ la fórmula

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

   a. Escriba $P(1)$. ¿Es $P(1)$ verdadera?
   b. Escriba $P(k)$.
   c. Escriba $P(k+1)$.
   d. En una demostración por inducción matemática para que la fórmula sea válida para todo entero $n \geq 1$, ¿qué se debe demostrar en el paso inductivo?

4. Para cada entero n con $n \geq 2$, sea $P(n)$ la fórmula

$$\sum_{i=1}^{n-1} i(i+1) = \frac{n(n-1)(n+1)}{3}.$$

   a. Escriba $P(2)$. ¿Es $P(2)$ verdadera?
   b. Escriba $P(k)$.
   c. Escriba $P(k+1)$.
   d. En una demostración por inducción matemática para que la fórmula sea válida para todo entero $n \geq 2$, ¿qué se debe demostrar en el paso inductivo?

5. Rellene las partes que faltan en la siguiente demostración que

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2$$

para todo entero $n \geq 1$.

Demostración: Sea la propiedad $P(n)$ la ecuación

$$1 + 3 + 5 + \cdots + (2n - 1) = n^2. \quad \leftarrow P(n)$$

Demostración de que P(1) es verdadera: Para establecer $P(1)$, debemos demostrar que cuando se sustituye 1 en lugar de n, el lado izquierdo es igual al lado derecho. Pero, cuando $n = 1$, el lado izquierdo es la suma de todos los enteros impares del 1 al $2 \cdot 1 - 1$, que es la suma de los enteros impares del 1 al 1, que es 1. El lado derecho es __(a)__, que también es igual a 1. Por tanto $P(1)$ es verdadera.

Demostración de que para todo entero k ≥ 1, si P(k) es verdadera entonces P(k + 1) es verdadera: Sea k cualquier entero tal que $k \geq 1$.

[Supongamos que P(k) es verdadera. Es decir:]

Supongamos que $1 + 3 + 5 + \cdots + (2k - 1) =$ __(b)__. $\leftarrow P(k)$
[Esta es la hipótesis inductiva.]

[Debemos demostrar que P(k + 1) es verdadera. Es decir:]

Debemos demostrar que

__(c)__ = __(d)__. $\leftarrow P(k+1)$

Pero el lado izquierdo de $P(k + 1)$ es

$$\begin{aligned} &1 + 3 + 5 + \cdots + (2(k+1) - 1) \\ &\quad = 1 + 3 + 5 + \cdots + (2k + 1) \quad \text{por álgebra} \\ &\quad = [1 + 3 + 5 + \cdots + (2k - 1)] + (2k + 1) \\ &\quad \text{el próximo al último término es } 2k - 1 \text{ ya que } \underline{\text{(e)}} \\ &\quad = k^2 + (2k + 1) \quad \text{por } \underline{\text{(f)}} \\ &\quad = (k + 1)^2 \quad \text{por álgebra} \end{aligned}$$

que es el lado derecho de $P(k+1)$ *[como se quería demostrar].*
[Puesto que hemos demostrado el paso básico y el paso inductivo, llegamos a la conclusión de que el enunciado es verdadero.]
La demostración anterior tenía notas para ayudar a que su flujo lógico sea más evidente. En la escritura matemática estándar, se omiten dichas notas.

Demuestre cada enunciado en los ejercicios del 6 al 9 con inducción matemática. No deduzca de ellos el teorema 5.2.2 o el teorema 5.2.3.

6. Para todo entero $n \geq 1$, $2 + 4 + 6 + \cdots + 2n = n^2 + n$.

7. Para todo entero $n \geq 1$,
$$1 + 6 + 11 + 16 + \cdots + (5n - 4) = \frac{n(5n-3)}{2}.$$

8. Para todo entero $n \geq 0$, $1 + 2 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$.

9. Para todo entero $n \geq 3$,
$$4^3 + 4^4 + 4^5 + \cdots + 4^n = \frac{4(4^n - 16)}{3}.$$

Demuestre cada uno de los enunciados en los ejercicios del 10 al 17 por inducción matemática.

10. $1^2 + 2^2 + \cdots + n^2 = \dfrac{n(n+1)(2n+1)}{6}$, para todo entero $n \geq 1$.

11. $1^3 + 2^3 + \cdots + n^3 = \left[\dfrac{n(n+1)}{2}\right]^2$, para todo entero $n \geq 1$.

12. $\dfrac{1}{1\cdot 2} + \dfrac{1}{2\cdot 3} + \cdots + \dfrac{1}{n(n+1)} = \dfrac{n}{n+1}$, para todo entero $n \geq 1$.

13. $\displaystyle\sum_{i=1}^{n-1} i(i+1) = \frac{n(n-1)(n+1)}{3}$, para todo entero $n \geq 2$.

14. $\displaystyle\sum_{i=1}^{n+1} i \cdot 2^i = n \cdot 2^{n+2} + 2$, para todo entero $n \geq 0$.

***H* 15.** $\displaystyle\sum_{i=1}^{n} i(i!) = (n+1)! - 1$, para todo entero $n \geq 1$.

16. $\left(1 - \dfrac{1}{2^2}\right)\left(1 - \dfrac{1}{3^2}\right)\cdots\left(1 - \dfrac{1}{n^2}\right) = \dfrac{n+1}{2n}$, para todo entero $n \geq 2$.

17. $\displaystyle\prod_{i=0}^{n}\left(\frac{1}{2i+1}\cdot\frac{1}{2i+2}\right) = \frac{1}{(2n+2)!}$, para todo entero $n \geq 0$.

***H* ∗ 18.** Si x no es un número real divisible por π, entonces para todo entero $n \geq 1$,
$$\operatorname{sen} x + \operatorname{sen} 3x + \operatorname{sen} 5x + \cdots + \operatorname{sen}(2n-1)x = \frac{1 - \cos 2nx}{2 \operatorname{sen} x}.$$

19. (Para los estudiantes que han estudiado cálculo) Utilice inducción matemática, la regla del producto de cálculo y los hechos que $\dfrac{d(x)}{dx} = 1$ y que $x^{k+1} = x \cdot x^k$ para demostrar que, para todo entero $\dfrac{d(x^n)}{dx} = nx^{n-1}$.

Use la fórmula de la suma de los primeros n enteros y/o la fórmula para la suma de una sucesión geométrica para evaluar las sumas en los ejercicios del 20 al 29 o para escribirlos en forma cerrada.

20. $4 + 8 + 12 + 16 + \cdots + 200$

21. $5 + 10 + 15 + 20 + \cdots + 300$

22. $3 + 4 + 5 + 6 + \cdots + 1000$

23. $7 + 8 + 9 + 10 + \cdots + 600$

24. $1 + 2 + 3 + \cdots + (k-1)$, donde k es un número entero y $k \geq 2$.

25. a. $1 + 2 + 2^2 + \cdots + 2^{25}$
b. $2 + 2^2 + 2^3 + \cdots + 2^{26}$

26. $3 + 3^2 + 3^3 + \cdots + 3^n$, donde n es un entero con $n \geq 1$

27. $5^3 + 5^4 + 5^5 + \cdots + 5^k$, donde k es cualquier número entero con $k \geq 3$.

28. $1 + \dfrac{1}{2} + \dfrac{1}{2^2} + \cdots + \dfrac{1}{2^n}$, donde n es un entero positivo

29. $1 - 2 + 2^2 - 2^3 + \cdots + (-1)^n 2^n$, donde n es un entero positivo

***H* 30.** Determine una fórmula con n, a, m y d para la suma $(a + md) + (a + (m+1)d) + (a + (m+2)d) + \cdots + (a + (m+n)d)$, donde m y n son enteros, $n \geq 0$ y a y d son números reales. Justifique su respuesta.

31. Determine una fórmula con a, r, m y n, para la suma
$$ar^m + ar^{m+1} + ar^{m+2} + \cdots + ar^{m+n}$$
donde m y n son enteros, $n \geq 0$ y a y r son números reales. Justifique su respuesta.

32. Tiene dos padres, cuatro abuelos, ocho bisabuelos y así sucesivamente.
a. Si todos sus antepasados eran distintos, ¿cuál sería el número total de sus antepasados desde hace 40 generaciones (contando a la generación de sus padres como la número uno)? (*Sugerencia:* Utilice la fórmula para la suma de una sucesión geométrica).
b. Suponiendo que cada generación representa 25 años, el tiempo es de 40 generaciones?
c. El número total de personas que han vivido alguna vez es de aproximadamente de 10 mil millones, lo que equivale a 10^{10} personas. Compare este hecho con la respuesta al inciso *a*). ¿Qué deduce?

Encuentre los errores en los fragmentos de demostración en los ejercicios del 33 al 35.

H 33. **Teorema:** Para cualquier entero $n \geq 1$,

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

"**Demostración (por inducción matemática):** Ciertamente, el teorema es verdadero para $n = 1$ ya que $1^2 = 1$ y $\frac{1(1+1)(2\cdot 1+1)}{6} = 1$. Por tanto, el paso básico es verdadero. Para el paso inductivo, supongamos que para algún entero $k \geq 1$, $k^2 = \frac{k(k+1)(2k+1)}{6}$. Debemos demostrar que $(k+1)^2 = \frac{(k+1)((k+1)+1)(2(k+1)+1)}{6}$."

H 34. **Teorema:** Para cualquier entero $n \geq 0$,

$$1 + 2 + 2^2 + \cdots + 2^n = 2^{n+1} - 1.$$

"**Demostración (por inducción matemática): Sea la propiedad** $P(n)$, $1 + 2 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$.
Demostración de que P(0) es verdadera:
El lado izquierdo de $P(0)$ es $1 + 2 + 2^2 + \cdots + 2^0 = 1$ y también el lado derecho es $2^{0+1} - 1 = 2 - 1 = 1$. Entonces, $P(0)$ es verdadera".

H 35. **Teorema**: Para cualquier entero $n \geq 1$,

$$\sum_{i=1}^{n} i(i!) = (n+1)! - 1.$$

"**Demostración (por inducción matemática): Sea la propiedad** $P(n)$, $\sum_{i=1}^{n} i(i!) = (n+1)! - 1$.

Demostración de que P(1) es verdadera: Cuando $n = 1$

$$\sum_{i=1}^{1} i(i!) = (1+1)! - 1$$

Por lo que $1(1!) = 2! - 1$

y $1 = 1$

Así $P(1)$ es verdadera".

✶ 36. Utilice el teorema 5.2.2 para demostrar que si m y n son números enteros positivos y m es cualquier impar, entonces $\sum_{k=0}^{m-1}(n+k)$ es divisible por m. ¿La conclusión vale si m es impar? Justifique su respuesta.

H ✶ 37. Utilice el teorema 5.2.2 y el resultado del ejercicio 10 para demostrar que si p es cualquier número primo con $p \geq 5$, entonces la suma de los cuadrados de cualesquiera p enteros consecutivos es divisible por p.

Respuestas del autoexamen

1. mayor o igual que un valor inicial 2. *a*) $P(a)$ es verdadera *b*) $P(k)$ es verdadera; hipótesis inductiva, $P(k+1)$ es verdadera

5.3 Inducción matemática II

Una buena demostración es la que nos hace más sabios. —I. Manin. *Un Curso de Lógica Matemática*, 1977

En los cursos de ciencias naturales, la deducción y la inducción se presentan como formas alternativas de pensamiento, la deducción es para inferir una conclusión a partir de principios generales usando las leyes del razonamiento lógico y la inducción es para enunciar un principio general después de observar que es válido en un gran número de casos concretos. En este sentido, entonces, la inducción *matemática* no es inductiva, sino deductiva. Una vez que se ha demostrado un teorema con inducción matemática, se sabe que es válido como si se hubiese demostrado con cualquier método matemático. El razonamiento inductivo, en el sentido de las ciencias naturales, *se* utiliza en matemáticas, pero sólo para hacer conjeturas, no para demostrarlas. Por ejemplo, observamos que

$$1 - \frac{1}{2} = \frac{1}{2}$$

$$\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = \frac{1}{3}$$

$$\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{4}\right) = \frac{1}{4}$$

Parece muy poco probable que ocurra este patrón por pura casualidad por lo que es razonable suponer (aunque no es seguro) que el patrón es verdadero en general. En un caso como éste, una demostración por inducción matemática (que se le pide que escriba en el ejercicio 1 del final de esta sección) llega a la esencia de por qué el patrón se conserva en general. Se revela el mecanismo matemático que requiere la veracidad de cada caso sucesor del anterior. Por ejemplo, en este ejemplo observe que si

$$\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\cdots\left(1-\frac{1}{k}\right)=\frac{1}{k},$$

entonces sustituyendo

$$\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\cdots\left(1-\frac{1}{k}\right)\left(1-\frac{1}{k+1}\right)$$
$$=\frac{1}{k}\left(1-\frac{1}{k+1}\right)=\frac{1}{k}\left(\frac{k+1-1}{k+1}\right)=\frac{1}{k}\left(\frac{k}{k+1}\right)=\frac{1}{k+1}.$$

Así, la inducción matemática hace del conocimiento del patrón general una cuestión de certeza matemática más que de vagas suposiciones.

En lo que resta en esta sección se muestra cómo utilizar la inducción matemática para demostrar tipos adicionales de enunciados tales como las propiedades de divisibilidad de los números enteros y las desigualdades. Los lineamientos básicos de las demostraciones son los mismos en todos los casos, pero los detalles de los pasos básico e inductivo difieren de uno a otro.

Ejemplo 5.3.1 Demostración de una propiedad de divisibilidad

Utilice la inducción matemática para demostrar que para todo $n \geq 0$, 2^{2n-1} es divisible por 3.

Solución Al igual que en las demostraciones anteriores de inducción matemática, es necesario identificar la propiedad $P(n)$. En este ejemplo, $P(n)$ es la frase

2^{2n-1} es divisible por 3.	← la propiedad ($P(n)$)

Sustituyendo, el enunciado para el paso básico, $P(0)$, es

$2^{2\cdot 0}-1$ es divisible por 3.	← básico ($P(0)$)

La suposición para el paso inductivo, $P(k)$, es

$2^{2k}-1$ es divisible por 3.	← hipótesis inductiva ($P(k)$)

y la conclusión que se demuestra, $P(k+1)$, es

$2^{2(k+1)}-1$ es divisible por 3.	← para demostrar ($P(k+1)$)

Recuerde que un entero m es divisible por 3 si y sólo si, $m = 3r$ para algún entero r. Ahora, el enunciado $P(0)$ es verdadero ya que $2^{2\cdot 0}-1=2^0-1=1-1=0$, que es divisible por 3 ya que $0 = 3 \cdot 0$.

Para demostrar el paso inductivo, supongamos que k es un entero mayor o igual a 0 tal que $P(k)$ es verdadera. Esto significa que $2^{2k}-1$ es divisible por 3. Entonces, se debe demostrar la veracidad de $P(k+1)$. O, en otras palabras, se debe demostrar que $2^{2(k+1)}-1$ es divisible por 3. Pero,

$$\begin{aligned} 2^{2(k+1)}-1 &= 2^{2k+2}-1 \\ &= 2^{2k}\cdot 2^2-1 \\ &= 2^{2k}\cdot 4-1. \end{aligned}$$

por las leyes de los exponentes

El objetivo es demostrar que esta cantidad, $2^{2k} \cdot 4 - 1$, es divisible por 3. ¿Por qué esto es así? Ya que la hipótesis inductiva, $2^{2k} - 1$ es divisible por 3 y $2^{2k} \cdot 4 - 1$ se parece a $2^{2k} - 1$. Observe que sucede, si se resta $2^{2k} - 1$ de $2^{2k} \cdot 4 - 1$:

$$\underbrace{2^{2k} \cdot 4 - 1}_{\uparrow} \quad - \quad \underbrace{(2^{2k} - 1)}_{\uparrow} \quad = \quad \underbrace{2^{2k} \cdot 3.}_{\uparrow}$$

¿divisible por 3? divisible por 3 divisible por 3

Sumando $2^{2k} - 1$ a ambos lados se obtiene

$$\underbrace{2^{2k} \cdot 4 - 1}_{\uparrow} \quad = \quad \underbrace{2^{2k} \cdot 3}_{\uparrow} \quad + \quad \underbrace{2^{2k} - 1.}_{\uparrow}$$

¿divisible por 3? divisible por 3 divisible por 3

Los dos términos de la suma en el lado derecho de esta ecuación son divisibles por 3, por lo que la suma es divisible por 3. (Vea el ejercicio 15 de la sección 4.3.) Por tanto, el lado izquierdo de la ecuación también es divisible por 3, que es lo que se quería demostrar.

Este análisis se resume de la siguiente manera:

Proposición 5.3.1

Para todo entero $n \geq 0$, $2^{2n} - 1$ es divisible por 3.

Demostración (por inducción matemática):

Sea la propiedad $P(n)$ la frase "$2^{2n} - 1$ es divisible por 3"

$2^{2n} - 1$ es divisible por 3. $\leftarrow P(n)$

Demostración de que P(0) es verdadera:

Para establecer $P(0)$, debemos demostrar que

$2^{2 \cdot 0} - 1$ es divisible por 3. $\leftarrow P(0)$

Pero,

$$2^{2 \cdot 0} - 1 = 2^0 - 1 = 1 - 1 = 0$$

y 0 es divisible por 3 ya que $0 = 3 \cdot 0$. Por tanto $P(0)$ es verdadera.

Demostración de que para todo entero $k \geq 0$, si $P(k)$ es verdadera entonces $P(k+1)$ también es verdadera:

[Supongamos que $P(k)$ es verdadera para un entero dado $k \geq 0$, pero elegido arbitrariamente. Es decir:] Sea k cualquier número entero con $k \geq 0$ y supongamos que

$2^{2k} - 1$ es divisible por 3. $\leftarrow P(k)$ hipótesis inductiva

Por definición de divisibilidad, esto significa que

$$2^{2k} - 1 = 3r \quad \text{para algún entero } r.$$

[Tenemos que demostrar que $P(k+1)$ es verdadera. Es decir:] Tenemos que demostrar que

$2^{2(k+1)} - 1$ es divisible por 3. $\leftarrow P(k+1)$

Pero

$$\begin{aligned} 2^{2(k+1)} - 1 &= 2^{2k+2} - 1 \\ &= 2^{2k} \cdot 2^2 - 1 && \text{por las leyes de los exponentes} \\ &= 2^{2k} \cdot 4 - 1 \\ &= 2^{2k}(3+1) - 1 \\ &= 2^{2k} \cdot 3 + (2^{2k} - 1) && \text{por las leyes del álgebra} \\ &= 2^{2k} \cdot 3 + 3r && \text{por hipótesis inductiva} \\ &= 3(2^{2k} + r) && \text{factorizando el 3} \end{aligned}$$

Pero $2^{2k} + r$ es un entero, porque es una suma de productos de números enteros y así, por definición de divisibilidad, $2^{2(k+1)} - 1$ es divisible por 3 *[como se quería demostrar]*.

[Puesto que hemos demostrado el paso básico y el paso inductivo, llegamos a la conclusión de que la proposición es verdadera.]

■

El ejemplo siguiente muestra el uso de inducción matemática para demostrar una desigualdad.

Ejemplo 5.3.2 Demostración de una desigualdad

Use inducción matemática para demostrar que para todo entero $n \geq 3$,

$$2n + 1 < 2^n.$$

Solución En este ejemplo de la propiedad $P(n)$ es la desigualdad

$$\boxed{2n + 1 < 2^n.} \quad \leftarrow \text{La propiedad } (P(n))$$

Sustituyendo, el enunciado para el paso básico, $P(3)$, es

$$\boxed{2 \cdot 3 + 1 < 2^3.} \quad \leftarrow \text{básico } (P(3))$$

La suposición para el paso inductivo, $P(k)$, es

$$\boxed{2k + 1 < 2^k,} \quad \leftarrow \text{hipótesis inductiva } (P(k))$$

y la conclusión a demostrar es

$$\boxed{2(k+1) + 1 < 2^{k+1}.} \quad \leftarrow \text{Para demostrar } (P(k+1))$$

Para demostrar el paso básico, observamos que el enunciado $P(3)$ es verdadero ya que $2 \cdot 3 + 1 = 7$, $2^3 = 8$ y $7 < 8$.

Para demostrar el paso inductivo, suponemos que la hipótesis inductiva, que $P(k)$ es verdadera para un entero $k \geq 3$. Esto significa que $2k + 1 < 2^k$ se supone que es verdadero para un entero dado $k \geq 3$, pero elegido arbitrariamente. Después, se deduce la veracidad de $P(k + 1)$. O, en otras palabras, se demuestra que la desigualdad $2(k + 1) + 1 < 2^{k+1}$ es verdadera. Pero al multiplicarse y reagrupar,

$$2(k + 1) + 1 = 2k + 3 = (2k + 1) + 2, \qquad 5.3.1$$

y sustituyendo la hipótesis inductiva,

$$(2k + 1) + 2 < 2^k + 2. \qquad 5.3.2$$

Por tanto

$$2(k + 1) + 1 \ < 2^k + 2$$

La parte del extremo izquierdo de la ecuación (5.3.1) es menor que la parte del extremo derecho de la desigualdad (5.3.2).

Si se puede demostrar que $2^k + 2$ es menor que 2^{k+1}, entonces se ha demostrado la desigualdad deseada. Pero como se puede sumar o restar la cantidad de 2^k a una desigualdad sin cambiar su dirección,

Nota En el apéndice A se presentan propiedades de orden

$$2^k + 2 < 2^{k+1} \quad \Leftrightarrow \quad 2 < 2^{k+1} - 2^k = 2^k(2 - 1) = 2^k.$$

Y puesto que multiplicar o dividir una desigualdad por 2 no cambia su dirección,

$$2 < 2^k \quad \Leftrightarrow \quad 1 = \frac{2}{2} < \frac{2^k}{2} = 2^{k-1} \quad \text{por las leyes de los exponentes.}$$

Esta última desigualdad es verdadera para todo $k \geq 2$. Por tanto, es verdadero que $2(k + 1) + 1 < 2^{k+1}$.

Este análisis se hace más fluido (pero menos intuitivo) en la siguiente demostración formal:

Proposición 5.3.2

Para todo entero $n \geq 3$, $2n + 1 < 2^n$.

Demostración (por inducción matemática):

Sea la propiedad $P(n)$ la desigualdad

$$2n + 1 < 2^n. \qquad \leftarrow P(n)$$

Demostración de que P(3) es verdadera:

Para establecer $P(3)$, debemos demostrar que

$$2 \cdot 3 + 1 < 2^3. \qquad \leftarrow P(3)$$

Pero,

$$2 \cdot 3 + 1 = 7 \quad \text{y} \quad 2^3 = 8 \quad \text{y} \quad 7 < 8.$$

Por tanto $P(3)$ es verdadera.

Demostración de que para todo entero k ≥ 3, si P(k) es verdadera entonces P(k + 1) también es verdadera:

[Supongamos que P(k) es verdadera para un entero dado $k \geq 3$, pero elegido arbitrariamente. Es decir:] Supongamos que k es cualquier entero con $k \geq 3$ tal que

$$2k + 1 < 2^k. \qquad \leftarrow P(k)$$

hipótesis inductiva

[Tenemos que demostrar que $P(k + 1)$ es verdadera. Es decir:] Debemos demostrar que

$$2(k + 1) + 1 < 2^{(k+1)},$$

o equivalentemente

$$2k + 3 < 2^{(k+1)}. \qquad \leftarrow P(k + 1)$$

Pero

$$2k + 3 = (2k + 1) + 2 \quad \text{por álgebra}$$

$$< 2^k + 2^k \quad \text{ya que } 2k + 1 < 2^k \text{ por hipótesis inductiva y porque } 2 < 2^k \text{ para todo entero } k \geq 2$$

$$\therefore 2k + 3 < 2 \cdot 2^k = 2^{k+1} \quad \text{por las leyes de los exponentes.}$$

[Esto es lo que necesita demostrar.]
[Ya que hemos demostrado el paso básico y el paso inductivo, llegamos a la conclusión de que la proposición es verdadera.]

■

El ejemplo siguiente muestra cómo utilizar la inducción matemática para demostrar que los términos de una sucesión satisfacen una cierta fórmula explícita.

Ejemplo 5.3.3 Demostración de una propiedad de una sucesión

Defina una sucesión $a_1, a_2, a_3, \ldots$ de la forma siguiente.*

$$a_1 = 2$$
$$a_k = 5a_{k-1} \quad \text{para todo entero } k \geq 2.$$

a. Escriba los cuatro primeros términos de la sucesión.

b. Se afirma que para cada entero $n \geq 0$, el enésimo término de la sucesión tiene el mismo valor que el dado por la fórmula $2 \cdot 5^{n-1}$. En otras palabras, la afirmación es que los términos de la sucesión satisfacen la ecuación $a_n = 2 \cdot 5^{n-1}$. Demuestre que esto es verdadero.

Solución

a. $a_1 = 2$.
$a_2 = 5a_{2-1} = 5a_1 = 5 \cdot 2 = 10$
$a_3 = 5a_{3-1} = 5a_2 = 5 \cdot 10 = 50$
$a_4 = 5a_{4-1} = 5a_3 = 5 \cdot 50 = 250.$

b. Utilice la inducción matemática para demostrar que cada término de la sucesión satisface la ecuación, empezando por demostrar que el primer término de la sucesión satisface la ecuación. Después suponga que un término a_k elegido arbitrariamente satisface la ecuación y demuestre que el término siguiente a_{k+1} también satisface la ecuación.

Demostración:

Sea $a_1, a_2, a_3, \ldots$ la sucesión definida mediante la especificación de que $a_1 = 2$ y $a_k = 5a_{k-1}$ para todo entero $k \geq 2$ y sea la propiedad $P(n)$ para la ecuación

$$a_n = 2 \cdot 5^{n-1}. \qquad \leftarrow P(n)$$

Utilizaremos la inducción matemática para demostrar que para todo entero $n \geq 1$, $P(n)$ es verdadera.

Demostración de que P(1) es verdadera:
Para establecer $P(1)$, debemos demostrar que

$$a_1 = 2 \cdot 5^{1-1}. \qquad \leftarrow P(1)$$

*Este es otro ejemplo de una definición recursiva. El tema general de la recursividad se analiza en la sección 5.6.

Pero el lado izquierdo de $P(1)$ es

$$a_1 = 2 \qquad \text{por definición de } a_1, a_2, a_3, \ldots,$$

y el lado derecho de $P(1)$ es

$$2 \cdot 5^{1-1} = 2 \cdot 5^0 = 2 \cdot 1 = 2.$$

Así, los dos lados de $P(1)$ son iguales a la misma cantidad y por tanto $P(1)$ es verdadera.

Demostración de que para todo entero $k \geq 1$, si $P(k)$ es verdadera entonces $P(k+1)$ también es verdadera:
[Supongamos que $P(k)$ es verdadera para un entero dado $k \geq 1$, pero elegido arbitrariamente. Es decir:] Sea k un número entero con $k \geq 0$ y supongamos que

$$a_k = 2 \cdot 5^{k-1}. \qquad \leftarrow P(k)$$
hipótesis inductiva

Por definición de divisibilidad, esto significa que

$$a_k = 2 \cdot 5^{k-1}.$$

[Tenemos que demostrar que $P(k+1)$ es verdadera. Es decir:] Debemos demostrar que

$$a_{k+1} = 2 \cdot 5^{(k+1)-1},$$

o, equivalentemente,

$$a_{k+1} = 2 \cdot 5^k. \qquad \leftarrow P(k+1)$$

Pero el lado izquierdo de $P(k+1)$ es

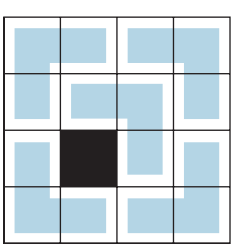
$$\begin{aligned} a_{k+1} &= 5a_{(k+1)-1} && \text{por definición de } a_1, a_2, a_3, \ldots \\ &= 5a_k && \text{ya que } (k+1)-1 = k \\ &= 5 \cdot (5 \cdot 5^{k-1}) && \text{por hipótesis inductiva} \\ &= 2 \cdot (5 \cdot 5^{k-1}) && \text{reagrupando} \\ &= 2 \cdot 5^k && \text{por las leyes de los exponentes} \end{aligned}$$

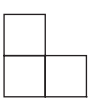
que es el lado derecho de la ecuación *[como se quería demostrar]*.

[Como hemos demostrado el paso básico y el paso inductivo, llegamos a la conclusión de que la fórmula es válida para todos los términos de la sucesión.] ■

Un problema con trominos

La palabra *poliominó*, es una generalización de *dominó*, que fue introducida por Salomón Golomb en 1954 cuando era un estudiante de 22 años en Harvard. Posteriormente, él y otros probaron muchas propiedades interesantes acerca de ellos y se convirtieron en la base para el popular juego de computadora *Tetris*. Un tipo particular de poliominó, llamado *tromino*, consiste de tres cuadrados juntos, que pueden ser de dos tipos:



en línea recta  y en forma de L 

Llama a un tablero que se forma con m cuadrados de lado tablero $m \times m$ ("m por m"). Observe que si se quita un cuadrado de un tablero 4×4, los cuadrados restantes puede ser completamente cubiertos por trominos en forma de L. Por ejemplo, cubrir un tablero como el que se muestra en la figura de la izquierda.

En su primer artículo sobre poliominós, Golomb incluyó una demostración del teorema siguiente. Es un hermoso ejemplo de un argumento por inducción matemática.

Teorema Cubierta de un tablero con trominos

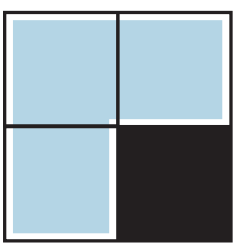
Para cualquier entero $n \geq 1$, si se quita un cuadrado de un tablero $2^n \times 2^n$, los cuadrados restantes pueden ser completamente cubiertos por trominos en forma de L.

La idea principal que lleva a una demostración de este teorema es la observación de que debido a que $2^{k+1} = 2 \cdot 2^k$, cuando un tablero $2^{k+1} \times 2^{k+1}$ se divide a la mitad tanto vertical como horizontalmente, cada mitad del lado tendrá una longitud 2^k y cada cuadrante resultante será un tablero $2^k \times 2^k$.

Demostración (por inducción matemática):

Sea la propiedad $P(n)$ la frase

> Si se quita cualquier cuadrado de un tablero de $2^n \times 2^n$,
> entonces, los cuadrados restantes pueden ser completamente cubiertos. ← $P(n)$
> Por trominos en forma de L



Demostración de que P(1) es verdadera:
Un tablero de $2^1 \times 2^1$ consiste sólo de cuatro cuadrados. Si se quita un cuadrado, los cuadrados restantes forman una L, que se puede cubrir con un único tromino en forma de L, como se muestra en la figura de la izquierda. Por tanto $P(1)$ es verdadera.

Demostración de que para todo entero $k \geq 1$, si P(k) es verdadera entonces P(k + 1) también es verdadera:

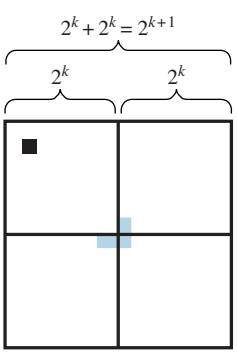
[Supongamos que P(k) es verdadera para un entero dado $k \geq 3$, pero elegido arbitrariamente. Es decir:] Sea k un entero tal que $k \geq 1$ y supongamos que

> Si se quita cualquier cuadrado de un tablero $2^k \times 2^k$,
> entonces, los cuadrados restantes se pueden cubrir completamente ← $P(k)$
> con trominos en forma de L.

$P(k)$ es la hipótesis inductiva.

[Tenemos que demostrar que $P(k + 1)$ es verdadera. Es decir:] Debemos demostrar que

> Si se quita cualquier cuadrado de un tablero de $2^{k+1} \times 2^{k+1}$,
> entonces, los cuadrados restantes pueden ser completamente cubiertos ← $P(k + 1)$
> por trominos en forma de L.



Considere un tablero de $2^{k+1} \times 2^{k+1}$ al que se le ha eliminado un cuadrado. Divida en cuatro cuadrantes iguales: Cada uno de ellos consistirá en un tablero $2^k \times 2^k$. En uno de los cuadrantes, se ha eliminado un cuadrado, por lo que, por hipótesis inductiva, todos los cuadrados que quedan en este cuadrante pueden ser completamente cubiertos por trominos en forma de L. Los otros tres cuadrantes se encuentran en el centro del tablero y el centro del tablero sirve como una esquina de un cuadrado de cada uno de los cuadrantes. Por consiguiente, un tromino en forma de L, será puesto en esos tres cuadrados centrales. En la figura de la izquierda se muestra esta situación. Por hipótesis inductiva, los cuadrados restantes en cada uno de los tres cuadrantes pueden ser completamente cubiertos por trominos en forma de L. Así, todos los cuadrados en el tablero $2^{k+1} \times 2^{k+1}$, excepto el que fue eliminado pueden ser completamente cubiertos por trominos en forma de L *[como se quería demostrar]*.

Autoexamen

1. La inducción matemática difiere del tipo de inducción utilizada en las ciencias naturales ya que es en realidad una forma de razonamiento _____.
2. La inducción matemática se puede utilizar para _____ suposiciones que se han hecho utilizando el razonamiento inductivo.

Conjunto de ejercicios 5.3

1. Con base en el análisis del producto $\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{4}\right)\cdots\left(1-\frac{1}{n}\right)$ del principio de esta sección, suponga una fórmula general para n. Demuestre su suposición con inducción matemática.

2. Experimente con los valores calculados del producto $\left(1+\frac{1}{1}\right)\left(1+\frac{1}{2}\right)\left(1+\frac{1}{3}\right)\cdots\left(1+\frac{1}{n}\right)$ para valores pequeños de n para suponer una fórmula de este producto para un n general. Demuestre su suposición con inducción matemática.

3. Observe que

$$\frac{1}{1\cdot 3}=\frac{1}{3}$$

$$\frac{1}{1\cdot 3}+\frac{1}{3\cdot 5}=\frac{2}{5}$$

$$\frac{1}{1\cdot 3}+\frac{1}{3\cdot 5}+\frac{1}{5\cdot 7}=\frac{3}{7}$$

$$\frac{1}{1\cdot 3}+\frac{1}{3\cdot 5}+\frac{1}{5\cdot 7}+\frac{1}{7\cdot 9}=\frac{4}{9}$$

Suponga una fórmula general y demuéstrela con inducción matemática.

H 4. Observe que

$$1=1,$$
$$1-4=-(1+2),$$
$$1-4+9=1+2+3,$$
$$1-4+9-16=-(1+2+3+4),$$
$$1-4+9-16+25=1+2+3+4+5.$$

Suponga una fórmula general y demuéstrela con inducción matemática.

5. Evalúe la suma $\sum_{k=1}^{n}\frac{k}{(k+1)!}$ para $n=1, 2, 3, 4$ y 5. Haga una suposición sobre una fórmula para esta suma para un n general y demuestre su suposición con inducción matemática.

6. Para cada n entero positivo, sea $P(n)$ la propiedad

$$5^n-1 \text{ es divisible por 4.}$$

a. Escriba $P(0)$. ¿Es $P(0)$ verdadera?
b. Escriba $P(k)$.
c. Escriba $P(k+1)$.
d. En una demostración por inducción matemática que esta propiedad de divisibilidad es válida para todo entero $n \geq 0$, ¿qué se debe demostrar en el paso inductivo?

7. Para cada entero positivo n, sea $P(n)$ la propiedad

$$2^n < (n+1)!.$$

a. Escriba $P(2)$. ¿Es $P(2)$ verdadera?
b. Escriba $P(k)$.
c. Escriba $P(\mathrm{k}+1)$.
d. En una demostración por inducción matemática que esta desigualdad es válida para todo entero $n \geq 2$, ¿qué debe demostrarse en el paso inductivo?

Demuestre cada enunciado en los ejercicios del 8 al 23 por inducción matemática.

8. 5^n-1 es divisible por 4, para cada entero $n \geq 0$.

9. 7^n-1 es divisible por 6, para cada entero $n \geq 0$.

10. n^3-7n+3 es divisible por 3, para cada entero $n \geq 0$.

11. $3^{2n}-1$ es divisible por 8, para cada entero $n \geq 0$.

12. Para cualquier entero $n \geq 0$, 7^n-2^n es divisible por 5.

H 13. Para cualquier entero $n \geq 0$, x^n-y^n es divisible por $x-y$, donde x y y son cualesquiera números enteros con $x \neq y$.

H 14. n^3-n es divisible por 6, para cada entero $n \geq 0$.

15. $n(n^2+5)$ es divisible por 6, para cada entero $n \geq 0$.

16. $2^n < (n+1)!$, Para todo entero $n \geq 2$.

17. $1+3n \leq 4^n$, para cada entero $n \geq 0$.

18. $5^n+9 < 6^n$, para todo entero $n \geq 2$.

19. $n^2 < 2^n$, para todo entero $n \geq 5$.

20. $2^n < (n+2)!$, para todo entero $n \geq 0$.

21. $\sqrt{n} < \frac{1}{\sqrt{1}}+\frac{1}{\sqrt{2}}+\cdots+\frac{1}{\sqrt{n}}$, para todo entero $n \geq 2$.

22. $1+nx \leq (1+x)^n$, para todos los números reales $x > -1$ y los enteros $n \geq 2$.

23. a. $n^3 > 2n+1$, para todo entero $n \geq 2$.
b. $n! > n^2$, para todo entero $n \geq 4$.

24. Una sucesión $a_1, a_2, a_3, \ldots$ se define haciendo $a_1=3$ y $a_k=7a_{k-1}$ para todo entero $k \geq 2$. Demuestre que $a_n=3\cdot 7^{n-1}$ para todo entero $n \geq 1$.

25. Una sucesión $b_0, b_1, b_2, \ldots$ se define haciendo $b_0=5$ y $b_k=4+b_{k-1}$ para todo entero $k \geq 1$. Demuestre que $b_n > 4n$ para todo entero $n \geq 0$.

26. Una sucesión $c_0, c_1, c_2, \ldots$ se define haciendo $c_0 = 3$ y $c_k = (c_{k-1})^2$ para todo entero $k \geq 1$. Demuestre que $c_n = 3^{2^n}$ para todo entero $n \geq 0$.

27. Una sucesión $d_1, d_2, d_3, \ldots$ se define haciendo $d_1 = 2$ y $d_k = \dfrac{d_{k-1}}{k}$ para todo entero $k \geq 2$. Demuestre que para todo entero $n \geq 1$,

$$d_n = \frac{2}{n!}.$$

28. Demuestre que para todos los enteros $n \geq 1$,

$$\frac{1}{3} = \frac{1+3}{5+7} = \frac{1+3+5}{7+9+11} = \cdots = \frac{1+3+\cdots+(2n-1)}{(2n+1)+\cdots+(4n-1)}.$$

29. Conforme llega a una reunión, cada uno de un grupo de empresarios saluda de mano a todas las personas presentes. Use inducción matemática para demostrar que si n personas asisten a la reunión entonces se producen, $[n(n-1)]/2$ saludos.

Para que una prueba por inducción matemática sea válida, el enunciado básico debe ser verdadero para $n = a$ y el argumento del paso inductivo debe ser correcto para cada entero $k \geq a$. En los ejercicios 30 y 31 encuentre los errores en las "demostraciones" por inducción matemática.

30. "**Teorema**": Para cualquier entero $n \geq 1$, todos los números de un conjunto de n números son iguales entre sí.

"**Demostración (por inducción matemática):** Evidentemente, es verdad que todos los números de un conjunto formado por un solo número son iguales entre sí, por lo que el paso básico es verdadero. Para el paso inductivo, sea $A = \{a_1, a_2, \ldots, a_k, a_{k+1}\}$ cualquier conjunto de $k+1$ números. Forma cada dos subconjuntos de tamaño k:

$$B = \{a_1, a_2, a_3, \ldots, a_k\} \quad \text{y}$$
$$C = \{a_1, a_3, a_4, \ldots, a_{k+1}\}$$

(B consiste de todos los números en A excepto a_{k+1} y C consiste de todos los números en A excepto a_2). Por hipótesis inductiva, todos los números en B iguales a a_1 y todos los números de C iguales a a_1 (ya que ambos conjuntos tienen sólo k números). Pero todos los números de A están en B o en C, por lo que todos los números en A son iguales a a_1, por lo que todos son iguales entre sí".

H 31. "**Teorema**": Para todo entero $n \geq 1$, $3^n - 2$ es par.

"**Demostración (por inducción matemática):** Supongamos que el teorema es verdadero para un entero k, donde $k \geq 1$, es decir, suponer que $3^k - 2$ es par. Debemos demostrar que $3^{k+1} - 2$ es par. Pero

$$3^{k+1} - 2 = 3^k \cdot 3 - 2 = 3^k(1+2) - 2$$
$$= (3^k - 2) + 3^k \cdot 2.$$

Ahora $3^k - 2$ es par por hipótesis inductiva y $3^k \cdot 2$ es par por inspección. Por tanto la suma de las dos cantidades es par (por el teorema 4.1.1). De lo que se deduce que el $3^{k+1} - 2$ es par, que es lo que necesitamos demostrar".

H 32. Algunos tableros de 5×5 con un cuadrado eliminado pueden ser completamente cubiertos por trominos en forma de L, mientras que en otros tableros de 5×5 no se pueden. Encuentre ejemplos de ambos tipos de tableros. Justifique su respuesta.

33. Considere un tablero de 4×6. Dibuje una cubierta del tablero con trominos en forma de L.

H 34. **a.** Use inducción matemática para demostrar que cualquier tablero de dimensiones $3 \times 2n$ puede ser completamente cubierto con trominos en forma de L para cualquier entero $n \geq 1$.

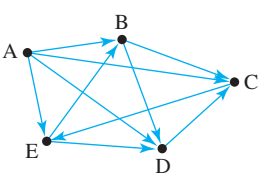
b. Sea n un entero mayor o igual a 1. Utilice el resultado del inciso *a*) para demostrar por inducción matemática que para todo entero m, cualquier tablero con dimensiones $2m \times 3n$ puede ser completamente cubierto con trominos en forma de L.

35. Sean m y n enteros cualesquiera que sean mayores o iguales a 1.

a. Demuestre que una condición necesaria para que un tablero $m \times n$ sea completamente cubierto con trominos en forma de L es que mn sea divisible por 3.

H b. Demuestre que tener que mn sea divisible por 3 no es una condición suficiente para que un tablero $m \times n$ sea completamente cubierto con trominos en forma de L.

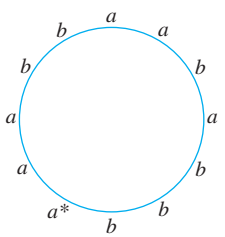
36. En un torneo de liguilla cada equipo juega contra cualquier otro equipo exactamente una vez. Si los equipos están etiquetados $T_1, T_2, \ldots, T_n$, entonces los resultados de un torneo se pueden representar con un dibujo, llamado *grafo dirigido*, en la que los equipos se representan como puntos y se dibuja una flecha de un punto a otro si y sólo si, el equipo representado por el primer punto gana al equipo representado por el segundo punto. Por ejemplo, el grafo dirigido que se presenta entonces muestra un resultado de un torneo de liguilla en el que participaron cinco equipos, A, B, C, D y E.



Use inducción matemática para demostrar que en un torneo de liguilla entre n equipos, donde $n \geq 2$, es posible etiquetar los equipos $T_1, T_2, \ldots, T_n$ tal que T_i gana T_{i+1} para todo $i = 1, 2, \ldots, n-1$. (Por ejemplo, en el caso anterior es $T_1 = A$, $T_2 = B$, $T_3 = C$, $T_4 = E$, $T_5 = D$) (*Sugerencia:* Dados $k+1$ equipos, elija uno, digamos T' y aplique la hipótesis inductivas a los equipos restantes para obtener un orden $T_1, T_2, \ldots, T_k$. Considere tres casos: T'gana a T_1, T' pierde con los primeros m equipos (donde $1 \leq m \leq k-1$) y les gana al $(m+1)$ésimo equipo y T' pierde con todos los otros equipos).

H ⋆ 37. En el borde exterior de un disco circular los números enteros de 1 a 30 están pintados en orden aleatorio. Demuestre que no importa en qué orden esté, debe haber tres números enteros consecutivos cuya suma es al menos 45.

***H* 38.** Suponga que n a's y n b's se distribuyen alrededor de la salida de un círculo. Use inducción matemática para demostrar que para todo entero $n \geq 1$, dado cualquier arreglo, es posible encontrar un punto de partida de modo que si uno viaja alrededor del círculo en el sentido de las manecillas del reloj, el número de a's que han pasado nunca es menor que el número b's que han pasado. Por ejemplo, en el diagrama que se muestra entonces, se podría empezar con la a con asterisco.



39. Para que un polígono sea **convexo** significa que todos los ángulos interiores son menores de 180 grados. Utilice la inducción matemática para demostrar que para todo $n \geq 3$, los ángulos de cualquier polígono convexo de n lados suman $180(n - 2)$ grados.

40. a. Demuestre que en un tablero de 8×8 alternando cuadrados en blanco y negro, si los cuadrados en la parte superior derecha e inferior izquierda se quitan del tablero restante no se puede cubrir con dominós. (*Sugerencia:* La inducción matemática no es necesaria para esta demostración).
    b. Use inducción matemática para demostrar que para todo n entero, si en un tablero de $2n \times 2n$ con cuadrados en blanco y negro alternados se le han retirado un cuadrado blanco y un cuadrado negro de cualquier lugar en el tablero, los cuadrados restantes se pueden cubrir con fichas de dominó.

Respuestas del autoexamen

1. deductivo 2. demostrar

5.4 Inducción matemática fuerte y el principio del buen orden de los números enteros

Las matemáticas nos llevan aún más lejos de lo humano en la región de absoluta necesidad, en la que no sólo el mundo real, sino todo lo que es posible, se debe cumplir.
—Bertrand Russell, 1902

La inducción matemática fuerte es similar a la inducción matemática ordinaria en que se trata de una técnica para establecer la verdad de una sucesión de enunciados acerca de los números enteros. Además, una demostración por inducción matemática fuerte consiste de un paso básico y de un paso inductivo. Sin embargo, el paso básico puede contener demostraciones para varios valores iniciales y en el paso inductivo la veracidad del predicado $P(n)$ se supone no sólo para un valor de n, sino para *todos* los valores k y después se demuestra la veracidad de $P(k + 1)$.

Principio de Inducción matemática fuerte

Sea $P(n)$ una propiedad que se define para n enteros y sean a y b enteros fijos con $a \leq b$. Suponga que los siguientes dos enunciados son verdaderas:

1. $P(a), P(a + 1), \ldots$ y $P(b)$ son todas verdaderas. (**Paso básico**.)
2. Para cualquier número entero $k \geq b$, si $P(i)$ es verdadera para todo enteros i de a a k, entonces $P(k + 1)$ es verdadera. (**Paso inductivo**.)

Entonces el enunciado

$$\text{para todo entero } n \geq a, P(n),$$

es verdadero. (La suposición de que $P(i)$ es verdadera para todo entero i de a a k se llama la **hipótesis inductiva**. Otra forma de indicar la hipótesis inductiva es decir, que $P(a), P(a + 1), \ldots, P(k)$ son todas verdaderas.)

Cualquier enunciado que se puede demostrar con inducción matemática ordinaria se puede demostrar con inducción matemática fuerte. La razón es que dado cualquier entero $k \geq b$, si sólo la veracidad de $P(k)$ implica la veracidad de $P(k + 1)$, entonces sin duda la veracidad de $P(a)$, $P(a + 1), \ldots$ y $P(k)$ implica la verdad de $P(k + 1)$. También es el caso que cualquier enunciado que se puede demostrar con inducción matemática fuerte se puede demostrar con inducción matemática común. Se esboza una demostración en el ejercicio 27 al final de esta sección.

En sentido estricto, el principio de inducción matemática fuerte se puede escribir con un paso básico si el paso inductivo se ha cambiado a "$\forall\, k \geq a - 1$, si $P(i)$ es verdadera para todo entero i de a a k, entonces $P(k + 1)$ es verdadera". La razón de esto es que el enunciado "$P(i)$ es verdadera para todo entero i de a a k" es vacuamente verdadero para $k = a - 1$. Por tanto, si la implicación en el paso inductivo es verdadero, entonces la conclusión de $P(a)$ también debe ser verdadera,* lo que demuestra el paso básico. Sin embargo, en muchos casos la prueba de la implicación para $k \geq b$ no funciona para $a \leq k \leq b$. Por tanto, es una buena idea adquirir el hábito de pensar por separado acerca de los casos donde $a \leq k \leq b$ incluyendo explícitamente un paso básico.

El principio de inducción matemática fuerte que se conoce bajo diversos nombres, tales como el *segundo principio de inducción*, el *segundo principio de inducción finita* y el *principio de inducción completa*.

Aplicación de la inducción matemática fuerte

El teorema de divisibilidad entre un primo establece que cualquier número entero mayor que 1 es divisible por un número primo. Probamos este teorema utilizando inducción matemática fuerte.

Ejemplo 5.4.1 Divisibilidad por un primo

Demuestre el teorema 4.3.4: Cualquier número entero mayor que 1 es divisible por un número primo.

Solución La idea para el paso inductivo es la siguiente: Si un entero dado mayor que 1 no es en sí primo, entonces es un producto de dos números enteros positivos pequeños, cada uno de ellos mayor que 1. Puesto que está suponiendo que cada uno de estos números enteros más pequeños es divisible por un número primo, por transitividad de la divisibilidad, los números primos también dividen al número entero con que se empezó.

Demostración (por inducción matemática fuerte):

Sea la propiedad $P(n)$ la frase

n es divisible por un número primo. $\leftarrow P(n)$

Demostración de que P(2) es verdadera:
Para establecer $P(2)$, debemos demostrar que

2 es divisible por un número primo. $\leftarrow P(2)$

Pero esto es así porque 2 es divisible por 2 y 2 es un número primo.

Demostración de que para todo entero $k \geq 2$, si P(i) es verdadera para todo entero i de 2 a k, entonces $P(k + 1)$ también es verdadera:

continúa en la página 270

*Si ha demostrado que un enunciado dado si-entonces es verdadero y si también sabe que la hipótesis es verdadera, entonces la conclusión debe ser verdadera.

Sea k un número entero con $k \geq 2$ y supongamos que

i es divisible por un número primo para todo entero i de 2 a k. ← hipótesis inductiva

Debemos demostrar que

$k + 1$ es divisible por un número primo. ← $P(k + 1)$

Caso 1 ($k + 1$ es primo): En este caso $k + 1$ es divisible por un número primo, o sea el mismo.

Caso 2 ($k + 1$ no es primo): En este caso $k + 1 = ab$, donde a y b son enteros con $1 < a < k + 1$ y $1 < b < k + 1$. Así, en particular, $2 \leq a \leq k$, por lo que por hipótesis inductiva, a es divisible por un número primo p. Además ya $k + 1 = ab$, se tiene que $k + 1$ es divisible por a. Por tanto ya $k + 1$ es divisible por a y a es divisible por p, por transitividad de la divisibilidad, $k + 1$ es divisible por el número primo p.

Por tanto, independientemente de si $k + 1$ es primo o no, es divisible por un número primo *[como se quería demostrar]*.

[Ya que hemos demostrado tanto el paso básico como el paso inductivo de la inducción matemática fuerte, llegamos a la conclusión de que el enunciado es verdadero.]

■

Tanto la inducción matemática común como la fuerte se pueden utilizar para mostrar el resultado de que los términos de ciertas sucesiones satisfacen ciertas propiedades. El ejemplo siguiente muestra cómo se hace esto con inducción fuerte.

Ejemplo 5.4.2 Demostración de una propiedad de una sucesión con inducción fuerte

Se define una sucesión $s_0, s_1, s_2, \ldots$ de la siguiente manera:

$$s_0 = 0, \quad s_1 = 4, \quad s_k = 6a_{k-1} - 5a_{k-2} \quad \text{para todo entero } k \geq 2.$$

a. Encuentre los cuatro primeros términos de esta sucesión.

b. Se afirma que para cada entero $n \geq 0$, el enésimo término de la sucesión tiene el mismo valor que el dado por la fórmula $5^n - 1$. En otras palabras, la afirmación es que todos los términos de la sucesión satisfacen la ecuación $s_n = 5^n - 1$. Demuestre que esta es verdadera.

Solución

a. $s_0 = 0, \qquad s_1 = 4, \qquad s_2 = 6s_1 - 5\, s_0 = 6 \cdot 4 - 5 \cdot 0 = 24,$
$s_3 = 6s_2 - 5\, s_1 = 6 \cdot 24 - 5 \cdot 4 = = 144 - 20 = 124$

b. Al utilizar inducción matemática fuerte para demostrar que cada término de la sucesión satisface la ecuación, el paso básico debe demostrar que los dos primeros términos la satisfacen. Esto es necesario porque, de acuerdo con la definición de sucesión, para calcular los valores de los últimos términos se requieren conocer los valores de los *dos* términos anteriores. Así si el paso básico sólo muestra que el primer término cumple la ecuación, no sería posible utilizar el paso inductivo para deducir que el segundo término satisface la ecuación. En el paso inductivo suponga que para un entero $k \geq 1$ elegido arbitrariamente, todos los términos de la sucesión de s_0 a s_k satisfacen la ecuación dada y, después deduzca que s_{k+1} también debe satisfacer la ecuación.

Demostración:

Sea $s_0, s_1, s_2, \ldots$ la sucesión definida mediante la especificación de que $s_0 = 0$, $s_1 = 4$ y $s_k = 6a_{k-1} - 5a_{k-2}$ para todo entero $k \geq 2$ y sea la propiedad $P(n)$ la fórmula

$$s_n = 5^n - 1 \qquad \leftarrow P(n)$$

Vamos a utilizar la inducción matemática fuerte para demostrar que para todo entero $n \geq 0$, $P(n)$ es verdadera.

Demostración de que P(0) y P(1) son verdaderas:
Para establecer $P(0)$ y $P(1)$, debemos demostrar que

$$s_0 = 5^0 - 1 \quad \text{y} \quad s_1 = 5^1 - 1. \qquad \leftarrow P(0) \quad \text{y} \quad P(1)$$

Pero, por definición de $s_0, s_1, s_2, \ldots$, tenemos que $s_0 = 0$ y $s_1 = 4$. Ya que $5^0 - 1 = 1 - 1 = 0$ y $5^1 - 1 = 5 - 1 = 4$, los valores de s_0 y s_1 de acuerdo con los valores dados por la fórmula.

Demostración de que para todo entero k ≥ 1, si P(i) es verdadera para todo entero i de 0 a k, entonces P(k + 1) también es verdadera:
Sea k un número entero con $k \geq 1$ y supongamos que

$$s_i = 5^i - 1 \text{ para todo entero } i \text{ con } 0 \leq i \leq k. \qquad \leftarrow \text{hipótesis inductiva}$$

Debemos demostrar que

$$s_{k+1} = 5^{k+1} - 1. \qquad \leftarrow P(k+1)$$

Pero puesto que $k \geq 1$, tenemos que $k + 1 \geq 2$ y así

$$\begin{aligned}
s_{k+1} &= 6s_k - 5s_{k-1} && \text{por definición de } s_0, s_1, s_2, \ldots \\
&= 6(5^k - 1) - 5(5^{k-1} - 1) && \text{por definición de hipótesis} \\
&= 6 \cdot 5^k - 6 - 5^k + 5 && \text{multiplicando y aplicando una ley de los exponentes} \\
&= (6 - 1)5^k - 1 && \text{factorizando el 6 y haciendo aritmética} \\
&= 5 \cdot 5^k - 1 && \text{por aritmética} \\
&= 5^{k+1} - 1 && \text{aplicando una ley de exponentes,}
\end{aligned}$$

[como se quería demostrar].

[Como hemos demostrado tanto el paso básico como el paso inductivo de la inducción matemática fuerte, llegamos a la conclusión de que el enunciado es verdadero.]

■

Otro uso de la inducción fuerte es el cálculo de productos. Se puede calcular un producto de cuatro números de muchas de maneras diferentes como lo indica la colocación de los paréntesis. Por ejemplo,

$((x_1x_2)x_3)x_4$ significa multiplicar x_1 y x_2, multiplique el resultado por x_3 y después multiplique ese número por x_4.

Y

$(x_1x_2)(x_3x_4)$ significa multiplicar x_1 y x_2, multiplique x_3 y x_4 y después tome el producto de los dos.

Observe que en los dos ejemplos anteriores, aunque los factores se multiplican en un orden diferente, el número de multiplicaciones —tres— es el mismo. Se utiliza inducción matemática fuerte para demostrar una generalización de este hecho.

Nota Al igual que muchas definiciones, para casos extremos esta puede parecer extraña, pero esto hace que las cosas funcionen muy bien

Convención

Acordamos decir que un solo número x_1, es un producto con un factor y se puede calcular con cero multiplicaciones.

Ejemplo 5.4.3 Número de multiplicaciones necesarias para multiplicar *n* números

Demuestre que para cualquier entero $n \geq 1$, si $x_1, x_2, \ldots, x_n$ son n números, entonces no importa cómo se insertan los paréntesis en su producto, el número de multiplicaciones que se utilizan para calcular el producto es $n - 1$.

Solución La veracidad del paso básico se sigue inmediatamente de la convención de un producto con un factor. El paso inductivo se basa en el hecho de que cuando varios números se multiplican entre sí, cada paso del proceso consiste en multiplicar dos cantidades individuales. Por ejemplo, el paso final para calcular $((x_1x_2)x_3)(x_4x_5)$ es multiplicar $(x_1x_2)x_3$ y x_4x_5. En general, si $k + 1$ números se multiplican, las dos cantidades en el paso final consisten de menos de $k + 1$ factores. Esto es lo que hace posible el uso de la hipótesis inductiva.

Demostración (por inducción matemática fuerte):

Sea la propiedad $P(n)$ la frase

> Si $x_1, x_2, \ldots, x_n$ son n números, entonces no importa cómo se insertan los paréntesis en su producto, el número de multiplicaciones que se usa para calcular el producto es $n - 1$. ← $P(n)$

Demostración de que P(1) es verdadera:
Para establecer $P(1)$, debemos demostrar que

> El número de multiplicaciones necesarias para calcular el producto de x_1 es $1 - 1$. ← $P(1)$

Esto es verdadero porque, por convención, x_1 es un producto que se puede calcular con multiplicaciones y $0 = 1 - 1$.

Demostración de que para todo entero $k \geq 1$, si P(i) es verdadera para todo entero i entre 1 y k, entonces P(k + 1) también es verdadera:
Sea k cualquier número entero con $k \geq 1$ y supongamos que

> Por todo entero i de 1 a k, si $x_1, x_2, \ldots, x_i$ son números, entonces no importa cómo se insertan paréntesis en su producto, el número de multiplicaciones para calcular el producto es $i - 1$. ← hipótesis inductiva

Debemos demostrar que

> Si $x_1, x_2, \ldots, x_{k+1}$ son $k + 1$ números, entonces no importa cómo se insertan paréntesis en su producto, el número de multiplicaciones que se usa para calcular el producto es $(k + 1) - 1 = k$. ← $P(k + 1)$

Considere un producto de $k + 1$ factores: $x_1, x_2, \ldots, x_{k+1}$. Cuando se inserta entre paréntesis para calcular el producto, alguna multiplicación está al final y cada uno de

los dos factores que componen la multiplicación final es un producto de menos de $k + 1$ factores. Sea L el producto de los factores de la izquierda y R el producto de los factores de la derecha y supongamos que L consiste de l factores y R consiste de r factores. Entonces $l + r = k + 1$, el número total de factores en el producto y

$$1 \leq l \leq k \quad \text{y} \quad 1 \leq r \leq k.$$

Por hipótesis inductiva, la evaluación de L tiene $l - 1$ multiplicaciones y la evaluación de R tiene $r - 1$ multiplicaciones. Debido a que se necesita una multiplicación final para evaluar $L \cdot R$, el número de multiplicaciones necesarias para evaluar el producto de todos los $k + 1$ factores es

$$(l - 1) + (r - 1) + 1 = (l + r) - 1 = (k + 1) - 1 = k.$$

[Esto es lo que se quería demostrar.]
[Como hemos demostrado el paso básico y el paso inductivo de la inducción matemática fuerte, llegamos a la conclusión de que el enunciado dado es verdadero.]

■

La inducción matemática fuerte hace posible una demostración del hecho frecuentemente usado en ciencias de la computación de que todo entero positivo n tiene una representación binaria entera única. La demostración se ve muy complicada, debido a toda la notación necesaria para escribir los distintos pasos. Pero la idea de la demostración es simple. Esta es que si los números enteros más pequeños que n tienen representación única como suma de potencias de 2, entonces la única representación de n como suma de potencias de 2 se puede encontrar tomando la representación de $n/2$ (o para $(n - 1)/2$ si n es impar) y multiplicándola por 2.

Teorema 5.4.1 Existencia y unicidad de representaciones de enteros binarios

Dado cualquier número entero positivo n, n tiene una representación única en la forma

$$n = c_r \cdot 2^r + c_{r-1} \cdot 2^{r-1} + \cdots + c_2 \cdot 2^2 + c_1 \cdot 2 + c_0,$$

donde r es un entero no negativo, $c_r = 1$ y $c_j = 1$ o 0 para todo $j = 0, 1, 2, \ldots, r - 1$.

Demostración:

Damos las demostraciones por separado de la inducción matemática fuerte para mostrar primero la existencia y segundo la unicidad de la representación binaria.

Existencia (demostración por inducción matemática fuerte): Sea la propiedad $P(n)$ la ecuación

$$n = c_r \cdot 2^r + c_{r-1} \cdot 2^{r-1} + \cdots + c_2 \cdot 2^2 + c_1 \cdot 2 + c_0, \qquad \leftarrow P(n)$$

donde r es un entero no negativo, $c_r = 1$ y $c_j = 1$ o 0 para todo $j = 0, 1,2, \ldots, r - 1$.

Demostración de que P(1) es verdadera:
Sea $r = 0$ y $c_0 = 1$. Entonces, $1 = c_r \cdot 2^r$ y así $n = 1$ se puede escribir en la forma requerida.

Demostración de que para todo entero $k \geq 1$, si P(i) es verdadera para todo entero i de 1 a k, entonces P(k + 1) es también verdadera:

continúa en la página 274

Sea k un entero con $k \geq 1$. Supongamos que para todo entero i de 1 a k,

$$i = c_r \cdot 2^r + c_{r-1} \cdot 2^{r-1} + \cdots + c_2 \cdot 2^2 + c_1 \cdot 2 + c_0, \qquad \leftarrow \text{hipótesis inductiva}$$

donde r es un entero no negativo, $c_r = 1$, $c_j = 1$ o 0 para toda $j = 0, 1, 2, \ldots, r-1$. Debemos demostrar que $k+1$ se puede escribir como suma de potencias de 2 en la forma requerida.

Caso 1 ($k+1$ es par): En este caso $(k+1)/2$ es un número entero y por hipótesis inductiva ya que $1 \leq (k+1)/2 \leq k$, entonces,

$$\frac{k+1}{2} = c_r \cdot 2^r + c_{r-1} \cdot 2^{r-1} + \cdots + c_2 \cdot 2^2 + c_1 \cdot 2 + c_0,$$

donde r es un entero no negativo, $c_r = 1$ y $c_j = 1$ o 0 para toda $j = 0, 1, 2, \ldots, r-1$. Multiplicando ambos lados de la ecuación por 2 se obtiene

$$k+1 = c_r \cdot 2^{r+1} + c_{r-1} \cdot 2^r + \cdots + c_2 \cdot 2^3 + c_1 \cdot 2^2 + c_0 \cdot 2,$$

que es una suma de potencias de 2 de la forma requerida.

Caso 2 ($k+1$ es impar): En este caso $k/2$ es un entero y por hipótesis inductiva ya que $1 \leq k/2 \leq k$, entonces,

$$\frac{k}{2} = c_r \cdot 2^r + c_{r-1} \cdot 2^{r-1} + \cdots + c_2 \cdot 2^2 + c_1 \cdot 2 + c_0,$$

donde r es un entero no negativo, $c_r = 1$ y $c_j = 1$ o 0 para toda $j = 0, 1, 2, \ldots, r-1$. Multiplicando ambos lados de la ecuación por 2 y sumando 1 se obtiene

$$k+1 = c_r \cdot 2^{r+1} + c_{r-1} \cdot 2^r + \cdots + c_2 \cdot 2^3 + c_1 \cdot 2^2 + c_0 \cdot 2 + 1,$$

que es también una suma de potencias de 2 de la forma requerida.

Los argumentos anteriores muestran que, independientemente de si $k+1$ es par o impar, $k+1$ tiene una representación de la forma requerida. *[O, en otras palabras, $P(k+1)$ es verdadera como se quería demostrar.]*

[Como hemos demostrado el paso básico y el paso inductivo de la inducción matemática fuerte, la existencia de la mitad del teorema es verdadera.]

Unicidad: Para probar la unicidad, supongamos que existe un entero n con dos representaciones diferentes como suma de potencias enteras no negativas de 2. Igualando las dos representaciones y eliminando todos los términos idénticos se obtiene

$$2^r + c_{r-1} \cdot 2^{r-1} + \cdots + c_1 \cdot 2 + c_0 = 2^s + d_{s-1} \cdot 2^{s-1} + \cdots + d_1 \cdot 2 + d_0 \qquad 5.4.1$$

donde r y s son números enteros no negativos y cada c_i y cada d_i son iguales a 0 o a 1. Sin perder generalidad, podemos suponer que $r < s$. Pero la fórmula para la suma de una sucesión geométrica (teorema 5.2.3) y ya que $r < s$,

$$\begin{aligned} 2^r + c_{r-1} \cdot 2^{r-1} + \cdots + c_1 \cdot 2 + c_0 &\leq 2^r + 2^{r-1} + \cdots + 2 + 1 = 2^{r+1} - 1 \\ &< 2^s. \end{aligned}$$

Por tanto

$$2^r + c_{r-1} \cdot 2^{r-1} + \cdots + c_1 \cdot 2 + c_0 < 2^s + d_{s-1} \cdot 2^{s-1} + \cdots + d_1 \cdot 2 + d_0,$$

que contradice a la ecuación (5.4.1). De ahí que la suposición es falsa, por lo que cualquier número entero n tiene una sola representación como suma de potencias enteras no negativas de 2.

El principio del buen orden para enteros

El principio del buen orden para enteros que se ve muy diferente de los comunes y sólidos principios de la inducción matemática, pero se puede demostrar que los tres principios son equivalentes. Es decir, si cualquiera de los tres es verdadero, entonces también lo son las otras dos.

Principio del buen orden para los enteros

Sea S un conjunto de números enteros que contienen uno o más números enteros todos los cuales son mayores que un entero fijo. Entonces S tiene un mínimo elemento.

Observe que cuando el contexto hace la referencia clara, escribiremos simplemente "el principio del buen orden" en lugar de "el principio del buen orden de los números enteros".

Ejemplo 5.4.4 Determinación del mínimo elemento

En cada caso, si el conjunto tiene un elemento mínimo, diga cuál es. Si no, explique por qué no se viola, el principio del buen orden.

a. El conjunto de todos los números reales positivos.

b. El conjunto de todos los números enteros n no negativos tales que $n^2 < n$.

c. El conjunto de todos los números enteros no negativos de la forma $46 - 7k$, donde k es un número entero.

Solución

a. No hay un mínimo número real positivo. Porque, si x es cualquier número real positivo, entonces $x/2$ es un número real positivo que es menor que x. No ocurre violación del principio del buen orden ya que el principio del buen orden sólo se refiere a conjuntos de enteros y este conjunto no es un conjunto de números enteros.

b. No hay al *menos* un entero no negativo n tal que $n^2 < n$ porque no hay entero no negativo que satisfaga esta desigualdad. El principio del buen orden no es violado ya que el principio del buen orden sólo se refiere a los conjuntos que contienen al menos un elemento.

c. La siguiente tabla muestra los valores de $46 - 7k$ para varios valores de k.

k	0	1	2	3	4	5	6	7	$\cdots$	-1	-2	-3	$\cdots$
$46 - 7k$	46	39	32	25	18	11	4	-3	$\cdots$	53	60	67	$\cdots$

La tabla le indica y puede confirmar fácilmente, que $46 - 7k < 0$ para $k \geq 7$ y que $46 - 7k \geq 46$ para $k \leq 0$. Por tanto, de los otros valores en la tabla, es evidente que 4 es el menor entero no negativo de la forma $46 - 7k$. Este corresponde a $k = 6$. ■

Otra forma de ver el análisis del ejemplo 5.4.4*c*) es observar que al restar seis veces 7 de 46 queda 4 y este es el menor entero no negativo obtenido por la resta repetida, de 7 de 46. En otras palabras, 6 es el cociente y el 4 es el residuo de la división de 46 por 7. De manera más general, en la división de cualquier número entero n por cualquier número entero positivo d, el residuo r es el menor entero no negativo de la forma $n - dk$. Este es el corazón de la siguiente demostración de la parte de la existencia del teorema de cociente-residuo (la parte que garantiza la existencia de un cociente y un residuo de la división de

un entero entre un entero positivo). Para una demostración de unicidad del cociente y el residuo, vea el ejercicio 18 de la sección 4.6.

Teorema del cociente-residuo (Parte de existencia)

Dado cualquier número entero n y cualquier número entero positivo d, existen enteros q y r tales que

$$n = dq + r \quad \text{y} \quad 0 \leq r < d.$$

Demostración:

Sea S el conjunto de todos los números enteros no negativos de la forma

$$n - dk,$$

donde k es un número entero. Este conjunto tiene al menos un elemento. *[Porque, si n es negativo, entonces*

$$n - 0 \cdot d = n \geq 0,$$

y así $n - 0 \cdot d$ está en S. Y si n es negativo, entonces

$$n - nd = \underbrace{n}_{<0}\underbrace{(1 - d)}_{\leq 0 \text{ ya que } d \text{ es un entero positivo}} \geq 0,$$

y así $n - nd$ está en S.] De lo que se deduce por el principio del buen orden de los números enteros que S contiene un mínimo elemento r. Entonces, para algún entero dado $k = q$,

$$n - dq = r$$

[ya que cada número entero en S se puede escribir de esta forma]. Sumando dq a ambos lados se obtiene

$$n = dq + r.$$

Además, $r < d$. *[Supongamos que $r \geq d$. Entonces*

$$n - d(q + 1) = n - dq - d = r - d \geq 0,$$

y así $n - d(q + 1)$ sería un entero no negativo en S que es menor que r. Pero r es el menor entero en S. Esta contradicción muestra que la suposición de que $r \geq d$ debe ser falsa.] Los argumentos anteriores demuestran que existen enteros r y q para los que

$$n = dq + r \quad \text{y} \quad 0 \leq r < d.$$

[Esto es lo que se quería demostrar.]

Otra consecuencia del principio del buen orden es el hecho de que cualquier sucesión estrictamente decreciente de números enteros no negativos es finita. Es decir, si $r_1, r_2, r_3, \ldots$ es una sucesión de números enteros no negativos que satisfacen

$$r_i = r_{i+1}$$

para toda $i \geq 1$, entonces $r_1, r_2, r_3, \ldots$ es una sucesión finita. *[Por el principio del buen orden dicha sucesión tiene un mínimo elemento r_k. De lo que se deduce que r_k debe ser el término final de la sucesión ya que si hubiera un término r_{k+1}, entonces puesto que la sucesión es estrictamente decreciente, $r_{k+1} < r_k$, lo que sería una contradicción.]* Este hecho es frecuentemente usado en ciencias de la computación para demostrar que los algoritmos terminan después de un número finito de pasos.

Autoexamen

1. En una demostración por inducción matemática fuerte el paso básico podrá exigir la comprobación de una propiedad $P(n)$ para más _____ valor de n.
2. Supongamos que en el paso básico para una demostración de inducción matemática fuerte la propiedad $P(n)$ se comprobó para todo entero n de a a b. Entonces en el paso inductivo se supone que para cualquier entero $k \geq b$, la propiedad $P(n)$ es verdadera para todos los valores de i para _____ a _____ y se demuestra que _____ es verdadera.
3. De acuerdo con el principio del buen orden de los enteros, si un conjunto S de enteros contiene al menos _____ y hay algún entero que es menor o igual para todo _____, entonces _____.

Conjunto de ejercicios 5.4

1. Supongamos que $a_1, a_2, a_3, \ldots$ es una sucesión definida de la siguiente manera:

$$a_1 = 1, a_2 = 3,$$
$$a_k = a_{k-2} + 2a_{k-1} \quad \text{para todo entero } k \geq 3.$$

Demuestre que a_n es impar para todo entero $n \geq 1$.

2. Supongamos $b_1, b_2, b_3, \ldots$ es una sucesión definida de la siguiente manera:

$$b_1 = 4, b_2 = 12$$
$$b_k = b_{k-2} + b_{k-1} \quad \text{para todo entero } k \geq 3.$$

Demuestre que b_n es divisible por 4 para todo entero $n \geq 1$.

3. Supongamos que $c_0, c_1, c_2, \ldots$ es una sucesión definida de la siguiente manera:

$$c_0 = 2, c_1 = 2, c_2 = 6,$$
$$c_k = 3c_{k-3} \quad \text{para todo entero } k \geq 3.$$

Demuestre que c_n es par para todo entero $n \geq 0$.

4. Supongamos que $d_1, d_2, d_3, \ldots$ es una sucesión definida de la siguiente manera:

$$d_1 = \frac{9}{10}, \; d_2 = \frac{10}{11},$$
$$d_k = d_{k-1} \cdot d_{k-2} \quad \text{para todo entero } k \geq 3.$$

Demuestre que $0 < d_n \leq 1$ para todo entero $n \geq 0$.

5. Supongamos que $e_0, e_1, e_2, \ldots$ es una sucesión definida de la siguiente manera:

$$e_0 = 12, e_1 = 29$$
$$e_k = 5e_{k-1} - 6e_{k-2} \quad \text{para todo entero } k \geq 2.$$

Demuestre que $e_n = 5 \cdot 3^n + 7 \cdot 2^n$ para todo entero $n \geq 0$.

6. Supongamos que $f_0, f_1, f_2, \ldots$ es una sucesión definida de la siguiente manera:

$$f_0 = 5, f_2 = 16$$
$$f_k = 7f_{k-1} - 10f_{k-2} \quad \text{para todo entero } k \geq 2.$$

Demuestre que $f_n = 3 \cdot 2^n + 2 \cdot 5^n$ para todo entero $n \geq 0$.

7. Supongamos que $g_1, g_2, g_3, \ldots$ es una sucesión definida de la siguiente manera:

$$g_1 = 3, g_2 = 5$$
$$g_k = 3g_{k-1} - 2g_{k-2} \quad \text{para todo entero } k \geq 3.$$

Demuestre que $g_n = 2^n + 1$ para todo entero $n \geq 1$.

8. Supongamos que $h_0, h_1, h_2, \ldots$ es una sucesión definida de la siguiente manera:

$$h_0 = 1, h_1 = 2, h_2 = 3,$$
$$h_k = h_{k-1} + h_{k-2} + h_{k-3} \quad \text{para todo entero } k \geq 3.$$

a. Demuestre que $h_n \leq 3^n$ para todo entero $n \geq 0$.
b. Suponga que s es un número real tal que $s^3 \geq s^2 + s + 1$ (Esto implica que $s > 1.83$). Demuestre que $h_n \leq s^n$ para toda $n \geq 2$.

9. Defina una sucesión $a_1, a_2, a_3, \ldots$ de la siguiente manera: $a_1 = 1$, $a_2 = 3$ y $a_k = a_{k-1} + a_{k-2}$ para todo entero $k \geq 3$. (Esta sucesión se conoce como la sucesión de Lucas). Utilice la inducción matemática fuerte para demostrar que $a_n \leq \left(\frac{7}{4}\right)^n$ para todo entero $n \geq 1$.

H 10. El problema que se utilizó para introducir la inducción matemática común en la sección 5.2 también se puede resolver usando inducción matemática fuerte. Sea $P(n)$ "cualquier colección de n monedas puede obtenerse usando una combinación de monedas de 3¢ y 5¢". Utilice inducción matemática fuerte para demostrar que $P(n)$ es verdadera para todo entero $n \geq 14$.

11. Empiece a resolver un rompecabezas, encontrando dos piezas que coincidan y se ajusten juntas. Cada paso subsecuente de la solución consiste en encajar dos bloques compuestos de una o varias piezas que previamente se han ensamblado. Utilice inducción matemática fuerte para demostrar que el número de pasos necesarios para poner juntas todas las n piezas de un rompecabezas es $n - 1$.

H 12. Los lados de una pista circular contienen una sucesión de latas de gasolina. La cantidad total de latas es suficiente para que cierto automóvil haga un circuito completo de la pista y todo podría encajar en el tanque de gasolina del automóvil a la vez. Use inducción matemática para demostrar que es posible encontrar una ubicación inicial del automóvil, para que sea capaz de recorrer toda la pista utilizando las cantidades distintas de gasolina en las latas que se encuentran en el camino.

H 13. Utilice inducción matemática fuerte para demostrar la existencia de parte de la factorización única de números enteros (teorema 4.3.5): Cada entero mayor que 1 es un número primo o un producto de números primos.

14. Cualquier producto de dos o más números enteros es el resultado de sucesivas multiplicaciones de dos enteros a la vez. Por

ejemplo, aquí se presentan algunas de las formas en que puede calcularse $a_1a_2a_3a_4$: $(a_1a_2)(a_3a_4)$ o $((a_1a_2)a_3)a_4)$ o $a_1((a_2a_3)a_4)$. Utilice inducción matemática fuerte para demostrar que cualquier producto de dos o más enteros impares es impar.

15. Cualquier suma de dos o más números enteros es el resultado de las sumas sucesivas de dos números enteros a la vez. Por ejemplo, aquí están algunas de las maneras en las que $a_1 + a_2 + a_3 + a_4$, se pudiera calcular: $(a_1 + a_2) + (a_3 + a_4)$ o $((a_1 + a_2) + a_3) + a_4)$ o $a_1 + ((a_2 + a_3) + a_4)$. Utilice inducción matemática fuerte para demostrar que cualquier suma de dos o más enteros pares es par.

H 16. Utilice inducción matemática fuerte para demostrar que para cualquier entero $n \geq 2$, si n es par, cualquier suma de n enteros impares es par y si n es impar, entonces cualquier suma de n enteros impares es impar.

17. Calcule 4^1, 4^2, 4^3, 4^4, 4^5, 4^6, 4^7 y 4^8. Haga una suposición acerca del dígito de las unidades de 4^n, donde n es un entero positivo. Utilice inducción matemática fuerte para demostrar su suposición.

18. Calcule 9^0, 9^1, 9^2, 9^3, 9^4 y 9^5. Haga una suposición acerca del dígito de las unidades de 9^n, donde n es un entero positivo. Utilice inducción matemática fuerte para demostrar su suposición.

19. Encuentre el error en la siguiente "demostración" que pretende demostrar que toda potencia entera no negativa de cada número real distinto de cero es 1.

"**Demostración:** Sea r cualquier número distinto de cero y sea la propiedad $P(n)$ la ecuación $r^n = 1$.

Demostración de que P(0) es verdadera: $P(0)$ es verdadera porque $r^0 = 1$, por definición, de potencia cero.
Demostración de que para todo entero k ≥ 0, si P(i) es verdadera para todo entero i de 0 a k, entonces P(k + 1) también es verdadera: Sea k cualquier número entero con $k \geq 0$ y supongamos que $r^i = 1$ para todo entero i de 0 a k. Esta es la hipótesis inductiva. Debemos demostrar que $r^k + 1 = 1$. Ahora

$$\begin{aligned} r^{k+1} &= r^{k+k-(k-1)} && \text{ya que } k + k - (k - 1) \\ &&& = k + k - k + 1 = k + 1 \\ &= \frac{r^k \cdot r^k}{r^{k-1}} && \text{por las leyes de los exponentes} \\ &= \frac{1 \cdot 1}{1} && \text{por hipótesis inductiva} \\ &= 1. \end{aligned}$$

Así $r^{k+1} = 1$ *[como se quería demostrar]*.

[Como se ha demostrado el paso básico y el paso inductivo de la inducción matemática fuerte, llegamos a la conclusión de que el enunciado es verdadero.]".

20. Utilice el principio del buen orden de los números enteros para demostrar el teorema 4.3.4: Cada número entero mayor que 1 es divisible por un número primo.

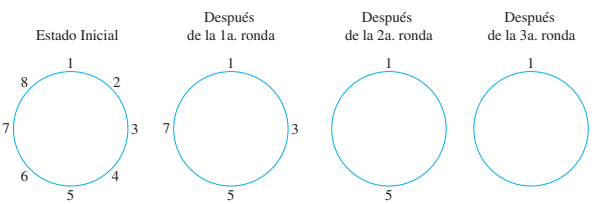
21. Utilice el principio del buen orden de los números enteros para demostrar la existencia de la parte de la factorización única del teorema de números enteros: Cada número entero mayor que 1 es primo o bien un producto de números primos.

22. **a.** La propiedad de Arquímedes para los números racionales establece que para todos los números racionales r, existe un entero n tal que $n > r$. Demuestre esta propiedad.
    b. Demuestre que dado cualquier número racional r, el número $-r$ es también racional.
    c. Utilice los resultados de los incisos *a*) y *b*) para demostrar que dado cualquier número racional r, existe un entero m tal que $m < r$.

H 23. Utilice los resultados del ejercicio 22 y el principio del buen orden de los números enteros para demostrar que dado cualquier número racional r, existe un entero m tal que $m \leq r < m + 1$.

24. Utilice el principio del buen orden para demostrar que, dado cualquier entero $n \geq 1$, existe un entero m impar y un entero no negativo k tal que $n = 2^k \cdot m$.

25. Imagine una situación en la que ocho personas, numeradas consecutivamente del 1 al 8, están dispuestos en un círculo. Comenzando con la persona #1, cada dos personas en el círculo es eliminada. El proceso de eliminación continúa hasta que sólo quede una persona. En la primera ronda las personas numerados con 2, 4, 6 y 8 son eliminados, en la segunda ronda las personas numeradas con 3 y 7 son eliminadas y en la tercera ronda la persona #5 se elimina. Así que después de la tercera ronda sólo la persona #1 permanece, como se muestra abajo.



a. Dado un conjunto de dieciséis personas dispuestas en círculo y numeradas, consecutivamente del 1 al 16, liste los números de las personas que son eliminados en cada ronda, si se elimina una persona cada dos personas y el proceso de eliminación continua hasta que sólo queda una persona. Supongamos que el punto de partida es la persona # 1.
b. Utilice la inducción matemática para demostrar que para todo entero $n \geq 1$, dado cualquier conjunto de 2^n personas dispuestas en un círculo y numeradas consecutivamente del 1 al 2^n, si se empieza con la persona #1 y repetidamente alrededor del círculo elimina sucesivamente cada segunda persona, a la larga sólo se mantendrá la persona #1.
c. Utilice el resultado del inciso *b*) para demostrar que para cualquier n números enteros no negativos y m con $2^n \leq 2^n + m < 2^{n+1}$, si $r = 2^n + m$, entonces, dado cualquier conjunto de personas dispuestas r en un círculo y numeradas consecutivamente del 1 al r, si se inicia con la persona #1 y se repite varias veces alrededor del círculo eliminando sucesivamente cada dos personas, a la larga la única persona que se mantiene es la $\#(2m + 1)$.

26. Supongamos que $P(n)$ es una propiedad tal que
    1. $P(0)$, $P(1)$, $P(2)$ son todas verdaderas,
    2. Para todo entero $k \geq 0$, si $P(k)$ es verdadera, entonces $P(3k)$ es verdadera. ¿Debe seguir que $P(n)$ es verdadera para todo entero $n \geq 0$? En caso afirmativo, explique por qué, si no, dé un contraejemplo.

27. Demuestre que si un enunciado se puede demostrar con inducción matemática fuerte, entonces se puede demostrar con inducción matemática ordinaria. Para esto, sea $P(n)$ una propiedad que se define para n enteros y supongamos que los siguientes dos enunciados son verdaderos:
    1. $P(a)$, $P(a+1)$, $P(a+2), \ldots, P(b)$.
    2. Para cualquier entero $k \geq b$, si $P(i)$ es verdadera para todo entero i de a a k, entonces $P(k+1)$ es verdadera.

    El principio de inducción matemática fuerte nos permite concluir de inmediato que $P(n)$ es verdadera para todo entero $n \geq a$. ¿Podemos llegar a la misma conclusión utilizando el principio de inducción matemática ordinaria? ¡Sí! Para ver esto, sea $Q(n)$ la propiedad

    $P(j)$ es verdadera para todo entero j con $a \leq j \leq n$.

    Después, utilice la inducción matemática ordinaria para demostrar que $Q(n)$ es verdadera para todo entero $n \geq b$. Es decir, demuestre que
    1. $Q(b)$ es verdadera.
    2. Para cualquier número entero $k \geq b$, si $Q(k)$ es verdadera, entonces $Q(k+1)$ es verdadera.

28. Dé ejemplos para enseñar la demostración del teorema 5.4.1.

H 29. Es un hecho que cada entero $n \geq 1$ se puede escribir en la forma

$$c_r \cdot 3^r + c_{r-1} \cdot 3^{r-1} + \cdots + c_2 \cdot 3^2 + c_1 \cdot 3 + c_0,$$

donde $c_r = 1$ o 2 y $c_i = 0$, 1 o 2 para todo entero $i = 0, 1, 2, \ldots, r-1$. Bosqueje una demostración de este hecho.

H ∗ 30. Utilice la inducción matemática para demostrar la parte de la existencia del teorema de cociente-residuo para enteros $n \geq 0$.

H ∗ 31. Demuestre que si se puede demostrar un enunciado por inducción matemática común, entonces se puede demostrar por el principio del buen orden.

H 32. Utilice el principio de inducción matemática ordinaria para probar el principio del buen orden para enteros.

Respuestas del autoexamen

1. de un 2. a; k; $P(k+1)$ 3. un número entero; entero en S, S contiene un mínimo elemento

5.5 Aplicación: exactitud de algoritmos

[P]rogramación confiable, debe ser una actividad de carácter innegablemente matemático .... Verá, en matemáticas se trata de pensar y hacer matemáticas siempre tratando de pensar lo mejor posible. —Edsger W. Dijkstra (1981)

The University of Texas at Austin

Edsger W. Dijkstra (1930-2002)

¿Qué significa que un programa de computadora sea exacto? Cada programa está diseñado para realizar una tarea específica a calcular la media o la mediana de un conjunto de números, calcular la cantidad de los cheques de pago de nómina de la empresa, reorganizar los nombres en orden alfabético y así sucesivamente. Diremos que un programa es exacto si produce la salida especifica en la documentación adjunta para cada conjunto de base de datos del tipo especificado en la documentación.*

La mayoría de los programadores escriben sus programas mediante una combinación de análisis lógico de ensayo y error. Para obtener que un programa corra todo, el programador debe corregir todos los errores de sintaxis (como escribir **ik** en vez de **if** o error al declarar una variable o usar una palabra clave restringida para un nombre de variable). Sin embargo, cuando se han eliminado los errores de sintaxis, el programa todavía puede contener errores lógicos que impidan que se produzca el resultado correcto. Con frecuencia, los programas se ponen a prueba utilizando conjuntos de datos de ejemplo en lo que se conoce de antemano la salida correcta. Y a menudo los datos de la muestra se eligen deliberadamente para probar la exactitud del programa en circunstancias extremas. Pero para la mayoría de los programas el número de posibles conjuntos de datos de entrada es infinito o inmanejablemente grande, por lo que ninguna cantidad de pruebas de programa puede dar plena seguridad de que el programa sea correcto para todos los posibles conjuntos de datos legales de entrada.

*Los consumidores de programas de computadora quieren una definición más estricta de la exactitud. Si un usuario pone datos de tipo incorrecto, el usuario desea un mensaje de error decente, no una falla del sistema.

Courtesy of Christiane Floyd

Robert W. Floyd (1936-2002)

Desde 1967, con la publicación de un artículo de Robert W. Floyd,* se ha dedicado considerable esfuerzo al desarrollo de métodos para probar programas correctos en el momento en que se componen. Uno de los pioneros en este esfuerzo, Edsger W. Dijkstra, afirmó que "ahora tomamos la posición de que no es sólo tarea del programador producir un programa exacto, sino también demostrar su exactitud de manera convincente".† Otro líder en el campo, David Gries, fue más allá al decir que "un programa y su prueba se deben desarrollar paso a paso, con la *prueba* que conduce el camino."** Si tales métodos con el tiempo se pueden utilizar para escribir grandes programas científicos y comerciales, los beneficios para la sociedad serán enormes.

Como con la mayoría de las técnicas que aún están en el proceso de desarrollo, los métodos para probar la exactitud del programa son un poco incómodos y difíciles de manejar. En esta sección damos una visión general del formato general de pruebas de exactitud y los detalles de una técnica fundamental, el *procedimiento del invariante del bucle*. En este momento, cambiamos el término *programa*, que se refiere a un lenguaje de programación particular, por el término más general *algoritmo*.

Afirmaciones

Considere un algoritmo que está diseñado para producir un estado final dado a partir de un estado inicial dado. Tanto el estado inicial como el final se pueden expresar como predicados que incluyen variables de entrada y de salida. A menudo, el predicado que describe el estado inicial se conoce como la **pre-condición del algoritmo** y el predicado que describe el estado final se llama la **post-condición del algoritmo**.

Ejemplo 5.5.1 Algoritmo de pre-condiciones y post-condiciones

Entonces se presentan pre y post condiciones para algunos algoritmos comunes.

a. Algoritmo para calcular un producto de enteros no negativos

Pre-condición: Las variables de entrada m y n son números enteros no negativos.

Post-condición: La variable de salida p es igual a mn.

b. Algoritmo para encontrar el cociente y el residuo de la división de un entero positivo entre otro

Pre-condición: Las variables de entrada a y b son enteros positivos.

Post-condición: Las variables de salida q y r son enteros tales que $a = bq + r$ y $0 \leq r < b$.

c. Algoritmo para ordenar un arreglo unidimensional de números reales

Pre-condición: La variable de entrada $A[1], A[2], \ldots, A[n]$ es un arreglo unidimensional de números reales.

Post-condición: La variable de salida $B[1], B[2], \ldots, B[n]$ es un arreglo unidimensional de números reales con los mismos elementos que $A[1], A[2], \ldots, A[n]$, pero con la propiedad de que $B[i] \leq B[j]$, siempre que $i \leq j$. ■

*R. W. Floyd, "Assigning meanings to programs", *Proc. Symp. Appl. Math.*, Amer. Math. Soc. **19** (1967), 19-32.

†Edsger Dijkstra en O. J. Dahl, E. W. Dijkstra y C. A. R. Hoare, *Structured Programming* (Londres: Academic Press, 1972), p. 5.

**David Gries, *The science of Programming* (Nueva York: Springer-Verlag, 1981), p. 164.

Una prueba de la exactitud del algoritmo consiste en mostrar que si la precondición para el algoritmo es verdadera para un conjunto de valores de las variables de entrada y si se ejecutan los enunciados de los algoritmos, entonces, la post-condición también es verdadera.

El principio de "divide y vencerás" ha sido útil en muchos aspectos de la programación de computadora y probar la exactitud del algoritmo no es una excepción. Los pasos de un algoritmo se dividen en secciones con afirmaciones acerca del estado actual de las variables del algoritmo que se insertan en puntos estratégicamente elegidos:

[*Afirmación 1: precondición para el algoritmo*]
{Enunciados del algoritmo}
[*Afirmación 2*]
{Frases del algoritmo}
⋮
[*Afirmación k − 1*]
{Frases del algoritmo}
[*Afirmación k: post-condición para el algoritmo*]

Los sucesivos pares de afirmaciones son tratados como pre y post-condiciones de los enunciados de los algoritmos entre ellos. Para cada $i = 1, 2, \ldots, k - 1$, una prueba que si la afirmación i es verdadera y todos los enunciados del algoritmo entre la afirmación i y la afirmación $(i + 1)$ se ejecutan, entonces, la afirmación $(i + 1)$ es verdadera. Una vez que se han terminado todas estas pruebas, se sabe que la afirmación k es verdadera. Y puesto que la afirmación 1 es igual que la precondición para el algoritmo y que la afirmación k es la misma que la post-condición para el algoritmo, se concluye que todo el algoritmo es correcto con respecto a su pre-y post-condiciones.

Invariantes de bucle

El método de los invariantes de bucle se utiliza para demostrar la exactitud de un bucle con respecto a ciertas pre y post condiciones. Se basa en el principio de inducción matemática. Supongamos que un algoritmo contiene un bucle **while** y que la entrada a este bucle está restringida por una condición G, llamada la **guarda**. Supongamos también que las afirmaciones que describen el estado actual de las variables del algoritmo se han colocado inmediatamente antes e inmediatamente después del bucle. La afirmación justo antes del bucle se llama la **precondición para el bucle** y el justo después se llama la **post-condición para el bucle**. El bucle escrito tiene la forma siguiente:

[*Pre-condición para el bucle*]
while (G)
    [*Enunciados en el cuerpo del bucle.*
    Ninguno contiene enunciados de ramificación
    que lleven fuera del bucle.]
end while
[*Post-condición para el bucle*]

• Definición

Un bucle se define como **exacto con respecto a su pre y post-condiciones**, si y sólo si, cada vez que las variables del algoritmo satisfacen la precondición para el bucle y el bucle termina después de un número finito de pasos, las variables del algoritmo satisfacen la post-condición para el bucle.

Cortesía de Tony Hoare

C. A. R. Hoare
(nacido en 1934)

El establecimiento de la exactitud de un bucle utiliza el concepto de invariante del bucle. Una **invariante del bucle** es un predicado con dominio en un conjunto de enteros, lo que satisface la condición: Para cada iteración del bucle, si el predicado es verdadero antes de la iteración, es verdadero después de la iteración. Además, si el predicado satisface las siguientes dos condiciones adicionales, el bucle será correcto con respecto a las pre-y post-condiciones:

1. Es verdadero antes de la primera iteración del bucle.
2. Si el bucle termina después de un número finito de iteraciones, la veracidad del invariante del bucle garantiza la veracidad de la post-condición del bucle.

El siguiente teorema, llamado *teorema del invariante del bucle*, formaliza estas ideas. Fue desarrollado por primera vez por C. A. R. Hoare en 1969.

Teorema 5.5.1 Teorema del invariante del bucle

Sea un bucle **while** con guarda G dada, junto con pre y post-condiciones que son predicados en las variables del algoritmo. También sea un predicado $I(n)$, llamado el **invariante del bucle**, se le dará; Si las cuatro propiedades son verdaderas, entonces el bucle es correcto con respecto a sus pre y post-condiciones.

I. Propiedad básica: La pre-condición para el bucle implica que $I(0)$ es verdadera antes de la primera iteración del bucle.

II. Propiedad inductiva: Para todo entero $k \geq 0$, si la guarda G y el invariante del bucle $I(k)$ son verdaderos antes de una iteración del bucle, entonces $I(k + 1)$ es verdadera después de la iteración del bucle.

III. Posible falsedad de la guarda: Después de un número finito de iteraciones del bucle, la guarda G se convierte en falsa.

IV. Exactitud de la post-condición: Si N es el menor número de iteraciones después de que G es falsa e $I(N)$ es cierto, entonces los valores de las variables algoritmo será tal como se especifica en la post-condición del bucle.

Demostración: El teorema del invariante del bucle se deduce con facilidad del principio de inducción matemática. Suponga que $I(n)$ es un predicado que satisface las propiedades de la I a la IV del teorema del invariante del bucle. *[Vamos a probar que el bucle es correcto con respecto a sus pre y post-condiciones.]* Las propiedades I y II son la base y los pasos inductivos necesarios para demostrar la verdad del siguiente enunciado:

Para todo entero $n \geq 0$, si el bucle **while** itera n veces, entonces $I(n)$ es verdadera. 5.5.1

Por tanto, por el principio de inducción matemática ya que tanto I como II son verdaderos, el enunciado (5.5.1) también es verdadero.

La propiedad III dice que la guarda G eventualmente se convierte en falsa. En ese momento el bucle se ha iterado un número de veces, por ejemplo N. Ya que $I(n)$ es verdadera después de la enésima iteración para todo $n \geq 0$, entonces $I(n)$ es verdadera después de la enésima iteración. Es decir, después de la enésima repetición la guarda es falsa y $I(N)$ es verdadera. Pero esta es la hipótesis de la propiedad IV, que es un enunciado if-then. Ya que el enunciado IV es verdadero (por suposición) y su hipótesis es verdadera (por el argumento que acabamos de dar), se tiene (por *modus ponens*) que su conclusión también es verdadera. Es decir, los valores de todas las variables del algoritmo después de la ejecución del bucle son los especificados en la post-condición para el bucle.

El invariante del bucle en el procedimiento para demostrar la exactitud de bucle puede parecer como un conejo en un sombrero. ¿De dónde viene? El hecho es que el desarrollo de un invariante del bucle bueno es un proceso difícil. Aunque el aprendizaje de cómo hacer está más allá del alcance de este libro, vale la pena hacerlo en un curso más avanzado. Las personas que han llegado a ser buenas en el proceso de exactitud han modificado de manera significativa sus perspectivas acerca de programación y han mejorado mucho su capacidad de escribir un buen código.

Otro aspecto difícil al manejar pruebas de exactitud se debe al hecho de que la ejecución de un algoritmo es un proceso dinámico, que se realiza en el tiempo. Conforme progresa la ejecución, los valores de las variables van cambiando, aunque a menudo sus nombres no cambian. En el análisis siguiente, cuando necesitamos hacer una distinción entre los valores de una variable justo antes de la ejecución de una frase del algoritmo y justo después de la ejecución de la frase, adjuntaremos los subíndices *viejo* y *nuevo* en el nombre de la variable.

Ejemplo 5.5.2 Exactitud de un bucle para calcular un producto

El siguiente bucle está diseñado para calcular el producto mx para un entero no negativo m y un número real x, sin utilizar una operación de multiplicación incorporada. Antes del bucle, las variables i y *productos* se han introducido y dan los valores iniciales de $i = 0$ y *producto* $= 0$.

[Pre-condición: m es un entero no negativo,
x es un número real, i = 0 y el producto = 0.]

while $(i \neq m)$

1. *producto*: *producto* $+ x$
2. $i := i + 1$

end while

[Post-condición: producto = mx]

Sea el invariante del bucle

$$I\,(n)\text{: } i = n \quad \text{y} \quad \text{el } \textit{producto} = nx$$

La condición de guarda G del bucle **while** es

$$G\text{: } i \neq m$$

Utilice el teorema del invariante del bucle para probar que el bucle **while** es correcto con respecto a la propuesta de las pre y post-condiciones.

Solución

I. Propiedad básica: *[$I(0)$ es verdadero antes de la primera iteración del bucle.]*

$I(0)$ es "$i = 0$ y el producto $= 0 \cdot x$", que es verdadero antes de la primera iteración del bucle porque $0 \cdot x = 0$.

II. Propiedad inductiva: *[Si $G \wedge I(k)$ es verdadero antes de una iteración de bucle (donde $k \geq 0$), entonces $I(k + 1)$ es verdadero después de la iteración del bucle.]*

Supongamos que k es un entero no negativo de tal manera que $G \wedge I(k)$ es verdadera antes de una iteración del bucle. Entonces, cuando la ejecución llega a la parte superior del bucle, $i \neq m$, *producto* $= kx$, e $i = k$. Ya que $i \neq m$, se pasa la guarda y se ejecuta el enunciado. Antes de la ejecución del enunciado 1,

$$\text{producto}_{\text{viejo}} = kx.$$

Por tanto la ejecución del enunciado 1 tiene el siguiente efecto:

$$\text{producto}_{\text{nuevo}} = \text{producto}_{\text{viejo}} + x = kx + x = (k + 1)x.$$

Del mismo modo, antes de que se ejecute el enunciado 2,

$$i_{\text{viejo}} = k,$$

así después de la ejecución del enunciado 2,

$$i_{\text{nuevo}} = i_{\text{viejo}} + 1 = k + 1.$$

Por tanto, después de la iteración del bucle, el enunciado $I(k + 1)$, a saber, ($i = k + 1$ y *producto* $= (k + 1)x$), es verdadero. Esto es lo que necesita demostrar.

III. Posible falsedad de la guarda: *[Después de un número finito de iteraciones del bucle, G se convierte en falso.]*

El guarda G es la condición $i \neq m$ y m es un entero no negativo. Por I y II, se sabe que

para todo entero $n \geq 0$, si el bucle se itera
n veces, entonces $i = n$ y el *producto* $= nx$.

Así después de m iteraciones del bucle, $i = m$. Por tanto G se convierte en falsa después de m iteraciones del bucle.

IV. Exactitud de la post-condición: *[Si N es el número menor de iteraciones después de lo que G es falsa e I(N) es verdadera, entonces el valor de las variables del algoritmo será tal como se especifica en la post-condición del bucle.]*

De acuerdo con la post-condición, el valor de *producto* después de la ejecución del bucle debe ser mx. Pero si G se convierte en falsa después de N iteraciones, $i = m$. Y si $I(N)$ es verdadera, $i = N$ y *producto* $= Nx$. Puesto que ambas condiciones (G falsa e $I(N)$, verdadera) se satisfacen, $m = i = N$ y *producto* $= mx$ cuando sea necesario. ■

En lo que resta de esta sección, se presentan pruebas de la exactitud de los bucles fundamentales en el algoritmo de la división y en el algoritmo de Euclides. (Estos algoritmos se presentaron en la sección 4.8.)

Exactitud del algoritmo de división

El algoritmo de la división se supone que debe tener un número entero no negativo y un entero positivo d y calcula los enteros no negativos q y r tales que $a = dq + r$ y $0 \leq r < d$. Inicialmente se introducen las variables r y q y se dan los valores $r = a$ y $q = 0$. El bucle crucial, con las pre y las post-condiciones escritas, es la siguiente:

[Pre-condición: a es un entero no negativo y d es un entero positivo, r = a y q = 0.]
while $(r \geq d)$
1. $r := r - d$
2. $q := q + 1$

end while
[Post-condición: q y r son números enteros no negativos con la propiedad de que $a = qd + r$ y $0 \leq r < d$.]

Demostración:

Para demostrar la exactitud del bucle, sea el invariante del bucle

$$I\,(n)\text{: } r = a - nd \geq 0 \quad \text{y} \quad n = q.$$

El guarda del bucle **while** es

$$G\text{: } r \geq d$$

I. Propiedad básica: *[I(0) es verdadera antes de la primera iteración del bucle.]*

$I(0)$ es "$r = a - 0 \cdot d \geq 0$ y $q = 0$". Pero por la precondición, $r = a$, $a \geq 0$ y $q = 0$. Por lo que ya que $a = a - 0 \cdot d$, entonces $r = a - 0 \cdot d$ y $I(0)$ es verdadera antes de la primera iteración del bucle.

II. Propiedad inductiva: *[Si $G \wedge I(k)$ es verdadera antes de una iteración del bucle (donde $k \geq 0$), $I\,(k + 1)$ es verdadera después de la iteración del bucle.]*

Supongamos que k es un entero no negativo tal que $G \wedge I\,(k)$ es verdadera antes de una iteración del bucle. Puesto que G es verdadera, $r \geq d$ y se introduce el bucle. También puesto que $I\,(k)$ es verdadero, $r = a - kd \geq 0$ y $k = q$. Por tanto, antes de la ejecución de los enunciados 1 y 2,

$$r_{\text{viejo}} \geq d \quad \text{y} \quad r_{\text{viejo}} = a - kd \quad \text{y} \quad q_{\text{viejo}} = k.$$

Cuando se ejecutan los enunciados 1 y 2, entonces,

$$r_{\text{nuevo}} = r_{\text{viejo}} - d = (a - kd) - d = a - (k + 1)d, \tag{5.5.2}$$

y

$$q_{\text{nuevo}} = q_{\text{viejo}} + 1 = k + 1 \tag{5.5.3}$$

Además ya que $r_{\text{viejo}} \geq d$ antes de la ejecución de los enunciados 1 y 2, después de la ejecución de estos enunciados,

$$r_{\text{nuevo}} = r_{\text{viejo}} - d \geq d - d \geq 0. \tag{5.5.4}$$

Poniendo juntas las ecuaciones (5.5.2), (5.5.3) y (5.5.4) se muestra que después de la iteración del bucle,

$$r_{\text{nuevo}} \geq \text{O y } r_{\text{nuevo}} = a - (k + 1)d \text{ y } q_{\text{nuevo}} = k + 1.$$

Por tanto I (k + 1) es verdadera.

III. Posible falsedad de la guarda: *[Después de un número finito de iteraciones del bucle, G se convierte en falsa.]*

El guarda G es la condición $r \geq d$. Cada iteración del bucle reduce el valor de r por d y sin embargo deja a r no negativo. Por tanto los valores de r forman una sucesión decreciente de números enteros no negativos y así (por el principio del buen orden) debe haber el más pequeño r como, por ejemplo $r_{\text{mín}}$. Entonces $r_{\text{mín}} < d$. *[Si $r_{mín}$ fuera mayor que d, el bucle se itera en otra ocasión y se obtendría un nuevo valor de r igual a $r_{mín} - d$. Pero este nuevo valor sería menor que $r_{mín}$ que estaría en contradicción con el hecho de que $r_{mín}$ es el residuo más pequeño obtenido por iteración repetida del bucle.]* Por tanto, tan pronto como el valor de $r = r_{\text{mín}}$, se calcula el valor de r y se convierte menor que d, por lo que el guarda de G es falsa.

IV. Exactitud de la post-condición: *[Si N es el menor número de iteraciones después de que G es falsa e I (N) es verdadera, entonces los valores de las variables del algoritmo serán tal como se especifica en la post-condición del bucle.]*

Supongamos que para algún entero no negativo N, G es falsa e $I\,(N)$ es verdadera. Entonces $r < d$, $r = a - Nd$, $r \geq 0$ y $q = N$. Ya que $q = N$, por sustitución,

$$r = a - qd.$$

O, sumando qd en ambos lados,

$$a = qd + r.$$

Combinando las dos desigualdades que implican a r se obtiene

$$0 \leq r < d.$$

Pero estos son los valores de q y r que se especifican en la post-condición, por lo que la demostración está completa. ■

Exactitud del teorema de Euclides

El algoritmo de Euclides se supone que debe tomar los enteros A y B con $A > B \geq 0$ y se calcula su máximo común divisor. Justo antes del bucle crucial, las variables a, b y r se han introducido con $a = A$, $b = B$ y $r = B$. El bucle crucial, con las pre y post-condiciones escritas, es el siguiente:

[Pre-condición: A y B son enteros
con $A > B \geq 0$, $a = A$, $b = B$, $r = B$.*]*

while $(b \neq 0)$

1. $r := a \bmod b$
2. $a := b$
3. $b := r$

end while

[Post-condición: $a = mcd\,(A, B)$*]*

Demostración:

Para demostrar la exactitud del bucle, sea el invariante

$$I\,(n)\text{: mcd}\,(a, b) = \text{mcd}\,(A, B) \quad \text{y} \quad 0 \leq b < a.$$

El guarda del bucle **while** es

$$G\text{: } b \neq 0$$

I. Propiedad básica: *[*$I\,(0)$ *es verdadero antes de la primera iteración del bucle.]* $I\,(0)$ es

$$\text{mcd}(A, B) = \text{mcd}(a, b) \quad \text{y} \quad 0 \leq b < a.$$

De acuerdo con la precondición,

$$a = A, \quad b = B, \quad r = B \quad \text{y} \quad 0 \leq B < A.$$

Por tanto $\text{mcd}(A, B) = \text{mcd}\,(a, b)$. Ya que $0 \leq B < A$, $b = B$ y $a = A$ entonces $0 \leq b < a$. Por tanto $I\,(0)$ es verdadera.

II. Propiedad inductiva: *[Si* $G \wedge I\,(k)$ *es verdadera antes de una iteración del bucle (donde* $k > 0$*),* $I\,(k + 1)$ *es verdadera después de la iteración del bucle.]*

Supongamos que k es un entero no negativo tal que $G \wedge I\,(k)$ es verdadero antes de una iteración del bucle. *[Tenemos que demostrar que I (k + 1) es verdadera después de la iteración del bucle.]* Puesto que G es verdadera, $b_{\text{viejo}} \neq 0$ y se introduce el bucle. Y como $I\,(k)$ es verdadera, inmediatamente antes de que se ejecute el enunciado 1,

$$\text{mcd}(a_{\text{viejo}}, b_{\text{viejo}}) = \text{mcd}\,(A, B) \quad \text{y} \quad 0 \leq b_{\text{viejo}} < a_{\text{viejo.}} \tag{5.5.5}$$

Después de la ejecución del enunciado 1,

$$r_{\text{nuevo}} = a_{\text{viejo}} \bmod b_{\text{viejo}}.$$

Por tanto, por el teorema de cociente-residuo,

$$a_{\text{viejo}} = b_{\text{viejo}} \cdot q + r_{\text{nuevo}} \text{ para algún entero } q$$

y r_{nuevo} tiene la propiedad que

$$0 \leq r_{\text{nuevo}} < b_{\text{viejo}}. \tag{5.5.6}$$

Por el lema 4.8.2,

$$\text{mcd}(a_{\text{viejo}}, b_{\text{viejo}}) = \text{mcd}(b_{\text{viejo}}, r_{\text{nuevo}}).$$

Así por la ecuación (5.5.5),

$$\text{mcd}(b_{\text{viejo}}, r_{\text{nuevo}}) = \text{mcd}(A, B). \tag{5.5.7}$$

Cuando se ejecutan los enunciados 2 y 3,

$$a_{\text{nuevo}} = b_{\text{viejo}} \text{ y } b_{\text{nuevo}} = r_{\text{nuevo}} \tag{5.5.8}$$

Sustituyendo las ecuaciones (5.5.8) en la ecuación (5.5.7) se obtiene

$$\text{mcd}(a_{\text{nuevo}}, b_{\text{nuevo}}) = \text{mcd}(A, B). \tag{5.5.9}$$

Y sustituyendo los valores de las ecuaciones en (5.5.8) en la desigualdad (5.5.6) se obtiene

$$0 \leq b_{\text{nuevo}} < a_{\text{nuevo.}} \tag{5.5.10}$$

Por tanto después de la iteración del bucle, por la ecuación (5.5.9) y la desigualdad (5.5.10),

$$\text{mcd}(a, b) = \text{mcd}(A, B) \text{ y } 0 \leq b < a,$$

que es $I\,(k + 1)$. *[Esto es lo que se necesita demostrar.]*

III. Posible falsedad de la guarda: *[Después de un número finito de iteraciones del bucle, G se convierte en falsa.]*

Cada valor de b obtenido por iteración repetida del bucle es no negativo y menor que el valor anterior de b. Por tanto, por el principio del buen orden, hay un menor valor $b_{\text{mín}}$. El hecho es que $b_{\text{mín}} = 0$. *[Si $b_{\text{mín}}$ no es 0, entonces el guarda es verdadero, por lo que el bucle se itera en otro momento. En esta iteración un valor de r se calcula que es menor que el valor anterior de b, $b_{\text{mín}}$. Entonces se cambia el valor de b a r, que es menor que $b_{\text{mín}}$. Esto contradice el hecho de que $b_{\text{mín}}$ es el menor valor de b obtenido por la iteración repetida del bucle. Por tanto $b_{\text{mín}} = 0$.]* Ya que $b_{\text{mín}} = 0$, la guarda es falso inmediatamente después de la iteración del bucle en el que se calcula $b_{\text{mín}}$.

IV. Exactitud de la post-condición: *[Si N es el menor número de iteraciones después de que G es falso e I(N) es verdadero, entonces los valores de las variables del algoritmo será tal como se especifica en la post-condición.]*

Supongamos que para algún entero no negativo N, G es falsa e $I\,(N)$ es verdadera. *[Tenemos que demostrar la verdad de la post-condición: a = mcd (A, B).]* Puesto que G es falso, $b = 0$ y puesto que $I(N)$ es verdadera,

$$\text{mcd}(a, b) = \text{mcd}(A, B). \tag{5.5.11}$$

Sustituyendo $b = 0$ en la ecuación (5.5.11) se obtiene

$$\text{mcd}(a, 0) = \text{mcd}(A, B).$$

Pero por el lema 4.8.1,

$$\text{mcd}(a, 0) = a.$$

Por tanto $a = \text{mcd(A, B)}$ *[como se quería demostrar]*.

Autoexamen

1. Una pre-condición para un algoritmo es _____ y un post- condición para un algoritmo es _____.
2. Un bucle se define como correcta con respecto a su pre-y post-condiciones, si y sólo si, cada vez que las variables del algoritmo satisfacen la pre-condición para el bucle y el bucle termina después de un número finito de pasos, entonces _____.
3. Para cada iteración de un bucle, si un invariante del bucle es verdadero antes de iteración del bucle, entonces _____.
4. Dado un bucle **while** con un guarda G y un predicado $I(n)$ si las siguientes cuatro propiedades son verdaderas, entonces el bucle es correcto con respecto a su pre-y post-condiciones:
   a) La pre-condición para el bucle implica que _____ antes de la primera iteración del bucle;
   b) Para todo entero $k \geq 0$, si el guarda G y el predicado $I(k)$ son ambos verdaderos antes de una iteración del bucle, entonces, _____.
   c) Después de un número finito de iteraciones del bucle, _____;
   d) Si N es el menor número de iteraciones después de que G es falso e I (N) es verdadero, entonces los valores de las variables algoritmo serán especificados como _____.

Conjunto de ejercicios 5.5

Los ejercicios del 1 al 5 contienen un bucle while y un predicado. En cada caso demuestre que si el predicado es verdadero antes de la entrada al bucle, entonces también lo es después de la salida del bucle.

1. bucle: **while** ($m \geq 0$ y $m \leq 100$)

$m := m + 1$

$n := n - 1$

end while

predicado: $m + n = 100$

2. bucle: **while** ($m \geq 0$ y $m \leq 100$)

$m := m + 4$

$n := n - 2$

end while

predicado: $m + n$ es impar

3. bucle: **while** ($m \geq 0$ y $m \leq 100$)

$m := 3 \cdot m$

$n := 5 \cdot n$

end while

predicado: $m^3 > n^2$

4. bucle: **while** ($n \geq 0$ y $n \leq 100$)

$n := n + 1$

end while

predicado: $2^n < (n + 2)!$

5. bucle: **while** ($n \geq 3$ y $n \leq 100$)

$n := n + 1$

end while

predicado: $2n + 1 \leq 2^n$

Cada uno de los ejercicios del 6 al 9 contiene un bucle while escrito con una pre y una post-condición y también un invariante del bucle. En cada caso, utilice el teorema del invariante del bucle para demostrar la exactitud del bucle con respecto a las pre y a las post condiciones.

6. *[Precondición: m es un entero no negativo, x es un número real, $i = 0$ y $exp = 1$.]*

while *($i \neq m$)*

1. $exp := exp \cdot x$
2. $i := i + 1$

end while

[Post-condición: $exp = x^m$]
invariante del bucle: I (n) es "exp $= x^n$ e $i = n$".

7. *[Precondición: mayor $= A[1]$ y $i = 1$]*

while ($i \neq m$)

1. $i := i + 1$
2. **if** $A[i] >$ mayor **then** mayor $:= A[i]$

end while

[Post-condición: mayor = valor máximo de $A[1], A[2], \ldots, A[m]$.]

invariante del bucle: $I(n)$ es "mayor = valor máximo de $A[1], A[2], \ldots, A[n+1]$ e $i = n + 1$".

8. *[Precondición: suma = A[1] e i = 1]*

while $(i \neq m)$

1. $i := i + 1$
2. suma := suma + $A[i]$

end while

[Post-condición: suma $= A[1] + A[2] + \cdots + A[m]$*]*
invariante del bucle: $I(n)$ es "$i = n + 1$ y *suma* $= A[1] + A[2] + \cdots + A[n+1]$".

9. *[Pre-condición: $a = A$ y A es un número entero positivo.]*

while $(a > 0)$

1. $a := a - 2$

end while

[Post-condición: $a = 0$ *si A es par y* $a = -1$ *si A es impar.]*
invariante del bucle: $I(n)$ es "Tanto a como A son enteros pares o ambos son enteros impares y $a \geq -1$".

H ✶ **10.** Demuestre la exactitud del bucle **while** del algoritmo 4.8.3 (en el ejercicio 24 del conjunto de ejercicios 4.8) con respecto a las siguientes pre y post-condiciones:

Pre-condición: A y B son números enteros positivos, $a = A$ y $b = B$.

Post-condición: Uno a o b es cero y el otro es distinto de cero. Cualquiera que sea distinto de cero es igual al mcd(A, B).

Utilice el invariante del bucle

$I(n)$ "1) a y b son números enteros no negativos con mcd(a, b) = mcd(A, B).
2) a lo más uno de a y b es igual a 0,
3) $0 \leq a + b \leq A + B - n$".

11. El siguiente bucle **while** implementa una forma de multiplicar dos números que fue desarrollada por los antiguos egipcios.

[*Pre-condición: A y B son números enteros positivos,* $x = A$ $y = B$ *y producto* $= 0$.*]*

while $(y \neq 0)$
$r := y \ mod \ 2$
if $r = 0$
then do $x := 2 \cdot x$
$y := y \ div \ 2$
end do
if $r = 1$
then do *producto* := producto + x
$y := y - 1$
end do
end while

[Post-condición: producto $= A \cdot B$*]*

Demuestre la exactitud de este bucle con respecto a su pre y post-condiciones por medio del invariante del bucle

$I(n)$: "xy + producto $= A \cdot B$".

✶ 12. La siguiente frase se podría agregar al invariante del bucle para el algoritmo de Euclides:

Existen enteros u, v, s y t tal que
$a = uA + vB$ y $b = SA + tB$. 5.5.12

a. Demuestre que esta frase es un invariante del bucle de

while $(y \neq 0)$
$r := a \ mod \ b$
$a := b$
$b := r$
end while

b. Demuestre que si inicialmente $a = A$ y $b = B$, entonces la frase (5.5.12) es verdadera antes de la primera iteración del bucle.
c. Explique cómo la prueba de exactitud para el algoritmo de Euclides junto con los resultados de *a*) y *b*) anteriores permiten concluir que, dado cualesquiera enteros A y B con $A > B \geq 0$, existen enteros u y v tales que mcd $(A, B) = uA + vB$.
d. Realmente, calculando u, v, s y t en cada etapa de ejecución del algoritmo de Euclides, encuentre los enteros u y v tales que mcd$(330, 156) = 330u + 156v$.

Respuestas del autoexamen

1. un predicado que describe el estado inicial de las variables de entrada para el algoritmo; un predicado que describe el estado final de las variables de salida para el algoritmo 2. las variables del algoritmo satisfacen la post-condición para el bucle 3. Es verdad después de la iteración del bucle 4. *a*) $I(0)$ es verdadera *b*) $I(k + 1)$ es verdadera después de la iteración del bucle *c*) el guarda G se convierte en falso *d*) en la post-condición del bucle

5.6 Definición de sucesión recursiva

Los naturalistas han observado que una pulga lleva sobre su cuerpo otras pulgas más pequeñas, que a su vez alimentan a otras pulgas más diminutas. Y así, hasta el infinito. —Jonathan Swift, 1733

Se puede definir una sucesión en muchas maneras diferentes. Una manera informal, es escribir los primeros términos con la expectativa de que el patrón general será obvio. Podríamos decir, por ejemplo, "considere la sucesión de 3, 5, 7, ...". Desafortunadamente, los malentendidos pueden ocurrir cuando se utiliza este enfoque. El siguiente término de la sucesión podría ser 9, si nos referimos a una sucesión de enteros impares o podría ser 11 si nos referimos a la sucesión de números primos impares.

La segunda manera de definir una sucesión es dar una fórmula explícita para su enésimo término. Por ejemplo, una sucesión $a_0, a_1, a_2, \ldots$ se puede especificar escribiendo

$$a_n = \frac{(-1)^n}{n+1} \quad \text{para todo entero } n \geq 0.$$

La ventaja de definir una sucesión con una fórmula tan explícita es que cada término de la sucesión está únicamente determinado y se puede calcular con un número fijo, finito de pasos, sustituyendo.

La tercera manera de definir una sucesión es el uso de la recursividad, como se hizo en los ejemplos 5.3.3 y 5.4.2. Para ello es necesario dar tanto una ecuación, llamada *relación de recurrencia*, que define cada término más adelante en la sucesión en función de términos anteriores y también uno o más valores iniciales de la sucesión.

A veces es muy difícil o imposible encontrar una fórmula explícita para una sucesión, pero *es* posible definir la sucesión usando la recursividad. Observe que la definición de sucesiones de forma recursiva es similar a la demostración de teoremas con inducción matemática. La relación de recurrencia es como el paso inductivo y las condiciones iniciales son como el paso básico. En efecto, el hecho de que las sucesiones se pueden definir de forma recursiva es equivalente al hecho de que la inducción matemática funciona como un método de la demostración.

• Definición

Una **relación de recurrencia** para una sucesión $a_0, a_1, a_2, \ldots$ es una fórmula que relaciona cada término de a_k con algunos de sus predecesores $a_{k-1}, a_{k-2}, \ldots, a_{k-i}$ donde i es un número entero con $k - i \geq 0$. Las **condiciones iniciales** para una relación de recurrencia especifican los valores de $a_0, a_1, a_2, \ldots, a_{i-1}$, si i es un entero fijo, o $a_0, a_1, \ldots a_m$, donde m es un número entero con $m \geq 0$, si i depende de k.

Ejemplo 5.6.1 Cálculo de términos de una sucesión definida recursivamente

Defina una sucesión $c_0, c_1, c_2, \ldots$ recursivamente de la siguiente manera: Para todo entero $k \geq 2$,

$$1) \quad c_k = c_{k-1} + kc_{k-2} + 1 \quad \text{relación de recurrencia}$$
$$2) \quad c_0 = 1 \quad \text{y} \quad c_1 = 2 \quad \text{condiciones iniciales.}$$

Encuentre c_2, c_3 y c_4.

Solución

$$\begin{aligned} c_2 &= c_1 + 2c_0 + 1 && \text{sustituyendo } k = 2 \text{ en (1)} \\ &= 2 + 2 \cdot 1 + 1 && \text{ya que } c_1 = 2 \text{ y } c_0 = 1 \text{ por (2)} \end{aligned}$$

$$
\begin{aligned}
3)\ \therefore c_2 &= 5 \\
c_3 &= c_2 + 3c_1 + 1 && \text{sustituyendo } k = 3 \text{ en (1)} \\
&= 5 + 3\cdot 2 + 1 && \text{ya que } c_2 = 5 \text{ por (3) y } c_1 = 2 \text{ por (2)} \\
4)\ \therefore c_3 &= 12 \\
c_4 &= c_3 + 4c_2 + 1 && \text{sustituyendo } k = 4 \text{ en (1)} \\
&= 12 + 4\cdot 5 + 1 && \text{ya que } c_3 = 12 \text{ por 94) y } c_2 = 5 \text{ por (3)} \\
5)\ \therefore c_4 &= 33
\end{aligned}
$$

■

Una relación de recurrencia dada se puede expresar de varias maneras diferentes.

Ejemplo 5.6.2 Escritura de una relación de recurrencia en más de una manera

Nota Piense en la relación de recurrencia como $s_{\square} = 3s_{\square - 1} - 1$, donde cualquier expresión entera positiva se puede colocar en la caja.

Sea $s_0, s_1, s_2, \ldots$ una sucesión que satisface la relación de recurrencia siguiente:

$$\text{para todo entero } k \geq 1, \quad s_k = 3s_{k-1} - 1.$$

Explique por qué la siguiente afirmación es verdadera:

$$\text{para todo entero } k \geq 0, \quad s_{k+1} = 3s_k - 1.$$

Solución En el lenguaje informal, la relación de recurrencia dice que cualquiera de los términos de la sucesión es igual a 3 veces el término anterior menos 1. Ahora, para cualquier entero $k \geq 0$, el término anterior a s_{k+1} es s_k. Así, para cualquier entero $k \geq 0$, $s_{k+1} = 3s_k - 1$. ■

Una sucesión definida de forma recursiva no necesita comenzar con un subíndice cero. Además, una relación de recurrencia dada puede ser satisfecha por muchas sucesiones diferentes, los valores reales de la sucesión se determinan por las condiciones iniciales.

Ejemplo 5.6.3 Sucesiones que satisfacen la misma relación de recurrencia

Sea $a_1, a_2, a_3, \ldots$ y $b_1, b_2, b_3, \ldots$ que satisfacen la relación de recurrencia que el término k-ésimo es igual a 3 veces el $(k-1)$-ésimo término para todo entero $k \geq 2$:

$$1) \quad a_k = 3a_{k-1} \quad \text{y} \quad b_k = 3b_{k-1}.$$

Pero supongamos que las condiciones iniciales para las sucesiones son diferentes:

$$2) \quad a_1 = 2 \quad \text{y} \quad b_1 = 1.$$

Determine: *a)* a_2, a_3, a_4 y *b)* b_2, b_3, b_4.

Solución

a. $a_2 = 3a_1 = 3\cdot 2 = 6$
$a_3 = 3a_2 = 3\cdot 6 = 18$
$a_4 = 3a_3 = 3\cdot 18 = 54$

b. $b_2 = 3b_1 = 3\cdot 1 = 3$
$b_3 = 3b_2 = 3\cdot 3 = 9$
$b_4 = 3b_3 = 3\cdot 9 = 27$

Por tanto $a_1, a_2, a_3, \ldots$ comienza en 2, 6, 18, 54, ... y
$b_1, b_2, b_3, \ldots$ comienza en 1, 3, 9, 27, ...

■

Ejemplo 5.6.4 Demostración que una sucesión dada por una fórmula explícita satisface una relación de recurrencia

La sucesión de **números de Catalan**, llamada así por el matemático belga Eugène Catalan (1814-1894), aparece en una notable variedad de contextos diferentes en matemáticas discretas. Se puede definir de la siguiente manera: Para cada entero $n \geq 1$,

$$C_n = \frac{1}{n+1}\binom{2n}{n}.$$

a. Encuentre C_1, C_2 y C_3.

b. Muestre que esta sucesión satisface la relación de recurrencia $C_k = \dfrac{4k-2}{k+1}C_{k-1}$ para todo entero $k \geq 2$

Academia real de Bélgica

Eugène Catalan (1814-1894)

Solución

a. $C_1 = \dfrac{1}{2}\binom{2}{1} = \dfrac{1}{2}\cdot 2 = 1, \quad C_2 = \dfrac{1}{3}\binom{4}{2} = \dfrac{1}{3}\cdot 6 = 2, \quad C_3 = \dfrac{1}{4}\binom{6}{3} = \dfrac{1}{4}\cdot 20 = 5$

b. Para obtener el k-ésimo y el $(k-1)$-ésimo términos de la sucesión, simplemente sustituimos k y $k-1$ en lugar de n en la fórmula explícita para $C_1, C_2, C_3, \ldots$.

$$C_k = \frac{1}{k+1}\binom{2k}{k}$$

$$C_{k+1} = \frac{1}{(k-1)+1}\binom{2(k-1)}{k-1} = \frac{1}{k}\binom{2k-2}{k-1}.$$

Después, comience con el lado derecho de la relación de recurrencia y transforme el lado izquierdo: para cada entero $k \geq 2$,

$$\begin{aligned}
\frac{4k-2}{k+1}C_{k-1} &= \frac{4k-2}{k+1}\left[\frac{1}{k}\binom{2k-2}{k-1}\right] && \text{sustituyendo}\\
&= \frac{2(2k-1)}{k+1}\cdot\frac{1}{k}\cdot\frac{(2k-2)!}{(k-1)!(2k-2-(k-1))!} && \text{por la fórmula de } n \text{ elija } r\\
&= \frac{1}{k+1}\cdot(2(2k-1))\cdot\frac{(2k-2)!}{(k(k-1)!)(k-1)!} && \text{reordenando los factores}\\
&= \frac{1}{k+1}\cdot(2(2k-1))\cdot\frac{1}{k!(k-1)!}\cdot(2k-2)!\cdot\frac{1}{2}\cdot\frac{1}{k}\cdot 2k. && \text{ya que } \tfrac{1}{2}\cdot\tfrac{1}{k}\cdot 2k = 1\\
&= \frac{1}{k+1}\cdot\frac{2}{2}\cdot\frac{1}{k!}\cdot\frac{1}{(k-1)!}\cdot\frac{1}{k}\cdot(2k)\cdot(2k-1)\cdot(2k-2)! && \text{reordenando los factores}\\
&= \frac{1}{k+1}\cdot\frac{(2k)!}{k!k!} && \text{ya que } k(k-1)! = k!,\ \tfrac{2}{2} = 1 \text{ y}\\
&&& 2k\cdot(2k-1)\cdot(2k-2)! = (2k)!\\
&= \frac{1}{k+1}\binom{2k}{k} && \text{por la fórmula de } n \text{ elija } r\\
&= C_k && \text{por definición de } C_1, C_2, C_3, \ldots.
\end{aligned}$$

■

Ejemplos de sucesiones definidas recursivamente

La recursión es una de las ideas centrales de la ciencia computacional. Resolver un problema de forma recursiva significa encontrar una manera de dividirlo en subproblemas más pequeños donde cada uno tiene la misma forma que el problema original y hacer esto de tal manera que cuando el proceso se repite muchas veces, los últimos subproblemas son

pequeños y fáciles de resolver y las soluciones de los subproblemas se pueden unir para formar una solución al problema original.

Probablemente la parte más difícil de resolver problemas de forma recursiva es averiguar la solución a los pequeños subproblemas del mismo tipo que el problema original lo que le dará una solución al problema en su conjunto. Se *supone* que conoce las soluciones a subproblemas más pequeños y se pregunta a sí mismo cuál es el mejor uso que puede hacer de ese conocimiento para resolver el problema más grande. La suposición de que los subproblemas más pequeños ya han sido resueltos se ha llamado el *paradigma recursivo* o el *salto recursivo de confianza*. Una vez que da este paso, tiene razón en la mitad de la parte más difícil del problema, pero por lo general, el camino hacia una solución de este punto, aunque difícil, es corta. El salto recursivo de confianza es similar a la hipótesis inductiva en una demostración por inducción matemática.

Ejemplo 5.6.5 La Torre de Hanoi

Cortesía de Francis Lucas

Édouard Lucas
(1842-1891)

En 1883 un matemático francés, Édouard Lucas, inventó un rompecabezas que se llama *La Torre de Hanoi* (*La Tour D'Hanoï*). El rompecabezas consiste de ocho discos de madera con agujeros en sus centros, que se apilaban en orden decreciente en uno de los postes en una fila de tres. En la figura 5.6.1, se muestra una copia de la cubierta de la caja. Se supone que los que juegan mueven todos los discos de uno en uno de un poste a otro, nunca colocan un disco más grande en la parte superior de uno más pequeño. Se dice que las instrucciones del rompecabezas se basan en una antigua leyenda hindú:

En los escalones del altar en el templo de Benarés, por muchos, muchos años los sacerdotes han estado moviendo una torre de 64 discos de oro de un poste a otro, uno por uno, no ponen uno más grande en la parte superior de uno menor. Cuando todos los discos se hayan transferido a la Torre y los sacerdotes caigan, será el fin del mundo.

Cortesía de Paul Stockmeyer

Figura 5.6.1

El rompecabezas ofrece un premio de diez mil francos (unos 34 000 dólares americanos de hoy) a cualquiera que pudiera mover una torre de 64 discos a mano siguiendo las reglas del juego. (Vea la figura 5.6.2 en la página siguiente). Suponiendo que haya transferido los discos de la manera más eficiente posible, ¿cuántos movimientos se requieren para ganar el premio?

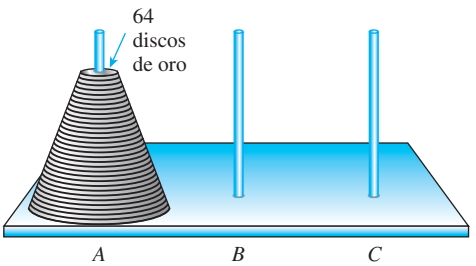


Figura 5.6.2

Solución Una manera elegante y eficiente para resolver este problema es pensar de forma recursiva. Supongamos que, de alguna manera u otra, se ha encontrado la manera más eficiente para la transferencia de un poste de $k - 1$ discos uno a uno de un poste a otro, obedeciendo la restricción de nunca colocar un disco más grande en la parte superior de uno más pequeño. ¿Cuál es la forma más eficiente de transferir de un poste de k discos a otro? La respuesta se esboza en la figura 5.6.3, donde el poste A es el poste inicial y el poste C es el poste objetivo y se describe de la siguiente manera:

Paso 1: Transfiera la parte superior de $k - 1$ discos de un poste A al poste B. Si $k > 2$, para la ejecución de este paso se requerirá un número de movimientos de los discos individuales entre los tres postes. Pero al momento de pensar de forma recursiva no se detenga en imaginar los detalles de cómo se producen esos movimientos.

Paso 2: Mueva el disco de la parte inferior del poste A al poste C.

Paso 3: Transfiera $k - 1$ discos de la parte superior del poste B al poste C. (De nuevo, si $k > 2$, la ejecución de este paso requerirá de más de un movimiento.)

Para ver que esta sucesión de movimientos es más eficiente, observe que para mover el disco del fondo de un poste de k discos de un poste a otro, primero se deben transferir $k - 1$ discos de la parte superior de un tercer poste para salir del paso. Por tanto la transferencia de k discos del poste A al poste C se requieren al menos dos transferencias de $k - 1$ discos de la parte superior: uno para transferir el disco de la parte inferior para liberar el disco inferior, de manera que se puede mover y otra para transferir de nuevo en la parte superior de la parte inferior del disco después de que el disco de la parte inferior se ha movido al poste C. Si el disco del fondo no se hubiera movido directamente del poste A al poste C, sino que primero se movieran al poste B, al menos serían necesarias dos transferencias adicionales de $k - 1$ discos de la parte superior: una para pasarlos de un poste A a un poste C para que el disco del fondo se pudiera mover del poste A al poste B y otra pila para moverlos del poste C para que el disco inferior se pudiera mover al poste C. Esto aumentaría el número total de movimientos y daría como resultado una transferencia menos eficiente.

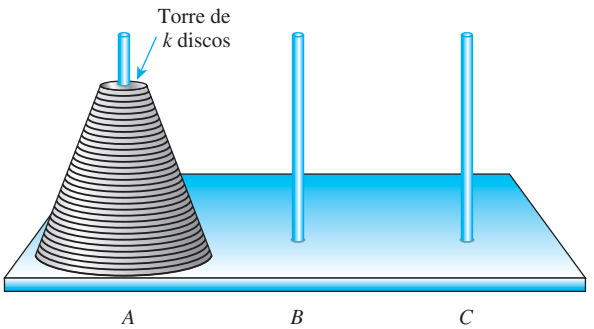
Así, la sucesión mínima de movimientos debe incluir pasar de la posición inicial a) a la posición b) a la posición c) y a la posición d). De lo que se tiene que

$$\left[\begin{array}{l}\text{el número mínimo de movimientos necesarios para transferir una torre de } k \text{ discos de un poste } A \text{ a un poste } C.\end{array}\right] = \left[\begin{array}{l}\text{el número mínimo de movimientos necesarios para ir de una posición } a) \text{ a la posición } b)\end{array}\right] + \left[\begin{array}{l}\text{el número mínimo de movimientos necesarios para ir de una posición } b) \text{ a la posición } c)\end{array}\right] + \left[\begin{array}{l}\text{el número mínimo de movimientos necesarios para ir de una posición } c) \text{ a la posición } d)\end{array}\right] \quad 5.6.1$$

Nota La definición de la sucesión es un paso crucial para resolver el problema. La relación de recurrencia y las condiciones iniciales se especifican en términos de la sucesión.

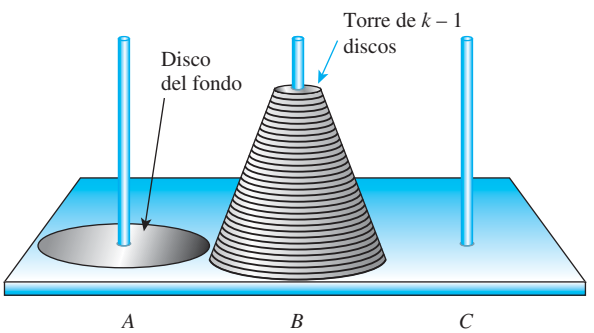
Para cada entero $n \geq 1$, sea

$$m_n = \left[\begin{array}{l}\text{el número mínimo de movimientos necesarios para transferir una torre de } n \text{ discos de un poste a otro}\end{array}\right]$$



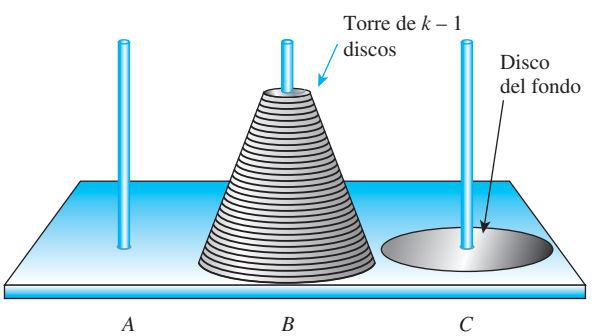
Posición inicial

a)



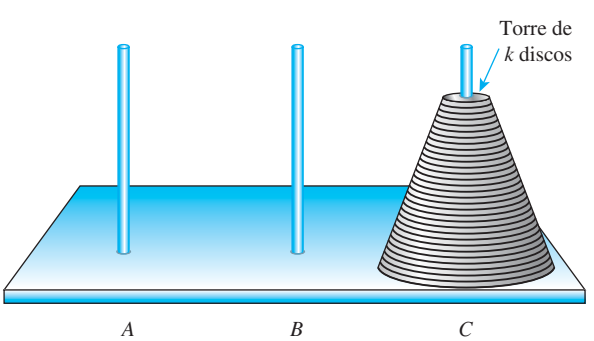
Posición después de transferir $k - 1$ discos de A a B

b)



Posición después del movimiento del disco de la parte inferior de A a C

c)



Posición después de transferir $k - 1$ discos de B a C

d)

Figura 5.6.3 Movimientos de la Torre de Hanoi

Note que los números m_n son independientes del etiquetado de los postes; toma el mismo número mínimo de movimientos transferir n discos del poste A al poste C, que por ejemplo, transferir n discos del poste A al poste B. También los valores de m_n son independientes del número de discos más grandes que puede estar debajo de los n superiores, siempre que permanezcan inmóviles mientras se mueven los n superiores. Debido a que los discos de la parte inferior son más grandes que los de la parte superior, los discos de arriba se pueden mover de un poste al otro, como si los discos de fondo no estuvieran presentes.

Para ir de la posición a) a la posición b) se requieren m_{k-1} movimientos, ir de la posición b) a la posición c) requiere sólo un movimiento, e ir de la posición c) a la posición d) requiere m_{k-1} movimientos. Por tanto, sustituyendo en la ecuación (5.6.1),

$$\begin{aligned} m_k &= m_{k-1} + 1 + m_{k-1} \\ &= 2m_{k-1} + 1 \qquad \text{para todo entero } k \geq 2. \end{aligned}$$

La condición inicial o básica, de esta recursión se encuentra utilizando la definición de la sucesión. Debido a que sólo se necesita un movimiento para mover un disco de un poste a otro,

$$m_1 = \left[\begin{array}{l} \text{el número mínimo de movimientos necesarios} \\ \text{para mover una torre de un disco de un poste a otro} \end{array} \right] = 1.$$

De ahí que la especificación completa la recursividad de la sucesión $m_1, m_2, m_3, \ldots$ es la siguiente:
Para todo entero $k \geq 2$,

$$\begin{aligned} &1) \quad m_k = 2m_{k-1} + 1 \qquad \text{relación de recurrencia} \\ &2) \quad m_1 = 1 \qquad\qquad\quad \text{condiciones iniciales} \end{aligned}$$

Aquí hay un cálculo de los siguientes cinco términos de la sucesión:

$$\begin{aligned} &3) \quad m_2 = 2m_1 + 1 = 2 \cdot 1 + 1 = 3 \qquad \text{por 1) y 2)} \\ &4) \quad m_3 = 2m_2 + 1 = 2 \cdot 3 + 1 = 7 \qquad \text{por 1) y 3)} \\ &5) \quad m_4 = 2m_3 + 1 = 2 \cdot 7 + 1 = 15 \qquad \text{por 1) y 4)} \\ &6) \quad m_5 = 2m_4 + 1 = 2 \cdot 15 + 1 = 31 \qquad \text{por 1) y 5)} \\ &7) \quad m_6 = 2m_5 + 1 = 2 \cdot 31 + 1 = 63 \qquad \text{por 1) y 6)} \end{aligned}$$

Volviendo a la leyenda, supongamos que los sacerdotes trabajen rápidamente y muevan un disco por segundo. Entonces el tiempo desde el comienzo de la creación hasta el fin del mundo sería de m_{64} segundos. En la siguiente sección se deduce una expresión analítica para m_n. Mientras tanto, podemos calcular m_{64} en una calculadora o una computadora, continuando el proceso iniciado anteriormente (¡inténtelo!). El resultado aproximado es

$$\begin{aligned} 1.844674 \times 10^{19} \text{ segundos} &\cong 5.84542 \times 10^{11} \text{ años} \\ &\cong 584.5 \text{ mil millones de años,} \end{aligned}$$

que se obtiene mediante la estimación de

$$\begin{array}{ccccccc} 60 & \cdot & 60 & \cdot & 24 & \cdot & (365.25) \\ \uparrow & & \uparrow & & \nwarrow & & \nwarrow \\ \text{segundos} & & \text{minutos} & & \text{horas} & & \text{días} \\ \text{por} & & \text{por} & & \text{por} & & \text{por} \\ \text{minuto} & & \text{hora} & & \text{día} & & \text{año} \end{array} \quad = \quad \begin{array}{c} 31\,557\,600 \\ \uparrow \\ \text{segundos} \\ \text{por} \\ \text{año} \end{array}$$

segundos en un año (hay 365.25 días en un año considerando los años bisiestos). Sorprendentemente, esta cifra está cerca de algunas estimaciones científicas de la ¡vida del universo! ■

Ejemplo 5.6.6 Números de Fibonacci


Bettmann/CORBIS

Fibonacci (Leonardo de Pisa) (1175-1250)

Uno de los primeros ejemplos de una sucesión definida de forma recursiva surge en los escritos de Leonardo de Pisa, más conocido como Fibonacci, que era el más grande matemático europeo de la Edad Media. En 1202 Fibonacci plantea el siguiente problema:

Un par de conejos (macho y hembra) nace a principios de año. Supongamos las siguientes condiciones:

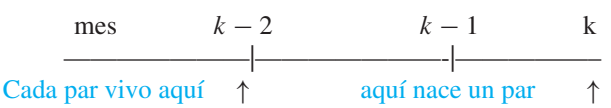
1. Los pares de conejos no son fértiles durante su primer mes de vida, pero a partir de entonces dan a luz a un nuevo par macho/hembra a fines de cada mes.

2. No mueren conejos.

¿Cuántos conejos habrá al final del año?

Solución Una manera de resolver este problema es caer en el centro del mismo usando recursividad. Supongamos que usted sabe cuántos pares de conejos había a fines de los meses anteriores. ¿Cuántos habrá a fines del presente mes?

La observación crucial es que el número de pares de conejos que nace a fines del mes k es el mismo que el número de pares vivos a fines del mes $k - 2$. ¿Por qué? Debido a que es exactamente el número de pares de conejos que estaban vivos a fines del mes $k - 2$, que eran fértiles durante el mes k. Los conejos nacidos a fines del mes $k - 1$ no eran.



Ahora el número de pares de conejos vivos a fines del mes k es igual al número de pares vivos a fines del mes $k - 1$ más los pares recién nacidos a fines del mes. Por tanto

Nota Es esencial reformular esta observación en términos de una sucesión.

$$\begin{bmatrix}\text{el número de pares de conejos vivos a fines del mes } k\end{bmatrix} = \begin{bmatrix}\text{el número de pares de conejos vivos a fines del mes } k-1\end{bmatrix} + \begin{bmatrix}\text{el número de pares de conejos nacidos a fines del mes } k\end{bmatrix}$$

$$= \begin{bmatrix}\text{el número de pares de conejos vivos a fines del mes } k-1\end{bmatrix} + \begin{bmatrix}\text{el número de pares de conejos vivos a fines del mes } k-2\end{bmatrix} \qquad 5.6.2$$

Para cada entero $n \geq 1$, sea

$$F_n = \begin{bmatrix}\text{el número de pares de conejos vivos a fines del mes } n\end{bmatrix}$$

y sea

$$\begin{aligned} F_0 &= \text{el número inicial de pares de conejos} \\ &= 1. \end{aligned}$$

Después sustituyendo en la ecuación (5.6.2), para todo entero $k \geq 2$,

$$F_k = F_{k-1} + F_{k-2}.$$

Ahora $F_0 = 1$, como ya se indicó y también $F_1 = 1$, ya que el primer par de conejos no es fértil hasta el segundo mes. De ahí que la especificación completa de la sucesión de Fibonacci es la siguiente: Para todo entero $k \geq 2$,

1) $F_k = F_{k-1} + F_{k-2}$ relación de recurrencia

2) $F_0 = 1 \qquad F_1 = 1$ condiciones iniciales

Para responder a la pregunta de Fibonacci, calculamos F_2, F_3 y así sucesivamente hasta F_{12}:

3) $F_2 = F_1 + F_0 = 1 + 1 = 2$ por 1) y 2)

4) $F_3 = F_2 + F_1 = 2 + 1 = 3$ por 1), 2) y 3)

5) $F_4 = F_3 + F_2 = 3 + 2 = 5$ por 1), 3) y 4)

6) $F_5 = F_4 + F_3 = 5 + 3 = 8$ por 1), 4) y 5)

7) $F_6 = F_5 + F_4 = 8 + 5 = 13$ por 1), 5) y 6)

8) $F_7 = F_6 + F_5 = 13 + 8 = 21$ por 1), 6) y 7)

9) $F_8 = F_7 + F_6 = 21 + 13 = 34$ por 1), 7) y 8)

10) $F_9 = F_8 + F_7 = 34 + 21 = 55$ por 1), 8) y 9)

11) $F_{10} = F_9 + F_8 = 55 + 34 = 89$ por 1), 9) y 10)

12) $F_{11} = F_{10} + F_9 = 89 + 55 = 144$ por 1), 10) y 11)

13) $F_{12} = F_{11} + F_{10} = 144 + 89 = 233$ por 1), 11) y 12)

Al final del duodécimo mes hay 233 pares de conejos o 466 conejos en total. ■

Ejemplo 5.6.7 Interés compuesto

En su vigésimo primer cumpleaños recibe una carta informándole que el día que nació, una excéntrica tía rica depositó $100 000 en una cuenta bancaria ganando 4% de interés compuesto anual y que ahora pretende poner la cuenta a su nombre, siempre y cuando pueda calcular cuánto vale la pena. ¿Cuál es la cantidad que hay actualmente en la cuenta?

Solución Para abordar este problema de forma recursiva, observe que

$$\left[\begin{array}{l}\text{la cantidad en la}\\ \text{cuenta a fines}\\ \text{de cualquier}\\ \text{año dado}\end{array}\right] = \left[\begin{array}{l}\text{la cantidad en}\\ \text{la cuenta a}\\ \text{fines del año}\\ \text{anterior}\end{array}\right] + \left[\begin{array}{l}\text{los intereses}\\ \text{ganados en la}\\ \text{cuenta durante}\\ \text{el año}\end{array}\right]$$

Ahora los intereses ganados durante el año son iguales a la tasa de interés de $4\% = 0.04$ veces la cantidad en la cuenta a fines del año anterior. Por tanto

$$\left[\begin{array}{l}\text{la cantidad en la}\\ \text{cuenta a fines}\\ \text{de cualquier}\\ \text{año dado}\end{array}\right] = \left[\begin{array}{l}\text{la cantidad}\\ \text{en la cuenta a}\\ \text{fines del año}\\ \text{anterior}\end{array}\right] + (0.04)\cdot \left[\begin{array}{l}\text{la cantidad}\\ \text{en la cuenta a}\\ \text{fines del año}\\ \text{anterior}\end{array}\right]. \qquad 5.6.3$$

Para cada entero positivo n, sea

$$A_n = \left[\begin{array}{l}\text{la cantidad en la cuenta}\\ \text{a fines del año } n\end{array}\right]$$

y sea

$$A_0 = \left[\begin{array}{l}\text{la cantidad inicial}\\ \text{en la cuenta}\end{array}\right] = \$100\,000.$$

Nota Nuevamente, un paso crucial es definir la sucesión de forma explícita.

Entonces, para cualquier año k dado, sustituyendo en la ecuación (5.6.3) se obtiene

$$\begin{aligned} A_k &= A_{k-1} + (0.04) \cdot A_{k-1} \\ &= (1 + 0.04) \cdot A_{k-1} = (1.04) \cdot A_{k-1} \end{aligned}$$ factorizando A_{k-1}.

En consecuencia, los valores de la sucesión $A_0, A_1, A_2, \ldots$ están completamente especificadas de la siguiente manera: para todo entero $k \geq 1$,

$$\begin{aligned} &1) \quad A_k = (1.04) \cdot A_{k-1} && \text{relación de recurrencia} \\ &2) \quad A_0 = \$100\,000 && \text{condición inicial.} \end{aligned}$$

El número 1.04 se llama *factor de crecimiento* de la sucesión.

En la siguiente sección se deduce una fórmula explícita para el valor de la cuenta en cualquier año n. El valor en su vigésimo primer cumpleaños también se puede calcular mediante la sustitución repetida siguiente:

$$\begin{array}{llllll} 3) & A_1 & = 1.04 \cdot A_0 & = (1.04) \cdot \$100\,000 & = \$104\,000 & \text{por 1) y 2)} \\ 4) & A_2 & = 1.04 \cdot A_1 & = (1.04) \cdot \$104\,000 & = \$108\,160 & \text{por 1) y 3)} \\ 5) & A_3 & = 1.04 \cdot A_2 & = (1.04) \cdot \$108\,160 & = \$112\,486.40 & \text{por 1) y 4)} \\ & & \vdots & & \vdots & \\ 22) & A_{20} & = 1.04 \cdot A_{19} & \cong (1.04) \cdot \$210\,684.92 & \cong \$219\,112.31 & \text{por 1) y 21)} \\ 23) & A_{21} & = 1.04 \cdot A_{20} & \cong (1.04) \cdot \$219\,112.31 & \cong \$227\,876.81 & \text{por 1) y 22)} \end{array}$$

El monto de la cuenta es de \$227 876.81 (al céntimo más cercano). Complete los puntos (para comprobar la aritmética) y ¡recoger su dinero! ■

Ejemplo 5.6.8 Interés compuesto con capitalización varias veces al año

Cuando una tasa de interés anual del i está compuesto m veces al año, la tasa de interés por periodo es i/m. Por ejemplo, si $3\% = 0.03$ interés anual compuesto trimestralmente, la tasa de interés pagada por trimestre es de $0.03/4 = 0.0075$.

Para cada entero $k \geq 1$, sea P_k = cantidad en la cuenta a fines del k-ésimo periodo, suponiendo que no haya depósitos o retiros adicionales. Entonces, los intereses ganados durante el k-ésimo periodo es igual a la cantidad depositada a fines del $(k - 1)$-ésimo periodo por la tasa de interés para el periodo:

$$\text{intereses ganados durante el } k\text{-ésimo periodo} = = P_{k-1}\left(\frac{i}{m}\right).$$

La cantidad en la cuenta a fines del k-ésimo periodo, P_k, es igual a la cantidad a fines del $(k - 1)$-ésimo periodo, P_{k-1}, más los intereses ganados durante el k-ésimo periodo:

$$P_k = P_{k-1} + P_{k-1}\left(\frac{i}{m}\right) = P_{k-1}\left(1 + \frac{i}{m}\right). \qquad 5.6.4$$

Supongamos que se deja \$10 000 en la cuenta al 3% capitalizable trimestralmente.

a. ¿Suponiendo que no hay otros depósitos o retiros, cuál será la cantidad en la cuenta al final de un año?

b. La **tasa de porcentaje anual (TPA)** es el porcentaje de incremento en el valor de la cuenta durante un periodo de un año. ¿Cuál es la TPA de esta cuenta?

Solución

a. Para cada entero $n \geq 1$, sea P_n = la cantidad en la cuenta después de n trimestres consecutivos, suponiendo que no hay otros depósitos o retiros y sea P_0 los \$ 10 000 iniciales.

Entonces por la ecuación (5.6.4) con $i = 0.03$ y $m = 4$, una relación de recurrencia para la sucesión $P_0, P_1, P_2, \ldots$ es

$$1) \quad P_k = P_{k-1}(1 + 0.0075) = (1.0075) \cdot P_{k-1} \qquad \text{para todo entero } k \geq 1.$$

La cantidad en la cuenta al final de un año (cuatro trimestres), P_4, se encuentra por sustituciones sucesivas:

$$2) \quad P_0 = \$10\,000$$
$$3) \quad P_1 = 1.0075 \cdot P_0 = (1.0075) \cdot \$10\,000.00 = \$10\,075.00 \qquad \text{por 1) y 2)}$$
$$4) \quad P_2 = 1.0075 \cdot P_1 = (1.0075) \cdot \$10\,075.00 = \$10\,150.56 \qquad \text{por 1) y 3)}$$
$$5) \quad P_3 = 1.0075 \cdot P_2 \cong (1.0075) \cdot \$10\,150.56 = \$10\,226.69 \qquad \text{por 1) y 4)}$$
$$6) \quad P_4 = 1.0075 \cdot P_3 \cong (1.0075) \cdot \$10\,226.69 = \$10\,303.39 \qquad \text{por 1) y 5)}$$

Por tanto después de un año en la cuenta hay \$10 303.39 (al céntimo más cercano).

b. El porcentaje de incremento del valor de la cuenta o la TPA, es

$$\frac{10\,303.39 - 10\,000}{10\,000} = 0.03034 = 3.034\%.$$

Definiciones recursivas de suma y producto

La suma y multiplicación se llaman operaciones *binarias* ya que sólo dos números se pueden sumar o multiplicado a la vez. Cuidadosas definiciones de sumas y productos de más de dos números utilizan recursividad.

• Definición

Dados los números $a_1, a_2, \ldots, a_n$, donde n es un entero positivo, la **suma de $i = 1$ a n de los a_i**, se denota por $\sum_{i=1}^{n} a_i$, que se define de la siguiente manera:

$$\sum_{i=1}^{1} a_i = a_1 \qquad \text{y} \qquad \sum_{i=1}^{n} a_i = \left(\sum_{i=1}^{n-1} a_i\right) + a_n, \quad \text{si } n > 1.$$

El **producto de $i = 1$ a n de los a_i**, se denota por $\prod_{i=1}^{n} a_i$, se define por

$$\prod_{i=1}^{1} a_i = a_1 \qquad \text{y} \qquad \prod_{i=1}^{n} a_i = \left(\prod_{i=1}^{n-1} a_i\right) \cdot a_n, \quad \text{si } n > 1.$$

El efecto de estas definiciones es especificar un *orden* con el que se calcule sumas y productos de más de dos números. Por ejemplo,

$$\sum_{i=1}^{4} a_i = \left(\sum_{i=1}^{3} a_i\right) + a_4 = \left(\left(\sum_{i=1}^{2} a_i\right) + a_3\right) + a_4 = ((a_1 + a_2) + a_3) + a_4.$$

Las definiciones recursivas se utilizan con inducción matemática para establecer varias propiedades generales de sumas y productos finitos.

Ejemplo 5.6.9 Una suma de sumas

Demuestre que para cualquier entero positivo n, si $a_1, a_2, \ldots, a_n$ y $b_1, b_2, \ldots, b_n$ son números reales, entonces

$$\sum_{i=1}^{n}(a_i + b_i) = \sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i.$$

Solución La demostración es por inducción matemática. Sea la propiedad $P(n)$ la ecuación

$$\sum_{i=1}^{n}(a_i + b_i) = \sum_{i=1}^{n} a_i + \sum_{i=1}^{n} b_i. \qquad \leftarrow P(n)$$

Debemos demostrar que $P(n)$ es verdadera para todo entero $n \geq 1$. Hacemos esto por inducción matemática sobre n.

Demostración de que P(1) es verdadera: Para establecer $P(1)$, debemos demostrar que

$$\sum_{i=1}^{1}(a_i + b_i) = \sum_{i=1}^{1} a_i + \sum_{i=1}^{1} b_i. \qquad \leftarrow P(1)$$

Sin embargo,

$$\sum_{i=1}^{1}(a_i + b_i) = a_1 + b_1 \qquad \text{por definición de } \Sigma$$

$$= \sum_{i=1}^{1} a_i + \sum_{i=1}^{1} b_i \qquad \text{también, por definición, de } \Sigma.$$

Por tanto $P(1)$ es verdadera.

Demostración de que para todo entero k ≥ 1, si P(k) es verdadera entonces P(k + 1) también es verdadera:
Supongamos que $a_1, a_2, \ldots, a_k, a_{k+1}$ y $b_1, b_2, \ldots, b_k, b_{k+1}$ son números reales y que para algunos $k \geq 1$

$$\sum_{i=1}^{k}(a_i + b_i) = \sum_{i=1}^{k} a_i + \sum_{i=1}^{k} b_i. \qquad \leftarrow P(n) \text{ hipótesis inductiva}$$

Debemos demostrar que

$$\sum_{i=1}^{k+1}(a_i + b_i) = \sum_{i=1}^{k+1} a_i + \sum_{i=1}^{k+1} b_i. \qquad \leftarrow P(k+1)$$

[Vamos a demostrar que el lado izquierdo de esta ecuación es igual al lado derecho].
Pero el lado izquierdo de la ecuación es

$$\begin{aligned}
\sum_{i=1}^{k+1}(a_i + b_i) &= \sum_{i=1}^{k}(a_i + b_i) + (a_{k+1} + b_{k+1}) && \text{por definición de } \Sigma \\
&= \left(\sum_{i=1}^{k} a_i + \sum_{i=1}^{k} b_i\right) + (a_{k+1} + b_{k+1}) && \text{por hipótesis inductiva} \\
&= \left(\sum_{i=1}^{k} a_i + a_{k+1}\right) + \left(\sum_{i=1}^{k} b_i + b_{k+1}\right) && \text{por las leyes asociativas y conmutativa del álgebra} \\
&= \sum_{i=1}^{k+1} a_i + \sum_{i=1}^{k+1} b_i && \text{por definición de } \Sigma
\end{aligned}$$

que es igual al lado derecho de la ecuación. *[Esto es lo que se quería demostrar.]* ■

Autoexamen

1. Una definición recursiva de una sucesión consiste en una _____ y de _____.
2. Una relación de recurrencia es una ecuación que define cada último término de una sucesión en función de los _____ de la sucesión.
3. Las condiciones iniciales para una definición recursiva de una sucesión compuesta de uno o más de los _____ de la sucesión.
4. Resolver un problema de forma recursiva significa dividir el problema en subproblemas más pequeños del mismo tipo que el problema inicial, al suponer _____ y encontrar cómo utilizar la suposición para _____.
5. Un paso crucial para resolver un problema de forma recursiva es definir una _____ en términos de la cual está la relación de recurrencia y las condiciones iniciales dadas.

Conjunto de ejercicios 5.6

Encuentre los cuatro primeros términos de cada una de las sucesiones definidas recursivamente en los ejercicios 1 al 8.

1. $a_k = 2a_{k-1} + k$, para todo entero $k \geq 2$
$a_1 = 1$

2. $b_k = b_{k-1} + 3k$, para todo entero $k \geq 2$
$b_1 = 1$

3. $c_k = k(c_{k-1})^2$, para todo entero $k \geq 1$
$c_0 = 1$

4. $d_k = k(d_{k-1})^2$, para todo entero $k \geq 1$
$d_0 = 3$

5. $s_k = s_{k-1} + 2s_{k-2}$, para todo entero $k \geq 2$
$s_0 = 1,\ s_1 = 1$

6. $t_k = t_{k-1} + 2t_{k-2}$, para todo entero $k \geq 2$
$t_0 = -1,\ t_1 = 2$

7. $u_k = ku_{k-1} - u_{k-2}$, para todo entero $k \geq 3$
$u_1 = 1,\ u_2 = 1$

8. $v_k = v_{k-1} + v_{k-2} + 1$, para todo entero $k \geq 3$
$v_1 = 1,\ v_2 = 3$

9. Sea $a_0, a_1, a_2, \ldots$ definida por la fórmula $a_n = 3n + 1$, para todo entero $n \geq 0$. Demuestre que esta sucesión satisface la relación de recurrencia $a_k = a_{k-1} + 3$, para todo entero $k \geq 1$.

10. Sea $b_0, b_1, b_2, \ldots$ definida por la fórmula $b_n = 4^n$, para todo entero $n \geq 0$. Demuestre que esta sucesión satisface la relación de recurrencia $b_k = 4\, b_{k-1}$, para todo entero $k \geq 1$.

11. Sea $c_0, c_1, c_2, \ldots$ definida por la fórmula $c_n = 2^n - 1$ para todo entero $n \geq 0$. Demuestre que esta sucesión satisface la relación de recurrencia

$$c_k = 2c_{k-1} + 1.$$

12. Sea $s_0, s_1, s_2, \ldots$ definida por la fórmula $s_n = \dfrac{(-1)^n}{n!}$, para todo entero $n \geq 0$. Demuestre que esta sucesión satisface la relación de recurrencia

$$s_k = \frac{-s_{k-1}}{k}.$$

13. Sea $t_0, t_1, t_2, \ldots$ definida por la fórmula $t_n = 2 + n$, para todo entero $n \geq 0$. Demuestre que esta sucesión satisface la relación de recurrencia

$$t_k = 2t_{k-1} - t_{k-2}.$$

14. Sea $d_0, d_1, d_2, \ldots$ definida por la fórmula $d_n = 3^n - 2^n$, para todo entero $n \geq 0$. Demuestre que esta sucesión satisface la relación de recurrencia

$$d_k = 5d_{k-1} - 6d_{k-2}.$$

***H* 15.** Para la sucesión de los números de Catalan definidos en el ejemplo 5.6.4, demuestre que para todo entero $n \geq 1$,

$$C_n = \frac{1}{4n+2}\left(\begin{array}{c} 2n+2 \\ n+1 \end{array}\right).$$

16. Use la relación de recurrencia y los valores de la sucesión de la *Torre de Hanoi* $m_1, m_2, m_3, \ldots$ analizada en el ejemplo 5.6.5 calcule m_7 y m_8.

17. *Torre de Hanoi con requisito de adyacencia*: Supongamos que, además del requisito de nunca mover un disco más grande en la parte superior a uno más pequeño, los sacerdotes que mueven los discos de la *Torre de Hanoi* también están autorizados sólo para mover los discos uno por uno de un poste a un poste *adyacente*. Suponga que los postes A y C están en los dos extremos de la fila A y que el poste B está en el centro. Sea

$$a_n = \left[\begin{array}{l} \text{el número mínimo de movimientos} \\ \text{necesarios para transferir de una} \\ \text{torre de } n \text{ discos del poste } A \text{ al} \\ \text{poste } C \end{array}\right].$$

a. Determine a_1, a_2 y a_3. b. Encuentre a_4.

c. Encuentre una relación de recurrencia para $a_1, a_2, a_3, \ldots$.

18. *Torre de Hanoi con requisito de adyacencia:* Supongamos que la misma situación que en el ejercicio 17. Sea

$$a_n = \left[\begin{array}{l} \text{el número mínimo de movimientos} \\ \text{necesarios para la transferencia de} \\ \text{una torre de } n \text{ discos del poste } A \\ \text{al poste } B \end{array}\right].$$

a. Determine b_1, b_2 y b_3. **b.** Encuentre b_4.

c. Demuestre que $b_k = a_{k-1} + 1 + b_{k-1}$ para todo entero $k \geq 2$, donde $a_1, a_2, a_3, \ldots$ es la sucesión definida en el ejercicio 17.

d. Demuestre que $b_k \leq 3\, b_{k-1} + 1$ para todo entero $k \geq 2$.

H✶ **e.** Demuestre que $b_k = 3\, b_{k-1} + 1$ para todo enteros $k \geq 2$.

19. *Torre de Hanoi de cuatro postes*: Supongamos que el problema de la *Torre de Hanoi* tiene cuatro postes en una fila en lugar de tres. Los discos se pueden transferir uno por uno de un poste a cualquier otro poste, pero en ningún momento se puede colocar un disco más grande en la parte superior de un disco más pequeño. Sea s_n el número mínimo de movimientos necesarios para transferir toda la torre de n discos de la torre del poste extremo izquierdo al poste del extremo derecho.

a. Determine s_1, s_2 y s_3. **b.** Encuentre s_4.

c. Demuestre que $s_k \leq 2\, s_{k-2} + 3$ para todo entero $k \geq 3$.

20. *Torre de Hanoi, postes en un círculo*: Supongamos que en vez de ser alineados en una fila, los tres postes de la *Torre de Hanoi* original se colocan en un círculo. Los sacerdotes mueven el disco de un poste a otro, pero sólo pueden mover un disco más en el sentido de las agujas del reloj y nunca pueden mover un disco más grande de la parte superior de uno más pequeño. Sea c_n el número mínimo de movimientos necesarios para transferir una pila de n discos de un poste al siguiente poste adyacente en la dirección de las agujas del reloj.

a. Justifique la desigualdad $c_k \leq 4\, c_{k-1} + 1$ para todo entero $k \geq 2$.

b. La expresión $4\, c_{k-1} + 1$ no es el número mínimo de movimientos necesarios para transferir una pila de k discos de un poste a otro. Explique, por ejemplo, ¿por qué $c_3 \neq 4c_2 + 1$.

21. *Doble Torre de Hanoi*: En esta variante de la *Torre de Hanoi* hay tres postes en una fila y $2n$ discos, dos de cada n diferentes tamaños, donde n es un entero positivo. En un principio uno de los postes contiene todos los discos colocados en la parte superior de cada uno de dos en dos de tamaño decreciente. Los discos son transferidos uno por uno de un poste a otro, pero en ningún momento puede un disco más grande colocarse en la parte superior de un disco más pequeño. Sin embargo, se puede colocar un disco en la parte superior de uno del mismo tamaño. Sea t_n el número mínimo de movimientos necesarios para transferir de una torre de $2n$ discos de un poste a otro.

a. Determine t_1 y t_2. **b.** Encuentre t_3.

c. Encuentre una relación de recurrencia para $t_1, t_2, t_3, \ldots$

22. *Variación de Fibonacci*: Un par de conejos (macho y hembra) nace a principios de año. Supongamos las siguientes condiciones (que son más realistas que las de Fibonacci):

1) Los pares de conejos no son fértiles durante su primer mes de vida, pero de ahí en adelante nacen cuatro pares macho/hembra a fines de cada mes.
2) No mueren conejos.

a. Sea $r_n =$ el número de pares de conejos vivos a fines del mes n, para cada entero $n \geq 1$ y sea $r_0 = 1$. Encuentre una relación de recurrencia para $r_0, r_1, r_2, \ldots$.

b. Calcule $r_0, r_1, r_2, r_3, r_4, r_5$ y r_6.

c. ¿Cuántos conejos habrá al final del año?

23. *Variación de Fibonacci*: Un par de conejos (macho y hembra) nace a principios de año. Suponga las siguientes condiciones:

1) Los pares de conejos no son fértiles durante los *dos* primeros meses de vida, pero después naces tres nuevos pares macho/hembra a fines de cada mes.
2) No mueren conejos.

a. Sea $s_n =$ el número de pares de conejos vivos a fines del mes n, para cada entero $n \geq 1$ y sea $s_0 = 1$. Encuentre una relación de recurrencia para $s_0, s_1, s_2, \ldots$.

b. Calcule s_0, s_1, s_2, s_3, s_4 y s_5.

c. ¿Cuántos conejos habrá al final del año?

En los ejercicios del 24 al 34, $F_0, F_1, F_2, \ldots$ es la sucesión de Fibonacci.

24. Use la relación de recurrencia y los valores de $F_0, F_1, F_2, \ldots$ que se dan en el ejemplo 5.6.6 para calcular F_{13} y F_{14}.

25. La sucesión de Fibonacci satisface la relación de recurrencia $F_k = F_{k-1} + F_{k-2}$ para todo entero $k \geq 2$.

a. Explique por qué lo siguiente es verdadero:

$$F_{k+1} = F_k + F_{k-1} \text{ para todo entero } k \geq 1.$$

b. Escribe una ecuación que exprese F_{k+2} en términos de F_{k+1} y F_k.

c. Escribe una ecuación que exprese F_{k+3} en términos de F_{k+2} y F_{k+1}.

26. Demuestre $F_k = 3F_{k-3} + 2F_{k-4}$ para todo entero $k \geq 4$.

27. Demuestre $F_k^2 - F_{k-1}^2 = F_k F_{k-1} - F_{k+1} F_{k-1}$, para todo entero $k \geq 1$.

28. Demuestre $F_{k+1}^2 - F_k^2 - F_{k-1}^2 = 2F_k F_{k-1}$, para todo entero $k \geq 1$.

29. Demuestre $F_{k+1}^2 - F_k^2 = F_{k-1} F_{k+2}$, para todo entero $k \geq 1$.

30. Use inducción matemática para demostrar que para todo entero $n \geq 0$, $F_{n+2} F_n - F_{n+1}^2 = (-1)^n$.

✶ 31. Utilice inducción matemática fuerte para probar que $F_n < 2^n$ para toda $n \geq 1$.

H ✶ **32.** Sea $F_0, F_1, F_2, \ldots$ la sucesión de Fibonacci definida en la sección 5.6. Demuestre que para todo entero $n \geq 0$, mcd $(F_{n+1}, F_n) = 1$.

33. Resulta que la sucesión Fibonacci satisface la siguiente fórmula explícita: Para todo entero $F_n \geq 0$,

$$F_n = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2} \right)^{n+1} - \left(\frac{1-\sqrt{5}}{2} \right)^{n+1} \right]$$

Compruebe que la sucesión definida por esta fórmula satisface la relación de recurrencia $F_k = F_{k-1} + F_{k-2}$ para todo entero $k \geq 2$.

H **34.** (Para los estudiantes que han estudiado cálculo) Determine $\lim_{n \to \infty} \left(\frac{F_{n+1}}{F_n} \right)$, suponiendo que el límite existe.

H ✶ 35. (Para estudiantes que han estudiado cálculo) Demuestre que $\lim_{n\to\infty}\left(\frac{F_{n+1}}{F_n}\right)$ existe.

36. (Para estudiantes que han estudiado cálculo) Defina $x_0, x_1, x_2, \ldots$ de la siguiente manera:

$$x_k = \sqrt{2 + x_{k-1}} \qquad \text{para todo entero } k \geq 1$$
$$x_0 = 0$$

Encuentre $\lim_{n\to\infty} x_n$. (Suponga que el límite existe).

37. *Interés compuesto*: Suponga que se deposita una cierta cantidad de dinero en una cuenta que paga 4% de interés anual compuesto trimestralmente. Para cada entero n positivo, sea R_n = la cantidad en la cuenta al final del enésimo trimestre, suponiendo que no hay otros depósitos o retiros y sea R_0 la cantidad depositada inicial.
   a. Encuentre una relación de recurrencia para $R_0, R_1, R_2, \ldots$
   b. Si $R_0 = \$5\,000$, encuentre la cantidad de dinero en la cuenta al final de un año.
   c. Determine la TPA de la cuenta.

38. *Interés compuesto*: Supongamos que deposita una cantidad de dinero dada en una cuenta que paga 3% de interés anual compuesto mensualmente. Para cada entero positivo n, que S_n = la cantidad en la cuenta al final del enésimo mes y sea S_0 la cantidad inicial depositada.
   a. Determine una relación de recurrencia para $S_0, S_1, S_2, \ldots$, suponiendo que no hay depósitos adicionales ni retiros durante el año.
   b. Si $S_0 = \$10\,000$, encuentre la cantidad de dinero en la cuenta al final de un año.
   c. Determinar la TPA de la cuenta.

39. Con cada paso que da al subir una escalera, puede desplazarse hacia arriba uno o dos escalones. Como resultado, puede subir toda la escalera subiendo un escalón a la vez, subiendo dos a la vez o subiendo una combinación de uno y dos escalones. Para cada número entero $n \geq 1$, si la escalera tiene n escalones, sea c_n el número de maneras diferentes de subir la escalera. Determine una relación de recurrencia para $c_1, c_2, c_3, \ldots$.

40. Un conjunto de bloques contiene bloques de las siguientes alturas 1, 2 y 4 centímetros. Imagine la construcción de torres apilando bloques de diferentes alturas directamente uno sobre el otro. (Una torre de altura de 6 cm puede obtenerse mediante seis bloques de 1 cm, tres bloques de 2 cm, un bloque 2 cm con un bloque de 4 cm en la parte superior, un bloque de 4 cm con un bloque de 2 cm en la parte superior, etc.). Sea t el número de maneras de construir una torre de altura n cm usando bloques del conjunto. (Suponga un número ilimitado de bloques de cada tamaño). Determine una relación de recurrencia para $t_1, t_2, t_3, \ldots$.

41. Use la definición recursiva de suma, junto con inducción matemática para probar la ley distributiva generalizada de que para todo entero positivo n, si $a_1, a_2, \ldots, a_n$ y c son números reales, entonces

$$\sum_{i=1}^{n} ca_i = c\left(\sum_{i=1}^{n} a_i\right).$$

42. Use la definición recursiva del producto, junto con inducción matemática, para demostrar que para todo entero positivo n, si $a_1, a_2, \ldots, a_n$ y $b_1, b_2, \ldots, b_n$ son números reales, entonces

$$\prod_{i=1}^{n}(a_i b_i) = \left(\prod_{i=1}^{n} a_i\right)\left(\prod_{i=1}^{n} b_i\right).$$

43. Use la definición recursiva del producto, junto con la inducción matemática, para demostrar que para todo entero positivo n, si $a_1, a_2, \ldots, a_n$ y c son números reales, entonces

$$\prod_{i=1}^{n}(ca_i) = c^n\left(\prod_{i=1}^{n} a_i\right).$$

H 44. La desigualdad del triángulo para todos los estados de valor absoluto que para todos los números reales a y b, $|a + b| \leq |a| + |b|$. Utilice la definición recursiva de la suma, la desigualdad del triángulo, la definición de valor absoluto y la inducción matemática para demostrar que para todo entero positivo n, si $a_1, a_2, \ldots, a_n$ son números reales, entonces

$$\left|\sum_{i=1}^{n} a_i\right| \leq \sum_{i=1}^{n} |a_i|.$$

Respuestas del autoexamen

1. relación de recurrencia; las condiciones iniciales 2. términos anteriores 3. valores de los primeros términos 4. que los subproblemas más pequeños ya han sido resueltos; resolver el problema inicial 5. sucesión

5.7 Solución por iteración de las relaciones de recurrencia

El sentido más agudo de la deducción lógica, es el que con frecuencia menos hace inferencias fuertes y rápidas. —Bertrand Russell, 1872-1970

Suponga que tiene una sucesión que satisface una relación de recurrencia dada y unas condiciones iniciales. Con frecuencia es útil conocer una fórmula explícita para la sucesión,

especialmente si necesita calcular términos con subíndices muy grandes o si necesita examinar propiedades generales de la sucesión. Dicha fórmula explícita se llama una **solución** de la relación de recurrencia. En esta sección, se analizan métodos para resolver relaciones de recurrencia. Por ejemplo, en el texto y en los ejercicios de esta sección, vamos a mostrar que la sucesión de la *Torre de Hanoi* del ejemplo 5.6.5 satisface la fórmula

$$m_n = 2^n - 1,$$

y que la sucesión de interés compuesto del ejemplo 5.6.7 satisface

$$A_n = (1.04)^n \cdot \$100\,000.$$

El método de iteración

El método más básico para encontrar una fórmula explícita para una sucesión definida de forma recursiva es la **iteración**. La iteración funciona como sigue: Dada una sucesión a_0, $a_1, a_2, \ldots$, definida por una relación de recurrencia y condiciones iniciales, inicie a partir de las condiciones iniciales y calcule los términos sucesivos de la sucesión hasta que aparezca un patrón de desarrollo. En ese momento, proponga una fórmula explícita.

Ejemplo 5.7.1 Encuentre una fórmula explícita

Sea $a_0, a_1, a_2, \ldots$ la sucesión definida recursivamente de la siguiente manera: Para todo entero $k \geq 1$,

1) $a_k = a_{k-1} + 2$ relación de recurrencia
2) $a_0 = 1$ condición inicial.

Utilice iteración para proponer una fórmula explícita para la sucesión.

Solución Recuerde que decir

$$a_k = a_{k-1} + 2 \quad \text{para todo entero } k \geq 1$$

significa

$$a_{\square} = a_{\square - 1} + 2$$ no importa qué número entero positivo se coloque en la caja $\square$.

En particular,

$$a_1 = a_0 + 2,$$
$$a_2 = a_1 + 2,$$
$$a_3 = a_2 + 2,$$

y así sucesivamente. Ahora se usa la condición inicial para comenzar un proceso de sustituciones sucesivas en estas ecuaciones, no sólo de los números (como se hizo en la sección 5.6), sino de *expresiones numéricas*.

La razón para el uso de expresiones numéricas más que de números es porque en estos problemas usted está buscando un patrón numérico que subyace a una fórmula general. El secreto del éxito es dejar la mayor parte de la aritmética sin hacer. Sin embargo, es necesario eliminar paréntesis para ir de un paso al siguiente. Por el contario, pronto terminaría con un nido de paréntesis asombrosamente grande. Por otra parte, casi siempre es útil usar anotaciones para reagrupar sumas, restas y multiplicaciones de números que se repiten. Así, por ejemplo, podría escribir

$5 \cdot 2$ en vez de $2 + 2 + 2 + 2 + 2$

y

2^5 en lugar de $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2$.

Observe que no se pierde ninguna información acerca de los patrones de números cuando se utilizan estas notaciones cortas.

Así es como funciona el proceso para la sucesión dada:

$a_0 = 1$ — condición inicial

$a_1 = a_0 + 2 = 1 + 2$ — por sustitución

$a_2 = a_1 + 2 = (1 + 2) + 2 = 1 + 2 + 2$ — eliminando paréntesis

$a_3 = a_2 + 2 = (1 + 2 + 2) + 2 = 1 + 2 + 2 + 2$ — eliminando el paréntesis, de nuevo, escribir $2 \cdot 3$ en lugar de $2 + 2 + 2$?

$a_4 = a_3 + 2 = (1 + 2 + 2 + 2) + 2 = 1 + 2 + 2 + 2 + 2$ — eliminando el paréntesis, de nuevo, definitivamente escribimos $4 \cdot 2$ en vez de $2 + 2 + 2 + 2$, la longitud de la cadena de 2 sale de control.

Sugerencia No haga aritmética *excepto*

- sustituya $n \cdot 1$ y $1 \cdot n$ por 1
- reformatee los números repetidos
- quite los paréntesis

Dado que parece útil usar la abreviatura $k \cdot 2$ en lugar de $2 + 2 + \cdots + 2$ (k veces), empezamos de nuevo desde a_0.

$a_0 = 1 = 1 + 0 \cdot 2$ — la condición inicial

$a_1 = a_0 + 2 = 1 + 2 = 1 + 1 \cdot 2$ — por sustitución

$a_2 = a_1 + 2 = (1 + 2) + 2 = 1 + 2 \cdot 2$

$a_3 = a_2 + 2 = (1 + 2 \cdot 2) + 2 = 1 + 3 \cdot 2$

$a_4 = a_3 + 2 = (1 + 3 \cdot 2) + 2 = 1 + 4 \cdot 2$ — En este punto, ciertamente parece probable que el patrón general es $1 + n \cdot 2$; compruebe si el siguiente cálculo es compatible con éste.

$a_5 = a_4 + 2 = (1 + 4 \cdot 2) + 2 = 1 + 5 \cdot 2$ — ¡Lo es! Así que adelante y se escribe una respuesta. Es sólo una suposición, después de todo.

$\vdots$

Se supone: $a_n = 1 + n \cdot 2 = 1 + 2n$

La respuesta obtenida para este problema es sólo una suposición. Para estar seguro de la exactitud de esta suposición, se tendrá que comprobar por inducción matemática. Más adelante en esta sección, vamos a mostrar cómo se hace esto. ■

Una sucesión como la del ejemplo 5.7.1, en la que cada término es igual al término anterior más una constante fija, se llama una *sucesión aritmética*. En los ejercicios al final de esta sección se le pide que muestren que el enésimo término de una sucesión aritmética es siempre igual al valor inicial de la sucesión más n veces la constante fija.

• Definición

Una sucesión $a_0, a_1, a_2, \ldots$ se llama una **sucesión aritmética**, si y sólo si, existe una constante d tal que

$$a_k = a_{k-1} + d \quad \text{para todo entero } k \geq 1.$$

De lo que se tiene que,

$$a_n = a_0 + dn \qquad \text{para todo entero } n \geq 0.$$

Ejemplo 5.7.2 Una sucesión aritmética

Bajo la acción de la gravedad, un objeto que cae en el vacío alrededor de 9.8 metros por segundo (m/s) más rápido cada segundo de lo que cayó el segundo anterior. Por tanto, al despreciar la resistencia del aire, la velocidad de un paracaidista a la salida de un avión es de aproximadamente 9.8 m/s un segundo después de la salida, $9.8 + 9.8 = 19.6$ m/s dos segundos después de la salida y así sucesivamente. Si se desprecia la resistencia de aire, ¿cuál es la rapidez con la que el paracaidista cae 60 segundos después de salir del avión?

Solución Sea s_n la velocidad del paracaidista en m/seg n segundos después de salir del avión si no hubiera resistencia del aire. Así s_0 es la velocidad inicial y dado que el paracaidista viajaría a 9.8 m/s cada segundo más rápido que el segundo anterior,

$$s_k = s_{k-1} + 9.8 \text{ m/s} \quad \text{para todo entero } k \geq 1.$$

De lo que se deduce que $s_0, s_1, s_2, \ldots$ es una sucesión aritmética con una constante fija de 9.8 y por tanto

$$s_n = s_0 + (9{,}8)n \quad \text{para todo entero } n \geq 0.$$

Por tanto sesenta segundos después de salir y despreciando la resistencia del aire, el paracaidista viajará a una velocidad de

$$s_{60} = 0 + (9.8)(60) = 588 \text{ m/s}.$$

Observe que 588 m/s es más de la mitad de un kilómetro por segundo o más de un tercio de milla por segundo, que es muy rápido para que viaje un ser humano. Felizmente para el paracaidista, considerando la resistencia del aire baja la velocidad considerablemente. ■

En una sucesión aritmética, cada término es igual al término anterior, más una constante fija. En una sucesión geométrica, cada término es igual al término anterior por una constante fija. Las sucesiones geométricas se presentan en una gran variedad de aplicaciones, tales como los modelos de interés compuesto, en ciertos modelos de crecimiento de la población, en desintegración radiactiva y en el número de operaciones necesarias para ejecutar ciertos algoritmos informáticos.

Ejemplo 5.7.3 Fórmula explícita de una sucesión geométrica

Sea r una constante fija distinta de cero y supongamos una sucesión $a_0, a_1, a_2, \ldots$ definida en forma recursiva de la siguiente manera:

$$a_k = ra_{k-1} \text{ para todo entero } k \geq 1,$$
$$a_0 = a.$$

Utilice iteración para inferir una fórmula explícita para esta sucesión.

Solución

$$a_0 = a$$
$$a_1 = ra_0 = ra$$
$$a_2 = ra_1 = r(ra) = r^2a$$
$$a_3 = ra_2 = r(r^2a) = r^3a$$
$$a_4 = ra_3 = r(r^3a) = r^4a$$
$$\vdots$$

Se supone: $a_n = r^n a = ar^n$ para cualquier número entero arbitrario $n \geq 0$

En los ejercicios al final de esta sección, se le pide que demuestre que esta fórmula es correcta. ■

• Definición

Una sucesión $a_0, a_1, a_2, \ldots$ se llama una **sucesión geométrica**, si y sólo si, existe una constante r tal que

$$a_k = ra_{k-1} \quad \text{para todo entero } k > 1$$

De lo que se tiene que,

$$a_n = a_0 r^n \quad \text{para todo entero } n \geq 0$$

Ejemplo 5.7.4 Una sucesión geométrica

Como se muestra en el ejemplo 5.6.7, si un banco paga intereses a una tasa de 4% anual compuesto anualmente y A_n denota la cantidad en la cuenta al final del año n, entonces, $A_k = (1.04)\, A_{k-1}$, para todo entero $k \geq 1$, suponiendo que no haya depósitos o retiros durante el año. Supongamos que la cantidad inicial depositada es de \$100 000 y suponga que no se hacen depósitos o retiros adicionales.

a. ¿Cuánto habrá en la cuenta al final, de 21 años?

b. ¿En cuántos años la cuenta tendrá 1 000 000 de dólares?

Solución

a. $A_0, A_1, A_2, \ldots$ es una sucesión geométrica con un valor inicial de 100 000 y una constante multiplicadora de 1.04. Por tanto,

$$A_n = \$100\,000 \cdot (1.04)^n \quad \text{para todo entero } n \geq 0.$$

Después de 21 años, la cantidad en la cuenta será

$$A_{21} = \$100\,000 \cdot (1.04)^{21} \cong \$227\,876.81.$$

Esta es la misma respuesta que la obtenida en el ejemplo 5.6.7, pero se calcula con mayor facilidad (al menos si se utiliza una calculadora con una tecla de potencia, tales como $\boxed{\wedge}$ o $\boxed{x^y}$).

b. Sea t el número de años necesarios para que la cuenta crezca a \$1 000 000. Entonces,

$$\$1\,000\,000 = \$100\,000 - (1.04)^t.$$

Dividiendo ambos lados por 100 mil se obtiene

$$10 = (1.04)^t,$$

y tomando logaritmos naturales de ambos lados se obtiene

$$\ln(10) = \ln(1.04)^t.$$

Nota En la sección 7.2 se repasan las propiedades de los logaritmos.

Entonces

$$\ln(10) \cong t \ \ln(1.04)$$

ya que $\log_b(x^a) = a \log_b(x)$ (vea el ejercicio 35 de la sección 7.2).

y así

$$t = \frac{\ln(10)}{\ln(1.04)} \cong 58.7$$

Por tanto la cuenta crecerá a \$1 000 000 en aproximadamente 58.7 años. ■

Una propiedad importante de una sucesión geométrica con multiplicador constante mayor que 1 es que sus términos aumentan muy rápidamente en tamaño conforme los subíndices se hacen más y más grandes. Por ejemplo, los diez primeros términos de una sucesión geométrica con un multiplicador constante de 10 son

$$1, 10, 10^2, 10^3, 10^4, 10^5, 10^6, 10^7, 10^8, 10^9.$$

Así, en su décimo término, la sucesión ya tiene el valor $10^9 = 1\,000\,000\,000 = 1$ mil millones. El siguiente cuadro indica algunas cantidades que son aproximadamente iguales a ciertas potencias de 10.

10^7	≅ número de segundos en un año
10^9	≅ número de bytes de memoria en una computadora personal
10^{11}	≅ número de neuronas en un cerebro humano
10^{17}	≅ edad del universo en segundos (de acuerdo con una teoría)
10^{31}	≅ número de segundos para procesar todas las posiciones posibles de un juego de damas, si los movimientos se procesan con una velocidad de 1 por cada mil millonésimo de segundo
10^{81}	≅ número de átomos en el universo
10^{111}	≅ número de segundos para procesar todas las posiciones posibles de un juego de ajedrez si los movimientos se procesan con una velocidad de 1 por cada mil millonésimo de segundo

Uso de fórmulas para simplificar soluciones obtenidas por iteración

Las fórmulas explícitas obtenidas por iteración a menudo se pueden simplificar mediante el uso de fórmulas como las desarrolladas en la sección 5.2. Por ejemplo, de acuerdo con la fórmula de la suma de una sucesión geométrica con un término inicial igual a 1 (teorema 5.2.3), para cada número real r, excepto $r = 1$,

$$1 + r + r^2 + \cdots + r^n = \frac{r^{n+1} - 1}{r - 1} \text{ para todo entero } n \geq 0.$$

Y de acuerdo con la fórmula de la suma de los n primeros enteros (teorema 5.2.2),

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2} \text{ para todo entero } n \geq 1.$$

Ejemplo 5.7.5 Una fórmula explícita para la sucesión de la *Torre de Hanoi*

Recordemos que la sucesión de la *Torre de Hanoi* $m_1, m_2, m_3, \ldots$ del ejemplo 5.6.5 satisface la relación de recurrencia

$$m_k = 2\,m_{k-1} + 1 \quad \text{para todo entero } k \geq 2$$

y tiene la condición inicial

$$m_1 = 1.$$

Use iteración para inferir una fórmula explícita para esta sucesión y haga uso de una fórmula de la sección 5.2 para simplificar la respuesta.

Solución por iteración

$$m_1 = 1$$

$$m_{②} = 2m_1 + 1 = 2\cdot 1 + 1 = 2^{①} + 1,$$

$$m_{③} = 2m_2 + 1 = 2(2+1) + 1 = 2^{②} + 2 + 1,$$

$$m_{④} = 2m_3 + 1 = 2(2^2 + 2 + 1) + 1 = 2^{③} + 2^2 + 2 + 1,$$

$$m_{⑤} = 2m_4 + 1 = 2(2^3 + 2^2 + 2 + 1) + 1 = 2^{④} + 2^3 + 2^2 + 2 + 1.$$

Estos cálculos muestran que cada término hasta m_5 es la suma de potencias sucesivas de 2, iniciando con $2^0 = 1$ y va hasta 2^k, donde k es 1 menos que el subíndice del término. El patrón parece continuar a términos más altos ya que cada término se obtiene del anterior multiplicado por 2 y sumando 1, multiplicando por 2 eleva el exponente de cada componente de la suma de 1 y sumando el 1 que se perdió atrás cuando el 1 anterior se multiplicó por 2. Por ejemplo, para $n = 6$,

$$m_6 = 2m_5 + 1 = 2(2^4 + 2^3 + 2^2 + 2 + 1) + 1 = 2^5 + 2^4 + 2^3 + 2^2 + 2 + 1.$$

Por tanto, parece que, en general,

$$m_n = 2^{n-1} + 2^{n-2} + \cdots + 2^2 + 2 + 1.$$

Con la fórmula de la suma de una sucesión geométrica (teorema 5.2.3),

$$2^{n-1} + 2^{n-2} + \cdots + 2^2 + 2 + 1 = \frac{2^n - 1}{2 - 1} = 2^n - 1.$$

Por tanto, la fórmula explícita parece ser

$$m_n = 2^n - 1 \quad \text{para todo entero } n \geq 1.$$ ■

Un error común cuando se hacen problemas de este tipo es usar mal las leyes del álgebra, por ejemplo, por la ley distributiva,

$$a \cdot (b + c) = a \cdot b + a \cdot c \text{ para todos los números reales } a, b \text{ y } c.$$

Así, en particular, por $a = 2$, $b = 2$ y $c = 1$,

$$2\cdot(2+1) = 2\cdot 2 + 2\cdot 1 = 2^2 + 2.$$

De lo que se tiene que

$$2\cdot(2+1) + 1 = (2^2 + 2) + 1 = 2^2 + 2 + 1.$$

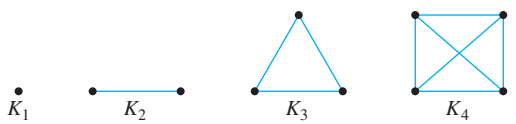
¡Precaución! No es verdad que

~~$2\cdot(2+1)+1 = 2^2+1+1$.~~

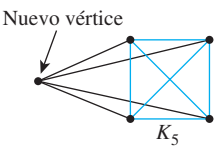
Esto está tachado porque es falso.

Ejemplo 5.7.6 Uso de la fórmula para la suma de los primeros *n* enteros positivos

Sea K_n la imagen obtenida al dibujar n puntos (que llamamos *vértices*) y se une cada par de vértices con un segmento de recta (que llamamos *arista*). (En el capítulo 10 se analizan estos objetos en un contexto más general.) Entonces, K_1, K_2, K_3, K_4 y son los siguientes:



Observe que K_5 puede obtenerse a partir de K_4 agregando un vértice y dibujando extremos entre este nuevo vértice y todos los vértices de K_4 (los antiguos vértices). La razón de que con este procedimiento se obtenga el resultado correcto es que cada par de antiguos vértices ya está unido con una arista y al agregar las nuevas aristas se une cada par de vértices que consiste de uno antiguo y de uno nuevo.



Por tanto el número de aristas de $K_5 = 4 +$ el número de aristas de K_4.

Por el mismo razonamiento, para todo entero $k \geq 2$, el número de aristas de K_k es $k - 1$ más que el número de aristas de K_{k-1}. Es decir, si para cada entero $n \geq 1$

$$s_n = \text{el número de aristas de } K_n,$$

entonces, $s_k = s_{k-1} + (k-1)$ para todo entero $k \geq 2$.
Observe que s_1, es el número de aristas de K_1, que es 0 y se usa iteración para encontrar una fórmula explícita para $s_1, s_2, s_3, \ldots$.

Solución Ya que

$$s_k = s_{k-1} + (k-1) \text{ para } \textit{todo} \text{ entero } k \geq 2$$

y

$$s_{①} = 0 \qquad (1-1)$$

entonces, en particular,

$$s_{②} = s_1 + 1 = 0 + 1, \qquad (2-1)$$

$$s_{③} = s_2 + 2 = (0+1) + 2 = 0 + 1 + 2, \qquad (3-1)$$

$$s_{④} = s_3 + 3 = (0+1+2) + 3 = 0 + 1 + 2 + 3, \qquad (4-1)$$

$$s_{⑤} = s_4 + 4 = (0+1+2+3) + 4 = 0 + 1 + 2 + 3 + 4, \qquad (5-1)$$

$$\vdots$$

Se supone: $s_{(n)} = 0 + 1 + 2 + \cdots + (n-1)$.

Pero por el teorema 5.2.2,

$$0 + 1 + 2 + 3 + \cdots + (n-1) = \frac{(n-1)n}{2} = \frac{n(n-1)}{2}.$$

Por tanto, parece que

$$s_n = \frac{n(n-1)}{2}.$$

■

Comprobación de lo exacto de una fórmula con inducción matemática

Como se puede ver en algunos de los ejemplos anteriores, el proceso de resolución de una relación de recurrencia con iteración puede involucrar cálculos complicados. Es muy fácil cometer un error y obtener una fórmula errónea. Por eso es importante confirmar sus cálculos comprobando la exactitud de la fórmula. La forma más común de hacer esto es utilizar inducción matemática.

Ejemplo 5.7.7 Uso de inducción matemática para comprobar la exactitud de una solución para una relación de recurrencia

En el ejemplo 5.6.5 se obtuvo una fórmula para la sucesión de la *Torre de Hanoi*. Utilice inducción matemática para demostrar que esta fórmula es correcta.

Solución ¿Qué significa demostrar la exactitud de una fórmula para una sucesión definida en forma recursiva? Dada una sucesión de números que satisface una cierta relación de recurrencia y la condición inicial, su trabajo es demostrar que cada término de la sucesión satisface la fórmula explícita propuesta. En este caso, se necesita demostrar el enunciado siguiente:

> Si $m_1, m_2, m_3, \ldots$ es la sucesión definida por
> $m_k = 2m_{k-1} + 1$ para todo entero $k \geq 2$ y
> $m_1 = 1$,
> entonces $m_n = 2^n - 1$ para todo entero $n \geq 1$.

Demostración de exactitud:

Sea $m_1, m_2, m_3, \ldots$ la sucesión definida mediante la especificación de que $m_1 = 1$ y $m_k = 2m_{k+1} + 1$ para todo entero $k \geq 2$ y sea la propiedad $P(n)$ la ecuación

$$m_n = 2^n - 1 \qquad \leftarrow P(n)$$

Vamos a utilizar la inducción matemática para demostrar que para todo entero $n \geq 1$, $P(n)$ es verdadera.

Demostración de que P(1) es verdadera:
Para establecer $P(1)$, debemos demostrar que

$$m_1 = 2^1 - 1. \qquad \leftarrow P(1)$$

Pero el lado izquierdo de $P(1)$ es

$$m_1 = 1 \qquad \text{por definición de } m_1, m_2, m_3, \ldots,$$

y la parte derecha de $P(1)$ es

$$2^1 - 1 = 2 - 1 = 1.$$

Así, los dos lados de $P(1)$ son iguales a la misma cantidad y por tanto $P(1)$ es verdadera.

Demostración de que para todo entero $k \geq 1$, si $P(k)$ es verdadera entonces $P(k+1)$ también es verdadera:
[Supongamos que $P(k)$ es verdadera para un entero $k \geq 1$ dado, pero elegido arbitrariamente. Es decir:] Supongamos que k es un entero con $k \geq 1$ tal que

$$m_k = 2^k - 1. \qquad \leftarrow P(k) \text{ hipótesis inductiva}$$

[Debemos demostrar que $P(k+1)$ es verdadera. Es decir:] Debemos demostrar que

$$m_{k+1} = 2^{k+1} - 1. \qquad \leftarrow P(k+1)$$

Pero el lado izquierdo de $P(k+1)$ es

$$\begin{aligned} m_{k+1} &= 2m_{(k+1)-1} + 1 && \text{por definición de } m_1, m_2, m_3, \ldots \\ &= 2m_k + 1 \\ &= 2(2^k - 1) + 1 && \text{sustituyendo la hipótesis inductiva} \\ &= 2^{k+1} - 2 + 1 && \text{por la ley distributiva y el hecho de que } 2 \cdot 2^k = 2^{k-1} \\ &= 2^{k+1} - 1 && \text{por álgebra básica} \end{aligned}$$

que es igual al lado derecha de $P(k+1)$. *[Puesto que los pasos básico y de inducción ya se han demostrado, se deduce por inducción matemática que la fórmula propuesta es válida para todos los enteros $n \geq 1$.]* ■

Descubriendo que una fórmula explícita es incorrecta

El ejemplo siguiente muestra cómo el proceso de tratar de comprobar una fórmula por inducción matemática puede revelar un error.

Ejemplo 5.7.8 Uso de comprobación por inducción matemática para encontrar un error

Sea $c_0, c_1, c_2, \ldots$ la sucesión definida de la siguiente manera:

$$\begin{aligned} c_k &= 2\,c_{k-1} + k \qquad \text{para todo entero } k \geq 1, \\ c_0 &= 1. \end{aligned}$$

Supongamos que los cálculos indican que $c_0, c_1, c_2, \ldots$ satisface la fórmula explícita siguiente:

$$c_n = 2^n + n \qquad \text{para todo entero } n \geq 0.$$

¿Es correcta esta fórmula?

Solución Iniciamos con demostrar el enunciado por inducción matemática y vemos lo que se desarrolla. La fórmula propuesta pasa el paso básico de la demostración de inducción sin problemas, por una parte, $c_0 = 1$ por definición y por otro lado, $2^0 + 0 = 1 + 0 = 1$ también.

En el paso inductivo, supongamos que

$$c_k = 2^k + k \qquad \text{para algún entero } k \geq 0 \qquad \text{Esta es la hipótesis inductiva.}$$

y entonces debe demostrar que

$$c_{k+1} = 2^{k+1} + (k+1).$$

Para hacerlo, se comienza con c_{k+1}, sustituyendo de la relación de recurrencia y después se utiliza la hipótesis inductiva de la siguiente manera:

$$\begin{aligned} c_{k+1} &= 2c_k + (k+1) && \text{por la relación de recurrencia} \\ &= 2(2^k + k) + (k+1) && \text{sustituyendo la hipótesis inductiva} \\ &= 2^{(k+1)} + 3k + 1 && \text{por álgebra básica} \end{aligned}$$

Para finalizar la comprobación, por tanto, es necesario demostrar que

$$2^{k+1} + 3k + 1 = 2^{k+1} + (k+1).$$

Ahora, esta ecuación es equivalente a

$$2k = 0 \quad \text{restando } 2^{k+1} + k + 1 \text{ de ambos lados.}$$

lo que equivale a

$$k = 0 \quad \text{dividiendo ambos lados entre 2.}$$

Pero esto es falso ya k puede ser *cualquier* entero no negativo.

Observe que cuando $k = 0$, entonces $k + 1 = 1$ y

$$c_1 = 2 \cdot 1 + 1 = 3 \quad \text{y} \quad 2^1 + 1 = 3.$$

Así, la fórmula da el valor correcto para c_1. Sin embargo, cuando $k = 1$, entonces $k + 1 = 2$ y

$$c_2 = 2 \cdot 3 + 2 = 8 \quad \text{mientras que} \quad 2^2 + 2 = 4 + 2 = 6.$$

Así que la fórmula no da el valor correcto para c_2. Por tanto la sucesión $c_0, c_1, c_2, \ldots$ no satisface la fórmula propuesta. ■

Una vez que se haya encontrado que una fórmula propuesta es falsa, debe buscar hacia atrás en sus cálculos para ver dónde ha cometido un error, corríjalo y vuelva a intentarlo.

Autoexamen

1. Utilizando iteración encuentre una fórmula explícita para una sucesión definida de forma recursiva, comience con _____ y utilice sustitución sucesiva en la _____ en busca de un patrón numérico.
2. En cada paso del proceso de iteración, es importante para eliminar _____.
3. Si un solo número, por ejemplo a, se suma a sí mismo k veces en uno de los pasos de la iteración, sustituya la suma por la expresión _____.
4. Si un solo número, por ejemplo a, se multiplica a sí mismo k veces en uno de los pasos de la iteración, sustituya el producto por la expresión _____.
5. Una sucesión aritmética general $a_0, a_1, a_2, \ldots$ con valor inicial a_0 y constante fija d satisface la recurrencia real _____ y tiene la fórmula explícita _____.
6. Una sucesión geométrica general $a_0, a_1, a_2, \ldots$ con valor inicial a_0 y constante fija r satisface la relación de recurrencia _____ y tiene la fórmula explícita _____.
7. Cuando una fórmula explícita para una sucesión definida de forma recursiva se ha obtenido por iteración, la exactitud de ésta se puede comprobar por _____.

Conjunto de ejercicios 5.7

1. La fórmula

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$$

es verdadera para todo entero $n \geq 1$. Utilice este hecho para resolver cada uno de los siguientes problemas:

a. Si k es un número entero y $k \geq 2$, encuentre una fórmula para la expresión $1 + 2 + 3 + \cdots + (k-1)$.

b. Si n es un entero y $n \geq 1$, encuentre una fórmula para la expresión $3 + 2 + 4 + 6 + 8 + \cdots + 2n$.

c. Si n es un entero y $n \geq 1$, encuentre una fórmula para la expresión $3 + 3 \cdot 2 + 3 \cdot 3 + \cdots + 3 \cdot n + n$.

2. La fórmula

$$1 + r + r^2 + \cdots + r^n = \frac{r^{n+1} - 1}{r - 1}$$

es verdadero para todos los números reales r excepto para $r = 1$ y para todo entero $n \geq 0$. Utilice este hecho para resolver cada uno de los siguientes problemas:

a. Si i es un entero e $i \geq 1$, encuentre una fórmula para la expresión $1 + 2 + 2^2 + \cdots + 2^{i-1}$.

b. Si n es un entero y $n \geq 1$, encuentre una fórmula para la expresión $3^{n-1} + 3^{n-2} + \cdots + 3^2 + 3 + 1$.

c. Si n es un entero y $n \geq 2$, encuentre una fórmula para la expresión $2^n + 2^{n-2} \cdot 3 + 2^{n-3} \cdot 3 + \cdots + 2^2 \cdot 3 + 2 \cdot 3 + 3$.

d. Si n es un entero y $n \geq 1$, encuentre una fórmula para la expresión

$$2^n - 2^{n-1} + 2^{n-2} - 2^{n-3} + \cdots + (-1)^{n-1} \cdot 2 + (-1)^n.$$

En cada uno de los ejercicios del 3 al 15 se define en forma recursiva una sucesión. Utilice iteración para inferir una fórmula explícita para la sucesión. Utilice las fórmulas de la sección 5.2 para simplificar sus respuestas siempre que sea posible.

3. $a_k = ka_{k-1}$, para todo entero $k \geq 1$
$a_0 = 1$

4. $b_k = \dfrac{b_{k-1}}{1 + b_{k-1}}$, para todo entero $k \geq 1$
$b_0 = 1$

5. $c_k = 3c_{k-1} + 1$, para todo entero $k \geq 2$
$c_1 = 1$

***H* 6.** $d_k = 2d_{k-1} + 3$, para todo entero $k \geq 2$
$d_t = 2$

7. $e_k = 4e_{k-1} + 5$, para todo entero $k \geq 1$
$e_0 = 2$

8. $f_k = f_{k-1} + 2^k$, para todo entero $k \geq 2$
$f_1 = 1$

***H* 9.** $g_k = \dfrac{g_{k-1}}{g_{k-1} + 2}$, para todo entero $k \geq 2$
$g_1 = 1$

10. $h_k = 2^k - h_{k-1}$, para todo entero $k \geq 1$
$h_0 = 1$

11. $p_k = p_{k-1} + 2 \cdot 3^k$
$p_1 = 2$

12. $s_k = s_{k-1} + 2k$, para todo entero $k \geq 1$
$s_0 = 3$

13. $t_k = t_{k-1} + 3k + 1$, para todo entero $k \geq 1$
$t_0 = 0$

***14.** $x_k = 3x_{k-1} + k$, para todo entero $k \geq 2$
$x_1 = 1$

15. $y_k = y_{k-1} + k^2$, para todo entero $k \geq 2$
$y_1 = 1$

16. Resuelva la relación de recurrencia obtenida como respuesta al ejercicio 18*c*) de la sección 5.6.

17. Resuelva la relación de recurrencia obtenida como respuesta al ejercicio 21*c*) de la sección 5.6.

18. Suponga que d es una constante fija y $a_0, a_1, a_2, \ldots$ es una sucesión que satisface la relación de recurrencia $a_k = a_{k-1} + d$, para todos los enteros $k \geq 1$. Use inducción matemática para demostrar que $a_n = a_0 + nd$, para todo entero $n \geq 0$.

19. A un trabajador se le promete una bonificación si puede aumentar su productividad por dos unidades al día todos los días durante un periodo de 30 días. Si en el día 0 produce 170 unidades, ¿cuántas unidades produce en 30 días para calificar para el bono?

20. Una corredora por objetivos mejora su tiempo en una carrera dada en 3 segundos por día. Si en el día 0 corre la carrera en 3 minutos, ¿qué tan rápido debe correr el día 14 para lograr el objetivo?

21. Supongamos que r es una constante fija y $a_0, a_1, a_2, \ldots$ es una sucesión que satisface la relación de recurrencia $a_k = ra_{k-1}$, para todo entero $k \geq 1$ y $a_0 = a$. Use inducción matemática para demostrar que $a_n = ar^n$, para todo entero $n \geq 0$.

22. Como se muestra en ejemplo 5.6.8, si un banco paga intereses a una tasa i compuesto m veces al año, entonces la cantidad de P_k al final de k periodos (donde un periodo $= (1/m)$-ésimo de un año) satisface la relación de recurrencia $P_k = [1 + (i/m)]\, P_{k-1}$ con condición inicial $P_0 =$ la cantidad inicial depositada. Determine una fórmula explícita para P_n.

23. Suponga que la población de un país aumenta a un ritmo constante de 3% por año. Si la población es de 50 millones en un momento dado, ¿cuál va a ser 25 años más tarde?

24. Una cadena de cartas funciona de la siguiente manera: Una persona envía una copia de la carta a cinco amigos, cada uno de los cuales envía una copia a cinco amigos, cada uno de los cuales envía una copia a cinco amigos y así sucesivamente. ¿Cuántas personas han recibido copias de la carta después de la vigésima repetición de este proceso, suponiendo que ninguna persona recibe más de una copia?

25. Un algoritmo dado de computadora ejecuta el doble de operaciones cuando corre una entrada de tamaño k así como cuando corre una entrada de tamaño $k - 1$ (donde k es un entero que es mayor que 1). Cuando el algoritmo se ejecuta con una entrada de tamaño 1, ejecuta siete operaciones. ¿Cuántas operaciones tiene que ejecutar cuando corre una entrada de tamaño 25?

26. Una persona que ahorra para su jubilación hace un depósito inicial de \$1 000 a una cuenta bancaria ganando intereses a una tasa de 3% anual compuesto mensualmente y cada mes deposita \$200 más a la cuenta.

a. Para cada entero no negativo n, sea A_n la cantidad en la cuenta al final de n meses. Determine una relación de recurrencia que relacione a A_k con A_{k-1}.

***H* b.** Utilice iteración para encontrar una fórmula explícita para A_n.

c. Utilice inducción matemática para demostrar lo correcto de la fórmula que haya obtenido en el inciso *b*).

d. ¿Cuánto habrá en la cuenta al finalizar 20 años? ¿Y al finalizar 40 años?

***H* e.** ¿En cuántos años habrá en la cuenta una cantidad de \$10 000?

27. Una persona pide prestado $3 000 en una tarjeta de crédito del banco con una tasa nominal de 18% al año, ¿Cuánto en realidad le cobran con una tasa de 1.5% al mes?

H **a.** ¿Cuál es la tasa de porcentaje anual (TPA) para la tarjeta? (Vea el ejemplo 5.6.8 para la definición de TPA.)

b. Suponga que la persona no hace ningún cargo adicional en la tarjeta y paga al banco $150 cada mes para pagar el préstamo. Sea B_n el saldo de la tarjeta después de n meses. Determine una fórmula explícita para B_n.

H **c.** ¿Cuánto tiempo necesitará para pagar la deuda?

d. ¿Cuál es la cantidad total de dinero que tendrá que pagar la persona por el préstamo?

En los ejercicios 28 al 42 utilice inducción matemática para demostrar la exactitud de la fórmula que obtuvo en el ejercicio de referencia.

28. Ejercicio 3	29. Ejercicio 4	30. Ejercicio 5
31. Ejercicio 6	32. Ejercicio 7	33. Ejercicio 8
34. Ejercicio 9	**H** 35. Ejercicio 10	36. Ejercicio 11
H **37.** Ejercicio 12	38. Ejercicio 13	39. Ejercicio 14
40. Ejercicio 15	41. Ejercicio 16	42. Ejercicio 17

En cada uno de los ejercicios 43 al 49 se define una sucesión de forma recursiva. *a*) Utilice iteración para inferir una fórmula explícita para la sucesión. *b*) Utilice inducción matemática fuerte para comprobar que la fórmula del inciso *a*) es correcta.

43. $a_k = \dfrac{a_{k-1}}{2a_{k-1} - 1}$, para todo entero $k \geq 1$
$a_0 = 2$

44. $b_k = \dfrac{2}{b_{k-1}}$, para todo entero $k \geq 2$
$b_1 = 1$

45. $v_k = v_{\lfloor (k)2 \rfloor} + v_{\lfloor (k+1))2 \rfloor} + 2$, para todo entero $k \geq 2$,
$v_1 = 1$.

H **46.** $s_k = 2s_{k-2}$, para todo entero $k \geq 2$,
$s_0 = 1, s_1 = 2$.

47. $t_k = k - t_{k-1}$, para todo entero $k \geq 1$,
$t_0 = 0$.

H **48.** $w_k = w_{k-2} + k$, para todo entero $k \geq 3$,
$w_1 = 1, w_2 = 2$.

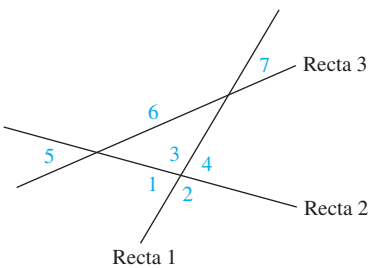
H **49.** $u_k = u_{k-2} \cdot u_{k-1}$, para todo entero $k \geq 2$,
$u_0 = u_1 = 2$.

En los ejercicios 50 y 51 determine si la sucesión que se define de forma recursiva satisface la fórmula explícita $a_n = (n - 1)^2$, para todo entero $n \geq 1$.

50. $a_k = 2a_{k-1} + k - 1$, para todo entero $k \geq 2$
$a_1 = 0$

51. $a_k = (a_{k-1} + 1)^2$, para todo entero $k \geq 2$
$a_1 = 0$

52. Una sola recta divide un plano en dos regiones. Dos rectas (cruzando) pueden dividir un plano en cuatro regiones, tres rectas pueden dividir en siete regiones (vea la figura). Sea P_n el número máximo de regiones en las que n rectas dividen un plano, donde n es un entero positivo.



a. Deduzca una relación de recurrencia de P_k en términos de P_{k-1}, para todo entero $k \geq 2$.

b. Utilice iteración de inferir una fórmula explícita para P_n.

53. Calcule $\begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}^n$ para valores pequeños de n (hasta unos 5 o 6).

Suponga fórmulas explícitas para las entradas en esta matriz y demuestre su suposición con inducción matemática.

54. En economía el comportamiento de una economía de un periodo a otro con frecuencia se modela por las relaciones de recurrencia. Sea Y_k el ingreso en el periodo k y C_k el consumo en el periodo k. En un modelo económico, los ingresos en un periodo se supone que es la suma del consumo en ese periodo más la inversión y el gasto público (que se supone que son constantes de un periodo a otro) y el consumo en cada periodo se supone que es una función lineal de los ingresos del periodo anterior. Es decir,

$Y_k = C_k + E$ donde E es la suma de la inversión más de los gastos del gobierno

$C_k = c + mY_{k-1}$ donde c y m son constantes.

Sustituyendo la segunda ecuación en la primera se obtiene $Y_k = E + c + mY_{k-1}$.

a. Use iteración en la relación de recurrencia anterior para obtener

$$Y_n = (E + c)\left(\frac{m^n - 1}{m - 1}\right) + m^n Y_0$$

para todo entero $n \geq 1$.

b. (Para los estudiantes que han estudiado cálculo) Demuestre que si $0 < m < 1$, entonces $\lim_{n \to \infty} Y_n = \dfrac{E + c}{1 - m}$.

Respuestas del autoexamen

1. condiciones iniciales; relación de recurrencia 2. paréntesis 3. $k \cdot a$ 4. a^k 5. $a_k = a_{k-1} + d$; $a_n = a_0 + dn$ 6. $a_k = ra_{k-1}$; $a_n = a_0 r^n$ 7. inducción matemática

5.8 Relaciones lineales de recurrencia de segundo orden con coeficientes constantes

Genio es 1% inspiración y 99% transpiración. —Thomas Alva Edison, 1932

En la sección 5.7 analizamos cómo encontrar fórmulas explícitas para las sucesiones recursivamente definidas mediante iteración. Esta es una técnica básica que no requiere ninguna herramienta especial más allá de la capacidad de discernir patrones. En muchos casos, sin embargo, un patrón no es fácilmente discernible y se deben utilizar otros métodos. Una variedad de técnicas disponibles para encontrar fórmulas explícitas para las clases especiales de las sucesiones recursivamente definidas. El método se explica en esta sección funciona para la sucesión de Fibonacci y otras sucesiones definidas de forma similar.

• Definición

Una **relación lineal de recurrencia homogénea de segundo orden con coeficientes constantes** es una relación de recurrencia de la forma

$$a_k = Aa_{k-1} + Ba_{k-2} \quad \text{para todo entero } k \geq \text{algún entero fijo,}$$

donde A y B son números reales fijos con $B \neq 0$.

"Segundo orden" se refiere al hecho de que la expresión para a_k contiene los dos términos anteriores a_{k-1} y a_{k-2}, "lineal" al hecho de que a_{k-1} y a_{k-2} aparecen en términos separados y a la primera potencia, "homogénea" al hecho de que el grado total de cada término es el mismo (por tanto no hay término constante) y "coeficientes constantes" al hecho de que A y B son números reales fijos que no dependen de k.

Ejemplo 5.8.1 Relaciones lineales homogéneas de recurrencia de segundo orden con coeficientes constantes

Indique si cada una de las siguientes expresiones es una relación lineal homogénea de recurrencia de segundo orden con coeficientes constantes:

a. $a_k = 3a_{k-1} + 2a_{k-2}$

b. $b_k = b_{k-1} + b_{k-2} + b_{k-3}$

c. $c_k = \frac{1}{2}c_{k-1} - \frac{3}{7}c_{k-2}$

d. $d_k = d_{k-1}^2 + d_{k-1} \cdot d_{k-2}$

e. $e_k = 2e_{k-2}$

f. $f_k = 2f_{k-1} + 1$

g. $g_k = g_{k-1} + g_{k-2}$

h. $h_k = (-1)h_{k-1} + (k-1)h_{k-2}$

Solución

a. Sí; $A = 3$ y $B = 2$

b. No; no de segundo orden

c. Sí; $A = \frac{1}{2}$ y $B = -\frac{3}{7}$

d. No; no lineal

e. Sí; $A = 0$ y $B = 2$

f. No; no es homogénea

g. Sí; $A = 1$ y $B = 1$

h. No; coeficientes no constantes ■

El caso de raíces distintas

Considere una relación de recurrencia lineal homogénea de segundo orden con coeficientes constantes:

$$a_k = Aa_{k-1} + Ba_{k-2} \quad \text{para todo entero } k \geq 2, \tag{5.8.1}$$

donde A y B son números reales fijos. La relación (5.8.1) se cumple cuando todos los $a_i = 0$, pero también tiene soluciones distintas de cero. *Suponga* que para algún número t con $t \neq 0$, la sucesión

$$1, t, t^2, t^3, \ldots, t^n, \ldots$$

satisface la relación (5.8.1). Esto significa que cada término de la sucesión es igual a A veces el término anterior más B veces el término anterior. Así que para todo entero $k \geq 2$,

$$t^k = At^{k-1} + Bt^{k-2}.$$

En particular, cuando $k = 2$, la ecuación se convierte en

$$t^2 = At + B$$

o, equivalentemente,

$$t^2 - At - B = 0. \tag{5.8.2}$$

Esta es una ecuación de segundo grado y los valores de t que hacen que sea verdad se pueden encontrar ya sea factorizando o utilizando la fórmula cuadrática.

Ahora trabaje hacia atrás. *Suponga* que t es un número que satisfaga la ecuación (5.8.2). ¿La sucesión $1, t, t^2, t^3, \ldots, t^n, \ldots$, satisfacen la relación (5.8.1)? Para responder a esta pregunta, multiplique la ecuación (5.8.2) por t^{k-2} para obtener

$$t^{k-2} \cdot t^2 - t^{k-2} \cdot At - t^{k-2} \cdot B = 0.$$

Esto es equivalente a

$$t^k - At^{k-1} - Bt^{k-2} = 0$$

o

$$t^k = At^{k-1} + Bt^{k-2}.$$

Por tanto la respuesta es sí: $1, t, t^2, t^3, \ldots, t^n, \ldots$ satisface la relación (5.8.1)

Este análisis demuestra el siguiente lema.

Lema 5.8.1

Sean A y B números reales. Una relación de recurrencia de la forma

$$a_k = Aa_{k-1} + Ba_{k-2} \quad \text{para todo entero } k \geq 2 \tag{5.8.1}$$

se satisface con la sucesión

$$1, t, t^2, t^3, \ldots, t^n, \ldots,$$

donde t es un número real distinto de cero, si y sólo si, t satisface la ecuación

$$t^2 - At - B = 0 \tag{5.8.2}$$

La ecuación (5.8.2) se llama la *ecuación característica* de la relación de recurrencia.

• Definición

Dada una relación de recurrencia lineal homogénea de segundo orden con coeficientes constantes:

$$a_k = Aa_{k-1} + Ba_{k-2} \quad \text{para todo entero } k \geq 2 \tag{5.8.1}$$

la **ecuación característica de la relación** es

$$t^2 - At - B = 0 \tag{5.8.2}$$

Ejemplo 5.8.2 Uso de la ecuación característica para encontrar soluciones a una relación de recurrencia

Considere la relación de recurrencia que especifica que el k-ésimo término de una sucesión es igual a la suma de los $(k - 1)$-ésimo término más dos veces el $(k - 2)$-ésimo término. Es decir,

$$a_k = Aa_{k-1} + 2a_{k-2} \quad \text{para todo entero } k \geq 2. \tag{5.8.3}$$

Determine todas las sucesiones que satisfacen la relación (5.8.3) y tienen la forma

$$1, t, t^2, t^3, \ldots, t^n, \ldots$$

donde t es distinto de cero.

Solución Por el lema 5.8.1, la relación (5.8.3) se satisface con una sucesión $1, t, t^2, t^3, \ldots, t^n, \ldots$ si y sólo si, t satisface la ecuación característica

$$t^2 - t - 2 = 0.$$

Ya que

$$t^2 - t - 2 = (t - 2)(t + 1),$$

los únicos valores posibles de t son 2 y -1. De lo que se deduce que las sucesiones

$$1, 2, 2^2, 2^3, \ldots, 2^n, \ldots \quad \text{y} \quad 1, -1, (-1)^2, (-1)^3, \ldots, (-1)^n, \ldots$$

son ambas soluciones para la relación (5.8.3) y no hay otras soluciones de esta forma. Observe que estas sucesiones se pueden escribir más simplemente como

$$1, 2, 2^2, 2^3, \ldots, 2^n, \ldots \quad \text{y} \quad 1, -1, 1, -1, \ldots, (-1)^n, \ldots.$$ ■

El ejemplo anterior muestra cómo encontrar dos sucesiones distintas que satisfacen una relación de recurrencia de segundo orden lineal homogénea con coeficientes constantes dada. Resulta que cualquier combinación lineal de dichas sucesiones produce otra sucesión que también satisface la relación.

Lema 5.8.2

Si $r_0, r_1, r_2, \ldots$ y $s_0, s_1, s_2, \ldots$ son sucesiones que satisfacen la misma relación de recurrencia de segundo orden lineal homogénea con coeficientes constantes y si C y D son *cualesquiera* números, entonces la sucesión $a_0, a_1, a_2, \ldots$ definida por la fórmula

$$a_n = Cr_n + Ds_n \quad \text{para todo entero } n \geq 0$$

también satisface la misma relación de recurrencia.

continúa en la página 320

Demostración: Supongamos que $r_0, r_1, r_2, \ldots$ y $s_0, s_1, s_2, \ldots$ son sucesiones que cumplen la misma relación de recurrencia lineal homogénea de segundo orden con coeficientes constantes. En otras palabras, supongamos que para algunos números reales A y B,

$$r_k = Ar_{k-1} + Br_{k-2} \quad \text{y} \quad s_k = As_{k-1} + Bs_{k-2} \tag{5.8.4}$$

para todo entero $k \geq 2$. Supongamos también que C y D son números. Sea $a_0, a_1, a_2, \ldots$ la sucesión definida por

$$a_n = Cr_n + Ds_n \quad \text{para todo entero } n \geq 0 \tag{5.8.5}$$

[Debemos demostrar que $a_0, a_1, a_2, \ldots$ satisface la misma relación de recurrencia que $r_0, r_1, r_2, \ldots$ y $s_0, s_1, s_2, \ldots$ Es decir, debemos demostrar que $a_k = Aa_{k-1} + Ba_{k-2}$, para todos los enteros] $k \geq 2$.
Para todo entero $k \geq 2$,

$$\begin{aligned} Aa_{k-1} + Ba_{k-2} &= A(Cr_{k-1} + Ds_{k-1}) + B(Cr_{k-2} + Ds_{k-2}) && \text{sustituyendo (5.8.5)} \\ &= C(Ar_{k-1} + Br_{k-2}) + D(As_{k-1} + Bs_{k-2}) && \text{por álgebra básica} \\ &= Cr_k + Ds_k && \text{sustituyendo (5.8.4)} \\ &= a_k && \text{sustituyendo (5.8.5)} \end{aligned}$$

Por tanto $a_0, a_1, a_2, \ldots$ satisface la misma relación de recurrencia que $r_0, r_1, r_2, \ldots$ y $s_0, s_1, s_2, \ldots$ *[como se quería demostrar]*.

Dada una relación de recurrencia lineal homogénea de segundo orden con coeficientes constantes, si la ecuación característica tiene dos raíces distintas, entonces se pueden utilizar en conjunto los lemas 5.8.1 y 5.8.2 para encontrar una sucesión en particular que satisfaga tanto la relación de recurrencia como a las dos condiciones iniciales dadas.

Ejemplo 5.8.3 Determine la combinación lineal que satisface las condiciones iniciales

Encuentre una sucesión que satisfaga la relación de recurrencia del ejemplo 5.8.2,

$$a_k = a_{k-1} + 2a_{k-2} \quad \text{para todo entero } k \geq 2, \tag{5.8.3}$$

y que también satisface las condiciones iniciales

$$a_0 = 1 \quad \text{y} \quad a_1 = 8.$$

Solución En el ejemplo 5.8.2, ambas sucesiones

$$1, 2, 2^2, 2^3, \ldots, 2^n, \ldots \quad \text{y} \quad 1, -1, 1, -1, \ldots, (-1)^n, \ldots$$

satisfacen la relación (5.8.3) (aunque no cumplan las condiciones iniciales). Por el lema 5.8.2, por tanto, cualquier sucesión $a_0, a_1, a_2, \ldots$ que satisface una fórmula explícita de la forma

$$a_n = C \cdot 2^n + D(-1)^n \tag{5.8.6}$$

donde C y D son números, también satisface la relación (5.8.3). Puede encontrar C y D para que $a_0, a_1, a_2, \ldots$ satisfaga las condiciones iniciales dadas sustituyendo $n = 0$ y $n = 1$ en la ecuación (5.8.6) y despejando C y D:

$$\begin{aligned} a_0 &= 1 = C \cdot 2^0 + D(-1)^0, \\ a_1 &= 8 = C \cdot 2^1 + D(-1)^1. \end{aligned}$$

Cuando se simplifica, se obtiene el sistema

$$1 = C + D$$
$$8 = 2C - D,$$

que puede resolverse de varias maneras. Por ejemplo, si agrega las dos ecuaciones, se obtiene

$$9 = 3C,$$

y así

$$C = 3.$$

Entonces, sustituyendo en $1 = C + D$, se obtiene

$$D = -2.$$

De lo que se deduce que la sucesión $a_0, a_1, a_2, \ldots$ dada por

$$a_n = 3 \cdot 2^n + (-2)(-1)^n = 3 \cdot 2^n - 2(-1)^n,$$

para enteros $n \geq 0$, satisface tanto la relación de recurrencia como las condiciones iniciales dadas. ■

Las técnicas de los ejemplos 5.8.2 y 5.8.3 se pueden usar para encontrar una fórmula explícita para cualquier sucesión que satisface una relación de recurrencia lineal homogénea de segundo orden con coeficientes constantes para la que la ecuación característica tiene raíces distintas, siempre que se conozcan los dos primeros términos de la sucesión. Esto se precisa en el siguiente teorema.

Teorema 5.8.3 Teorema de raíces diferentes

Supongamos que una sucesión de $a_0, a_1, a_2, \ldots$ satisface una relación de recurrencia

$$a_k = Aa_{k-1} + Ba_{k-2} \tag{5.8.1}$$

para algunos números reales A y B con $B \neq 0$ y todos los enteros $k \geq 2$. Si la ecuación característica

$$t^2 - At - B = 0 \tag{5.8.2}$$

tiene dos raíces distintas r y s, entonces, $a_0, a_1, a_2, \ldots$ está dada por la fórmula explícita

$$a_n = Cr^n + Ds^n$$

donde C y D son los números cuyos valores se determinan por los valores de a_0 y a_1.

Nota: Decir "C y D se determinan por los valores de a_0 y a_1" significa que C y D son soluciones del sistema de ecuaciones simultáneas

$$a_0 = Cr^0 + Ds^0 \quad \text{y} \quad a_1 = Cr^1 + Ds^1,$$

o, equivalentemente,

$$a_0 = C + D \quad \text{y} \quad a_1 = Cr + Ds.$$

En el ejercicio 19 de fin de esta sección se le pide que demuestre que este sistema siempre tiene una solución cuando $r \neq s$.

Demostración: Supongamos que para algunos números reales A y B, una sucesión $a_0, a_1, a_2, \ldots$ satisface la relación de recurrencia $a_k = Aa_{k-1} + Ba_{k-2}$, para todos los enteros $k \geq 2$ y supongamos que la ecuación característica $t^2 - At - B = 0$ tiene dos raíces distintas r y s. Vamos a demostrar que

$$\text{para todo entero } n \geq 0, \quad a_n = Cr^n + Ds^n,$$

donde C y D son números tales que

$$a_0 = Cr^0 + Ds^0 \quad \text{y} \quad a_1 = Cr^1 + Ds^1.$$

Sea $P(n)$ la ecuación

$$a_n = Cr^n + Ds^n. \qquad \leftarrow P(n)$$

Usamos el método de inducción matemática fuerte para demostrar que $P(n)$ es verdadera para todo entero $n \geq 0$. En el paso básico, hemos demostrado que $P(0)$ y $P(1)$ son verdaderas. Hacemos esto porque en el paso inductivo necesitamos la ecuación para mantener $n = 0$ y $n = 1$ para demostrar que vale para $n = 2$.

Demostración de que P(0) y P(1) son verdaderas: La veracidad de $P(0)$ y $P(1)$ es automática ya que C y D son exactamente los números que hacen verdaderas a las siguientes ecuaciones:

$$a_0 = Cr^0 + Ds^0 \quad \text{y} \quad a_1 = Cr^1 + Ds^1.$$

Demostración de que para todo entero k ≥ 1, si P(i) es verdadera para todo entero i entre 0 y k, entonces P(k + 1) también es verdadera: Supongamos que $k \geq 1$ y para todos los enteros i de 0 a k,

$$a_i = Cr^i + Ds^i. \qquad \text{hipótesis inductiva}$$

Debemos demostrar que

$$a_{k+1} = Cr^{k+1} + Ds^{k+1}. \qquad \leftarrow P(k+1)$$

Ahora por la hipótesis inductiva,

$$a_k = Cr^k + Ds^k \quad \text{y} \quad a_{k-1} = Cr^{k-1} + Ds^{k-1},$$

así

$$\begin{aligned}
a_{k+1} &= Aa_k + Ba_{k-1} && \text{por definición } a_0, a_1, a_2, \ldots \\
&= A(Cr^k + Ds^k) + B(Cr^{k-1} + Ds^{k-1}) && \text{por hipótesis inductiva} \\
&= C(Ar^k + Br^{k-1}) + D(As^k + Bs^{k-1}) && \text{combinando términos semejantes} \\
&= Cr^{k+1} + Ds^{k+1} && \text{por el lema 5.8.1.}
\end{aligned}$$

Esto es lo que se quería demostrar.

[La razón de que la última igualdad se deduzca del lema 5.8.1 es que r y s satisfacen la ecuación característica (5.8.2), las sucesiones, $r^0, r^1, r^2, \ldots$ y $s^0, s^1, s^2, \ldots$ satisfacen la relación de recurrencia (5.8.1).]

Observación La t del lema 5.8.1 y C y D en el lema 5.8.2 y en el teorema 5.8.3 se refieren a ellos simplemente como números. Esto es para permitir la posibilidad de complejos, así como de valores de números reales. Si las dos raíces de la ecuación característica de la relación de recurrencia son números reales, entonces, C y D serán reales. Pero si las raíces son números complejos no reales, entonces, C y D serán números complejos no reales.

El ejemplo siguiente muestra cómo utilizar el teorema raíces distintas para encontrar una fórmula explícita para la sucesión de Fibonacci.

Ejemplo 5.8.4 Una fórmula para la sucesión de Fibonacci

La sucesión de Fibonacci, $F_0, F_1, F_2, \ldots$, satisface la relación de recurrencia

$$F_k = F_{k-1} + F_{k-2} \quad \text{para todo } k \geq 2$$

con condiciones iniciales

$$F_0 = F_1 = 1.$$

Encuentre una fórmula explícita para esta sucesión.

Solución La sucesión de Fibonacci satisface parte de la hipótesis del teorema de raíces distintas ya que la relación de Fibonacci es una relación de recurrencia de segundo orden lineal homogénea con coeficientes constantes ($A = 1$ y $B = 1$). ¿La segunda parte de la hipótesis también se satisface? ¿La ecuación característica

$$t^2 - t - 1 = 0$$

tiene raíces distintas? Usando la fórmula cuadrática, las raíces son

$$t = \frac{1 \pm \sqrt{1 - 4(-1)}}{2} = \begin{cases} \dfrac{1+\sqrt{5}}{2} \\ \dfrac{1-\sqrt{5}}{2} \end{cases}$$

y así que la respuesta es sí. De lo que se deduce del teorema de raíces distintas que la sucesión de Fibonacci está dada por la fórmula explícita

$$F_n = C\left(\frac{1+\sqrt{5}}{2}\right)^n + D\left(\frac{1-\sqrt{5}}{2}\right)^n \quad \text{para todo entero } n \geq 0, \qquad 5.8.7$$

donde C y D son los números cuyos valores se determinan por el hecho de que $F_0 = F_1 = 1$. Para encontrar C y D, se escribe

$$F_0 = 1 = C\left(\frac{1+\sqrt{5}}{2}\right)^0 + D\left(\frac{1-\sqrt{5}}{2}\right)^0 = C \cdot 1 + D \cdot 1 = C + D$$

y

$$\begin{aligned} F_1 = 1 &= C\left(\frac{1+\sqrt{5}}{2}\right)^1 + D\left(\frac{1-\sqrt{5}}{2}\right)^1 \\ &= C\left(\frac{1+\sqrt{5}}{2}\right) + D\left(\frac{1-\sqrt{5}}{2}\right) \end{aligned}$$

Así, el problema es encontrar a los números C y D tales que

$$C + D = 1$$

y

$$C\left(\frac{1+\sqrt{5}}{2}\right) + D\left(\frac{1-\sqrt{5}}{2}\right) = 1.$$

Esto puede parecer complicado, pero de hecho es sólo un sistema de dos ecuaciones con dos incógnitas. En el ejercicio 7 al final de esta sección, se le pide demostrar que

$$C = \frac{1+\sqrt{5}}{2\sqrt{5}} \quad \text{y} \quad D = \frac{-(1-\sqrt{5})}{2\sqrt{5}}.$$

Sustituyendo estos valores para C y D en la fórmula (5.8.7) se obtiene

$$F_n = \left(\frac{1+\sqrt{5}}{2\sqrt{5}}\right)\left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{-(1-\sqrt{5})}{2\sqrt{5}}\right)\left(\frac{1-\sqrt{5}}{2}\right)^n,$$

Nota Los números $(1+\sqrt{5})/2$ y $(1-\sqrt{5})/2$ están relacionadas con la razón dorada de los matemáticos griegos. Vea el ejercicio 24 de fin de esta sección.

o, simplificando,

$$F_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^{n+1} - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^{n+1} \qquad 5.8.8$$

para todo entero $n \geq 0$. Sorprendentemente, a pesar de que la fórmula para F_n implica a $\sqrt{5}$, todos los valores de la sucesión de Fibonacci son enteros. ■

El caso de una sola raíz

Considere de nuevo la relación de recurrencia

$$a_k = Aa_{k-1} + Ba_{k-2} \quad \text{para todo entero } k \geq 2, \qquad 5.8.1$$

donde A y B son números reales, pero ahora suponga que la ecuación característica

$$t^2 - At - B = 0 \qquad 5.8.2$$

tiene una sola raíz real r. Por el lema 5.8.1, una sucesión que satisface la relación de recurrencia es

$$1, r, r^2, 3r^3, \ldots, r^n, \ldots$$

Pero otra sucesión que también satisface la relación es

$$0, r, 2r^2, 3r^3, \ldots, nr^n, \ldots$$

Para ver por qué esto es así, observe que dado que r es la raíz única de $t^2 - At - B = 0$, el lado izquierdo de la ecuación se puede factorizar como $(t-r)^2$ y así

$$t^2 - At - B = (t-r)^2 = t^2 = t^2 - 2rt + r^2. \qquad 5.8.9$$

Igualando los coeficientes de la ecuación (5.8.9) se obtiene

$$A = 2r \quad \text{y} \quad B = -r^2. \qquad 5.8.10$$

Sea $s_0, s_1, s_2, \ldots$, la sucesión definida por la fórmula

$$S_n = nr^n \quad \text{para todo entero } n \geq 0.$$

Entonces,

$$\begin{aligned}
As_{k-1} + Bs_{k-2} &= A(k-1)r^{k-1} + B(k-2)r^{k-2} && \text{por definición} \\
&= 2r(k-1)r^{k-1} - r^2(k-2)r^{k-2} && \text{sustituyendo de 5.8.10} \\
&= 2(k-1)r^k - (k-2)r^k \\
&= (2k-2-k+2)r^k \\
&= kr^k && \text{por álgebra básica} \\
&= s_k && \text{por definición.}
\end{aligned}$$

Así $s_0, s_1, s_2, \ldots$ satisface la relación de recurrencia. Este argumento demuestra el siguiente lema.

Lema 5.8.4

Sean A y B son números reales y suponga que la ecuación característica

$$t^2 - At - B = 0$$

tiene una sola raíz r. Entonces ambas sucesiones $1, r^1, r^2, r^3, \ldots, r^n, \ldots$ y $0, r, 2r^2, 3r^3, \ldots, nr^n, \ldots$ satisfacen la relación de recurrencia

$$a_k = Aa_{k-1} + Ba_{k-2}$$

para todo entero $k \geq 2$.

Los lemas 5.8.2 y 5.8.4 se puede utilizar para establecer el *teorema de una sola raíz*, que dice cómo encontrar una fórmula explícita para cualquier sucesión definida recursivamente que satisface una relación de recurrencia de segundo orden lineal homogénea con coeficientes constantes para que la ecuación característica tenga una sola raíz. En conjunto, los teoremas de una sola raíz y de raíces distintas cubren todas las relaciones de recurrencia de segundo orden lineales homogéneas con coeficientes constantes. La demostración del teorema de una sola raíz es muy similar a la del teorema de raíces distintas y se deja como ejercicio.

Teorema 5.8.5 Teorema de una sola raíz

Supongamos que una sucesión $a_0, a_1, a_2, \ldots$, satisface una relación de recurrencia

$$a_k = Aa_{k-1} + Ba_{k-2}$$

para algunos números reales A y B con $B \neq 0$ y para todos los enteros $k \geq 2$. Si la ecuación característica $t^2 - At - B = 0$ tiene una raíz única (real) r, entonces, $a_0, a_1, a_2, \ldots$ está dada por la fórmula explícita

$$a_n = Cr^n + Dnr^n,$$

donde C y D son los números reales cuyos valores se determinan por los valores de a_0 y de cualquier otro valor conocido de la sucesión.

Ejemplo 5.8.5 Caso de una sola raíz

Supongamos que una sucesión $b_0, b_1, b_2, \ldots$, satisface la relación de recurrencia

$$b_k = 4b_{k-1} - 4b_{k-2} \quad \text{para todo entero } k \geq 2, \tag{5.8.11}$$

con condiciones iniciales

$$b_0 = 1 \quad \text{y} \quad b_1 = 3.$$

Determine una fórmula explícita para $b_0, b_1, b_2, \ldots$.

Solución Esta sucesión satisface una parte de la hipótesis del teorema de una sola raíz ya que satisface una relación de recurrencia de segundo orden lineal homogénea con coeficientes constantes ($A = 4$ y $B = -4$). La condición de una única raíz también se cumple ya que la ecuación característica

$$t^2 - 4t + 4 = 0$$

tiene la única raíz $r = 2$ [*ya que* $t^2 - 4t + 4 = (t - 2)^2$].

Lo que se deduce del teorema de una sola raíz que $b_0, b_1, b_2, \ldots$, está dado por la fórmula explícita

$$b_n = C \cdot 2^n + Dn2^n \quad \text{para todo entero } n \geq 0, \tag{5.8.12}$$

donde C y D son números reales cuyos valores se determinan por el hecho de que $b_0 = 1$ y $b_1 = 3$. Para encontrar C y D, se escribe

$$b_0 = 1 = C \cdot 2^0 + D \cdot 0 \cdot 2^0 = C$$

y

$$b_1 = 3 = C \cdot 2^1 + D \cdot 1 \cdot 2^1 = 2C + 2D.$$

Por tanto el problema es encontrar los números C y D tales que

$$C = 1$$

y

$$2C + 2D = 3.$$

Sustituyendo $C = 1$ en la segunda ecuación se obtiene

$$2 + 2D = 3,$$

y así

$$D = \frac{1}{2}.$$

Ahora sustituyendo $C = 1$ y $D = \frac{1}{2}$ en la fórmula (5.8.12) se concluye que

$$b_n = 2^n + \frac{1}{2}n2^n = 2^n\left(1 + \frac{n}{2}\right) \quad \text{para todo entero } n \geq 0. \qquad \blacksquare$$

Autoexamen

1. Una relación de recurrencia de segundo orden lineal homogénea con coeficientes constantes es una relación de recurrencia de la forma _____ para todo entero $k \geq$ _____, donde _____.
2. Dada una relación de recurrencia de la forma $a_k = Aa_{k-1} + Ba_{k-2}$ para todo entero $k \geq 2$, la ecuación característica de la relación es _____.
3. Si una sucesión $a_1, a_2, a_3, \ldots$, se define con una relación de recurrencia de segundo orden lineal homogénea con coeficientes constantes y la ecuación característica para la relación tiene dos raíces distintas r y s (que pueden ser números complejos), entonces la sucesión está dada por una fórmula explícita de la forma _____.
4. Si una sucesión $a_1, a_2, a_3, \ldots$ se define con una relación de recurrencia lineal de segundo orden homogénea con coeficientes constantes y la ecuación característica de la relación sólo tiene una sola raíz r, entonces la sucesión está dada por una fórmula explícita de la forma _____.

Conjunto de ejercicios 5.8

1. ¿Cuáles de las siguientes expresiones son relaciones de recurrencia de segundo orden lineales homogéneas con coeficientes constantes?
   a. $a_k = 2a_{k-1} - 5a_{k-2}$ b. $b_k = kb_{k-1} + b_{k-2}$
   c. $c_k = 3c_{k-1} \cdot c_{k-2}^2$ d. $d_k = 3d_{k-1} + d_{k-2}$
   e. $r_k = r_{k-1} - r_{k-2} - 2$ f. $s_k = 10s_{k-2}$
2. ¿Cuáles de las siguientes expresiones son relaciones de recurrencia de segundo orden lineales homogéneas con coeficientes constantes?
   a. $a_k = (k-1)a_{k-1} + 2ka_{k-2}$
   b. $b_k = -b_{k-1} + 7b_{k-2}$
   c. $c_k = 3c_{k-1} + 1$
   d. $d_k = 3d_{k-1}^2 + d_{k-2}$
   e. $r_k = r_{k-1} - 6r_{k-3}$
   f. $s_k = s_{k-1} + 10s_{k-2}$
3. Sea $a_0, a_1, a_2, \ldots$, la sucesión definida por la fórmula explícita

   $$a_n = C \cdot 2^n + D \quad \text{para todo entero } n \geq 0,$$

   donde C y D son números reales.
   a. Encuentre C y D para que $a_0 = 1$ y $a_1 = 3$. ¿A qué es igual a_2 en este caso?
   b. Encuentre C y D para que $a_0 = 0$ y $a_1 = 2$. ¿A qué es igual a_2 en este caso?

4. Sea $b_0, b_1, b_2, \ldots$, la sucesión definida por la fórmula explícita

$$b_n = C \cdot 3^n + D(-2)^n \quad \text{para todo entero } n \geq 0,$$

donde C y D son números reales.
   a. Encuentre C y D tal que $b_0 = 0$ y $b_1 = 5$. ¿A qué es igual b_2 en este caso?
   b. Encuentre C y D tal que $b_0 = 3$ y $b_1 = 4$. ¿A qué es igual b_2 en este caso?

5. Sea $a_0, a_1, a_2, \ldots$, la sucesión definida por la fórmula explícita

$$a_n = C \cdot 2^n + D \quad \text{para todo entero } n \geq 0,$$

donde C y D son números reales. Demuestre que para cualquier elección de C y D,

$$a_k = 3a_{k-1} - 2a_{k-2} \quad \text{para todo entero } k \geq 2.$$

6. Sea $b_0, b_1, b_2, \ldots$, la sucesión definida por la fórmula explícita

$$b_n = C \cdot 3^n + D(-2)^n \quad \text{para todo entero } n \geq 0,$$

donde C y D son números reales. Demuestre que para cualquier elección de C y D,

$$b_k = b_{k-1} + 6b_{k-2} \quad \text{para todo entero } k \geq 2.$$

7. Resuelva el sistema de ecuaciones del ejemplo 5.8.4 para obtener

$$C = \frac{1+\sqrt{5}}{2\sqrt{5}} \quad \text{y} \quad D = \frac{-(1-\sqrt{5})}{2\sqrt{5}}.$$

En cada uno de los ejercicios 8 al 10: *a*) suponga una sucesión de la forma $1.t.t^2.t^3 \ldots t^n \ldots$ donde $t \neq 0$, satisface la relación de recurrencia dada (pero no necesariamente las condiciones iniciales) y encuentre todos los valores posibles de t: *b*) suponga una sucesión que satisface las condiciones iniciales dadas, así como la relación de recurrencia y encuentre una fórmula explícita para la sucesión.

8. $a_k = 2a_{k-1} + 3a_{k-2}$, para todo entero $k \geq 2$
$a_0 = 1, a_1 = 2$

9. $b_k = 7b_{k-1} - 10b_{k-2}$, para todo entero $k \geq 2$
$b_0 = 2, b_1 = 2$

10. $c_k = c_{k-1} + 6c_{k-2}$, para todo entero $k \geq 2$
$c_0 = 0, c_1 = 3$

En cada uno de los ejercicios 11 al 16 suponga una sucesión que satisfaga la relación de recurrencia dada y las condiciones iniciales. Encuentre una fórmula explícita para la sucesión.

11. $d_k = 4d_{k-2}$, para todo entero $k \geq 2$
$d_0 = 1,\ d_1 = -1$

12. $e_k = 9e_{k-2}$, para todo entero $k \geq 2$
$e_0 = 0,\ e_1 = 2$

13. $r_k = 2r_{k-1} - r_{k-2}$, para todo entero $k \geq 2$
$r_0 = 1,\ r_1 = 4$

14. $s_k = -4s_{k-1} - 4s_{k-2}$, para todo entero $k \geq 2$
$s_0 = 0,\ s_1 = -1$

15. $t_k = 6t_{k-1} - 9t_{k-2}$, para todo entero $k \geq 2$
$t_0 = 1,\ t_1 = 3$

***H* 16.** $s_k = 2s_{k-1} + 2s_{k-2}$, para todo entero $k \geq 2$
$s_0 = 1,\ s_1 = 3$

17. Encuentre una fórmula explícita para la sucesión del ejercicio 39 en la sección 5.6

18. Supongamos que las dos sucesiones $s_0, s_1, s_2, \ldots$ y $t_0, t_1, t_2, \ldots$ satisfacen la misma relación de recurrencia de segundo orden lineal homogénea con coeficientes constantes:

$$s_k = 5s_{k-1} - 4s_{k-2} \quad \text{para todo entero } k \geq 2,$$
$$t_k = 5t_{k-1} - 4t_{k-2} \quad \text{para todo entero } k \geq 2.$$

Demuestre que la sucesión de $2s_0 + 3t_0, 2s_1 + 3t_1, 2s_2 + 3t_2, \ldots$ también cumple la misma relación. En otras palabras, demuestre que

$$2s_k + 3t_k = 5(2s_{k-1} + 3t_{k-1}) - 4(2s_{k-2} + 3t_{k-2})$$

para todo entero $k \geq 2$. *No* use el lema 5.8.2.

19. Demuestre que si r, s, a_0 y a_1 son números con $r \neq s$, entonces existen números únicos C y D, tales que

$$C + D = a_0$$
$$Cr + Ds = a_1.$$

20. Demuestre que si r es un número real distinto de cero, k y m son números enteros distintos y a_k y a_m son números reales, entonces existen los números únicos reales C y D, tales que

$$Cr^k + kDr^k = a_k$$
$$Cr^m + lDr^m = a_m.$$

***H* 21.** Demuestre el teorema 5.8.5 para el caso en el que los valores de C y D se determinan por a_0 y a_1.

Los ejercicios 22 y 23 están destinados a estudiantes que están familiarizados con los números complejos.

22. Encuentre una fórmula explícita para una sucesión $a_0, a_1, a_2, \ldots$ que satisface

$$a_k = 2a_{k-1} - 2a_{k-2} \quad \text{para todo entero } k \geq 2$$

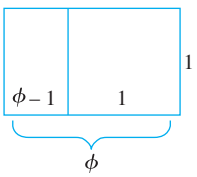
con condiciones iniciales $a_0 = 1$ y $a_1 = 2$.

23. Encuentre una fórmula explícita para una sucesión $b_0, b_1, b_2, \ldots$ que satisface

$$b_k = 2b_{k-1} - 5b_{k-2} \quad \text{para todo entero } k \geq 2$$

con condiciones iniciales $b_0 = 1$ y $b_1 = 1$.

24. Los números $\frac{1+\sqrt{5}}{2}$ y $\frac{1-\sqrt{5}}{2}$ que se presentan en la fórmula explícita para la sucesión de Fibonacci están relacionados con una cantidad llamada la *razón dorada* en las matemáticas griegas. Considere un rectángulo de longitud ϕ unidades y altura de 1, donde $\phi > 1$.



Divida al rectángulo en un rectángulo y un cuadrado como se muestra en el diagrama anterior. El cuadrado es de 1 unidad por cada lado y el rectángulo tiene lados de longitud 1 y $\phi - 1$. Los griegos antiguos consideraban que el rectángulo exterior tenia proporciones perfectas (digamos que las longitudes de sus lados se encontraban en una razón dorada entre sí) si el cociente de la longitud entre el ancho del rectángulo exterior era igual al cociente de la longitud entre el ancho del rectángulo interior. Es decir,

$$\frac{\phi}{1} = \frac{1}{\phi - 1}.$$

a. Demuestre que ϕ satisface la siguiente ecuación cuadrática: $t^2 - t - 1 = 0$.
b. Encuentre las dos soluciones de $t^2 - t - 1 = 0$ y llámelas ϕ_1 y ϕ_2.
c. Exprese la fórmula explícita para la sucesión de Fibonacci, en términos de ϕ_1 y ϕ_2.

Respuestas del autoexamen

1. $a_k = Aa_{k-1} + Ba_{k-2}$; 2; A y B son números reales fijos con $B \neq 0$ 2. $t^2 - At - B = 0$ 3. $a_n = Cr^n + Ds^n$, donde C y D son números reales o complejos 4. $a_n = Cr^n + Dnr^n$, donde C y D son números reales

5.9 Definiciones generales recursivas e inducción estructural

GENIO: ¡Oh!, no conoce los acrónimos recursivos? Pensé que todos sabían acerca de ellos. Verá, "DIOS" significa "DIOS sobre Djinn", que se puede ampliar como "DIOS sobre Djinn, sobre Djinn" y que puede, a su vez, ampliarse como "DIOS sobre Djinn, sobre Djinn, sobre Djinn" —que puede, a su vez, ampliarse aún más... . Usted puede ir tan lejos como quiera.
AQUILES: ¡Pero nunca terminará!
GENIO: Por supuesto que no. Nunca se puede ampliar totalmente a DIOS.
—Douglas Hofstadter, Gödel, Escher, Bach, 1979

Las sucesiones de números no son los únicos objetos que se pueden definir de forma recursiva. En esta sección se analizan las definiciones recursivas para los conjuntos y funciones. Se introduce también la *inducción estructural*, que es una versión de la inducción matemática que se utiliza para probar las propiedades de los conjuntos definidos recursivamente.

Conjuntos definidos recursivamente

Para definir un conjunto de objetos de forma recursiva, se identifica un número de objetos básicos que forman parte del conjunto y se dan las reglas que muestran cómo construir nuevos elementos a partir de los viejos. Más formalmente, una definición recursiva de un conjunto consiste de los siguientes tres componentes:

I. BASE: Un enunciado de que ciertos objetos pertenecen al conjunto.

II. RECURSIÓN: Un conjunto de reglas que indican cómo formar nuevos conjuntos de objetos de un conjunto a partir de los que ya se sabe que están en el conjunto.

III. RESTRICCIÓN: Un enunciado de que no haya objetos que pertenezcan al conjunto distintas de los que provienen de I y II.

Ejemplo 5.9.1 Definición recursiva de expresiones booleanas

Nota Un ejemplo de expresión "legal" es $p \wedge (q \vee \sim r)$ y un ejemplo de una "ilegal" es $\wedge \sim pqr \vee$.

El conjunto de expresiones booleanas se introdujo en la sección 2.4 como expresiones "legales", que incluyen las letras del alfabeto, tales como p, q y r y los símbolos $\wedge$, $\vee$ y $\sim$. Para precisar qué expresiones son legales, el conjunto de expresiones booleanas en general se define más de un alfabeto de forma recursiva.

I. BASE: Cada símbolo del alfabeto es una expresión booleana.

II. RECURSIÓN: Si P y Q son expresiones booleanas, entonces también lo son

$$a)\ (P \wedge Q) \text{ y } b)\ (P \vee Q) \text{ y } c)\ \sim P.$$

III. RESTRICCIÓN: No hay expresiones booleanas sobre el alfabeto distintos que los obtenidos de I y II.

Se deduce del hecho de que la siguiente es una expresión booleana sobre el alfabeto inglés $\{a, b, c, \ldots, x \text{ y, } z\}$:

$$(\sim(p \wedge q) \vee (\sim r \wedge p)).$$

Solución
1) Por I, p, q y r son expresiones booleanas.
2) Por 1) y IIa) y c), $(p \wedge q)$ y $\sim r$ son expresiones booleanas.
3) Por 2) y IIc) y a), $\sim(p \wedge q)$ y $(\sim r \wedge p)$ son expresiones booleanas.
4) Por 3) y IIb), $(\sim(p \wedge q) \vee (\sim r \wedge p))$ es una expresión booleana. ■

• Definición

Sea S un conjunto finito con al menos un elemento. Una **cadena sobre S** es una sucesión finita de elementos de S. Los elementos de S se llaman **caracteres** de la cadena y la **longitud** de una cadena es el número de caracteres que contiene, la **cadena nula sobre S** se define como la "cadena" sin caracteres. Por lo general se denota con ϵ y se dice que tiene una longitud 0.

Ejemplo 5.9.2 El conjunto de cadenas sobre un alfabeto

Considere el conjunto S de todas las cadenas en a y b. S se define recursivamente de la siguiente manera:

I. BASE: ϵ está en S, donde ϵ es la cadena nula.

II. RECURSIÓN: Si $s \in S$, entonces

$$a)\ sa \in S \text{ y } b)\ sb \in S,$$

donde sa y sb son las concatenaciones de s con a y b, respectivamente.

III. RESTRICCIÓN: No hay nada en S que no sean los objetos definidos en I y II. Deduzca el hecho de que $ab \in S$.

Solución
1) Por I, $\epsilon \in S$.
2) Por 1) y IIa), $\epsilon a \in S$. Pero ϵa es la concatenación de la cadena nula y a, que es igual a a. Así $a \in S$.
3) Por 2) y IIb), $ab \in S$. ■

Ejemplo 5.9.3 Juegos de cadenas con ciertas propiedades

En *Gödel, Escher, Bach*, de Douglas Hofstadter introduce la siguiente forma recursiva definida como conjunto de cadenas de M y de U, que él llama sistema MIU.*

I. BASE: MI está en el sistema MIU.

II. RECURSIÓN:

a. Si xI se encuentra en el sistema MIU, donde x es una cadena, entonces, xIU está en el sistema MIU. (En otras palabras, puede agregar una U para cualquier cadena que termina en I. Por ejemplo ya que MI está en el sistema, así es MIU.)

b. Si Mx está en el sistema MIU, donde x es una cadena, entonces Mxx está en el sistema MIU. (En otras palabras, puede repetir todos los caracteres de una cadena que siguen a una M inicial. Por ejemplo, si MIU está en el sistema, así es $MUIUI$.)

c. Si $xIIIy$ está en el sistema MIU, donde x y y son cadenas (posiblemente nulo), entonces xUy está también en el sistema MIU. (En otras palabras, puede reemplazar III por U. Por ejemplo, si $MIIII$ está en el sistema, por lo que son MIU y MUI.)

d. Si $xUUy$ está en el sistema MIU, donde x y y son cadenas (posiblemente nulo), entonces xUy está también en el sistema MIU. (En otras palabras, puede reemplazar UU por U. Por ejemplo, si $MIIUU$ está en el sistema, por lo que es $MIIU$.)

III. RESTRICCIÓN: No hay cadenas que las que se deducen de I y II están en el sistema MIU.

Deduzca el hecho de que $MUIU$ está en el sistema MIU.

Solución 1) Por I, MI está en el sistema MIU.

2) Por 1) y II*b*), MII está en el sistema MIU.

3) Por 2) y II*b*), $MIIII$ está en el sistema MIU.

4) Por 3) y II*c*), MUI está en el sistema MIU.

5) Por 4) y II*a*), $MUIU$ está en el sistema MIU. ■

Ejemplo 5.9.4 Estructuras paréntesis

Ciertas configuraciones de paréntesis en expresiones algebraicas son "legales" *[tales como* (())()*y*()()()*]*, mientras que otros no lo son *[tales como*)()))*y*()))(((*]*. Esta es una definición recursiva para generar el conjunto P de la configuración legal de paréntesis.

I. BASE: () está en P.

II. RECURSIÓN:

a. Si E está en P, por lo que es (E).

b. Si E y F están en P, por lo que es EF.

III. RESTRICCIÓN: No hay configuraciones de paréntesis que estén en P que no sean los derivados de I y II.

Deduzca el hecho de que (())() está en P.

Solución 1) por I, () está en P.

2) Por 1) y II*a*), (()) está en P.

3) Por 2), 1) y II*b*), (())() está en P. ■

*Douglas Hofstadter, *Gödel, Escher, Bach* (Nueva York: Basic Books), pp 33-35.

Demostración de propiedades respecto de conjuntos definidos recursivamente

Cuando se ha definido un conjunto de forma recursiva, se puede utilizar una versión de inducción matemática, llamado **inducción estructural**, para demostrar que todos los objetos en el conjunto satisfacen una propiedad dada.

Inducción estructural para los conjuntos definidos recursivamente

Sea S un conjunto que se ha definido de forma recursiva y considere una propiedad que los objetos en S pueden o no satisfacer. Para demostrar que todos los objetos en S satisface la propiedad:

1. Demuestre que cada objeto en la BASE para S satisface la propiedad;
2. Demuestre que para cada regla en la RECURSIÓN, si la regla se aplica a objetos en S que satisfacen la propiedad, entonces, los objetos definidos por la regla también satisfacen la propiedad.

Debido a que ningún otro objeto que los obtenidos a través de la BASE y condiciones de RECURSIÓN se encuentran en S, debe ser que todos los objetos en S satisfacen la propiedad.

Ejemplo 5.9.5 Dé una propiedad del conjunto de estructuras de paréntesis

Considere el conjunto P de todas las configuraciones gramaticales de paréntesis que se definen en el ejemplo 5.9.4. Demuestre que todas las configuraciones en P contienen un número igual de paréntesis izquierdo y derecho.

Solución

Demostración (por inducción estructural): Dada cualquier configuración de paréntesis, sea la propiedad que afirma que tiene el mismo número de paréntesis a la izquierda y la derecha.

Demostración de que cada objeto en la BASE para P satisface la propiedad: El único objeto en la base de P es (), que tiene un paréntesis izquierdo y un paréntesis derecho, por lo que tiene el mismo número de paréntesis a la izquierda y derecha.

Demostración de que para cada regla en la RECURSIÓN para P, si la regla se aplica a un objeto en P que satisface la propiedad, entonces el objeto definido por la regla también satisface la propiedad:
La recursión para P consiste de dos reglas que se denotan por IIa) y IIb).

Supongamos que E es una configuración de paréntesis que tiene el mismo número de paréntesis a la izquierda y derecha. Cuando se aplica a E, la regla IIa) el resultado es (E), por tanto el número de paréntesis a la izquierda y el número de paréntesis de la derecha aumenta en uno. Dado que estos números son iguales, para empezar, siguen siendo iguales cuando cada uno se incrementa en uno.

Supongamos que E y F son configuraciones de paréntesis con el mismo número de paréntesis a la izquierda y la derecha. Por ejemplo E tiene m paréntesis izquierdos y derechos y F tiene n paréntesis derechos e izquierdos. Cuando se aplica la regla IIb), el resultado es EF, que tiene el mismo número, es decir, $m + n$, de paréntesis izquierdos y derechos.

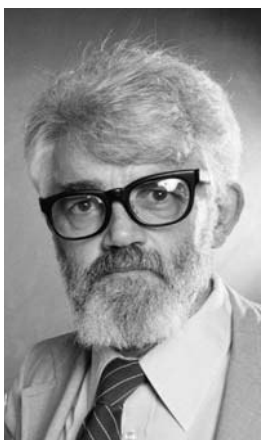
Así, cuando cada regla en la RECURSIÓN se aplica a una configuración de paréntesis en P con el mismo número de paréntesis izquierdos y derechos, el resultado es una configuración con un número igual de paréntesis izquierdos y derechos.

Por tanto, todas las estructuras en P tiene el mismo número de paréntesis izquierdos y derechos. ■

Funciones recursivas

Se dice que una función está **definida recursivamente** o es una **función recursiva** si su regla de definición se refiere a sí misma. Debido a esta autoreferencia, a veces es difícil saber si una función recursiva dada está bien definida. Las funciones recursivas son de gran importancia en la teoría de la computación en la ciencia computacional.

Ejemplo 5.9.6 Función 91 de McCarthy



Roger Ressmeyer/CORBIS

John McCarthy
(Nació en 1927)

La siguiente función $M : \mathbf{Z}^+ \to \mathbf{Z}$ fue definida por John McCarthy, un pionero en la teoría de la computación y en el estudio de la inteligencia artificial:

$$M(n) = \begin{cases} n - 10 & \text{si } n > 100 \\ M(M(n + 11)) & \text{si } n \leq 100 \end{cases}$$

para todos los enteros positivos n. Encuentre $M(99)$.

Solución Por el uso repetido de la definición de M,

$$\begin{aligned} M(99) &= M(M(110)) && \text{ya que } 99 \leq 100 \\ &= M(100) && \text{ya que } 110 > 100 \\ &= M(M(111)) && \text{ya que } 100 \leq 100 \\ &= M(101) && \text{ya que } 111 > 100 \\ &= 91 && \text{ya que } 101 > 100 \end{aligned}$$

Lo notable de esta función es que se toma el valor 91 para todos los enteros positivos menores o iguales a 101. (Se le pedirá demostrar esto en el ejercicio 20 al final de esta sección.) Por supuesto, para $n > 101$, $M(n)$ está bien definido ya que es igual a $n - 10$. ■

Ejemplo 5.9.7 La función de Ackermann

Wilhelm Ackermann
(1896-1962)

En la década de 1920 el lógico y matemático alemán Wilhelm Ackermann definió por primera vez una versión de la función que ahora lleva su nombre. Esta función es importante en la ciencia computacional porque ayuda a responder a la pregunta de qué se puede y qué no se puede calcular con una computadora. Se define en el conjunto de todos los pares de números enteros no negativos de la siguiente manera:

$$A(0,\ n) = n + 1 \qquad \text{para todo entero no negativo } n \qquad 5.9.1$$

$$A(m,\ 0) = A(m - 1,\ 1) \qquad \text{para todo entero positivo } m \qquad 5.9.2$$

$$A(m,\ n) = A(m - 1,\ A(m,\ n - 1)) \qquad \text{para todo entero positivo } m \text{ y } n \qquad 5.9.3$$

Determine $A(1, 2)$.

Solución

$$\begin{aligned} A(1, 2) &= A(0,\ A(1,\ 1)) && \text{por (5.9.3) con } m = 1 \text{ y } n = 2 \\ &= A(0,\ A(0,\ A(1,\ 0))) && \text{por (5.9.3) con } m = 1 \text{ y } n = 1 \\ &= A(0,\ A(0,\ A(0,\ 1))) && \text{por (5.9.2) con } m = 1 \\ &= A(0,\ A(0,\ 2)) && \text{por (5.9.1) con } n = 1 \\ &= A(0,\ 3) && \text{por (5.9.1) con } n = 2 \\ &= 4 && \text{por (5.9.1) con } n = 3. \end{aligned}$$

Las propiedades especiales de la función de Ackermann son una consecuencia de su tasa de crecimiento fenomenal. Mientras que los valores de $A(0, 0) = 1$, $A(1, 1) = 3$, $A(2, 2) = 7$ y $A(3, 3) = 61$ no son especialmente impresionantes,

$$A(4, 4) \cong 2^{2^{65536}}$$

y los valores de $A(n, n)$ continúan aumentando con una rapidez extraordinaria. ■

El argumento es un poco técnico, pero no es difícil demostrar que la función de Ackermann está bien definido. El siguiente es un ejemplo de una "definición" recursiva que no define una función.

Ejemplo 5.9.8 Una "función" recursiva no está bien definida

Considere el siguiente intento de definir una función recursiva G de $\mathbf{Z}^+$ a $\mathbf{Z}$. Para todo entero $n \geq 1$,

$$G(n) = \begin{cases} 1 & \text{si } n \text{ es } 1 \\ 1 + G\left(\frac{n}{2}\right) & \text{si } n \text{ es par} \\ G(3n - 1) & \text{si } n \text{ es impar y } n > 1. \end{cases}$$

¿G está bien definida? ¿Por qué?

Solución Supongamos que G es una función. Entonces, por definición de G,

$$\begin{aligned} G(1) &= 1, \\ G(2) &= 1 + G(1) = 1 + 1 = 2, \\ G(3) &= G(8) = 1 + G(4) = 1 + (1 + G(2)) = 1 + (1 + 2) = 4, \\ G(4) &= 1 + G(2) = 1 + 2 = 3. \end{aligned}$$

Sin embargo,

$$\begin{aligned} G(5) &= G(14) = 1 + G(7) = 1 + G(20) \\ &= 1 + (1 + G(10)) = 1 + (1 + (1 + G(5))) = 3 + G(5). \end{aligned}$$

Restando $G(5)$ de ambos lados se obtiene $0 = 3$, que es falso. Dado que la suposición de que G es una función conduce lógicamente a un enunciado falso, se deduce que G no es una función. ■

Una ligera modificación de la fórmula del ejemplo 5.9.8 produce una "función", cuyo estado de definición es desconocido. Considere la siguiente fórmula: Para todo entero $n \geq 1$,

$$T(n) = \begin{cases} 1 & \text{si } n \text{ es } 1 \\ T\left(\frac{n}{2}\right) & \text{si } n \text{ es par} \\ T(3n + 1) & \text{si } n \text{ es impar.} \end{cases}$$

En la década de 1930, un estudiante, Luther Collatz, se interesó en el comportamiento de una función relacionada g, que se define de la siguiente manera: $g(n) = n/2$ si n es par y $g(n) = 3n + 1$ si n es impar. Collatz supone que para cualquier número positivo inicial n, el cálculo de los valores sucesivos de $g(n)$, $g^2(n)$, $g^3(n)$, ... finalmente produce el número 1. Determine si esta suposición es verdadera o falsa que se llama **problema $3n + 1$** (o el **problema $3x + 1$**). Si la suposición de Collatz es verdadera, la fórmula para T define una función, si la suposición es falsa, T no está bien definida. Desde la publicación de este libro, la respuesta no es conocida, a pesar de que el cálculo por computadora ha establecido que es válido para valores muy grandes de n.

Autoexamen

1. La BASE para una definición recursiva de un conjunto es _____.
2. La RECURSIÓN para una definición recursiva de un conjunto es _____.
3. La RESTRICCIÓN para una definición recursiva de un conjunto es _____.
4. Una manera de demostrar que un elemento dado está en un conjunto definido de forma recursiva es comenzar con un elemento o elementos en el _____ y aplicar las reglas de la _____ hasta obtener el elemento dado.
5. Otra manera de mostrar que un elemento dado está en un conjunto definido de forma recursiva es utilizar _____ para caracterizar todos los elementos del conjunto y luego observar que el elemento dado satisface la caracterización.
6. Para probar que todo elemento de un conjunto S definido de forma recursiva satisface una propiedad dada, muestre que _____ y que, para cada regla en la RECURSIÓN, si _____ entonces _____.
7. Se dice que una función que se define de forma recursiva si y sólo si, _____.

Conjunto de ejercicios 5.9

1. Considere el conjunto de expresiones booleanas definidas en el ejemplo 5.9.1. Dé deducciones que muestran que cada una de las siguientes es una expresión booleana sobre el alfabeto inglés $\{a, b, c, \ldots, x, y, z\}$.
   a. $(\sim p \vee (q \wedge (r \vee \sim s)))$
   b. $(p \vee q) \vee \sim ((p \wedge \sim s) \wedge r))$

2. Sea S definida en el ejemplo 5.9.2. Dé deducciones que muestren que cada uno de los siguientes está en S.
   a. aab b. bb

3. Considere el sistema MIU analizado en el ejemplo 5.9.3. Dé deducciones que muestren que cada uno de los siguientes está en el sistema MIU.
   a. $MIUI$
   b. $MUIIU$

4. El conjunto de expresiones aritméticas sobre los números reales se pueden definir recursivamente de la siguiente manera:
   I. BASE: Cada número real r es una expresión aritmética.
   II. RECURSIÓN: Si u y v son expresiones aritméticas, entonces, las siguientes son expresiones aritméticas:
   a. $(+u)$ b. $(-u)$
   c. $(u + v)$ d. $(u - v)$
   e. $(u \cdot v)$ f. $\left(\frac{u}{v}\right)$
   III. RESTRICCIÓN: No hay expresiones aritméticas sobre los números reales distintos de los obtenidos de I y II.

   (Observe que la *expresión* $\left(\frac{u}{v}\right)$ es legal, aunque el valor de v puede ser 0). Dé deducciones que muestren que cada una de las siguientes es una expresión aritmética.
   a. $((2 \cdot (0.3–4.2)) + (-7))$ b. $\left(\frac{(9 \cdot (6.1 + 2))}{((4–7) \cdot 6)}\right)$

5. Defina un conjunto S de forma recursiva como sigue:
   I. BASE: $1 \in S$
   II. RECURSIÓN: Si $s \in S$, entonces
   a. $0s \in S$ b. $1s \in S$
   III. RESTRICCIÓN: No hay nada en S que no sean objetos definidos en I y II.
   Use inducción estructural para demostrar que cada cadena en S termina en 1.

6. Defina un conjunto S de forma recursiva como sigue:
   I. BASE: $a \in S$
   II. RECURSIÓN: Si $s \in S$, entonces,
   a. $sa \in S$ b. $sb \in S$
   III. RESTRICCIÓN: No hay nada en S que no sean objetos definidos en I y II.
   Use inducción estructural para demostrar que cada cadena en S comienza con una a.

7. Defina un conjunto S de forma recursiva como sigue:
   I. BASE: $\epsilon \in$ S
   II. RECURSIÓN: Si $s \in S$, entonces
   a. $bs \in S$ b. $sb \in S$
   c. $saa \in S$ d. $aas \in S$
   III. RESTRICCIÓN: No hay nada en S que no sean objetos definidos en I y II.
   Use inducción estructural para demostrar que cada cadena en S contiene un número par de a.

8. Defina un conjunto S de forma recursiva como sigue:
   I. BASE: $1 \in S$, $2 \in S$, $3 \in S$, $4 \in S$, $5 \in S$, $6 \in S$, $7 \in S$, $8 \in S$, $9 \in S$
   II. RECURSIÓN: Si $s \in S$ y $t \in S$, entonces,
   a. $s0 \in S$ b. $st \in S$
   III. RESTRICCIÓN: No hay nada en S que no sean objetos definidos en I y II.
   Use inducción estructural para demostrar que ninguna cadena en S representa un entero con un cero principal.

H 9. Defina un conjunto S de forma recursiva como sigue:
   I. BASE: $1 \in S$, $3 \in S$, $5 \in S$, $7 \in S$, $9 \in S$
   II. RECURSIÓN: Si $s \in S$ y $t \in S$, entonces
   a. $st \in S$ b. $2s \in S$
   c. $4s \in S$ d. $6s \in S$
   e. $8s \in S$
   III. RESTRICCIÓN: No hay nada en S que no sean objetos definidos en I y II.
   Use inducción estructural para demostrar que cada cadena en S representa un entero impar.

H 10. Defina un conjunto S de forma recursiva como sigue:
   I. BASE: $0 \in S$, $5 \in S$
   II. RECURSIÓN: Si $s \in S$ y $t \in S$, entonces
   a. $s + t \in S$ b. $s - t \in S$
   III. RESTRICCIÓN: No hay nada en S que no sean objetos definidos en I y II.
   Use inducción estructural para probar que todo número entero en S es divisible por 5.

11. Define un conjunto S de forma recursiva como sigue:
   I. BASE: $0 \in S$
   II. RECURSIÓN: Si $s \in S$, entonces
   a. $s + 3 \in S$ b. $s - 3 \in S$
   III. RESTRICCIÓN: No hay nada en S que no sean objetos definidos en I y II.
   Use inducción estructural para probar que todo número entero en S es divisible por 3.

H ✶12. ¿Es la cadena MU en el sistema MIU? Utilice inducción estructural para demostrar su respuesta.

13. Considere el conjunto P de estructuras de paréntesis definidas en el ejemplo 5.9.4. Dé deducciones que muestren que cada uno de los siguientes está en P.
   a. ()(()) b. (())(())

✶14. Determine si alguna de las siguientes estructuras de paréntesis está en el conjunto P que se define en el ejemplo 5.9.4. Use inducción estructural para demostrar sus respuestas.
   a. ()(() b. (()()))(()

15. Dé una definición recursiva para el conjunto de todas las cadenas de 0 y 1 que tienen el mismo número de 0 como de 1.

16. Dé una definición recursiva para el conjunto de todas las cadenas de 0 y 1 para que todos los 0 preceden todos los 1.

17. Dé una definición recursiva para el conjunto de todas las cadenas de a y b que contienen un número impar de a.

18. Dé una definición recursiva para el conjunto de todas las cadenas de a y b que contienen exactamente una a.

19. Utilice la definición de la función 91 de McCarthy del ejemplo 5.9.6 para mostrar lo siguiente:
   a. $M(86) = M(91)$ b. $M(91) = 91$

✶20. Demuestre que la función 91 de McCarthy es igual a 91 para todos los enteros positivos menores o iguales a 101.

21. Utilice la definición de la función de Ackermann del ejemplo 5.9.7 para calcular lo siguiente:
   a. $A(1, 1)$ b. $A(2, 1)$

22. Utilice la definición de la función de Ackermann para mostrar lo siguiente:
   a. $A(1, n) = n + 2$, para todos los enteros no negativos n.
   b. $A(2, n) = 3 + 2n$, para todos los enteros no negativos n.
   c. $A(3, n) = 8 \cdot 2^n - 3$, para todos los enteros no negativos n.

23. Calcule $T(2)$, $T(3)$, $T(4)$, $T(5)$, $T(6)$ y $T(7)$ de la "función" T definida después del ejemplo 5.9.8.

24. Un estudiante A trata de definir una función $F : \mathbf{Z}^+ \to \mathbf{Z}$ por la regla

$$F(n) = \begin{cases} 1 & \text{si } n \text{ es 1} \\ F\left(\frac{n}{2}\right) & \text{si } n \text{ es par} \\ 1 + F(5n - 9) & \text{si } n \text{ es impar y } n > 1 \end{cases}$$

para todo entero $n \geq 1$. El estudiante B afirma que F no está bien definida. Justifique la afirmación del estudiante B.

25. Un estudiante C trata de definir una función G: $\mathbf{Z}^+ \to \mathbf{Z}$ por la regla

$$G(n) = \begin{cases} 1 & \text{si } n \text{ es 1} \\ G\left(\frac{n}{2}\right) & \text{si } n \text{ es par} \\ 2 + G(3n - 5) & \text{si } n \text{ es impar y } n > 1 \end{cases}$$

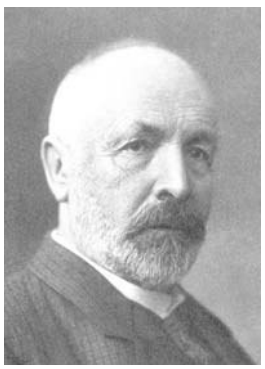
para todo entero $n \geq 1$. El estudiante D afirma que G no está bien definida. Justifique la afirmación del estudiante D.

Respuestas del autoexamen

1. un enunciado de que ciertos objetos pertenecen al conjunto 2. un conjunto de reglas que indican cómo formar nuevos objetos de conjunto a partir de los que ya se conocen del conjunto 3. un enunciado de que no hay objetos que pertenezcan al conjunto distintos de los que provienen de la BASE o la RECURSIÓN 4. BASE; RECURSIÓN 5. inducción estructural 6. cada objeto en la BASE satisface la propiedad; la regla se aplica a los objetos en la base, los objetos definidos por la regla también satisfacen la propiedad 7. su dominio de definición se refiere a sí mismo

CAPÍTULO 6

TEORÍA DE CONJUNTOS



Colección de David Eugene Smith, Universidad de Columbia

Georg Cantor (1845-1918)

A fines del siglo XIX, Georg Cantor fue el primero en darse cuenta de la utilidad potencial de investigar propiedades de los conjuntos en general, a diferencia de las propiedades de los elementos de que se componen. Muchos matemáticos de su tiempo se resistieron a aceptar la validez del trabajo de Cantor. Sin embargo, ahora, la abstracta teoría de conjuntos es considerada como el fundamento del pensamiento matemático. Todos los objetos matemáticos (¡aún los números!) pueden definirse en términos de conjuntos y el lenguaje de la teoría de conjuntos se utiliza en todos los temas matemáticos.

En este capítulo agregamos las definiciones básicas y la notación de la teoría de conjuntos que se introdujeron en el capítulo 1 y se muestra cómo establecer propiedades de los conjuntos mediante el uso de demostraciones y contraejemplos. También presentamos la noción del álgebra booleana, que explica cómo deducir sus propiedades y analizar las relaciones entre las equivalencias lógicas e identidades de conjuntos. El capítulo termina con un análisis de una famosa "paradoja" de la teoría de conjuntos y su relación con la ciencia computacional.

6.1 Teoría de conjuntos: definiciones y el método del elemento de demostración

La introducción de abstracciones adecuadas es nuestra única ayuda mental para organizar y dominar la complejidad. —E. W. Dijkstra, 1930-2002

Las palabras *conjunto* y *elemento* son términos indefinidos de la teoría de conjuntos tales como *frase*, *verdadero* y *falso* son términos indefinidos de la lógica. El fundador de la teoría de conjuntos, Georg Cantor, sugirió imaginar a un conjunto como una "colección M de todos los objetos definidos y separados de nuestra intuición o de nuestro pensamiento. Estos objetos se llaman los elementos de M". Cantor utilizó la letra M porque es la primera letra de la palabra conjunto en alemán: *Menge*.

Siguiendo el espíritu de la notación de Cantor (aunque no la letra), sea S un conjunto y a un elemento de S. Entonces, como se indica en la sección 1.2, $a \in S$ significa que a es un elemento de S, $a \notin S$ significa que a no es un elemento de S, $\{1, 2, 3\}$ se refiere al conjunto cuyos elementos son 1, 2 y 3 y $\{1, 2, 3, \ldots\}$ se refiere al conjunto de todos los enteros positivos. Si S es un conjunto y $P(x)$ es una propiedad que los elementos de S pueden o no pueden satisfacer, entonces se podrá definir un conjunto al escribir

$$A = \{x \in S \mid P(x)\},$$

el conjunto de todos — tal que

que se lee "el conjunto de todos los x en S tales que P de x".

¡Precaución! No olvide incluir las palabras "el conjunto de todos".

Subconjuntos: demostración y refutación

Empezamos por reescribir lo que significa que un conjunto A sea un subconjunto de un conjunto B como un enunciado condicional universal formal:

$$A \subseteq B \quad \Leftrightarrow \quad \forall x, \text{ si } x \in A \text{ entonces } x \in B.$$

La negación es, por tanto, existencial:

$$A \not\subseteq B \quad \Leftrightarrow \quad \exists x, \text{ tal que } x \in A \text{ y } x \notin B.$$

Un *subconjunto propio* de un conjunto es un subconjunto que no es igual al conjunto que lo contiene. Por tanto,

A es un **subconjunto propio** de B $\Leftrightarrow$

1) $A \subseteq B$ y
2) existe al menos un elemento en B que no está en A.

Ejemplo 6.1.1 Demostración de si un conjunto es un subconjunto de otro

Sea $A = \{1\}$ y $B = \{\mathbf{1}, \{1\}\}$.

a. ¿Es $A \subseteq B$?

b. Si es así, ¿es A un subconjunto propio de B?

Solución

Nota Un conjunto como $\{1\}$, con sólo un elemento, se llama un **conjunto unitario o singleton**.

a. Ya que $A = \{1\}$, A tiene un único elemento, a saber, el símbolo 1. Este elemento también es uno de los elementos en el conjunto de B. Por tanto cada elemento en A está en B y así $A \subseteq B$.

b. B tiene dos elementos distintos, el símbolo 1 y el conjunto $\{1\}$ cuyo único elemento es 1. Ya que $1 \neq \{1\}$, el conjunto $\{1\}$ no es un elemento de A y así hay un elemento de B que no es un elemento de A. Por lo que A es un subconjunto propio de B. ■

Ya que hemos definido lo que significa para un conjunto ser un subconjunto de otro por medio de un enunciado condicional universal, podemos utilizar el método de demostración directa para establecer una relación de subconjunto. Esta demostración se llama *argumento del elemento* y es la técnica de demostración esencial de la teoría de conjuntos.

Argumento del elemento: el método básico para demostrar que un conjunto es un subconjunto de otro

Sean los conjuntos X y Y dados. Para demostrar que $X \subseteq Y$,

1. **suponga** que x es un elemento particular arbitrariamente elegido de X,
2. **demuestre** que x es un elemento de Y.

Ejemplo 6.1.2 Demostrando y refutando relaciones de subconjunto

Defina los conjuntos A y B de la siguiente manera:

$$A = \{m \in \mathbf{Z} \mid m = 6r + 12 \text{ para alguna } r \in \mathbf{Z}\}$$

$$B = \{n \in \mathbf{Z} \mid n = 3s \text{ para alguna } s \in \mathbf{Z}\}$$

a. Diseñe una demostración para $A \subseteq B$. b. Demuestre que $A \subseteq B$.
c. Refute que $B \subseteq A$.

Solución

a. **Diseño de una demostración:**
Suponga que x es un elemento particular arbitrariamente elegido de A.

.
.
.

Por tanto, x es un elemento de B.

b. **Demostración:**
Suponga que x es un elemento particular arbitrariamente elegido de A.
[Debemos demostrar que $x \in B$. Por definición de B, esto significa que debemos demostrar que $x = 3 \cdot$ (algún entero).]

Por definición de A, existe un entero r tal que $x = 6r + 12$.
[Considerando que $x = 6r + 12$, ¿podemos expresar a x como $3 \cdot$ (algún entero)? Es decir, ¿es $6r + 12 = 3 \cdot$ (algún entero)? Sí, $6r + 12 = 3 \cdot (2r + 4)$.]

Sea $s = 2r + 4$.
[Debemos comprobar que s es un número entero.]

Entonces, s es un entero porque productos y sumas de enteros son enteros.
[Ahora debemos comprobar que $x = 3s$.]

También $3s = 3(2r + 4) = 6r + 12 = x$,
Así, por definición de B, x es un elemento de B,
[que es lo que se quería demostrar].

c. Refutar un enunciado significa mostrar que es falso y para demostrar que es falso que $B \subseteq A$, debe encontrar un elemento de B que no sea un elemento de A. Por las definiciones de A y B, esto significa que debe encontrar un entero x de la forma $3 \cdot$ (algún entero) que no se puede escribir en forma $6 \cdot$ (algún entero) $+ 12$. Un poco de experimentación revela que funcionan distintos números. Por ejemplo, puede hacer $x = 3$. Entonces $x \in B$ porque $3 = 3 \cdot 1$, pero $x \notin A$ porque no hay ningún entero r tal que $3 = 6r + 12$. Por si existiera dicho entero, entonces,

Nota Recuerde que la notación $P(x) \Rightarrow Q(x)$ significa que cada elemento que hace que $P(x)$ sea verdadero también hace que $Q(x)$ sea verdadero.

$$\begin{array}{rrl} & 6r + 12 = 3 & \text{por suposición} \\ \Rightarrow & 2r + 4 = 1 & \text{dividiendo ambos lados por 3} \\ \Rightarrow & 2r = 3 & \text{restando 4 de ambos lados} \\ \Rightarrow & r = 3/2 & \text{dividiendo ambos lados por 2,} \end{array}$$

pero $3/2$ no es un entero. Por tanto, $3 \in B$ pero $3 \notin A$ y así $B \not\subseteq A$. ■

Igualdad de conjuntos

Recuerde que por el axioma de extensión, A y B son iguales si y sólo si, tienen exactamente los mismos elementos. Reiteramos esto como una definición que utiliza el idioma de los subconjuntos.

• Definición

Dados los conjuntos A y B, A **es igual a** B, que se escribe $\boldsymbol{A = B}$, si y sólo si, cada elemento de A está en B y cada elemento de B está en A.

Simbólicamente:

$$A = B \quad \Leftrightarrow \quad A \subseteq B \text{ y } B \subseteq A.$$

Esta versión de la definición de igualdad implica lo siguiente:

> Para decir que un conjunto A es igual a un conjunto B, se debe cumplir que $A \subseteq B$ y se debe cumplir que $B \subseteq A$.

Ejemplo 6.1.3 Igualdad de conjuntos

Se definen los conjuntos A y B de la siguiente manera:

$$A = \{m \in \mathbf{Z} \mid m = 2a \text{ para algún entero } a\}$$

$$B = \{n \in \mathbf{Z} \mid n = 2b - 2 \text{ para algún entero } b\}$$

¿es, $A = B$?

Solución Sí. Para probar esto, deben demostrarse ambas relaciones de subconjunto $A \subseteq B$ y $B \subseteq C$.

Parte 1. Demostración de que $\boldsymbol{A \subseteq B}$:

Suponga que x es un elemento particular arbitrariamente elegido de A.

[Debemos demostrar que $x \in B$. Por definición de B, esto significa que tenemos que demostrar que $x = 2 \cdot$ (algún entero) $- 2$.]

Por definición, de A, existe un entero tal que $x = 2a$.

[Dado que $x = 2a$, ¿también se puede expresar a x como $2 \cdot$ (algún entero) $- 2$? Es decir, ¿existe un número entero, digamos b, tal que $2a = 2b - 2$? Resuelva para b para obtener $b = (2a + 2)/2 = a + 1$. Compruebe para ver si esto funciona.]

Sea $b = a + 1$.

[Primero compruebe que b es un número entero.]

Entonces, b también es un entero, ya que es una suma de números enteros.

[A continuación, compruebe que $x = 2b - 2$.]

También $2b - 2 = 2(a + 1) - 2 = 2a + 2 - 2 = 2a = x$,

Así, por definición de B, x es un elemento de B

[que es lo que se quería demostrar].

Parte 2. Demostración de que $\boldsymbol{B \subseteq A}$: Esta parte de la demostración se deja como ejercicio 2 al final de esta sección. ■

Diagramas de Venn

John Venn
(1834-1923)

Si los conjuntos A y B se representan como regiones en el plano, las relaciones entre A y B se pueden representar por dibujos, llamados **diagramas de Venn**, que fueron introducidos por el matemático británico John Venn en 1881. Por ejemplo, la relación $A \subseteq B$ se puede representar en una de las dos formas, que se muestran en la figura 6.1.1.

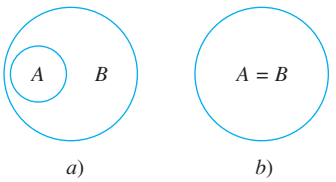


Figura 6.1.1 $A \subseteq B$

La relación $A \not\subseteq B$ se puede representar de tres formas diferentes con diagramas de Venn, como se muestra en la figura 6.1.2.

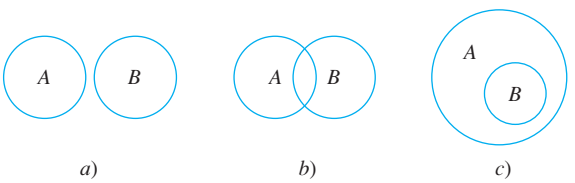


Figura 6.1.2 $A \not\subseteq B$

Si permitimos la posibilidad de que algunas subregiones de los diagramas de Venn no contengan ningún punto, entonces, la figura 6.1.1 diagrama *b*) se puede ver como un caso especial de *a*) si imaginamos que la parte de B fuera de A no contiene ningún punto. Del mismo modo, los diagramas *a*) y *c*) de figura 6.1.2 se pueden ver como casos especiales del diagrama *b*). Para obtener *a*) de *b*), imagine que la región que se superpone entre A y B no contiene ningún punto. Para obtener *c*), imagine que la parte de B que se encuentra fuera de A no contiene ningún punto. Sin embargo, en todos los tres diagramas sería necesario especificar que hay un punto en A que no está en B.

Ejemplo 6.1.4 Relaciones entre conjuntos de números

Dado que **Z**, **Q** y **R** son los conjuntos de los números enteros, números racionales y números reales, respectivamente, **Z** es un subconjunto de **Q** porque cada entero es racional (cualquier entero n se puede escribir en la forma $\frac{n}{1}$) y **Q** es un subconjunto de **R** porque cualquier número racional es real (cualquier número racional se puede representar como una longitud en la recta numérica). **Z** es un subconjunto propio de **Q** porque hay números racionales que no son enteros (por ejemplo, $\frac{1}{2}$) y **Q** es un subconjunto propio de **R** porque hay números reales que no son racionales (por ejemplo, $\sqrt{2}$). En la figura 6.1.3, esto se muestra con diagramas.

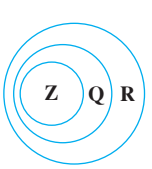
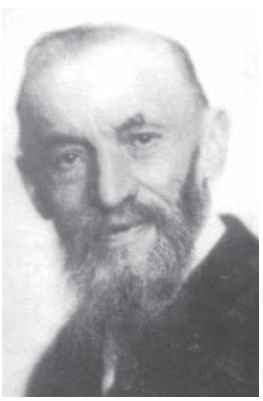


Figura 6.1.3

Operaciones con conjuntos

La mayoría de los análisis matemáticos se realizan dentro de algún contexto. Por ejemplo, en una determinada situación todos los conjuntos que se consideran podrían ser conjuntos de números reales. En esta situación, para este análisis el conjunto de números reales se llamaría el **conjunto universo** o **universo del discurso**.



Stock Montage

Giuseppe Peano (1858-1932)

• Definición

Sean A y B subconjuntos de un conjunto universo U.

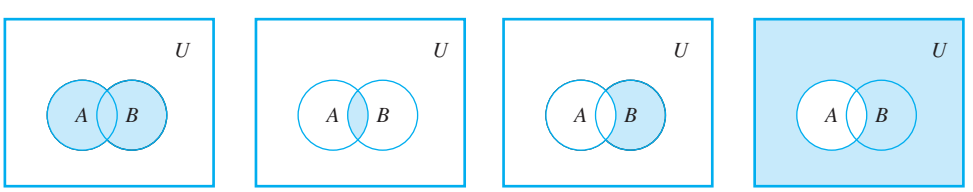
1. La **unión** de A y B, que se denota por $\boldsymbol{A \cup B}$, es el conjunto de todos los elementos que se encuentran en al menos uno de A o B.
2. La **intersección** de A y B, que se denota por $\boldsymbol{A \cap B}$, es el conjunto de todos los elementos que son comunes a ambos, a A y a B.
3. La **diferencia** de B menos A (o **complemento relativo** de A en B), que se denota por $\boldsymbol{B - A}$, es el conjunto de todos los elementos que se encuentran en B y que no están en A.
4. El **complemento** de A, que se denota por $\boldsymbol{A^c}$, es el conjunto de todos los elementos en U que no están en A.

Simbólicamente:

$$A \cup B = \{x \in U \mid x \in A \text{ o } x \in B\},$$
$$A \cap B = \{x \in U \mid x \in A \text{ y } x \in B\},$$
$$B - A = \{x \in U \mid x \in B \text{ y } x \notin A\},$$
$$A^c = \{x \in U \mid x \notin A\}.$$

Los símbolos $\in$, $\cup$ y $\cap$ se introdujeron en 1889 por el matemático italiano Giuseppe Peano.

En la figura 6.1.4, se muestran las representaciones del diagrama de Venn para la unión, intersección, diferencia y complemento.



La región sombreada representa $A \cup B$.

La región sombreada representa $A \cap B$.

La región sombreada representa $B - A$.

La región sombreada representa A^c.

Figura 6.1.4

Ejemplo 6.1.5 Uniones, intersecciones, diferencias y complementos

Sea el conjunto universo, el conjunto $U = \{a, b, c, d, e, f, g\}$ y sea $A = \{a, c, e, g\}$ y $B = \{d, e, f, g\}$. Determine $A \cup B$, $A \cap B$, $B - A$ y A^c.

Solución

$$A \cup B = \{a, c, d, e, f, g\} \qquad A \cap B = \{e, g\}$$
$$B - A = \{d, f\} \qquad A^c = \{b, d, f\}$$

■

Una notación conveniente para subconjuntos de los números reales son los intervalos.

• Notación

Dados los números reales a y b con $a \leq b$:

$$(a, b) = \{x \in \mathbf{R} \mid a < x < b\} \qquad [a, b] = \{x \in \mathbf{R} \mid a \leq x \leq b\}$$
$$(a, b] = \{x \in \mathbf{R} \mid a < x \leq b\} \qquad [a, b) = \{x \in \mathbf{R} \mid a \leq x < b\}.$$

Los símbolos ∞ y $-\infty$ se utilizan para indicar intervalos no acotados ya sea hacia la derecha o hacia la izquierda:

$$(a, \infty) = \{x \in \mathbf{R} \mid x > a\} \qquad [a, \infty) = \{x \in \mathbf{R} \mid x \geq a\}$$
$$(-\infty, b) = \{x \in \mathbf{R} \mid x < b\} \qquad [-\infty, b) = \{x \in \mathbf{R} \mid x \leq b\}.$$

Nota El símbolo ∞ no representa un número. Sólo indica lo ilimitado del intervalo.

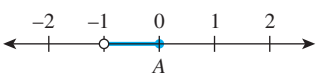
Observe que la notación para el intervalo (a, b) es idéntica a la notación para el par ordenado (a, b). Sin embargo, el contexto hace que no se puedan confundir.

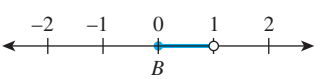
Ejemplo 6.1.6 Un ejemplo con intervalos

Sea el conjunto universo el conjunto $\mathbf{R}$ de todos los números reales y sea

$$A = (-1, 0] = \{x \in \mathbf{R} \mid -1 < x \leq 0\} \text{ y } B = [0, 1) = \{x \in \mathbf{R} \mid 0 \leq x < 1\}.$$

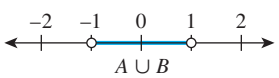
Estos conjuntos se muestran en las rectas numéricas que se presentan a continuación



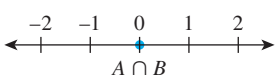


Determine $A \cup B$, $A \cap B$, $B - A$ y A^c.

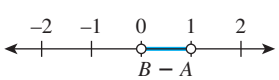
Solución

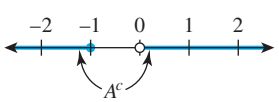


$$A \cup B = \{x \in \mathbf{R} \mid x \in (-1, 0] \text{ o } x \in [0, 1)\} = \{x \in \mathbf{R} \mid x \in (-1, 1)\} = (-1, 1).$$



$$A \cap B = \{x \in \mathbf{R} \mid x \in (-1, 0] \text{ y } x \in [0, 1)\} = \{0\}.$$





$$B - A = \{x \in \mathbf{R} \mid x \in [0, 1) \text{ y } x \notin (-1, 0]\} = \{x \in \mathbf{R} \mid 0 < x < 1\} = (0, 1)$$
$$A^c = \{x \in \mathbf{R} \mid \text{este no es el caso que } x \in (-1, 0]\}$$
$$= \{x \in \mathbf{R} \mid \text{este no es el caso que } (-1 < x \text{ y } x \leq 0)\} \quad \text{por definición de la doble desigualdad}$$
$$= \{x \in \mathbf{R} \mid x \leq -1 \text{ o } x > 0\} = \{-\infty, -1] \cup (0, \infty) \quad \text{por las leyes de De Morgan}$$

■

Las definiciones de uniones e intersecciones para más de dos conjuntos son muy similares a las definiciones de dos conjuntos.

• Definición

Uniones e intersecciones de una colección indexada de conjuntos
Dados los conjuntos de $A_0, A_1, A_2, \ldots$ que son subconjuntos de un conjunto universo U y dado un número entero no negativo n,

$$\bigcup_{i=0}^{n} A_i = \{x \in U \mid x \in A_i \text{ para al menos una } i = 0, 1, 2, \ldots, n\}$$

$$\bigcup_{i=0}^{\infty} A_i = \{x \in U \mid x \in A_i \text{ para al menos un entero no negativo } i\}$$

$$\bigcap_{i=0}^{n} A_i = \{x \in U \mid x \in A_i \text{ para todo } i = 0, 1, 2, \ldots, n\}$$

$$\bigcap_{i=0}^{\infty} A_i = \{x \in U \mid x \in A_i \text{ para todo enteros no negativos } i\}.$$

Nota $\bigcup_{i=0}^{n} A_i$ se lee "la unión de A-subíndice i desde i igual a cero hasta n".

Una notación alternativa para $\bigcup_{i=0}^{n} A_i$ es $A_0 \cup A_1 \cup \ldots \cup A_n$ y una notación alternativa para $\bigcap_{i=0}^{n} A_i$ es $A_0 \cap A_1 \cap \ldots \cap A_n$.

Ejemplo 6.1.7 Determinación de uniones e intersecciones de más de dos conjuntos.

Para cada entero positivo i sea $A_i = \left\{x \in \mathbf{R} \mid -\frac{1}{i} < x < \frac{1}{i}\right\} = A_i = \left(-\frac{1}{i}, \frac{1}{i}\right)$.

a. Determine $A_1 \cup A_2 \cup A_3$ y $A_1 \cap A_2 \cap A_3$. b. Determine $\bigcup_{i=1}^{\infty} A_i$ y $\bigcap_{i=1}^{\infty} A_i$.

Solución

a. $A_1 \cup A_2 \cup A_3 = \{x \in \mathbf{R} \mid x$ está en al menos uno de los intervalos $(-1, 1)$, o $\left(-\frac{1}{2}, \frac{1}{2}\right)$, o $\left(-\frac{1}{3}, \frac{1}{3}\right)\}$

$= \{x \in \mathbf{R} \mid -1 < x < 1\}$ ya que todos los elementos en $\left(-\frac{1}{2}, \frac{1}{2}\right)$ y $\left(-\frac{1}{3}, \frac{1}{3}\right)$ están en $(-1, 1)$

$= (-1, 1)$

$A_1 \cap A_2 \cap A_3 = \{x \in \mathbf{R} \mid x$ está en todos los intervalos $(-1, 1)$, y $\left(-\frac{1}{2}, \frac{1}{2}\right)$ y $\left(-\frac{1}{3}, \frac{1}{3}\right)\}$

$= \left\{x \in \mathbf{R} \mid -\frac{1}{3} < x < \frac{1}{3}\right\}$ porque $\left(-\frac{1}{3}, \frac{1}{3}\right) \subseteq \left(-\frac{1}{2}, \frac{1}{2}\right) \subseteq (-1, 1)$

$= \left(-\frac{1}{3}, \frac{1}{3}\right)$

b. $\bigcup_{i=1}^{\infty} A_i = \{x \in \mathbf{R} \mid x$ está en al menos uno de los intervalos $\left(-\frac{1}{i}, \frac{1}{i}\right)$, donde i es un entero positivo$\}$

$= \{x \in \mathbf{R} \mid -1 < x < 1\}$ porque todos los elementos de cada intervalo $\left(-\frac{1}{i}, \frac{1}{i}\right)$ están en $(-1, 1)$

$= (-1, 1)$

$\bigcap_{i=1}^{\infty} A_i = \{x \in \mathbf{R} \mid x$ está en todos los intervalos $\left(-\frac{1}{i}, \frac{1}{i}\right)$, donde i es un entero positivo$\}$

$= \{0\}$ ya que el único elemento en cada intervalo es 0

■

Conjunto vacío

Hemos establecido que un conjunto está definido por los elementos que lo componen. Si esto es así ¿puede existir un conjunto que no tenga elementos? Resulta que es conveniente contar con dicho conjunto. Por otra parte, cada vez que queríamos tomar la intersección de dos conjuntos o definir un conjunto especificando una propiedad, teníamos que comprobar que el resultado tuviera elementos y, por tanto, se clasificaría como un "conjunto cubierto". Por ejemplo, si $A = \{1, 3\}$ y $B = \{2, 4\}$, entonces $A \cap B$ no tiene elementos. Tampoco $\{x \in \mathbf{R} \mid x^2 = -1\}$ ya que ningún número real tienen cuadrados negativos.

Es algo inquietante hablar de un conjunto sin elementos, pero en matemáticas a menudo ocurre que las definiciones formuladas para adaptarse a un conjunto cuyas circunstancias son satisfechas por algunos casos extremos no previstos originalmente. Pero cambiar las definiciones para excluir los casos perjudicará gravemente la simplicidad y elegancia de la teoría de conjuntos.

En la sección 6.2 se mostrarán que hay sólo un conjunto sin elementos. Ya que es único, podemos darle un nombre especial. Se le llama **conjunto vacío** (o **conjunto nulo**) y se denota por el símbolo $\emptyset$. Por tanto $\{1, 3\} \cap \{2, 4\} = \emptyset$ y $\{x \in \mathbf{R} \mid x^2 = -1\} = \emptyset$.

Ejemplo 6.1.8 Un conjunto sin elementos

Describa el conjunto $D = \{x \in \mathbf{R} \mid 3 < x < 2\}$.

Solución Recuerde que $a < x < b$ significa que $a < x$ y $x < b$. Por tanto D consiste en todos los números reales que son tanto mayores de 3 como menores de 2. Ya que no hay tales números, D no tiene elementos y así $D = \emptyset$. ■

Particiones de conjuntos

En muchas aplicaciones de la teoría de conjuntos, los conjuntos se dividen en piezas no superpuestas (o *disjuntas*). Esa división se llama una *partición*.

• Definición

Dos conjuntos se llaman **disjuntos** si y sólo si, no tienen elementos en común.

Simbólicamente:

$$A \text{ y } B \text{ son disjuntos} \quad \Leftrightarrow \quad A \cap B = \emptyset$$

Ejemplo 6.1.9 Conjuntos disjuntos

Sea $A = \{1, 3, 5\}$ y $B = \{2, 4, 6\}$. ¿Son A y B disjuntos?

Solución Sí. Por inspección de A y B no tienen elementos en común, o, en otras palabras, $\{1, 3, 5\} \cap \{2, 4, 6\} = \emptyset$. ■

• Definición

Sean $A_1, A_2, A_3 \ldots$ **mutuamente disjuntos** (o por **pares disjuntos** que **no se superponen**) si y sólo si, ninguno de dos conjuntos A_i y A_j con subíndices distintos tienen elementos en común. Más precisamente, para toda $i, j = 1, 2, 3, \ldots$

$$A_i \cap A_j = \emptyset \text{ siempre que } i \neq j.$$

Ejemplo 6.1.10 Conjuntos mutuamente disjuntos

a. Sea $A_1 = \{3, 5\}$, $A_2 = \{1, 4, 6\}$ y $A_3 = \{2\}$. ¿Son A_1, A_2 y A_3 mutuamente disjuntos?

b. Sea $B_1 = \{2, 4, 6\}$, $B_2 = \{3, 7\}$ y $B_3 = \{4, 5\}$. ¿Son B_1, B_2, y B_3 mutuamente disjuntos?

Solución

a. Sí. A_1 y A_2 no tienen elementos en común, A_1 y A_3 no tienen elementos en común y A_2 y A_3 no tienen elementos en común.

b. No. B_1 y B_3 contienen ambos al 4. ■

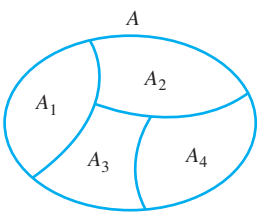


Figura 6.1.5 Una partición de un conjunto

Suponga que A, A_1, A_2, A_3 y A_4, son los conjuntos de puntos representados por las regiones que se muestran en figura 6.1.5. Entonces, A_1, A_2, A_3 y A_4, son subconjuntos de A y $A = A_1 \cup A_2 \cup A_3 \cup A_4$. Supongamos además que las cotas se asignan a las regiones que representan a A_2, A_3 y A_4, de tal manera que estos conjuntos son mutuamente disjuntos. Entonces A se le llama a una *unión de subconjuntos mutuamente disjuntos* y la colección de conjuntos $\{A_1, A_2, A_3, A_4\}$ se dice que es una *partición* de A.

• Definición

Una colección finita o infinita de conjuntos no vacíos $\{A_1, A_2, A_3 \ldots\}$ es una **partición** de un conjunto A si y sólo si,

1. A es la unión de todo A_i,
2. Los conjuntos $A_1, A_2, A_3, \ldots$ son mutuamente disjuntos.

Ejemplo 6.1.11 Particiones de conjuntos

a. Sea $A = \{1, 2, 3, 4, 5, 6\}$, $A_1 = \{1, 2\}$, $A_2 = \{3, 4\}$ y $A_3 = \{5, 6\}$. ¿Es $\{A_1, A_2, A_3\}$ una partición del A?

b. Sea $\mathbf{Z}$ el conjunto de todos los enteros y sea

$$T_0 = \{n \in \mathbf{Z} \mid n = 3k, \text{ para algunos enteros } k\},$$
$$T_1 = \{n \in \mathbf{Z} \mid n = 3k + 1, \text{ para algunos enteros } k\} \text{ y}$$
$$T_2 = \{n \in \mathbf{Z} \mid n = 3k + 2, \text{ para algunos enteros } k\}.$$

¿Es $\{T_0, T_1, T_2\}$ una partición de $\mathbf{Z}$?

Solución

a. Sí. Por inspección, $A = A_1 \cup A_2 \cup A_3$ y los conjuntos A_1, A_2, A_3 son mutuamente disjuntos.

b. Sí. Por el teorema de cociente-residuo, cada entero n se puede representar en exactamente una de las tres formas

$$n = 3k \quad \text{o} \quad n = 3k + 1 \quad \text{o} \quad n = 3k + 2,$$

para algún entero k. Esto implica que ningún entero puede estar en cualquiera de dos de los conjuntos T_0, T_1 o T_2. Por lo que T_0, T_1 y T_2 son mutuamente disjuntos. También implica que cada número entero está en uno de los conjuntos T_0, T_1 o T_2. Así $\mathbf{Z} = T_0 \cup T_1 \cup T_2$. ■

Conjunto potencia

Existen diversas situaciones en que es útil considerar al conjunto de todos los subconjuntos de un conjunto dado. El **axioma del conjunto potencia** garantiza que se trata de un conjunto.

• Definición

Dado un conjunto A, el **conjunto potencia** de A, que se denota con $\mathscr{P}(A)$, es el conjunto de todos los subconjuntos de A.

Ejemplo 6.1.12 Conjunto potencia de un conjunto

Determine el conjunto potencia del conjunto $\{x, y\}$. Es decir, encuentre $\mathscr{P}(\{x, y\})$.

Solución $\mathscr{P}(\{x, y\})$ es el conjunto de todos los subconjuntos de $\{x, y\}$. En la sección 6.2 se mostrará que $\emptyset$ es un subconjunto de cada conjunto y por tanto $\emptyset \in \mathscr{P}(\{x, y\})$. También cualquier conjunto es un subconjunto de sí mismo, así $\{x, y\} \in \mathscr{P}(\{x, y\})$. Los únicos otros subconjuntos de $\{x, y\}$ son $\{x\}$ y $\{y\}$, por lo que

$$\mathscr{P}(\{x, y\}) = \{\emptyset, \{x\}, \{y\}, \{\{x, y\}\}$$ ■

Productos cartesianos

Recuerde que la definición de un conjunto no se ve afectada por el orden en el que se listan sus elementos o por el hecho de que algunos elementos pueden ser listados más de una vez. Por tanto $\{a, b\}$, $\{b, a\}$ y $\{a, a, b\}$ todos representan el mismo conjunto. La notación de una *n-tupla ordenada* es una generalización de la notación para un par ordenado. (Vea la sección 1.2.) Que considera tanto el orden como la multiplicidad.

• Definición

Sea n un entero positivo y sean $x_1, x_2, \ldots, x_n$ elementos (no necesariamente distintos). La ***n*-tupla ordenada $(x_1, x_2, \ldots, x_n)$**, formada por $x_1, x_2, \ldots, x_n$ junto con el orden: primero x_1, después, x_2 y así sucesivamente hasta x_n. Una 2-tupla se llama un **par ordenado** y una 3-tupla ordenada es una **tripleta ordenada**.

Dos n-tuplas ordenadas $(x_1, x_2, \ldots, x_n)$ y $(y_1, y_2, \ldots, y_n)$ son **iguales** si y sólo si, $x_1 = y_1, x_2 = y_2, \ldots, x_n = y_n$.

Simbólicamente:

$$(x_1, x_2, \ldots, x_n) = (y_1, y_2, \ldots, y_n) \quad \Leftrightarrow \quad x_1 = y_1, x_2 = y_2, \ldots, x_n = y_n.$$

En particular,

$$(a, b) = (c, d) \quad \Leftrightarrow \quad a = c \text{ y } b = d.$$

Ejemplo 6.1.13 *n*-tuplas ordenadas

a. ¿Es $(1, 2, 3, 4) = (1, 2, 4, 3)$?

b. ¿Es $\left(3, (-2)^2, \frac{1}{2}\right) = \left(\sqrt{9}, 4, \frac{3}{6}\right)$?

Solución

a. No. Por definición de igualdad de 4-tuplas ordenadas,

$$(1, 2, 3, 4) = (1, 2, 4, 3) \Leftrightarrow 1 = 1, 2 = 2, 3 = 4 \text{ y } 4 = 3$$

Pero $3 \neq 4$, por lo que las 4-tuplas ordenadas no son iguales.

b. Sí. Por definición de igualdad de tripletas ordenadas,

$$\left(3, (-2)^2, \frac{1}{2}\right) = \left(\sqrt{9}, 4, \frac{3}{6}\right) \quad \Leftrightarrow \quad 3 = \sqrt{9} \text{ y } (-2)^2 = 4 \text{ y } \frac{1}{2} = \frac{3}{6},$$

Ya que estas ecuaciones son todas verdaderas, las dos tripletas ordenadas son iguales. ■

• Definición

Dados los conjuntos $A_1, A_2, \ldots, A_n$, el **producto cartesiano** de $A_1, A_2, \ldots, A_n$, que se denota por $\boldsymbol{A_1 \times A_2 \times \ldots \times A_n}$, es el conjunto de todas las n-tuplas ordenadas $(a_1, a_2, \ldots, a_n)$ donde $a_1 \in A_1, a_2 \in A_2, \ldots, a_n \in A_n$.

Simbólicamente:

$$A_1 \times A_2 \times \cdots A_n = \{(a_1, a_2, \ldots, a_n) \mid a_1 \in A_1, a_2 \in A_2, \ldots, a_n \in A_n\}.$$

En particular,

$$A_1 \times A_2 = \{(a_1, a_2) \mid a_1 \in A_1 \text{ y } a_2 \in A_2\}$$

es el producto cartesiano de A_1 y A_2.

Ejemplo 6.1.14 Productos cartesianos

Sea $A_1 = \{x, y\}$, $A_2 = \{1, 2, 3\}$ y $A_3 = \{a, b\}$.

a. Determine $A_1 \times A_2$. b. Determine $(A_1 \times A_2) \times A_3$. c. Determine $A_1 \times A_2 \times A_3$.

Solución

a. $A_1 \times A_2 = \{(x, 1), (x, 2), (x, 3), (y, 1), (y, 2), (y, 3)\}$

b. El producto cartesiano de A_1 y A_2 es un conjunto, por lo que se puede utilizar como uno de los conjuntos que constituyen otro producto cartesiano. Este es el caso para $(A_1 \times A_2) \times A_3$.

$$\begin{aligned}(A_1 \times A_2) \times A_3 &= \{(u, v) \mid u \in A_1 \times A_2 \text{ y } v \in A_3\} \quad \text{por definición de producto cartesiano} \\ &= \{((x, 1), a), ((x, 2), a), ((x, 3), a), ((y, 1), a), \\ &\quad ((y, 2), a), ((y, 3), a), ((x, 1), b), ((x, 2), b), ((x, 3), b), \\ &\quad ((y, 1), b), ((y, 2), b), ((y, 3), b)\}\end{aligned}$$

c. El producto cartesiano $A_1 \times A_2 \times A_3$ es superficialmente similar a, pero no es el mismo objeto matemático que $(A_1 \times A_2) \times A_3$. $(A_1 \times A_2) \times A_3$, es un conjunto de pares

ordenados en el que uno de los elementos es en sí mismo un par ordenado, mientras que $A_1 \times A_2 \times A_3$ es un conjunto de tripletas Por definición de producto cartesiano,

$$\begin{aligned} A_1 \times A_2 \times A_3 &= \{(u, v, w) \mid u \in A_1\ v \in A_2 \text{ y } w \in A_3\} \\ &= \{(x, 1, a), (x, 2, a), (x, 3, a), (y, 1, a), (y, 2, a), \\ &\quad (y, 3, a), (x, 1, b), (x, 2, b), (x, 3, b), (y, 1, b), \\ &\quad (y, 2, b), (y, 3, b)\}. \end{aligned}$$

■

Un algoritmo para comprobar si un conjunto es un subconjunto de otro (opcional)

Puede obtener alguna información adicional acerca del concepto de subconjunto considerando un algoritmo para comprobar si un conjunto finito es un subconjunto de otro. Ordenar los elementos de ambos conjuntos y comparar sucesivamente cada elemento del primer conjunto con cada elemento del segundo conjunto. Si algún elemento del primer conjunto no se encuentra igual que cualquier elemento del segundo, entonces, el primer conjunto no es un subconjunto del segundo. Pero si cada elemento del primer conjunto se encuentra que es igual a un elemento del segundo conjunto, entonces el primer conjunto es un subconjunto del segundo. El siguiente algoritmo formaliza este razonamiento.

Algoritmo 6.1.1 Demostración de si $A \subseteq B$

[Las entradas de los conjuntos A y B se representan como matrices unidimensionales $a[1], a[2], \ldots, a[m]$ *y* $b[1], b[2], \ldots, b[n]$, *respectivamente. Comenzando con* $a[1]$ *y para cada sucesivo* $a[i]$ *en A, se hace una comprobación para ver si* $a[i]$ *está en B. Para esto,* $a[i]$ *se compara con los elementos sucesivos de B. Si* $a[i]$ *no es igual a cualquier elemento de B, entonces la respuesta es dar el valor de "*$A \nsubseteq B$*". Si* $a[i]$ *es igual a algún elemento de B, el siguiente elemento sucesivo en A se comprueba para ver si está en B. Si cada elemento sucesivo de A se encuentra que está en B, entonces la respuesta nunca cambia de su valor inicial "*$A \subseteq B$*".]*

Entrada: *m [un entero positivo],* $a[1], a[2], \ldots, a[m]$ *[una matriz unidimensional que representa al conjunto A], n [es un entero positivo],* $b[1], b[2], \ldots, b[n]$ *[una matriz unidimensional que representa al conjunto B]*

Cuerpo del algoritmo:

$i := 1$, *respuesta* := "$A \subseteq B$"
while ($i \leq m$ y *respuesta* = "$A \subseteq B$")
  $j := 1$, *se encuentra* := "no"
    while ($j \leq n$ y *se encuentra* = "no")
      if $a[i] = b[j]$ **then** *se encuentra* := "sí"
      $j := j + 1$
    end while
    [Si se encuentra que no ha dado el valor "si" cuando la ejecución alcanza este punto, entonces $a[i] \notin B$*.]*
    if *se encuentra* = "no" **then** *respuesta* := "$A \subseteq B$"
    $i := i + 1$
end while

Salida: *respuesta [una cadena]*

Ejemplo 6.1.15 Seguimiento del algoritmo 6.1.1

Siga la acción del algoritmo 6.1.1 en las variables *i*, *j*, *se encuentra* y *respuesta* para $m = 3$, $n = 4$ y los conjuntos A y B se representan como los arreglos $a[1] = u$, $a[2] = v$, $a[3] = w$, $b[1] = w$, $b[2] = x$, $b[3] = y$ y $b[4] = u$.

Solución

i	1					2					3
j	1	2	3	4	5	1	2	3	4	5	
se encuentra	no			sí		no					
respuesta	$A \subseteq B$									$A \not\subseteq B$	

En los ejercicios al final de esta sección, se le pide que escriba un algoritmo para comprobar si un elemento dado está en un conjunto dado. Para hacer esto, puede representar al conjunto como un arreglo unidimensional y compare el elemento dado con los elementos sucesivos del arreglo para determinar si los dos elementos son iguales. Si es así, entonces el elemento está en el conjunto; si el elemento dado no es igual a cualquier elemento de la matriz, entonces, el elemento no está en el conjunto.

Autoexamen

Las respuestas del autoexamen se encuentran al final de cada sección.

1. La notación $A \subseteq B$ se lee "_____" y significa que _____.
2. Para utilizar un elemento de argumento para demostrar que un conjunto X es un subconjunto de un conjunto Y, suponga que _____ y demuestre que _____.
3. Para refutar que un conjunto X es un subconjunto de un conjunto Y, muestre que existe _____.
4. Un elemento x está en $A \cup B$ si y sólo si, _____.
5. Un elemento x está en $A \cap B$ si y sólo si, _____.
6. Un elemento x está en $B - A$ si y sólo si, _____.
7. Un elemento x está en A^c si y sólo si, _____.
8. El conjunto vacío es un conjunto con _____.
9. El conjunto potencia de un conjunto A es _____.
10. Los conjuntos A y B son disjuntos si y sólo si, _____.
11. Una colección de conjuntos no vacíos $A_1, A_2, A_3, \ldots$ es una partición de un conjunto A si y sólo si, _____.
12. Dados los conjuntos de $A_1, A_2, \ldots, A_n$, el producto cartesiano $A_1 \times A_2 \times \cdots \times A_n$ es _____.

Conjunto de ejercicios 6.1*

1. ¿En cada uno de los ejercicios *a*) al *f*), responda las preguntas siguientes: ¿es $A \subseteq B$? ¿Es $B \subseteq A$? ¿Es ya sea A o B un subconjunto propio del otro?

   a. $A = \{2, \{2\}, (\sqrt{2})^2\}$, $B = \{2, \{2\}, \{\{2\}\}\}$

   b. $A = \{3, \sqrt{5^2 - 4^2}, 24 \bmod 7\}$, $B = \{8 \bmod 5\}$

   c. $A = \{\{1, 2\}, \{2, 3\}\}$, $B = \{1, 2, 3\}$

   d. $A = \{a, b, c\}$, $B = \{\{a\}, \{b\}, \{c\}\}$

   e. $A = \{\sqrt{16}, \{4\}\}$, $B = \{4\}$

   f. $A = \{x \in \mathrm{R} \mid \cos x \in \mathrm{Z}\}$, $B = \{x \in \mathbf{R} \mid \operatorname{sen} x \in \mathbf{Z}\}$

2. Complete la demostración del ejemplo 6.1.3: demuestre que $B \subseteq A$ donde

$$A = \{m \in \mathbf{Z} \mid m = 2a \text{ para algún entero } a\}$$

y

$$B = \{n \in \mathbf{Z} \mid n = 2b - 2 \text{ para algún entero } b\}$$

*Para los ejercicios con números o letras azules, las soluciones están dadas en el apéndice B. El símbolo **H** indica que sólo se da una sugerencia o una solución parcial. El símbolo ✶ indica que el ejercicio es más difícil de lo normal.

3. Sean los conjuntos R, S y T definidos de la siguiente manera:

$$R = \{x \in \mathbf{Z} \mid x \text{ es divisible por } 2\}$$
$$S = \{y \in \mathbf{Z} \mid y \text{ es divisible por } 3\}$$
$$T = \{z \in \mathbf{Z} \mid z \text{ es divisible por } 6\}$$

a. ¿Es $R \subseteq T$? Explique.
b. ¿Es $T \subseteq R$? Explique.
c. ¿Es $T \subseteq S$? Explique.

4. Sea $A = \{n \in \mathbf{Z} \mid n = 5r$ para algún entero $r\}$ y $B = \{m \in \mathbf{Z} \mid m = 20s$ para algún entero $s\}$.
a. ¿Es $A \subseteq B$? Explique. b. ¿Es $B \subseteq A$? Explique.

5. Sea $C = \{n \in \mathbf{Z} \mid n = 6r - 5$ para algún entero $r\}$ y $D = \{m \in \mathbf{Z} \mid m = 3s + 1$ para algún entero $s\}$.
Demuestre o refute cada uno de los siguientes enunciados.
a. $C \subseteq D$ b. $D \subseteq C$.

6. Sea $A = \{x \in \mathbf{Z} \mid x = 5a + 2$ para algún entero $a\}$, $B = \{y \in \mathbf{Z} \mid y = 10b - 3$ para algún entero $b\}$ y $C = \{z \in \mathbf{Z} \mid z = 10c + 7$ para algún entero $c\}$.
Demuestre o refute cada uno de los siguientes enunciados.
a. $A \subseteq B$ b. $B \subseteq A$. ***H*** **c.** $B = C$.

7. Sea $A = \{x \in \mathbf{Z} \mid x = 6a + 4$ para algún entero $a\}$, $B = \{y \in \mathbf{Z} \mid y = 18b - 2$ para algún entero $b\}$ y $C = \{z \in \mathbf{Z} \mid z = 18c + 16$ para algún entero $c\}$.
Demuestre o refute cada uno de los siguientes enunciados.
a. $A \subseteq B$ b. $B \subseteq A$. c. $B = C$.

8. Describa con palabras cómo leer cada uno de los siguientes enunciados. A continuación, escriba la notación abreviada para cada conjunto.
a. $\{x \in U \mid x \in A$ y $x \in B\}$
b. $\{x \in U \mid x \in A$ o $x \in B\}$
c. $\{x \in U \mid x \in A$ y $x \notin B\}$
d. $\{x \in U \mid x \notin A\}$

9. Complete los siguientes enunciados sin utilizar los símbolos $\cup$, $\cap$, o $-$.
a. $x \notin A \cup B$ si y sólo si, _____.
b. $x \notin A \cap B$ si y sólo si, _____.
c. $x \notin A - B$ si y sólo si, _____.

10. Sea $A = \{1, 3, 5, 7, 9\}$, $B = \{3, 6, 9\}$ y $C = \{2, 4, 6, 8\}$. Determine cada uno de los siguientes enunciados:
a. $A \cup B$ **b.** $A \cap B$ **c.** $A \cup C$ **d.** $A \cap C$
e. $A - B$ f. $B - A$ g. $B \cup C$ h. $B \cap C$

11. Sea el conjunto universo, el conjunto $\mathbf{R}$ de todos los números reales y sea $A = \{x \in \mathbf{R} \mid 0 < x \leq 2\}$, $B = \{x \in \mathbf{R} \mid 1 \leq x < 4\}$ y $C = \{x \in \mathbf{R} \mid 3 \leq x < 9\}$. Determine cada uno de los siguientes enunciados:
a. $A \cup B$ b. $A \cap B$ c. A^c d. $A \cup C$
e. $A \cap C$ f. B^c g. $A^c \cap B^c$
h. $A^c \cup B^c$ i. $(A \cap B)^c$ j. $(A \cup B)^c$

12. Sea el conjunto universo, el conjunto $\mathbf{R}$ de todos los números reales y sea $A = \{x \in \mathbf{R} \mid -3 \leq x \leq 0\}$, $B = \{x \in \mathbf{R} \mid -1 < x < 2\}$ y $C = \{x \in \mathbf{R} \mid 6 < x \leq 8\}$. Determine cada uno de los siguientes enunciados:
a. $A \cup B$ b. $A \cap B$ c. A^c d. $A \cup C$
e. $A \cap C$ f. B^c g. $A^c \cap B^c$
h. $A^c \cup B^c$ i. $(A \cap B)^c$ j. $(A \cup B)^c$

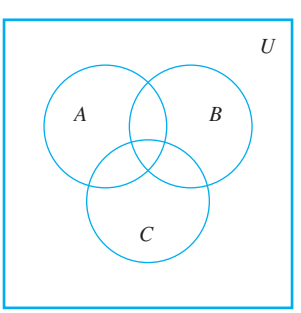
13. Indique cuáles de las siguientes relaciones son verdaderas y cuáles son falsas:
a. $\mathbf{Z}^+ \subseteq \mathbf{Q}$ **b.** $\mathbf{R}^- \subseteq \mathbf{Q}$
c. $\mathbf{Q} \subseteq \mathbf{Z}$ **d.** $\mathbf{Z}^- \cup \mathbf{Z}^+ = \mathbf{Z}$
e. $\mathbf{Z}^- \cap \mathbf{Z}^+ = \emptyset$ f. $\mathbf{Q} \cap \mathbf{R} = \mathbf{Q}$
g. $\mathbf{Q} \cup \mathbf{Z} = \mathbf{Q}$ h. $\mathbf{Z}^+ \cap \mathbf{R} = \mathbf{Z}^+$
i. $\mathbf{Z} \cup \mathbf{Q} = \mathbf{Z}$

14. Para cada uno de los siguientes enunciados, dibuje un diagrama de Venn para los conjuntos A, B y C que satisface las condiciones dadas:
a. $A \subseteq B$; $C \subseteq B$; $A \cap C = \emptyset$
b. $C \subseteq A$; $B \cap C = \emptyset$

15. Dibuje los diagramas de Venn para describir los conjuntos A, B y C que satisfacen las condiciones dadas.
a. $A \cap B = \emptyset$, $A \subseteq C$, $C \cap B \neq \emptyset$
b. $A \subseteq B$, $C \subseteq B$, $A \cap C \neq \emptyset$
c. $A \cap B \neq \emptyset$, $B \cap C \neq \emptyset$, $A \cap C = \emptyset$, $A \not\subseteq B$, $C \not\subseteq B$

16. Sea $A = \{a, b, c\}$, $B = \{b, c, d\}$ y $C = \{b, c, e\}$.
a. Determine $A \cup (B \cap C)$, $(A \cup B) \cap C$ y $(A \cup B) \cap (A \cup C)$. ¿Cuáles de estos conjuntos son iguales?
b. Determine $A \cap (B \cup C)$, $(A \cap B) \cup C$ y $(A \cap B) \cup (A \cap C)$. ¿Cuáles de estos conjuntos son iguales?
c. Determine $(A - B) - C$, $A - (B - C)$. ¿Cuáles de estos conjuntos son iguales?

17. Considere el diagrama de Venn que se muestra a continuación. Para cada uno de los enunciados del *a*) al *f*), copie el diagrama y sombree la región correspondiente al conjunto indicado.
a. $A \cap B$ b. $B \cup C$ c. A^c
d. $A - (B \cup C)$ e. $(A \cup B)^c$ f. $A^c \cup B^c$



18. **a.** ¿Está el número 0 en $\emptyset$? ¿Por qué?
b. ¿Es $\emptyset = \{\emptyset\}$? ¿Por qué?
c. ¿Es $\emptyset \in \{\emptyset\}$? ¿Por qué?
d. ¿Es $\emptyset \in \emptyset$? ¿Por qué?

19. Sea $A_i = \{i, i^2\}$ para todo entero $i = 1, 2, 3, 4$.
a. ¿$A_1 \cup A_2 \cup A_3 \cup A_4 =$?
b. ¿$A_1 \cap A_2 \cap A_3 \cap A_4 =$?
c. ¿Son A_1, A_2, A_3 y A_4 mutuamente disjuntos? Explique.

20. Sea $B_i = \{x \in \mathbf{R} \mid 0 \leq x \leq i\}$ para todo entero $i = 1, 2, 3, 4$.
a. ¿$B_1 \cup B_2 \cup B_3 \cup B_4 =$?
b. ¿$B_1 \cap B_2 \cap B_3 \cap B_4 =$?
c. ¿Son B_1, B_2, B_3 y B_4 mutuamente disjuntos? Explique.

21. Sea $C_i = \{i, -i\}$ para todo entero no negativo i.
a. $\bigcup_{i=0}^{4} C_i =$? b. $\bigcap_{i=0}^{4} C_i =$?

c. ¿Son $C_0, C_1, C_2, \ldots$ mutuamente disjuntos? Explique.

d. $\bigcup_{i=0}^{n} C_i = ?$ e. $\bigcap_{i=0}^{n} C_i = ?$

f. $\bigcup_{i=0}^{\infty} C_i = ?$ g. $\bigcap_{i=0}^{\infty} C_i = ?$

22. Sea $D_i = \{x \in \mathbf{R} \mid -i \le x \le i\} = [-i, i]$ para todo entero no negativo i.

a. $\bigcup_{i=0}^{4} D_i = ?$ b. $\bigcap_{i=0}^{4} D_i = ?$

c. ¿Son $D_0, D_1, D_2, \ldots$ mutuamente disjuntos? Explique.

d. $\bigcup_{i=0}^{n} D_i = ?$ e. $\bigcap_{i=0}^{n} D_i = ?$

f. $\bigcup_{i=0}^{\infty} D_i = ?$ g. $\bigcap_{i=0}^{\infty} D_i = ?$

23. Sea $V_i = \left\{x \in \mathbf{R} \mid -\frac{1}{i} \le x \le \frac{1}{i}\right\} = \left[-\frac{1}{i}, \frac{1}{i}\right]$ para todo entero positivo i.

a. $\bigcup_{i=1}^{4} V_i = ?$ b. $\bigcap_{i=1}^{4} V_i = ?$

c. ¿Son $V_1, V_2, V_3, \ldots$ mutuamente disjuntos? Explique.

d. $\bigcup_{i=1}^{n} V_i = ?$ e. $\bigcap_{i=1}^{n} V_i = ?$

f. $\bigcup_{i=1}^{\infty} V_i = ?$ g. $\bigcap_{i=1}^{\infty} V_i = ?$

24. Sea $W_i = \{x \in \mathbf{R} \mid x > i\} = (i, \infty)$ para todo entero no negativo i.

a. $\bigcup_{i=0}^{4} W_i = ?$ b. $\bigcap_{i=0}^{4} W_i = ?$

c. ¿Son $W_0, W_1, W_2, \ldots$ mutuamente disjuntos? Explique.

d. $\bigcup_{i=0}^{n} W_i = ?$ e. $\bigcap_{i=0}^{n} W_i = ?$

f. $\bigcup_{i=0}^{\infty} W_i = ?$ g. $\bigcap_{i=0}^{\infty} W_i = ?$

25. Sea $R_i = \left\{x \in \mathbf{R} \mid 1 \le x \le 1 + \frac{1}{i}\right\} = \left[1, 1 + \frac{1}{i}\right]$ para todo entero positivo i.

a. $\bigcup_{i=1}^{4} R_i = ?$ b. $\bigcap_{i=1}^{4} R_i = ?$

c. ¿Son $R_1, R_2, R_3, \ldots$ mutuamente disjuntos? Explique.

d. $\bigcup_{i=1}^{n} R_i = ?$ e. $\bigcap_{i=1}^{n} R_i = ?$

f. $\bigcup_{i=1}^{\infty} R_i = ?$ g. $\bigcap_{i=1}^{\infty} R_i = ?$

26. Sea $S_i = \left\{x \in \mathbf{R} \mid 1 < x < 1 + \frac{1}{i}\right\} = \left(1, 1 + \frac{1}{i}\right)$ para todo entero positivo i.

a. $\bigcup_{i=1}^{4} S_i = ?$ b. $\bigcap_{i=1}^{4} S_i = ?$

c. ¿Son $S_1, S_2, S_3, \ldots$ mutuamente disjuntos? Explique.

d. $\bigcup_{i=1}^{n} S_i = ?$ e. $\bigcap_{i=1}^{n} S_i = ?$

f. $\bigcup_{i=1}^{\infty} S_i = ?$ g. $\bigcap_{i=1}^{\infty} S_i = ?$

27. **a.** ¿Es $\{\{a, d, e\}, \{b, c\}, \{d, f\}\}$ una partición de $\{a, b, c, d, e, f\}$?

b. ¿Es $\{\{w, x, v\}, \{u, y, q\}, \{p, z\}\}$ una partición de $\{p, q, u, v, w, x, y, z\}$?

c. ¿Es $\{\{5, 4\}, \{7, 2\}, \{1, 3, 4\}, \{6, 8\}\}$ una partición de $\{1, 2, 3, 4, 5, 6, 7, 8\}$?

d. ¿Es $\{\{3, 7, 8\}, \{2, 9\}, \{1, 4, 5\}\}$ una partición de $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$?

e. ¿Es $\{\{1, 5\}, \{4, 7\}, \{2, 8, 6, 3\}\}$ una partición de $\{1, 2, 3, 4, 5, 6, 7, 8\}$?

28. Sea E el conjunto de todos los enteros pares y O el conjunto de todos los enteros impares. ¿Es $\{E, O\}$ una partición de $\mathbf{Z}$, el conjunto de todos los enteros? Explique su respuesta.

29. Sea $\mathbf{R}$ es el conjunto de todos los números reales. ¿Es $\{\mathbf{R}^+, \mathbf{R}^-, \{0\}\}$ una partición de $\mathbf{R}$? Explique su respuesta.

30. Sea $\mathbf{Z}$ el conjunto de todos los enteros y sea

$A_0 = \{n \in \mathbf{Z} \mid n = 4k$, para algún entero $k\}$,

$A_1 = \{n \in \mathbf{Z} \mid n = 4k + 1$, para algún entero $k\}$,

$A_2 = \{n \in \mathbf{Z} \mid n = 4k + 2$, para algún entero $k\}$ y

$A_3 = \{n \in \mathbf{Z} \mid n = 4k + 4$, para algún entero $k\}$.

¿Es $\{A_0, A_1, A_2, A_3\}$ una partición de $\mathbf{Z}$? Explique su respuesta.

31. Suponga que $A = \{1, 2\}$ y $B = \{2, 3\}$. Determine cada uno de los siguientes enunciados

a. $\mathscr{P}(A \cap B)$ b. $\mathscr{P}(A)$

c. $\mathscr{P}(A \cup B)$ d. $\mathscr{P}(A \times B)$

32. **a.** Suponga que $A = \{1\}$ y $B = \{u, v\}$. Encuentre $\mathscr{P}(A \times B)$

b. Suponga que $X = \{a, b\}$ y $Y = \{x, y\}$. Determine $\mathscr{P}(X \times Y)$.

33. a. Determine $\mathscr{P}(\emptyset)$. **b.** Encuentre $\mathscr{P}(\mathscr{P}(\emptyset))$.

c. Determine $\mathscr{P}(\mathscr{P}(\mathscr{P}(\emptyset)))$.

34. Sea $A_1 = \{1, 2, 3\}$, $A_2 = \{u, v\}$, $A_3 = \{m, n\}$. Encuentre cada uno de los siguientes conjuntos:

a. $A_1 \times (A_2 \times A_3)$ b. $(A_1 \times A_2) \times A_3$

c. $A_1 \times A_2 \times A_3$

35. Sea $A = \{a, b\}$, $B = \{1, 2\}$ y $C = \{2, 3\}$. Determine cada uno de los siguientes conjuntos.

a. $A \times (B \cup C)$ **b.** $(A \times B) \cup (A \times C)$

c. $A \times (B \cap C)$ d. $(A \times B) \cap (A \times C)$

36. Siga la acción del algoritmo 6.1.1 sobre las variables i, j, *se encuentra* y *respuesta* para $m = 3$, $n = 3$ y los conjuntos A y B representados por los arreglos $a[1] = u$, $a[2] = v$, $a[3] = w$, $b[1] = w$, $b[2] = u$ y $b[3] = v$.

37. Siga la acción del algoritmo 6.1.1 sobre las variables i, j, *se encuentra* y *respuesta* para $m = 4$, $n = 4$ y los conjuntos A y B representados por los arreglos $a[1] = u$, $a[2] = v$, $a[3] = w$, $a[4] = x$, $b[1] = r$, $b[2] = u$, $b[3] = y$, $b[4] = z$.

38. Escriba un algoritmo para determinar si un elemento x pertenece a un conjunto dado, representado como un arreglo $a[1], a[2], \ldots, a[n]$.

Respuestas del autoexamen

1. el conjunto A es un subconjunto del conjunto B; para toda x, si $x \in A$, entonces, $x \in B$ (O: cada elemento de A es también un elemento de B) 2. x es cualquier elemento *[particular arbitrariamente elegido]* de X; x es un elemento de Y 3. un elemento en X que no está en Y 4. x está en A o x está en B (O: x está en al menos uno de los conjuntos A y B) 5. x está en A y x está en B (O: x está tanto en A como en B) 6. x está en B y x no está en A 7. x está en el conjunto universo y no está en A 8. no hay elementos 9. el conjunto de todos los subconjuntos de A 10. $A \cap B = \emptyset$ (O: A y B no tienen elementos en común) 11. A está en la unión de todos los conjuntos $A_1, A_2, A_3, \ldots$ y $A_i \cap A_j = \emptyset$ cada vez que $i \neq j$. 12. el conjunto de todas las n-tuplas ordenadas $(a_1, a_2, \ldots, a_n)$, donde a_i está en A_i para todo $i = 1, 2, \ldots, n$

6.2 Propiedades de conjuntos

... sólo el último renglón es un teorema verdadero —aquí todo lo demás es fantasía.
—Douglas Hofstadter, *Gödel, Escher, Bach,* 1979

Es posible enumerar muchas relaciones que involucran uniones, intersecciones, complementos y diferencias de conjuntos. Algunas de éstas son verdaderas para todos los conjuntos, mientras que otros no se conservan en algunos casos. En esta sección mostramos cómo establecer propiedades básicas de los conjuntos usando *argumentos de los elementos* y analizando una variación que se utiliza para probar que un conjunto está vacío. En la siguiente sección se mostrarán cómo refutar una propiedad de conjunto propuesta mediante la construcción de un contraejemplo y cómo utilizar una técnica algebraica para deducir nuevas propiedades del conjunto a partir de la definición de propiedades de conjuntos que ya se sabe que son verdaderas.

Empezamos por listar algunas propiedades que implican relaciones de subconjunto. Conforme las lea, considere que las operaciones de unión, intersección y diferencia tienen preferencia sobre la inclusión del conjunto. Así, por ejemplo, $A \cap B \subseteq C$ significa $(A \cap B) \subseteq C$.

Teorema 6.2.1 Algunas relaciones de subconjuntos

1. *Inclusión de intersección*: Para todos los conjuntos A y B,
$$a)\ A \cap B \subseteq A \quad \text{y} \quad b)\ A \cap B \subseteq B.$$
2. *Inclusión en la unión*: Para todos los conjuntos A y B,
$$a)\ A \subseteq A \cup B \quad \text{y} \quad b)\ B \subseteq A \cup B.$$
3. *Propiedad transitiva de subconjuntos*: Para todos los conjuntos A, B y C,
$$\text{si } A \subseteq B \text{ y } B \subseteq C, \text{ entonces } A \subseteq C.$$

La conclusión de cada inciso del teorema 6.2.1 establece que un conjunto x es un subconjunto de otro conjunto Y y para demostrarlos, suponga que x es cualquier elemento *[particular arbitrariamente elegido]* de X y demuestre que x es un elemento de Y.

En la mayoría de las demostraciones de las propiedades de conjuntos, el secreto de obtener la suposición de que x está en X a la conclusión de que x está en Y es pensar en términos de las definiciones de las operaciones básicas de conjuntos. Por ejemplo, la unión de conjuntos X y Y, $X \cup Y$, se define como

$$X \cup Y = \{x \mid x \in X \text{ o } x \in Y\}.$$

Esto significa que en cualquier momento se sabe que un elemento x está en $X \cup Y$, por lo que puede concluir que x debe estar en X *o* x debe estar en Y. Inversamente, en cualquier momento se sabe que un x dado está en algún conjunto X o está en algún conjunto Y, así que se puede concluir que x está en $X \cup Y$. Así, para cualesquiera conjuntos X y Y y cualquier elemento x,

$$x \in X \cup Y \quad \text{si y sólo si,} \quad x \in X \text{ o } x \in Y.$$

Versiones procesadas de las definiciones de las demás operaciones de conjunto se deducen similarmente y se resumen a continuación.

Versiones procesadas de las definiciones de conjunto

Sean X y Y subconjuntos de un conjunto universo U y supongamos que x y y son elementos de U.

1. $x \in X \cup Y \quad \Leftrightarrow \quad x \in X$ o $x \in Y$
2. $x \in X \cap Y \quad \Leftrightarrow \quad x \in X$ y $x \in Y$
3. $x \in X - Y \quad \Leftrightarrow \quad x \in X$ o $x \notin Y$
4. $x \in X^c \quad \Leftrightarrow \quad x \notin X$
5. $(x, y) \in X \times Y \quad \Leftrightarrow \quad x \in X$ y $y \in Y$

Ejemplo 6.2.1 Demostración de una relación de subconjunto

Demuestre el teorema 6.2.1(l)*a*): Para todos los conjuntos A y B $A \cap B \subseteq A$.

Solución Comenzamos por dar una demostración del enunciado y, después se explica cómo puede usted obtener una demostración.

Demostración:

> Suponga que A y B son conjuntos cualesquiera y suponga que x es cualquier elemento de $A \cap B$. Entonces $x \in A$ y $x \in B$ por definición de intersección. En particular, $x \in A$. Por tanto, $A \cap B \subseteq A$.

La estructura subyacente de esta demostración no es difícil, pero es más complicada de lo que sugiere la brevedad de la demostración. Lo importante primero es darse cuenta de que el enunciado a demostrar es universal (éste dice que para *todos* los conjuntos A y B, $A \cap B \subseteq A$). La demostración, por tanto, tiene el siguiente esquema:

Punto de partida: Supongamos que A y B son conjuntos cualesquiera (particulares arbitrariamente elegidos).

Para demostrar: $A \cap B \subseteq A$,
Ahora para demostrar que $A \cap B \subseteq A$, debe demostrar que

$$\forall x, \text{ si, } x \in A \cap B \text{ entonces } x \in A.$$

Pero este enunciado también es universal. Así, para demostrarlo,

suponga que x es un elemento en $A \cap B$

y, después,

demuestre que x está en A.

Completar los pasos entre "suponga" y "demuestre" es fácil si utiliza la versión procesada de la definición de intersección: decir que x está en $A \cap B$ significa que

$$x \text{ está en } A \quad \text{y} \quad x \text{ está en } B.$$

Esto le permite finalizar la demostración al deducir que, en particular,

$$x \text{ está en } A,$$

que era lo que se quería demostrar. Observe que esta deducción es sólo un caso especial de la forma de argumento válido

$$p \wedge q$$
$$\therefore p.$$

En su libro *Gödel, Escher, Bach*,* Douglas Hofstadter introduce la regla de fantasía de la demostración matemática. Hofstadter indica que al iniciar un argumento matemático con un *sí*, *sea* o *suponga*, está aumentando a un mundo de fantasía donde no son todos sólo hechos verdaderos en el mundo real, sino todo lo que está suponiendo es verdadero. Una vez que esté en ese mundo, puede suponer algo más. Que envía a un mundo de sub-fantasía donde no sólo todo está en el verdadero mundo de fantasía, sino también la cosa nueva que está suponiendo. Por supuesto puede continuar entrando en nuevos mundos de sub-fantasía de esta manera indefinidamente. Se vuelve a un nivel más cercano al mundo real cada vez que deduce una conclusión que forma todo un enunciado si-entonces o universal verdadero. Su objetivo en una demostración es continuar deduciendo dichas conclusiones hasta que vuelva al mundo desde el que hizo su primera suposición.

En ocasiones, los problemas matemáticos se establecen en la siguiente forma:

Suponga que (*enunciado* 1). Demuestre que (*enunciado* 2).

Cuando se utiliza esta expresión, el autor propone al lector agregar el enunciado 1 a su conocimiento matemático general y no hacer referencia explícita de esto en la demostración. En términos de Hofstadter, el autor invita al lector a entrar a un mundo de fantasía donde el enunciado 1 se conoce como verdadero y demostrar el enunciado 2 en este mundo de fantasía. Por tanto, el solucionador de tal problema comenzaría con una demostración con el punto de partida para una demostración del enunciado 2. Consideremos, por ejemplo, la siguiente reexpresión del ejemplo 6.2.1:

> Supongamos que A y B son conjuntos arbitrariamente elegidos.
> Demuestre $A \cap B \subseteq A$.

La demostración comenzará con "Suponga que $x \in A \cap B$" en el *entendido* de que A y B ya se han elegido arbitrariamente.

La demostración del ejemplo 6.2.1 se llama un argumento del elemento ya que muestra un conjunto que es un subconjunto de otro para demostrar que todos los elementos de un conjunto son también un elemento en el otro. En matemáticas superiores, los argumentos de los elementos son el método estándar para establecer relaciones entre conjuntos. A los estudiantes de secundaria a menudo se les permite justificar la definición de las propiedades usando diagramas de Venn. Este método es atractivo, pero ser matemáticamente riguroso puede ser más complicado que lo que se podría esperar. Los diagramas de Venn apropiados pueden dibujarse para dos o tres conjuntos, pero las explicaciones verbales necesarias para justificar las conclusiones inferidas a partir de ellos son normalmente tan largas como la prueba de un simple elemento.

En general, los diagramas de Venn no son muy útiles cuando el número de conjuntos es de cuatro o más. Por ejemplo, si se cumple el requisito de que un diagrama de Venn debe mostrar toda intersección posible de los conjuntos, es imposible dibujar un diagrama de Venn simétrico para cuatro conjuntos o, de hecho, para cualquier número de conjuntos no primo. En 2002, el equipo de científicos y matemáticos formado por Carla Savage, Jerrold Griggs y por el estudiante Charles Killian resolvieron un problema abierto desde hace mucho tiempo demostrando que es posible dibujar un diagrama de Venn simétrico para cualquier número primo de conjuntos. Sin embargo, para $n > 5$, las imágenes resultantes son ¡muy complicadas! La existencia de tales diagramas simétricos tiene aplicaciones en el área de ciencias de la computación llamado teoría de códigos.

**Gödel, Escher, Bach: An Eternal Golden Braid* (Nueva York: Basic Books, 1979).

Identidades de conjuntos

Una **identidad** es una ecuación que es universalmente válida para todos los elementos de un conjunto. Por ejemplo, la ecuación $a + b = b + a$ es una identidad para números reales, porque es verdadera para todos los números reales a y b. La colección de propiedades del conjunto en el teorema siguiente consiste completamente de identidades de conjuntos. Es decir, son ecuaciones que son verdaderas en todos los conjuntos en algún conjunto universo.

Teorema 6.2.2 Identidades de conjuntos

Sean todos los conjuntos que se refieren a continuación subconjuntos de un conjunto universo U.

1. *Leyes conmutativas:* Para todos los conjuntos A y B,
$$a)\ A \cup B = B \cup A \quad \text{y} \quad b)\ A \cap B = B \cap A.$$
2. *Leyes asociativas:* Para todos los conjuntos A, B y C,
$$a)\ (A \cup B) \cup C = A \cup (B \cup C) \quad \text{y}$$
$$b)\ (A \cap B) \cap C = A \cap (B \cap C).$$
3. *Leyes distributivas:* En todos los conjuntos, A, B y C,
$$a)\ A \cup (B \cap C) = (A \cup B) \cap (A \cup C) \quad \text{y}$$
$$b)\ A \cap (B \cup C) = (A \cap B) \cup (A \cap C).$$
4. *Leyes de identidad:* Para todos los conjuntos A,
$$a)\ A \cup \emptyset = A \quad \text{y} \quad b)\ A \cap U = A.$$
5. *Leyes de complemento:*
$$a)\ A \cup A^c = U \quad \text{y} \quad b)\ A \cap A^c = \emptyset.$$
6. *Ley de complemento doble:* Para todos los conjuntos A,
$$(A^c)^c = A.$$
7. *Leyes de idempotencia:* Para todos los conjuntos A,
$$a)\ A \cup A = A \quad \text{y} \quad b)\ A \cap A = A.$$
8. *Leyes de universos acotados:* Para todos los conjuntos A,
$$a)\ A \cup U = U \quad \text{y} \quad b)\ A \cap \emptyset = \emptyset.$$
9. *Leyes de De Morgan:* Para todos los conjuntos A y B,
$$a)\ (A \cup B)^c = A^c \cap B^c \quad \text{y} \quad b)\ (A \cap B)^c = A^c \cup B^c.$$
10. *Leyes de absorción:* Para todos los conjuntos A y B,
$$a)\ A \cup (A \cap B) = A \quad \text{y} \quad b)\ A \cap (A \cup B) = A.$$
11. *Complementos de U y $\emptyset$:*
$$a)\ U^c = \emptyset \quad \text{y} \quad b)\ \emptyset^c = U.$$
12. *Ley de diferencia de conjuntos:* Para todos los conjuntos A y B,
$$A - B = A \cap B^c.$$

Demostración de identidades de conjunto

La conclusión de cada parte del teorema 6.2.2 es que un conjunto es igual a otro conjunto. Como notamos en la sección 6.1,

Dos conjuntos son iguales $\Leftrightarrow$ cada uno de ellos es un subconjunto del otro.

El método derivado de este hecho es el modo más básico para demostrar la igualdad de conjuntos.

Método básico para demostrar que los conjuntos son iguales

Sean los conjuntos X y Y. Para demostrar que $X = Y$:

1. Demuestre que $X \subseteq Y$.
2. Demuestre que $Y \subseteq X$.

Ejemplo 6.2.2 Demostración de una ley distributiva

Demuestre que para todos los conjuntos A, B y C,

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

Solución La demostración de este hecho es un poco más complicada que la demostración en el ejemplo 6.2.1, por lo que primero deduzca su estructura lógica, después encuentre los argumentos del núcleo y termine con una demostración formal como un resumen. Como en el ejemplo 6.2.1, el enunciado a ser probado es universal y por tanto, por el método de la generalización de lo particular a lo genérico, la demostración tiene el siguiente esquema:

Punto de partida: Supongamos que A, B y C son conjuntos arbitrariamente elegidos.

A demostrar: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Ahora dos conjuntos son iguales si y sólo si, cada uno es un subconjunto del otro. Por tanto, deben demostrarse los siguientes dos enunciados:

$$A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$$

y

$$(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C).$$

Demostrar la primera expresión requiere demostrar que

$$\forall x, \text{ si } x \in A \cup (B \cap C) \text{ entonces } x \in (A \cup B) \cap (A \cup C).$$

Demostrar la segunda expresión requiere demostrar que

$$\forall x, \text{ si } x \in (A \cup B) \cap (A \cup C) \text{ entonces } x \in A \cup (B \cap C).$$

Observe que ambas instrucciones son universales. Por lo que para demostrar la primera expresión,

suponga que se tiene cualquier elemento x en $A \cup (B \cap C)$,

y después, **demuestre** que $x \in (A \cup B) \cap (A \cup C)$.

Y para demostrar la segunda expresión,

suponga que se tiene cualquier elemento x en $(A \cup B) \cap (A \cup C)$

y después, **demuestre** que: $x \in A \cup (B \cap C)$.

En la figura 6.2.1, la estructura de la demostración se ilustra por el tipo de diagrama que se utiliza a menudo en relación con programas estructurados. El análisis en el diagrama reduce la demostración a dos tareas concretas: complete los pasos indicados por puntos en los centros de los dos cuadros de la figura 6.2.1.

Suponga que A, B y C son conjuntos. *[Demuestre* $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$. *Es decir, demuestre* $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$ *y* $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$.*]*

Demuestre $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$. *[Es decir, demuestre que* $\forall x$, *si* $x \in A \cup (B \cap C)$ *entonces* $x \in (A \cup B) \cap (A \cup C)$.*]*

Suponga $x \in A \cup (B \cap C)$. *[Demuestre* $x \in (A \cup B) \cap (A \cup C)$.*]*

$\vdots$

Por lo que $x \in (A \cup B) \cap (A \cup C)$.

Por tanto $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$.

Demuestre $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$. *[Es decir, demuestre que* $\forall x$, *si* $x \in (A \cup B) \cap (A \cup C)$ *entonces* $x \in A \cup (B \cap C)$.*]*

Suponga $x \in (A \cup B) \cap (A \cup C)$. *[Demuestre* $x \in A \cup (B \cap C)$.*]*

$\vdots$

Por lo que $x \in A \cup (B \cap C)$.

Por tanto $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$.

Por lo que $(A \cup B) \cap (A \cup C) = A \cup (B \cap C)$.

Figura 6.2.1

Completar los pasos que faltan en el cuadro superior:

Para completar estos pasos, se irá de la suposición de que $x \in A \cup (B \cap C)$ a la conclusión de que $x \in (A \cup B) \cap (A \cup C)$.

Ahora cuando $x \in A \cup (B \cap C)$, entonces por definición de unión, $x \in A$ o $x \in (B \cap C)$. Pero cualquiera de estas posibilidades podrían ser el caso ya que se supone que x se elige arbitrariamente del conjunto de $A \cup (B \cap C)$. Así que hay que demostrar que puede llegar a la conclusión de que $x \in (A \cup B) \cap (A \cup C)$ independientemente de si x se encuentra en A o x se encuentra en $B \cap C$. Esto conduce a separar su análisis en dos casos: $x \in A$ y $x \in (B \cap C)$.

En el caso $x \in A$, su objetivo es mostrar que $x \in (A \cup B) \cap (A \cup C)$, que significa que $x \in (A \cup B)$ y $x \in (A \cup C)$ (por definición de intersección). Pero cuando $x \in A$, ambos enunciados $x \in (A \cup B)$ y $x \in (A \cup C)$ son verdaderos en virtud de x que se está en A.

Similarmente, para el caso de que $x \in (B \cap C)$, su objetivo también es demostrar que $x \in (A \cup B) \cap (A \cup C)$, que significa que $x \in (A \cup B)$ y $x \in (A \cup C)$. Pero cuando $x \in (B \cap C)$, entonces $x \in B$ y $x \in C$ (por definición de intersección) y por tanto $x \in A \cup B$ (en virtud de estar en B) y $x \in A \cup C$ (en virtud de estar en C).

Este análisis muestra que, independientemente de si $x \in A$ o $x \in B \cap C$, se obtiene la conclusión $x \in (A \cup B) \cap (A \cup C)$. Por tanto puede completar los pasos que se indican en el cuadro interior anterior.

Completando los pasos que faltan en el cuadro inferior:

Para completar estos pasos, necesita ir de la suposición de que $x \in (A \cup B) \cap (A \cup C)$ a la conclusión de que $x \in A \cup (B \cap C)$.

Cuando $x \in (A \cup B) \cap (A \cup C)$ es natural considerar los dos casos $x \in A$ y $x \notin A$. porque cuando x se encuentra en A, entonces el enunciado "$x \in A$ o $x \in B \cap C$" es sin duda verdadero y así x está en $A \cup (B \cap C)$ por definición de unión. Por tanto, sólo se necesita demostrar que aún en el caso cuando x no está en A y $x \in (A \cup B) \cap (A \cup C)$ y, entonces, $x \in A \cup (B \cap C)$.

Así suponiendo que x no está en A. Ahora digamos que $x \in (A \cup B) \cap (A \cup C)$ significa que $x \in A \cup B$ y que $x \in A \cup C$ (por definición de intersección). Pero cuando $x \in A \cup B$, entonces x está en al menos uno de A o B, así que puesto que x no está en A entonces, x debe estar en B. Similarmente, cuando $x \in A \cup C$, entonces x está al menos en uno en A o en C, así como x no está en A, entonces, x debe estar en C. Por tanto, cuando x no está en A y $x \in (A \cup B) \cap (A \cup C)$, entonces x está tanto en B como en C, lo que significa que $x \in B \cap C$. Se deduce que el enunciado "$x \in A$ o $x \in B \cap C$" es verdadero y por tanto $x \in A \cup (B \cap C)$ por definición de unión.

Este análisis muestra que si $x \in (A \cup B) \cap (A \cup C)$, entonces independientemente de si $x \in A$ o $x \notin A$, se puede concluir que $x \in A \cup (B \cap C)$. Por tanto, puede completar los pasos del cuadro interior de la parte inferior.

A continuación se muestra una demostración formal.

Teorema 6.2.2(3)*a*) Una ley distributiva para conjuntos

Para todos los conjuntos A, B y C,

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

Demostración:

Supongamos que A y B son conjuntos.

Demostración de que $A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$:

Suponga que $x \in A \cup (B \cap C)$. Por definición de unión, $x \in A$ o $x \in B \cap C$.

Caso 1 ($x \in A$): Ya que $x \in A$, entonces $x \in A \cup B$ por definición de unión y también $x \in A \cup C$ por definición de unión. Por tanto $x \in (A \cup B) \cap (A \cup C)$ por definición de intersección.

Caso 2 ($x \in B \cap C$): Dado que $x \in B \cap C$, entonces $x \in B$ y $x \in C$ por definición de intersección. Ya que $x \in B$, $x \in A \cup B$ y puesto que $x \in C$, $x \in A \cup C$, ambos por la definición de unión. Por tanto $x \in (A \cup B) \cap (A \cup C)$ por definición de intersección.

En ambos casos, $x \in (A \cup B) \cap (A \cup C)$. Por tanto $A \cup (B \cap C \subseteq (A \cup B) \cap (A \cup C)$ por definición del subconjunto.

Demostración de que $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$:

Suponga que $x \in (A \cup B) \cap (A \cup C)$. Por definición de intersección, $x \in A \cup B$ y $x \in A \cup C$. Considere los dos casos $x \in A$ y $x \notin A$.

Caso 1 ($x \in A$): Dado que $x \in A$, podemos inmediatamente concluir que $x \in A \cup (B \cap C)$ por definición de unión.

Caso 2 ($x \notin A$): Ya que $x \in A \cup B$, x está en al menos uno de A o B. Pero x no está en A; por tanto, x está en B. Similarmente, puesto que $x \in A \cup C$, x está al menos en uno de A o C. Pero x no está en A; por tanto x está en C. Hemos demostrado que tanto $x \in B$ y $x \in C$ y por tanto por definición de intersección, $x \in B \cap C$. Se deduce por definición de unión que $x \in A \cup (B \cap C)$.

En ambos casos $x \in A \cup (B \cap C)$. Por tanto, por definición de subconjunto $(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$.

Conclusión: Dado que se han demostrado ambas relaciones de subconjuntos, se deduce por definición de igualdad de conjuntos que $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

■

En el estudio de inteligencia artificial, los tipos de razonamiento utilizados anteriormente para obtener la demostración de la ley distributiva se llaman *encadenamiento hacia adelante* y *encadenamiento hacia atrás*. Lo primero que se muestra es visto como un objetivo a ser alcanzado a partir de una cierta posición inicial: el punto de partida. El análisis de este objetivo conduce a la realización de que si se logra un determinado puesto, entonces se alcanzará el objetivo. Llame a este trabajo sub-objetivo 1: SG_1. (Por ejemplo, si el objetivo es mostrar que $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$, entonces SG_1 mostraría que cada conjunto es un subconjunto del otro.) Análisis de SG_1 muestra que cuando aún se ha completado otro puesto, SG_1 se alcanzará. Llame a este sub-objetivo de trabajo 2: SG_2. Continuando de este modo, se construye una cadena de argumento que conduce hacia atrás del objetivo.

$$\boxed{\text{punto de partida}} \qquad \rightarrow SG_3 \rightarrow SG_2 \rightarrow SG_1 \rightarrow \boxed{\text{objetivo}}$$

En cierto momento, el encadenamiento hacia atrás se hace difícil, pero el análisis del actual sub-objetivo sugiere que puede ser accesible por una línea directa de argumento, llamado encadenamiento hacia adelante, desde el punto de partida. Con la información que se presenta en el punto de partida, se deduce otra pieza de información, I_1, de esa otra pieza de información, se deduce I_2 y así sucesivamente hasta que finalmente se alcanza uno de los sub-objetivos. Esto completa la cadena y demuestra el teorema. Una cadena completa se ilustra a continuación.

$$\boxed{\text{punto de partida}} \rightarrow I_1 \rightarrow I_2 \rightarrow I_3 \rightarrow I_4 \rightarrow SG_3 \rightarrow SG_2 \rightarrow SG_1 \rightarrow \boxed{\text{objetivo}}$$

Ya que el conjunto complemento se define en términos de *no* y ya que las uniones e intersecciones se definen en términos de *o* y *y*, no es de extrañar que existen análogos de leyes de De Morgan de la lógica para conjuntos.

Ejemplo 6.2.3 Demostración de una de las leyes de De Morgan para conjuntos

Demuestre que para todos los conjuntos A y B $(A \cup B)^c = A^c \cap B^c$.

Solución Como en los ejemplos anteriores, el enunciado a demostrar es universal, por lo que el punto de partida de la demostración y la conclusión que se muestra son las siguientes:

Punto de partida: Supongamos que A y B son conjuntos arbitrariamente elegidos.

A demostrar: $(A \cup B)^c = A^c \cap B^c$

Para hacer esto, se debe demostrar que $(A \cup B)^c \subseteq A^c \cap B^c$ y que $A^c \cap B^c \subseteq (A \cup B)^c$. Demostrar la primera expresión significa demostrar que

$$\forall x, \text{ si } x \in (A \cup B)^c \text{ entonces } x \in A^c \cap B^c.$$

Y demostrar la segunda expresión significa demostrar que,

$$\forall x, \text{ si } x \in A^c \cap B^c \text{ entonces } x \in (A \cup B)^c.$$

Puesto que cada uno de estos enunciados es universal y condicional, para la primera expresión,

suponga que $x \in (A \cup B)^c$,

y, después **demuestre** que $x \in A^c \cap B^c$.

Y para la segunda expresión,

suponga $x \in A^c \cap B^c$,

y, después, **demuestre** que $x \in (A \cup B)^c$.

Para completar los pasos de estos argumentos, utilice las versiones procesadas de las definiciones de complemento, unión e intersección y en qué puntos cruciales utiliza las leyes de De Morgan de lógica.

Teorema de 6.2.2(9*a*) Una ley de De Morgan para conjuntos

Para todos los conjuntos A y B $(A \cup B)^c = A^c \cap B^c$.

Demostración:
Suponga que A y B son conjuntos.

Demostración de que $(A \cup B)^c \subseteq A^c \cap B^c$:
[Debemos demostrar que $\forall x$, si $x \in (A \cup B)^c$ entonces $x \in A^c \cap B^c$.]
Supongamos que $x \in (A \cup B)^c$. *[Debemos demostrar que $x \in A^c \cap B^c$.]* Por definición de complemento,

$$x \notin A \cup B.$$

Pero decir que $x \notin A \cup B$ significa que

es falso que (x está en A o x está en B).

Por las leyes de De Morgan de la lógica, esto implica que

x no está en A y x no está en B,

que se puede escribir $x \notin A$ y $x \notin B$.

Así $x \in A^c$ y $x \in B^c$ por definición de complemento. Se deduce, por definición de intersección, que $x \in A^c \cap B^c$ *[como se quería demostrar]*. Así $(A \cup B)^c \subseteq A^c \cap B^c$ por definición de subconjunto.

Demostración de que $A^c \cap B^c \subseteq (A \cup B)^c$:
[Debemos demostrar que $\forall x$, si $x \in A^c \cap B^c$ entonces $x \in (A \cup B)^c$.]
Suponga que $x \in A^c \cap B^c$. *[Debemos demostrar que $x \in (A \cup B)^c$.]* Por definición de intersección, $x \in A^c$ y $x \in B^c$ y por definición de complemento,

$$x \notin A \quad \text{y} \quad x \notin B.$$

En otras palabras, x no está en A y x no está en B.

Por las leyes de lógica de De Morgan, esto implica que

es falso que (x está en A o x está en B),

que se puede escribir como $x \notin A \cup B$

por definición de unión. Por tanto, por definición de complemento, $x \in (A \cup B)^c$ *[como se quería demostrar]*. Se deduce que $A^c \cap B^c \subseteq (A \cup B)^c$ por definición del subconjunto.

Conclusión: Ya que ambas expresiones de conjuntos se han demostrado $(A \cup B)^c = A^c \cap B^c$ por definición de la igualdad del conjunto.

La propiedad del conjunto en el siguiente teorema dice que, si un conjunto es un sub-conjunto del otro, entonces su intersección es el menor de los dos conjuntos y su unión es la más grande de los dos conjuntos.

Teorema de 6.2.3 Intersección y unión con un sub-conjunto

Para cualesquiera conjuntos A y B, si $A \subseteq B$, entonces

$$a)\ A \cap B = A \quad \text{y} \quad b)\ A \cup B = B.$$

Demostración:

Parte a): Suponga que A y B son conjuntos con $A \subseteq B$. Para demostrar la parte $a)$ debemos demostrar que tanto $A \cap B \subseteq A$ y que $A \subseteq A \cap B$. Ya sabemos $A \cap B \subseteq A$ por inclusión de la propiedad de intersección. Para demostrar que $A \subseteq A \cap B$, sea $x \in A$. *[Debemos demostrar que $x \in A \cap B$.]* Ya que $A \subseteq B$, entonces también $x \in B$. Por tanto

$$x \in A \quad \text{y} \quad x \in B$$

y por tanto $$x \in A \cap B$$

por definición de intersección *[como se quería demostrar]*.

Demostración:

Parte b): La demostración de la parte $b)$ se deja como ejercicio.

■

Conjunto vacío

En la sección 6.1 se introdujo el concepto de un conjunto sin elementos y se prometió que en esta sección mostraríamos que es un conjunto único. Para ello, empezamos con la más básica (y la más extraña) propiedad de un conjunto sin elementos: es un subconjunto de todo conjunto. Para ver por qué esto es verdadero, sólo pregúntese, ¿podría ser falso?, ¿podría haber un conjunto sin elementos que *no* sea un sub-conjunto de un conjunto dado? El hecho fundamental es que la negación de un enunciado universal es existencial: si un conjunto B no es un sub-conjunto de un conjunto A, entonces existe un elemento en B que no está en A. Pero si B no tiene algún elemento, entonces no puede existir algún elemento.

Teorema 6.2.4 Un conjunto sin elementos es un subconjunto de cada conjunto

Si E es un conjunto sin elementos y A es cualquier conjunto, entonces, $E \subseteq A$.

Demostración (por contradicción):

Supongamos que no. *[Tomemos la negación del teorema y supongamos que es verdadera.]* Supongamos que existe un conjunto E sin elementos y un conjunto A tal que $E \not\subseteq A$. *[Debemos deducir una contradicción.]* Entonces habría un elemento de E que no es un elemento de A *[por definición de sub-conjunto]*. Pero no puede haber algún elemento ya que E no tiene elementos. Esto es una contradicción. *[Por tanto la suposición de que hay conjuntos E y A, donde E no tiene elementos y $E \not\subseteq A$, es falso y por tanto el teorema es verdadero.]*

La veracidad del teorema 6.2.4 también puede entenderse apelando la noción de verdad vacía. Si E es un conjunto sin elementos y A es cualquier conjunto, entonces decir que $E \subseteq A$ es lo mismo que decir que

$$\forall x, \text{ si } x \in E, \text{ entonces } x \in A.$$

Pero puesto que E no tiene elementos, este enunciado condicional es vacuamente verdadero.

¿Cuántos conjuntos sin elementos existen? Sólo uno.

Corolario 6.2.5 Unicidad del conjunto vacío

Hay sólo un conjunto sin elementos.

Demostración:

Suponga que E_1 y E_2 son dos conjuntos sin elementos. Por el teorema 6.2.4, $E_1 \subseteq E_2$ puesto que E_1 no tiene elementos. E_2 tampoco tiene elementos. Por tanto, $E_1 = E_2$ por definición de igualdad de conjuntos.

Se deduce del corolario 6.2.5 que el conjunto de los elefantes rosa es igual al conjunto de todos los números reales cuyo cuadrado es -1 ¡porque cada conjunto no tiene elementos! Dado que sólo hay un conjunto sin elementos, se justifica llamarlo por un nombre especial, conjunto vacío (o conjunto nulo) y se denota con el símbolo especial $\emptyset$.

Observe que mientras $\emptyset$ es el conjunto sin elementos, el conjunto $\{\emptyset\}$ tiene un elemento, el conjunto vacío. Esto es similar a la convención en la programación en los lenguajes de computadora LISP y Scheme, en los que ( ) indica la lista vacía y (( )) denota la lista cuyo único elemento es la lista vacía.

Suponga que necesita mostrar que un cierto conjunto equivale al conjunto vacío. Por el corolario 6.2.5 es suficiente para demostrar que el conjunto no tiene elementos. Ya que puesto que sólo hay un conjunto sin elementos (a saber, $\emptyset$), si el conjunto dado no tiene elementos y, entonces, debe ser igual a $\emptyset$.

Método del elemento para demostrar que un conjunto es igual al conjunto vacío

Demostrar que un conjunto X es igual al conjunto vacío $\emptyset$, equivale a demostrar que X no tiene elementos. Para esto, suponga que X tiene un elemento y se deduce una contradicción.

Ejemplo 6.2.4 Demostración de que un conjunto es vacío

Demuestre el teorema de 6.2.2(8)*b*). Es decir, demuestre que para cualquier conjunto A, $A \cap \emptyset = \emptyset$.

Solución Sea A un conjunto *[particular arbitrariamente elegido]*. Para demostrar que $A \cap \emptyset = \emptyset$, es suficiente para demostrar que $A \cap \emptyset$ no tiene elementos *[por el método del elemento para la demostración de un conjunto igual al conjunto vacío]*. Suponga que no. Es decir, suponga que hay un elemento x tal que $x \in A \cap \emptyset$. Entonces, por definición de intersección, $x \in A$ y $x \in \emptyset$. En particular, $x \in \emptyset$. Pero esto es imposible, ya que $\emptyset$ no tiene elementos. *[Esta contradicción demuestra que la suposición de que hay un elemento x en $A \cap \emptyset$ es falso. Por lo que $A \cap \emptyset$ no tiene elementos, como se quería demostrar.]* Por tanto $A \cap \emptyset = \emptyset$. ■

Ejemplo 6.2.5 Una demostración para un enunciado condicional

Demuestre que para todos los conjuntos A, B y C, si $A \subseteq B$ y $B \subseteq C^c$, entonces $A \cap C = \emptyset$.

Solución Puesto que el enunciado es universal y condicional, se inicia con el método de demostración directa:

Suponga que A, B y C son conjuntos arbitrariamente elegidos
que satisfacen la condición: A $\subseteq$ B y $B \subseteq C^c$.

Demuestre que $A \cap C = \emptyset$.

Dado que la conclusión de que se muestra es que un conjunto dado está vacío, puede utilizar el principio por demostrar que un conjunto es igual al conjunto vacío. A continuación se muestra una demostración completa.

Proposición 6.2.6

Para todos los conjuntos A, B y C, si $A \subseteq B$ y $B \subseteq C^c$, entonces, $A \cap C = \emptyset$.

Demostración:

Suponga que A, B y C son conjuntos cualesquiera tales que $A \subseteq B$ y $B \subseteq C^c$. Debemos demostrar que $A \cap C = \emptyset$. Supongamos que no. Es decir, supongamos que hay un elemento x en $A \cap C$. Por definición de intersección, $x \in A$ y $x \in C$. Entonces, ya que $A \subseteq B$, $x \in B$ por definición de subconjunto. También, puesto que $B \subseteq C^c$, entonces también por definición de subconjunto $x \in C^c$. De la definición de complemento se tiene que $x \notin C$. Por tanto, $x \in C$ y $x \notin C$, que es una contradicción. Por tanto la suposición de que hay un elemento x en $A \cap C$ es falsa y así $A \cap C = \emptyset$ *[como se quería demostrar]*.

■

Ejemplo 6.2.6 Una ley distributiva generalizada

Demuestre que para todos los conjuntos A y $B_1, B_2, B_3, \ldots, B_n$,

$$A \cup \left(\bigcap_{i=1}^{n} B_i \right) = \bigcap_{i=1}^{n} (A \cup B_i).$$

Solución Compare esta demostración con la que se da en el ejemplo 6.2.2. Aunque la notación es más compleja, las ideas básicas son las mismas.

Demostración:

Supongamos que A y $B_1, B_2, B_3, \ldots, B_n$ son conjuntos cualesquiera.

Parte 1. Demostración de que $A \cup \left(\bigcap_{i=1}^{n} B_i\right) \subseteq \bigcap_{i=1}^{n}(A \cup B_i)$**:**

Suponga que x es cualquier elemento en $A \cup \left(\bigcap_{i=1}^{n} B_i\right)$. *[Debemos demostrar que x está en* $\bigcap_{i=1}^{n}(A \cup B_i)$ *.]*

Por definición de unión, $x \in A$ o $x \in \bigcap_{i=1}^{n} B_i$.

Caso 1. $x \in A$**:** En este caso, es verdadero por definición de unión que para todo $i = 1, 2, \ldots, n$, $x \in A \cup B_i$. Por tanto $x \in \bigcap_{i=1}^{n}(A \cup B_i)$.

Caso 2. $x \in \bigcap_{i=1}^{n} B_i$**:** En este caso, por definición de intersección general, tenemos que para todos los enteros $i = 1, 2, \ldots, n$, $x \in B_i$. Por tanto, por definición de unión, para todos los enteros $i = 1, 2, \ldots, n$, $x \in A \cup B_i$ y por tanto, por definición de intersección general, $x \in \bigcap_{i=1}^{n}(A \cup B_i)$. Por tanto, en cualquier caso, $x \in \bigcap_{i=1}^{n}(A \cup B_i)$ *[como se quería demostrar]*.

Parte 2. Demostración de que $\bigcap_{i=1}^{n}(A \cup B_i) \subseteq A \cup \left(\bigcap_{i=1}^{n} B_i\right)$**:**

Suponga que x es cualquier elemento en $\bigcap_{i=1}^{n}(A \cup B_i)$. *[Tenemos que demostrar que x está en* $A \cup \left(\bigcap_{i=1}^{n} B_i\right)$*.]*

Por definición de intersección, $x \in A \cup B_i$ para todo entero $i = 1, 2, \ldots, n$. Ya sea $x \in A$ o $x \notin A$.

Caso 1. $x \in A$**:** En este caso, $x \in A \cup \left(\bigcap_{i=1}^{n} B_i\right)$, por definición de unión.

Caso 2. $x \notin A$**:** Por definición de intersección, $x \in A \cup B_i$ para todo entero $i = 1, 2, \ldots, n$. Ya que $x \notin A$, x debe estar en cada B_i para cada entero $i = 1, 2, \ldots, n$. Por tanto, por definición de intersección, $x \in \bigcap_{i=1}^{n} B_i$ y así, por definición de unión, $x \in A \cup \left(\bigcap_{i=1}^{n} B_i\right)$.

***Conclusión*:** Puesto que ambos conjuntos de expresiones están demostradas, se deduce por definición de igualdad de conjuntos que $A \cup \left(\bigcap_{i=1}^{n} B_i\right) = \bigcap_{i=1}^{n}(A \cup B_i)$. ■

Autoexamen

1. Demuestre que un conjunto X es un subconjunto de un conjunto $A \cap B$, suponga que x es cualquier elemento de X y demuestre que $x \in A$ _____ $x \in B$.
2. Demuestre que un conjunto X es un subconjunto de un conjunto $A \cup B$, suponga que x es cualquier elemento de X y demuestre que $x \in A$ _____ $x \in B$.
3. Demuestre que un conjunto $A \cup B$ es un subconjunto de un conjunto X, comience con cualquier elemento x en $A \cup B$ y considere los dos casos _____ y _____. A continuación, demuestre que en ambos casos _____.
4. Demuestre que un conjunto $A \cap B$ es un subconjunto de un conjunto X, suponga que _____ y demuestre que _____.
5. Demuestre que un conjunto X es igual a un conjunto Y, demuestre que _____ y que _____.
6. Demuestre que un conjunto X que no es igual a un conjunto Y, necesita encontrar un elemento que esté en _____ y no _____ o que se encuentra en _____ y no _____.

Conjunto de ejercicios 6.2

1. **a.** Decir que un elemento está en $A \cap (B \cup C)$ significa que está en __(1)__ y __(2)__.
   b. Decir que un elemento está en $(A \cap B) \cup C$ significa que está en __(1)__ o en __(2)__.
   c. Decir que un elemento está en $A - (B \cup C)$ significa que está en __(1)__ y no en __(2)__.
2. Los siguientes son dos demostraciones que para todos los conjuntos A y B, $A - B \subseteq A$. La primera es menos formal y la segunda es más formal. Complete los espacios en blanco.
   a. **Demostración**: Suponga que A y B son conjuntos cualesquiera. Para demostrar que $A - B \subseteq A$, tenemos que demostrar que cada elemento en __(1)__ está en __(2)__. Pero cualquier elemento

en $A - B$ está en __(3)__ y no en __(4)__ (por definición de $A - B$). En particular, dicho elemento está en A.

b. **Demostración:** Suponga que A y B son conjuntos cualesquiera y que $x \in A - B$. *[Debemos demostrar que __(1)__.]* Por definición de diferencia, $x \in$ __(2)__ y $x \notin$ __(3)__. En particular, $x \in$ __(4)__ *[que es lo que se quería demostrar].*

3. La siguiente es una demostración que para todos los conjuntos A, B y C, si $A \subseteq B$ y $B \subseteq C$, entonces $A \subseteq C$. Complete los espacios en blanco.

Demostración: Supongamos que A, B y C son conjuntos y $A \subseteq B$ y $B \subseteq C$. Para mostrar que $A \subseteq C$, tenemos que demostrar que cada elemento en __(a)__ está en __(b)__. Pero dado cualquier elemento en A, ese elemento está también en __(c)__ (porque $A \subseteq B$), por lo que ese elemento está también en __(d)__ (porque __(e)__). Por tanto $A \subseteq C$.

4. La siguiente es una demostración que para todos los conjuntos A y B. Si $A \subseteq B$, entonces $A \cup B \subseteq B$. Complete los espacios en blanco.

Demostración: Suponga que A y B son conjuntos cualesquiera y $A \subseteq B$. *[Tenemos que demostrar que __(a)__.]* Sea que $x \in$ __(b)__. *[Tenemos que demostrar que __(c)__.]* Por definición de unión, $x \in$ __(d)__ __(e)__ $x \in$ __(f)__. En caso de que $x \in$ __(g)__, entonces ya que $A \subseteq B$, $x \in$ __(h)__. En caso de que $x \in B$, entonces claramente $x \in B$. Así en cualquier caso, $x \in$ __(i)__ *[como se quería demostrar].*

5. Demuestre que para todos los conjuntos A y B $(B - A) = B \cap A^c$.

H 6. La siguiente es una demostración de que para cualesquiera conjuntos A, B y C, $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$. Complete los espacios en blanco.

Demostración: Supongamos que A, B y C son conjuntos cualesquiera.

1) Demostración de que $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$:
Sea $x \in A \cap (B \cup C)$. *[Debemos demostrar que $x \in$ __(a)__.]* Por definición de intersección, $x \in$ __(b)__ y $x \in$ __(c)__. Por tanto, $x \in A$ y, por definición de unión, $x \in B$ o __(d)__.

***Caso 1* ($x \in A$ y $x \in B$):** en este caso, por definición de intersección, $x \in$ __(e)__ y así, por definición de unión, $x \in (A \cap B) \cup (A \cap C)$.

***Caso 2* ($x \in A$ y $x \in C$):** En este caso, __(f)__.
Así en cualquier caso, $x \in (A \cap B) \cup (A \cap C)$ *[como se quería demostrar].*
[Así $A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)$ por definición de subconjunto.]

2) $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$:
Sea $x \in (A \cap B) \cup (A \cap C)$. *[Debemos demostrar que __(a)__.]* Por definición de unión, $x \in A \cap B$ __(b)__ $x \in A \cap C$.

***Caso 1* $x \in (A \cap B)$:** En este caso, por definición de intersección, $x \in A$ __(c)__ $x \in B$. Ya que $x \in B$, entonces, por definición de unión, $x \in B \cup C$. Por lo que $x \in A$ y $x \in B \cup C$ y así, por definición de intersección, $x \in$ __(d)__ .

***Caso 2* ($x \in A \cap C$):** En este caso, __(e)__.
En cualquier caso, $x \in A \cap (B \cup C)$ *[como se quería demostrar]. [Así $(A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)$ por definición de subconjunto.]*

3) *Conclusión*: *[Ya que se han demostrado ambas relaciones del subconjunto, se deduce, por definición de igualdad de conjuntos, que __(a)__.]*

Use un argumento de elemento para demostrar cada enunciado en los ejercicios del 7 al 19. Suponga que todos los conjuntos son subconjuntos de un conjunto universo U.

H 7. Para todos los conjuntos A y B $(A \cap B)^c = A^c \cup B^c$.

8. Para todos los conjuntos A y B $(A \cap B) \cup (A \cap B^c) = A$.

H 9. Para todos los conjuntos A, B y C

$$(A - B) \cup (C - B) = (A \cup C) - B.$$

10. Para todos los conjuntos A, B y C

$$(A - B) \cap (C - B) = (A \cap C) - B.$$

H 11. Para todos los conjuntos A y B $A \cup (A \cap B) = A$.

12. Para todo conjunto A, $A \cup \emptyset = A$.

13. Para todos los conjuntos A, B y C, si $A \subseteq B$ entonces $A \cap C \subseteq B \cap C$.

14. Para todos los conjuntos A, B y C, si $A \subseteq B$ entonces $A \cup C \subseteq B \cup C$.

15. Para todos los conjuntos A y B, si $A \subseteq B$ entonces $B^c \subseteq A^c$.

H 16. Para todos los conjuntos A, B y C, si $A \subseteq B$ y $A \subseteq C$ entonces $A \subseteq B \cap C$.

17. Para todos los conjuntos A, B y C, si $A \subseteq C$ y $B \subseteq C$ entonces $A \cup B \subseteq C$.

18. Para todos los conjuntos A, B y C

$$A \times (B \cup C) = (A \times B) \cup (A \times C).$$

19. Para todos los conjuntos A, B y C

$$A \times (B \cap C) = (A \times B) \cap (A \times C).$$

20. Encuentre el error en la siguiente "demostración" que para todos los conjuntos A, B y C, si $A \subseteq B$ y $B \subseteq C$ entonces $A \subseteq C$.

"Demostración: Suponga que A, B y C son conjuntos tales que $A \subseteq B$ y $B \subseteq C$. Ya que $A \subseteq B$, hay un elemento x tal que $x \in A$ y $x \in B$. Ya que $B \subseteq C$, hay un elemento x tal que $x \in B$ y $x \in C$. Por lo que hay un elemento x tal que $x \in A$ y $x \in C$ y por tanto $A \subseteq C$ ".

H 21. Encuentre el error en la siguiente "demostración".

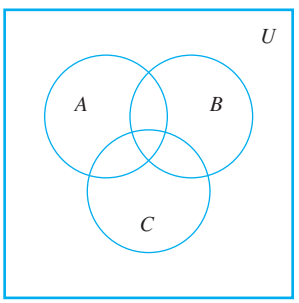
"**Teorema**": Para todos los conjuntos A y B, $A^c \cup B^c \subseteq (A \cup B)^c$.

"Demostración: Supongamos que A y B son conjuntos y $x \in A^c \cup B^c$. Entonces $x \in A^c$ o $x \in B^c$ por definición de unión. Se deduce que $x \notin A$ o $x \notin B$ por definición de complemento y así $x \notin A \cup B$ por definición de unión. Por lo que, $x \in (A \cup B)^c$ por definición de complemento y por tanto $A^c \cup B^c \subseteq (A \cup B)^c$".

22. Determine el error en la siguiente "demostración" que para todos los conjuntos A y B $(A - B) \cup (A \cap B) \subseteq A$.

"Demostración: Suponga que A y B son conjuntos y suponga que $x \in (A - B) \cup (A \cap B)$. Si $x \in A$ entonces $x \in A - B$. Entonces, por definición de diferencia $x \in A$ y $x \notin B$. Por tanto $x \in A$ y así por definición de subconjunto $(A - B) \cup (A \cap B) \subseteq A$".

23. Considere el siguiente diagrama de Venn.



a. En una copia del diagrama, ilustre una de las leyes distributivas sombreando la región correspondiente $A \cup (B \cap C)$ y en otra $(A \cup B) \cap (A \cup C)$.
b. En una copia del diagrama ilustre la otra ley distributiva sombreando la región correspondiente a $A \cap (B \cup C)$ y en otra $(A \cap B) \cup (A \cap C)$.
c. En una copia del diagrama ilustre una de las leyes de De Morgan sombreando la región correspondiente a $(A \cup B)^c$ y en otra $A^c \cap B^c$. (Quite al conjunto C de sus diagramas.)
d. En una copia del diagrama ilustre otra de las leyes de De Morgan sombreando la región correspondiente a $(A \cap B)^c$ y en otra $A^c \cup B^c$. (Quite al conjunto C de sus diagramas.)

24. Complete los espacios en blanco en la siguiente demostración que para todos los conjuntos A y B, $(A - B) \cap (B - A) = \emptyset$.

Demostración: Sean A y B conjuntos cualesquiera y suponga que $(A - B) \cap (B - A) \neq \emptyset$. Es decir, suponga que hay un elemento x en __(a)__. Por definición de __(b)__, $x \in A - B$ y $x \in$ __(c)__. Entonces, por definición de diferencia, $x \in A$ y $x \notin B$ y $x \in$ __(d)__ y $x \notin$ __(e)__. En particular $x \in A$ y $x \notin$ __(f)__ que es una contradicción. Por tanto *[la suposición de que* $(A - B) \cap (B - A) \neq \emptyset$ *es falso y así]* __(g)__.

Utilice el método del elemento probando que un conjunto es igual al conjunto vacío para demostrar cada enunciado de los ejercicios 25 al 35. Se supone que todos los conjuntos son subconjuntos de un conjunto universo U.

25. Para todos los conjuntos A y B, $(A \cap B) \cap (A \cap B^c) = \emptyset$.

26. Para todos los conjuntos A, B y C,

$$(A - C) \cap (B - C) \cap (A - B) = \emptyset.$$

27. Para todos los subconjuntos A de un conjunto universo U, $A \cap A^c = \emptyset$.

28. Si U denota un conjunto universo, entonces $U^c = \emptyset$.

29. Para todos los conjuntos A, $A \times \emptyset = \emptyset$.

30. Para todos los conjuntos A y B, si $A \subseteq B$ entonces $A \cap B^c = \emptyset$.

31. Para todos los conjuntos A y B, si $B \subseteq A^c$ entonces $A \cap B = \emptyset$.

32. Para todos los conjuntos A, B y C, si $A \subseteq B$ y $B \cap C = \emptyset$ entonces $A \cap C = \emptyset$.

33. Para todos los conjuntos A, B y C, si $C \subseteq B - A$, entonces, $A \cap C = \emptyset$.

34. Para todos los conjuntos A, B y C,

si $B \cap C \subseteq A$, entonces $(C - A) \cap (B - A) = \emptyset$.

35. Para todos los conjuntos A, B, C y D,

si $A \cap C = \emptyset$, entonces $(A \times B) \cap (C \times D) = \emptyset$.

Demuestre cada enunciado de los ejercicios del 36 al 41.

***H* 36.** Para todos los conjuntos A y B,
a. $(A - B) \cup (B - A) \cup (A \cap B) = A \cup B$
b. Los conjuntos $(A - B)$, $(B - A)$ y $(A \cap B)$ son mutuamente disjuntos.

37. Para todo entero $n \geq 1$, si A y $B_1, B_2, B_3, \ldots$ son conjuntos cualesquiera, entonces,

$$A \cap \left(\bigcup_{i=1}^{n} B_i \right) = \bigcup_{i=1}^{n} (A \cap B_i).$$

***H* 38.** Para todo entero $n \geq 1$, si $A_1, A_2, A_3, \ldots$ y B son conjuntos cualesquiera, entonces,

$$\bigcup_{i=1}^{n} (A_i - B) = \left(\bigcup_{i=1}^{n} A_i \right) - B.$$

39. Para todo entero $n \geq 1$, si $A_1, A_2, A_3, \ldots$ y B son conjuntos cualesquiera, entonces

$$\bigcap_{i=1}^{n} (A_i - B) = \left(\bigcap_{i=1}^{n} A_i \right) - B.$$

40. Para todo entero $n \geq 1$, si A y $B_1, B_2, B_3, \ldots$ son conjuntos cualesquiera, entonces

$$\bigcup_{i=1}^{n} (A \times B_i) = A \times \left(\bigcup_{i=1}^{n} B_i \right).$$

41. Para todo entero $n \geq 1$, si A y $B_1, B_2, B_3, \ldots$ son conjuntos cualesquiera, entonces

$$\bigcap_{i=1}^{n} (A \times B_i) = A \times \left(\bigcap_{i=1}^{n} B_i \right).$$

Respuestas del autoexamen

1. y 2. o 3. $x \in A$; $x \in B$; $x \in X$ 4. $x \in A \cap B$ (O: x es un elemento tanto de A como de B); $x \in X$ 5. $X \subseteq Y$; $Y \subseteq X$ 6. X; en Y; Y; en X

6.3 Refutaciones, demostraciones algebraicas y álgebra booleana

Si un hecho está en contra del sentido común y, sin embargo, nos vemos obligados a aceptar y hacer frente a este hecho, aprendemos a alterar nuestra noción del sentido común.
—*La experiencia matemática*, Phillip J. Davis y Reuben Hersh, 1981

En la sección 6.2 dimos ejemplos sólo de propiedades de conjuntos que eran verdaderas. Sin embargo, en ocasiones, una propiedad propuesta es falsa. Comenzamos esta sección analizando cómo refutar una propiedad propuesta. Después demostraremos un teorema importante sobre el conjunto potencia de un conjunto y después analizamos un método "algebraico" para deducir propiedades nuevas de conjuntos a partir de las propiedades que ya se sabe que son verdaderas. Finalizamos la sección con una introducción al álgebra booleana.

Refutación de una supuesta propiedad de un conjunto

Recuerde que para demostrar que un enunciado universal es falso, es suficiente con encontrar un ejemplo (llamado un contraejemplo) para el cual es falso.

Ejemplo 6.3.1 Determinación de un contraejemplo para un conjunto identidad

¿Es verdadera la siguiente propiedad de conjuntos?

Para todos los conjuntos A, B y C $(A - B) \cup (B - C) = A - C$.

Solución Observe que la propiedad es verdadera si y sólo si,

la igualdad dada se cumple para *todos* los conjuntos A, B y C.

Por lo que es falsa si y sólo si,

hay conjuntos A, B y C para los que la igualdad *no* se cumple.

Una forma de resolver este problema es imaginar los conjuntos A, B y C mediante la elaboración de un diagrama de Venn como el que se muestra en figura 6.3.1. Si supone que cualquiera de las ocho regiones del diagrama puede estar vacía de puntos, entonces, el diagrama es muy general.

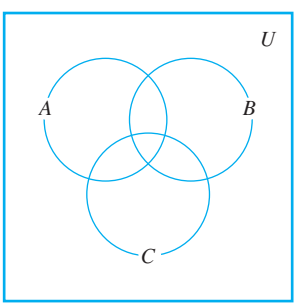


Figura 6.3.1

Encuentre y sombree la región correspondiente a $(A - B) \cup (B - C)$. Después sombree la región correspondiente a $A - C$. Éstas se muestran en la figura 6.3.2 en la siguiente página.

Comparando las regiones sombreadas parece indicar que la propiedad es falsa. Por ejemplo, si hay un elemento en B que no está en A o en C, entonces este elemento estaría en $(A - B) \cup (B - C)$ (ya que está en B y no en C) pero no estaría en $A - C$ ya que $A - C$ no contiene nada fuera de A. Del mismo modo, un elemento que está en A y en C pero no en B estaría en $(A - B) \cup (B - C)$ (ya que está en A y no en B), pero no estaría en $A - C$ (ya que estaría tanto en A como en C).

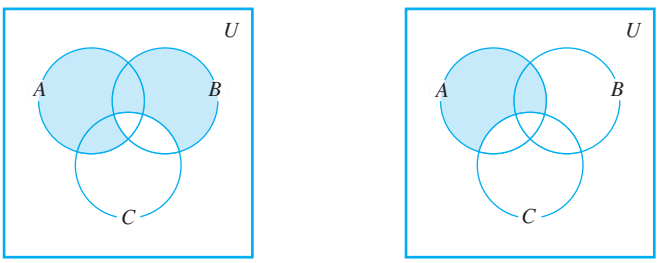


Figura 6.3.2

Construya un contraejemplo concreto para confirmar su respuesta y asegúrese de que no ha cometido un error en el dibujo o al analizar los diagramas. Una forma es poner uno de los enteros, de los ejercicios 1 al 7 en cada una de las siete subregiones encerradas por los círculos que representan a A, B y C. Si la propiedad propuesta del conjunto implica complementos del conjunto, también sería útil etiquetar la región fuera de los círculos y por tanto ponemos el número 8 ahí. (Vea la figura 6.3.3.) Después, defina conjuntos discretos A, B y C de todos los números en sus respectivas sub-regiones.

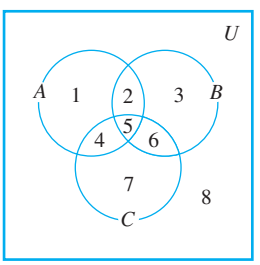


Figura 6.3.3

Contraejemplo 1: Sea $A = \{1, 2, 4, 5\}$, $B = \{2, 3, 5, 6\}$ y $C = \{4, 5, 6, 7\}$. Entonces,

$$A - B = \{1, 4\}, \quad B - C = \{2, 3\} \quad \text{y} \quad A - C = \{1, 2\}.$$

Por tanto

$$(A - B) \cup (B - C) = \{1, 4\} \cup \{2, 3\} = \{1, 2, 3, 4\}, \quad \text{mientras que} \quad A - C = \{1, 2\}.$$

Ya que $\{1, 2, 3, 4\} \neq \{1, 2\}$, tenemos que $(A - B) \cup (B - C) \neq A - C$.

Un contraejemplo más económico se puede obtener mediante la observación de que mientras el conjunto B contenga un elemento, como por ejemplo 3, que no se encuentre en A, entonces independientemente de si B contiene otros elementos e independientemente de que A y C contengan algún elemento $(A - B) \cup (B - C) \neq A - C$.

Contraejemplo 2: Sea $A = \emptyset$, $B = \{3\}$ y $C = \emptyset$. Entonces,

$$A - B = \emptyset, \quad B - C = \{3\} \quad \text{y} \quad A - C = \emptyset.$$

Por tanto $\quad (A - B) \cup (B - C) \neq \emptyset \cup \{3\} = \{3\}, \quad$ mientras que $\quad A - C = \emptyset.$

Ya que $\{3\} \neq \emptyset$, tenemos que $(A - B) \cup (B - C) \neq A - C$.

Nota Compruebe que cuando $A = C = \{4\}$ y $B = \emptyset$, $(A - B) \cup (B - C) \neq A - C$.

Otro contraejemplo económico requiere sólo que $A = C =$ a conjunto singleton, como $\{4\}$, mientras que B es el conjunto vacío.

Estrategia de solución de problemas

¿Cómo se puede descubrir si un enunciado universal dado acerca de los conjuntos es verdadero o falso? Existen dos enfoques básicos: el optimista y el pesimista. En el enfoque optimista, simplemente sumérjase y comience tratando de demostrar el enunciado, preguntando, ¿qué necesito demostrar? y ¿cómo demostrarlo? En el enfoque pesimista, se inicia buscando en su mente un conjunto de condiciones que deben cumplirse para construir un contraejemplo. Con estos enfoques puede comenzar y tener éxito inmediatamente o puede tener dificultad. El truco consiste en estar listo para cambiar al otro planteamiento si lo que intenta no parece prometedor. Para preguntas más difíciles, puede alternar varias veces entre los dos enfoques antes de llegar a la respuesta correcta.

El número de subconjuntos de un conjunto

El teorema siguiente establece el hecho importante que si un conjunto tiene n elementos, su conjunto potencia tiene 2^n elementos. La demostración utiliza inducción matemática y se basa en las siguientes observaciones. Suponga que X es un conjunto y z es un elemento de X.

1. Los subconjuntos de X se pueden dividir en dos grupos: aquellos que no contienen a z y los que contienen a z.
2. Los subconjuntos de X que no contienen a z son los mismos que los subconjuntos de $X - \{z\}$.
3. Los subconjuntos de X que no contienen a z pueden coincidir hasta uno por uno con los subconjuntos de X que contienen a z haciendo coincidir cada subconjunto A que no contiene a z con el subconjunto $A \cup \{z\}$ que contiene a z. Por tanto, hay muchos subconjuntos de X que contienen a z como subconjuntos existen de X que no contienen a z. Por ejemplo, si $X = \{x, y, z\}$, la tabla siguiente muestra la correspondencia entre subconjuntos de X que no contienen a z y subconjuntos de X que contienen a z.

Subconjuntos de X que no contienen a z		Subconjuntos de X que contienen a z
$\emptyset$	$\longleftrightarrow$	$\emptyset \cup \{z\} = \{z\}$
$\{x\}$	$\longleftrightarrow$	$\{x\} \cup \{z\} = \{x, z\}$
$\{y\}$	$\longleftrightarrow$	$\{y\} \cup \{z\} = \{y, z\}$
$\{x, y\}$	$\longleftrightarrow$	$\{x, y\} \cup \{z\} = \{x, y, z\}$

Teorema 6.3.1

Para todos los enteros $n \geq 0$, si un conjunto X tiene n elementos entonces, $\mathscr{P}(X)$ tiene 2^n elementos.

Demostración (por inducción matemática):

Sea la propiedad $P(n)$ la frase

Cualquier conjunto con n elementos tiene 2^n subconjuntos. $\leftarrow P(n)$

Demostración de que P(0) es verdadera:
Para establecer $P(0)$, debemos demostrar que

Cualquier conjunto con 0 elementos tiene 2^0 subconjuntos. $\leftarrow P(0)$

continúa en la página 370

Pero el único conjunto con cero elementos es el conjunto vacío y el único subconjunto del conjunto vacío es el mismo. Por tanto, un conjunto con cero elementos tiene un subconjunto. Puesto que $1 = 2^0$, tenemos que $P(0)$ es verdadero.

Demostración de que para todo entero $k \geq 0$, si $P(k)$ es verdadero, entonces $P(k + 1)$ también es verdadero:
[Supongamos que $P(k)$ es verdadero para un entero dado pero arbitrariamente elegido $k \geq 0$. Es decir:]
Suponga que k es cualquier entero con $k \geq 0$ tal que

Cualquier conjunto con k elementos tiene 2^k subconjuntos. ← $P(k)$ hipótesis inductiva

[Tenemos que demostrar que $P(k + 1)$ es verdadero. Es decir:] Debemos demostrar que

Cualquier conjunto con $k + 1$ elementos tiene 2^{k+1} subconjuntos. ← $P(k + 1)$

Sea X un conjunto con $k + 1$ elementos. Ya que $k + 1 \geq 1$, podemos elegir un elemento z en X. Observe que cualquier subconjunto de X contiene a z o no. Además, cualquier subconjunto de X que no contiene a z es un subconjunto de $X - \{z\}$. Y cualquier subconjunto A de $X - \{z\}$ puede coincidir con un subconjunto B, igual a $A \cup \{z\}$, de X que contiene a z. En consecuencia, hay tantos subconjuntos de X que contienen a z como los que no la contienen y por tanto hay dos veces más subconjuntos de X como subconjuntos hay de $X - \{z\}$. Pero $X - \{z\}$ tiene k elementos y por tanto

el número de subconjuntos de $X - \{z\} = 2^k$ por hipótesis inductiva.

Por tanto,

$$\begin{aligned} \text{el número de subconjuntos de } X &= 2 \cdot (\text{el número de subconjuntos de } X - \{z\}) \\ &= 2 \cdot (2^k) && \text{por sustitución} \\ &= 2^{k+1} && \text{por álgebra básica.} \end{aligned}$$

[Esto es lo que se quería demostrar.]
[Puesto que hemos demostrado tanto el paso básico como el paso inductivo, concluimos que el teorema es verdadero.]

Demostraciones "algebraicas" de identidades de conjuntos

Sea U el conjunto universo y considere el conjunto potencia de U, $\mathscr{P}(U)$. Las identidades del conjunto dadas en el teorema 6.2.2 conservan todos los elementos de $\mathscr{P}(U)$. Una vez que se ha establecido un cierto número de identidades y otras propiedades, se pueden deducir nuevas propiedades algebraicamente sin tener que utilizar argumentos de método del elemento. Resulta que sólo las identidades (1-5) del teorema 6.2.2 son necesarias para demostrar cualquier otra identidad que implique uniones, intersecciones y complementos. Con la identidad de adición (12), la ley del conjunto diferencia, se puede establecer cualquier identidad de conjunto que implica uniones, intersecciones, complementos y conjuntos diferencia.

Para utilizar propiedades conocidas para deducir nuevas, es necesario utilizar el hecho de que estas propiedades son enunciados universales. Como las leyes del álgebra para números reales, que se aplican a una gran variedad de situaciones diferentes. Se supone que todos los conjuntos son subconjuntos de $\mathscr{P}(U)$, entonces por ejemplo, una de las leyes distributivas establece que

para todos los conjuntos A, B y C, $\quad A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$.

Esta ley se puede ver como un modelo general en el que se pueden colocar cualesquiera tres conjuntos dados. Así, por ejemplo, si A_1, A_2 y A_3 representan conjuntos dados, entonces

$$\underbrace{A_1}_{A} \cap (\underbrace{A_2}_{B} \cup \underbrace{A_3}_{C}) = (\underbrace{A_1}_{A} \cap \underbrace{A_2}_{B}) \cup (\underbrace{A_1}_{A} \cap \underbrace{A_3}_{C}),$$

donde A_1 desempeña la función de A, A_2 desempeña el papel de B y A_3 desempeña el papel de C. Del mismo modo, si W, X, Y y Z son conjuntos cualesquiera dados, entonces, por la ley distributiva,

$$\underbrace{(W \cap X)}_{A} \cap (Y \cup Z) = (\underbrace{(W \cap X)}_{A} \cap Y) \cup (\underbrace{(W \cap X)}_{A} \cap Z),$$

donde $W \cap X$ desempeña el papel de A, Y desempeña el papel de B y Z desempeña el papel de C.

Ejemplo 6.3.2 Deducción de una propiedad de diferencia de conjuntos

Construya una demostración algebraica de que para todos los conjuntos A, B y C,

$$(A \cup B) - C = (A - C) \cup (B - C).$$

Mencione una propiedad del teorema 6.2.2 para cada paso de la demostración.

Solución Sean A, B y C conjuntos cualesquiera. Entonces,

$$\begin{aligned}
(A \cup B) - C &= (A \cup B) \cap C^c && \text{por la ley de la diferencia de conjuntos} \\
&= C^c \cap (A \cup B) && \text{por la ley conmutativa para } \cap \\
&= (C^c \cap A) \cup (C^c \cap B) && \text{por la ley distributiva} \\
&= (A \cap C^c) \cup (B \cap C^c) && \text{por la ley conmutativa para } \cap \\
&= (A - C) \cup (B - C) && \text{por la ley de la diferencia de conjuntos}
\end{aligned}$$

■

Ejemplo 6.3.3 Deducción de una identidad de conjuntos utilizando propiedades de $\emptyset$

Construya una demostración algebraica para todos los conjuntos A y B

$$A - (A \cap B) = A - B.$$

Mencione una propiedad de teorema 6.2.2 para cada paso de la demostración.

Solución Suponga que A y B son conjuntos cualesquiera. Entonces

$$\begin{aligned}
A - (A \cap B) &= A \cap (A \cap B)^c && \text{por la ley de la diferencia de conjuntos} \\
&= A \cap (A^c \cup B^c) && \text{por las leyes de De Morgan} \\
&= (A \cap A^c) \cup (A \cap B^c) && \text{por la ley distributiva} \\
&= \emptyset \cup (A \cap B^c) && \text{por la ley de complemento} \\
&= (A \cap B^c) \cup \emptyset && \text{por la ley conmutativa para } \cup \\
&= A \cap B^c && \text{por la ley de identidad para } \cup \\
&= A - B && \text{por la ley de la diferencia de conjuntos}
\end{aligned}$$

■

Para muchas personas una demostración algebraica parece más atractiva que un elemento de demostración, pero con frecuencia la demostración de un elemento es realmente más simple. Por ejemplo, en el ejemplo 6.3.3 anterior, puede ver inmediatamente que $A - (A \cap B) = A - B$ porque un elemento que está en $A - (A \cap B)$ significa que está en A y no en ambos, A y B y esto equivale a decir que está en A y no en B.

Ejemplo 6.3.4 Deducción de una ley asociativa generalizada

¡Precaución! Cuando se realizan problemas similares a los ejemplos del 6.3.2 al 6.3.4, asegúrese de utilizar la definición de propiedades exactamente como se establecieron.

Demuestre que para conjuntos cualesquiera A_1, A_2, A_3 y A_4,

$$((A_1 \cup A_2) \cup A_3) \cup A_4 = A_1 \cup ((A_2 \cup A_3) \cup A_4).$$

Mencione una propiedad de teorema 6.2.2 para cada paso de la demostración.

Solución Sea A_1, A_2, A_3 y A_4 conjuntos cualesquiera. Entonces

$$((A_1 \cup A_2) \cup A_3) \cup A_4 = (A_1 \cup (A_2 \cup A_3)) \cup A_4$$ por la ley asociativa para $\cup$ con A_1 jugando el papel de A, A_2 interpretando el papel de B y A_3 juega el papel de C

$$= A_1 \cup ((A_2 \cup A_3) \cup A_4)$$ por la ley asociativa para $\cup$ con A_1 en el papel de A, $A_2 \cup A_3$, interpretando el papel de B y A_4, jugando el papel de C. ■

Autoexamen

1. Dada una identidad de conjuntos propuesta que implique a las variables A, B y C, la forma más común para demostrar que la ecuación en general no se cumple es encontrar conjuntos concretos A, B y C que, cuando se sustituyen por las variables del conjunto en la ecuación, _____.
2. Cuando se utiliza el método algebraico para demostrar una identidad definida, es importante _____ en cada paso.
3. Cuando se aplica una propiedad del teorema 6.2.2, se debe utilizar _____ como está establecida.

Conjunto de ejercicios 6.3

Para cada uno de los ejercicios del 1 al 4 buscar un contraejemplo para demostrar que el enunciado es falso. Suponga que todos los conjuntos son subconjuntos de un conjunto universo U.

1. Para todos los conjuntos A, B y C $(A \cap B) \cup C = A \cap (B \cup C)$.
2. Para todos los conjuntos A y B $(A \cup B)^c = A^c \cup B^c$.
3. Para todos los conjuntos A, B y C, si $A \not\subseteq B$ y $B \not\subseteq C$ entonces $A \not\subseteq C$.
4. Para todos los conjuntos A, B y C, si $B \cap C \subseteq A$ entonces $(A - B) \cap (A - C) = \emptyset$.

Para cada uno de los ejercicios del 5 al 21 demuestre cada enunciado que sea verdadero y encuentre un contraejemplo para cada enunciado sea falso. Suponga que todos los conjuntos son subconjuntos de un conjunto universo U.

5. Para todos los conjuntos A, B y C, $A - (B - C) = (A - B) - C$.
6. Para todos los conjuntos A y B, $A \cap (A \cup B) = A$.
7. Para todos los conjuntos A, B y C
$$(A - B) \cap (C - B) = A - (B \cup C).$$
8. Para todos los conjuntos A y B, si $A^c \subseteq B$ entonces, $A \cup B = U$.
9. Para todos los conjuntos A, B y C, si $A \subseteq C$ y $B \subseteq C$ entonces $A \cup B \subseteq C$.
10. Para todos los conjuntos A y B, si $A \subseteq B$ entonces $A \cap B^c = \emptyset$.

H 11. Para todos los conjuntos A, B y C, si $A \subseteq C$ entonces $A \cap (B \cap C)^c = \emptyset$.

H 12. Para todos los conjuntos A, B y C
$$A \cap (B - C) = (A \cap B) - (A \cap C).$$

13. Para todos los conjuntos A, B y C
$$A \cup (B - C) = (A \cup B) - (A \cup C).$$

H 14. Para todos los conjuntos A, B y C, si $A \cap C \subseteq B \cap C$ y $A \cup C \subseteq B \cup C$, entonces $A \subseteq B$.

H 15. Para todos los conjuntos A, B y C, si $A \cap C \subseteq B \cap C$ y $A \cup C \subseteq B \cup C$, entonces $A = B$.

16. Para todos los conjuntos A y B, si $A \cap B = \emptyset$ entonces $A \times B = \emptyset$.
17. Para todos los conjuntos A y B, si $A \subseteq B$ entonces $\mathscr{P}(A) \subseteq \mathscr{P}(B)$.
18. Para todos los conjuntos A y B, $\mathscr{P}(A \cup B) \subseteq \mathscr{P}(A) \cup \mathscr{P}(B)$.

H 19. Para todos los conjuntos A y B, $\mathscr{P}(A) \cup \mathscr{P}(B) \subseteq \mathscr{P}(A \cup B)$.

20. Para todos los conjuntos A y B, $\mathscr{P}(A \cap B) = \mathscr{P}(A) \cap \mathscr{P}(B)$.
21. Para todos los conjuntos A y B, $\mathscr{P}(A \times B) = \mathscr{P}(A) \times \mathscr{P}(B)$.
22. Escriba una negación para cada uno de los siguientes enunciados. Indicando cuál es verdadero, el enunciado o su negación. Justifique sus respuestas.
    a. $\forall$ los conjuntos S, $\exists$ un conjunto T tal que $S \cap T = \emptyset$.
    b. $\exists$ un conjunto S tal que $\forall$ los conjuntos T, $S \cup T = \emptyset$.

H 23. Sea $S = \{a, b, c\}$ y para cada entero $i = 0, 1, 2, 3$, sea S_i el conjunto de todos los subconjuntos de S que tienen i elementos. Liste los elementos en S_0, S_1, S_2 y S_3. ¿Es $\{S_0, S_1, S_2, S_3\}$ una partición de $\mathscr{P}(S)$?

24. Sea $S = \{a, b, c)$ y sea S_a el conjunto de todos los subconjuntos de S que contiene a a, sea S_b el conjunto de todos los subconjuntos de S que contienen a b, sea S_c el conjunto de todos los subconjuntos de S que contienen a c y sea $S_\emptyset$ el conjunto cuyo único elemento es $\emptyset$. ¿Es $\{S_a, S_b, S_c, S_\emptyset\}$ un partición de $\mathscr{P}(S)$?

25. Sea $A = \{t, u, v, w\}$ y sea S_1 el conjunto de todos los subconjuntos de A que no contienen a w y S_2 el conjunto de todos los subconjuntos de A que contienen a w.
a. Encuentre a S_1 **b.** Determine a S_2.
c. ¿Son S_1 y S_2 disjuntos?
d. compare los tamaños de S_1 y S_2.
e. ¿Cuántos elementos se encuentran en $S_1 \cup S_2$?
f. ¿Cuál es la relación entre $S_1 \cup S_2$ y $\mathscr{P}(A)$?

H ∗ 26. El problema siguiente, fue ideado por Ginger Bolton, lo presentó en la edición de enero de 1989 del *College Mathematics Journal* (Vol. 20, No. 1, p. 68): Dado un número entero positivo $n \geq 2$, sea S el conjunto de todos los subconjuntos no vacíos de $\{2, 3, \ldots, n\}$. Para cada $S_i \in S$, sea P_i el producto de los elementos de S_i. Demuestre o refute que

$$\sum_{i=1}^{2^{n-1}-1} P_i = \frac{(n+1)!}{2} - 1.$$

En los ejercicios 27 y 28 dé una razón para cada paso de la deducción.

27. Para todos los conjuntos A, B y C,

$$(A \cup B) \cap C = (A \cap C) \cup (B \cap C).$$

Demostración: Suponga que A, B y C son conjuntos cualesquiera. Entonces,

$$\begin{aligned}(A \cup B) \cap C &= C \cap (A \cup B) && \text{por } \underline{\text{(a)}}\\ &= (C \cap A) \cup (C \cap B) && \text{por } \underline{\text{(b)}}\\ &= (A \cap C) \cup (B \cap C) && \text{por } \underline{\text{(c)}}.\end{aligned}$$

H 28. Para todos los conjuntos A, B y C,

$$(A \cup B) - (C - A) = A \cup (B - C).$$

Demostración: Suponga que A, B y C son conjuntos cualesquiera. Entonces,

$$\begin{aligned}(A \cup B) - (C - A) &= (A \cup B) \cap (C - A)^c && \text{por } \underline{\text{(a)}}\\ &= (A \cup B) \cap (C \cap A^c)^c && \text{por } \underline{\text{(b)}}\\ &= (A \cup B) \cap (A^c \cap C)^c && \text{por } \underline{\text{(c)}}\\ &= (A \cup B) \cap ((A^c)^c \cup C^c) && \text{por } \underline{\text{(d)}}\\ &= (A \cup B) \cap (A \cup C^c) && \text{por } \underline{\text{(e)}}\\ &= A \cup (B \cap C^c) && \text{por } \underline{\text{(f)}}\\ &= A \cup (B - C) && \text{por } \underline{\text{(g)}}\end{aligned}$$

H 29. Faltan algunos pasos de la siguiente demostración de que, para todos los conjuntos $(A \cup B) - C = (A - C) \cup (B - C)$. Indique qué son y, después, escriba la demostración correctamente.

Demostración: Sean A, B y C conjuntos cualesquiera. Entonces,

$$\begin{aligned}(A \cup B) - C &= (A \cup B) \cap C^c && \text{por la ley de diferencia de conjuntos}\\ &= (A \cup C^c) \cup (B \cap C^c) && \text{por la ley distributiva}\\ &= (A - C) \cup (B - C) && \text{por la ley de diferencia de conjuntos}\end{aligned}$$

En los ejercicios 30 y 40, construya una demostración algebraica para el enunciado dado. Cite una propiedad del teorema 6.2.2 para cada paso.

30. Para todos los conjuntos A, B y C

$$(A \cap B) \cup C = (A \cup C) \cap (B \cup C).$$

31. Para todos los conjuntos A y B, $A \cup (B - A) = A \cup B$.

32. Para todos los conjuntos A y B, $(A - B) \cup (A \cap B) = A$.

33. Para todos los conjuntos A y B, $(A - B) \cap (A \cap B) = \emptyset$.

34. Para todos los conjuntos A, B y C,

$$(A - B) - C = A - (B \cup C).$$

35. Para todos los conjuntos A y B, $A - (A - B) = A \cap B$.

36. Para todos los conjuntos A y B, $((A^c \cup B^c) - A)^c = A$.

37. Para todos los conjuntos A y B, $(B^c \cup (B^c - A))^c = B$.

38. Para todos los conjuntos A y B, $A - (A \cap B) = A - B$.

H 39. Para todos los conjuntos A y B,

$$(A - B) \cup (B - A) = (A \cup B) - (A \cap B).$$

40. Para todos los conjuntos A, B y C,

$$(A - B) - (B - C) = A - B.$$

En los ejercicios del 41 al 43 simplifique la expresión dada. Cite una propiedad del teorema 6.2.2 en cada paso.

H 41. $A \cap ((B \cup A^c) \cap B^c)$

42. $(A - (A \cap B)) \cap (B - (A \cap B))$

43. $((A \cap (B \cup C)) \cap (A - B)) \cap (B \cup C^c)$

44. Considere la siguiente propiedad de conjuntos: para todos los conjuntos A y B, $A - B$ y B son disjuntos.
a. Utilice un argumento de elemento para obtener la propiedad.
b. Utilice un argumento algebraico para deducir la propiedad (mediante la aplicación de propiedades del teorema 6.2.2).
c. Comente sobre qué método encontró más fácil.

45. Considerar la siguiente propiedad de conjuntos: para todos los conjuntos A, B y C, $(A - B) \cup (B - C) = (A \cup B) - (B \cap C)$.
a. Utilice un argumento de elemento para obtener la propiedad.
b. Utilice un argumento algebraico para deducir la propiedad (mediante la aplicación de propiedades del teorema 6.2.2).
c. Comente sobre qué método encontró más fácil.

Definición: Dados los conjuntos A y B, la **diferencia simétrica de A y B**, que se denota por $A \triangle B$ es

$$A \triangle B = (A - B) \cup (B - A).$$

46. Sean $A = \{1, 2, 3, 4\}$, $B = \{3, 4, 5, 6\}$ y $C = \{5, 6, 7, 8\}$. Determine cada uno de los siguientes conjuntos:
a. $A \triangle B$ b. $B \triangle C$
c. $A \triangle C$ d. $(A \triangle B) \triangle C$

Con referencia a la definición de diferencia simétrica dada antes. Demuestre cada una de las expresiones de los ejercicios 47 al 52, suponiendo que A, B y C son todos subconjuntos de un conjunto universo U.

47. $A \triangle B = B \triangle A$ **48.** $A \triangle \emptyset = A$

49. $A \triangle A^c = U$ 50. $A \triangle A = \emptyset$

H 51. Si $A \triangle C = B \triangle C$, entonces $A = B$.

H 52. $(A \triangle B) \triangle C = A \triangle (B \triangle C)$.

H 53. Deduzca la identidad de conjuntos $A \cup (A \cap B) = A$ de las propiedades enumeradas en el teorema de la 6.2.2(l) a la (9). Comience demostrando que para todo subconjunto B de un conjunto universo U, $U \cup B = U$. Después intersecte ambos lados con A y deduzca la identidad.

54. Deduzca la identidad de conjuntos $A \cap (A \cup B) = A$ de las propiedades listadas en el teorema de la 6.2.2(l) a la (9). Inicie demostrando que para todos los subconjuntos B de un conjunto universo U, $\emptyset = \emptyset \cap B$. Después, realice la unión de ambas partes con A y deduzca la identidad.

Respuestas del autoexamen

1. hacen que el miembro izquierdo sea diferente del lado derecho *(O: resultan valores diferentes en los dos lados de la ecuación)* 2. *citar una de las propiedades de teorema 6.2.2 (O: dar una razón)* 3. *exactamente*

6.4 Álgebra booleana, paradoja de Russell y el problema del paro

Nadie nos expulsará del paraíso creado por Cantor.
—David Hilbert (1862-1943)

La tabla 6.4.1 resume las principales características de las equivalencias lógicas del teorema 2.1.1 y las propiedades de conjuntos del teorema 6.2.2. Observe qué tan similares son las entradas de las dos columnas.

Equivalencias lógicas	Propiedades de conjuntos
Para todas las variables de enunciado p, q y r:	Para todos los conjuntos A, B y C:
a. $p \vee q \equiv q \vee p$ b. $p \wedge q \equiv q \wedge p$	a. $A \cup B = B \cup A$ b. $A \cap B = B \cap A$
a. $p \wedge (q \wedge r) \equiv p \wedge (q \wedge r)$ b. $p \vee (q \vee r) \equiv p \vee (q \vee r)$	a. $A \cup (B \cup C) \equiv A \cup (B \cup C)$ b. $A \cap (B \cap C) \equiv A \cap (B \cap C)$
a. $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$ b. $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$	a. $A \cap (B \cup C) \equiv (A \cap B) \cup (A \cap C)$ b. $A \cup (B \cap C) \equiv (A \cup B) \cap (A \cup C)$
a. $p \vee \mathbf{c} \equiv p$ b. $p \wedge \mathbf{t} \equiv p$	a. $A \cup \emptyset = A$ b. $A \cap U = A$
a. $p \vee \sim p \equiv \mathbf{t}$ b. $p \wedge \sim p \equiv \mathbf{c}$	a. $A \cup A^c = U$ b. $A \cap A^c = \emptyset$
$\sim(\sim p) \equiv p$	$(A^c)^c = A$
a. $p \vee p \equiv p$ b. $p \wedge p \equiv p$	a. $A \cup A = A$ b. $A \cap A = A$
a. $p \vee \mathbf{t} \equiv \mathbf{t}$ b. $p \wedge \mathbf{c} \equiv \mathbf{c}$	a. $A \cup U = U$ b. $A \cap \emptyset = \emptyset$
a. $\sim(p \vee q) \equiv \sim p \wedge \sim q$ b. $\sim(p \wedge q) \equiv \sim p \vee \sim q$	a. $(A \cup B)^c = A^c \cap B^c$ b. $(A \cap B)^c = A^c \cup B^c$
a. $p \vee (p \wedge q) \equiv p$ b. $p \wedge (p \vee q) \equiv p$	a. $A \cup (A \cap B) \equiv A$ b. $A \cap (A \cup B) \equiv A$
a. $\sim\mathbf{t} \equiv \mathbf{c}$ b. $\sim\mathbf{c} \equiv \mathbf{t}$	a. $U^c = \emptyset$ b. $\emptyset^c = U$

Tabla 6.4.1

Si hace que $\vee$ (o) corresponda a $\cup$ (unión), $\wedge$ (y) corresponda a $\cap$ (intersección), **t** (una tautología) corresponda a U (un conjunto universo), **c** (una contradicción) corresponda a $\emptyset$ (el conjunto vacío) y $\sim$ (negación) corresponda a ^{c} (complementación), entonces, puede ver que la estructura del conjunto de las formas de enunciado con las operaciones $\vee$ y $\wedge$ es esencialmente idéntica a la estructura del conjunto de subconjuntos de un conjunto universo con operaciones $\cup$ y $\cap$. De hecho, ambos son casos especiales de la misma estructura general, conocida como *álgebra booleana*. La idea esencial de una álgebra booleana fue introducida por el autodidacta inglés matemático/lógico George Boole en 1847 en un libro titulado *Análisis matemático de la lógica*. Durante el resto del siglo XIX, Boole y otros desarrollaron y aclararon el concepto hasta llegar a la forma en que la usamos hoy en día.

En esta sección se muestra cómo deducir las diferentes propiedades asociadas con una álgebra booleana de un conjunto de exactamente cinco axiomas.

• Definición: Álgebra booleana

Una **álgebra booleana** es un conjunto B junto con dos operaciones, que generalmente son denotadas con $+$ y $\cdot$, tal que para todas a y b en B tanto $a + b$ como $a \cdot b$ están en B y se cumplen las siguientes propiedades:

1. *Leyes conmutativas:* Para todas a y b en B,
$$a)\ a + b = b + a \quad \text{y} \quad b)\ a \cdot b = b \cdot a.$$
2. *Leyes asociativas:* Para todas a, b y c en B,
$$a)\ (a + b) + c = a + (b + c) \quad \text{y} \quad b)\ (a \cdot b) \cdot c = a \cdot (b \cdot c).$$
3. *Leyes distributivas:* Para todas a, b y c en B,
$$a)\ a + (b \cdot c) = (a + b) \cdot (a + c) \quad \text{y} \quad b)\ a \cdot (b + c) = (a \cdot b) + (a \cdot c).$$
4. *Leyes de identidad:* Existen elementos distintos 0 y 1 en B tal que para toda a en B,
$$a)\ a + 0 = a \quad \text{y} \quad b)\ a \cdot 1 = a.$$
5. *Leyes de complemento:* Para cada a en B, existe un elemento en B, que se denota por $\overline{a}$ y se llama el **complemento** o **negación** de a, tal que
$$a)\ a + \overline{a} = 1 \quad \text{y} \quad b)\ a \cdot \overline{a} = 0.$$

En cualquier álgebra booleana, el complemento de cada elemento es único, las cantidades 0 y 1 son únicos y se deducen identidades análogas a las del teorema 2.1.1 y el teorema 6.2.2.

Teorema 6.4.1 Propiedades del álgebra booleana

Sea B cualquier álgebra booleana.

1. *Unicidad de la ley de complemento:* Para toda a y x en B, si $a + x = 1$ y $a \cdot x = 0$ entonces $x = \overline{a}$.
2. *Unicidad de* 0 *y* 1*:* Si existe x en B tal que $a + x = a$ para toda a en B, entonces, $x = 0$ y si existe y en B tal que $a \cdot y = a$ para toda a en B, entonces $y = 1$.
3. *Ley del doble complemento:* Para toda $a \in B$, $\overline{(\overline{a})} = a$.

continúa en la página 376

4. *Ley de idempotencia:* Para toda $a \in B$,

$$a)\ a + a = a \quad \text{y} \quad b)\ a \cdot a = a.$$

5. *Ley de acotamiento universal:* Para toda $a \in B$,

$$a)\ a + 1 = 1 \quad \text{y} \quad b)\ a \cdot 0 = 0.$$

6. *Leyes de De Morgan:* Para todas a y $b \in B$,

$$a)\ \overline{a + b} = \overline{a} \cdot \overline{b} \quad \text{y} \quad b)\ \overline{a \cdot b} = \overline{a} + \overline{b}.$$

7. *Leyes de absorción:* Para todas a y $b \in B$,

$$a)\ (a + b) \cdot a = a \quad \text{y} \quad b)\ (a \cdot b) + a = a.$$

8. *Complementos de* 0 *y* 1*:*

$$a)\ \overline{0} = 1 \quad \text{y} \quad b)\ \overline{1} = 0.$$

Demostración:

Parte 1. Unicidad de la ley de complemento
Suponga que a y x son elementos particulares de B arbitrariamente elegidos, que satisfacen la siguiente hipótesis: $a + x = 1$ y $a \cdot x = 0$. Entonces,

$x = x \cdot 1$	porque 1 es una identidad para $\cdot$
$= x \cdot (a + \overline{a})$	por la ley de complemento para $+$
$= x \cdot a + x \cdot \overline{a}$	por la ley distributiva para $\cdot$ sobre $+$
$= a \cdot x + x \cdot \overline{a}$	por la ley conmutativa para $\cdot$
$= 0 + x \cdot \overline{a}$	por hipótesis
$= a \cdot \overline{a} + x \cdot \overline{a}$	por la ley de complemento para $\cdot$
$= (\overline{a} \cdot a) + (\overline{a} \cdot x)$	por la ley conmutativa para $\cdot$
$= \overline{a} \cdot (a + x)$	por la ley distributiva para $\cdot$ sobre $+$
$= \overline{a} \cdot 1$	por hipótesis
$= \overline{a}$	porque 1 es una identidad para $\cdot$.

Las demostraciones de las otras partes del teorema se analizan en los ejemplos que siguen y en los ejercicios.

Es posible que observe que todas las partes de la definición de una álgebra booleana y la mayor parte del teorema 6.4.1 contienen enunciados apareados. Por ejemplo, las leyes distributivas establecen que para toda a, b y c en B,

$$a)\ a + (b \cdot c) = (a + b) \cdot (a + c) \quad \text{y} \quad b)\ a \cdot (b + c) = (a \cdot b) + (a \cdot c),$$

y las leyes de identidad establecen que para toda a en B,

$$a)\ a + 0 = a \quad \text{y} \quad b)\ a \cdot 1 = a.$$

Observe que cada uno de los enunciados apareados pueden obtenerse de otro intercambiando todos los signos $+$ y $\cdot$ e intercambiando 1 y 0. Dichos intercambios transforman cualquier identidad booleana en su identidad **doble**. Se puede demostrar que el doble de cualquier identidad booleana es también una identidad. Este hecho a menudo se llama el **principio de la dualidad** para una álgebra booleana.

Ejemplo 6.4.1 Demostración de la ley del complemento doble

Demuestre que para todos los elementos a en una álgebra booleana B, $\overline{(\overline{a})} = a$.

Solución Inicie suponiendo que B es una álgebra booleana y a es cualquier elemento de B. La base de la demostración es la unicidad de la ley de complemento: que cada elemento en B tiene un complemento único que satisface ciertas ecuaciones con respecto a éste. Así si se puede demostrar que a satisface esas ecuaciones con respecto a $\overline{a}$, entonces, a debe ser el complemento de $\overline{a}$.

Teorema 6.4.1(3) Ley del doble complemento

Para todo elemento a en una álgebra booleana B, $\overline{(\overline{a})} = a$.

Demostración:

Suponga que B es una álgebra booleana y a es cualquier elemento de B. Entonces

$$\begin{aligned} \overline{a} + a &= a + \overline{a} && \text{por la ley conmutativa} \\ &= 1 && \text{por la ley de complemento para 1} \end{aligned}$$

y

$$\begin{aligned} \overline{a} \cdot a &= a \cdot \overline{a} && \text{por la ley conmutativa} \\ &= 0 && \text{por la ley de complemento para 0.} \end{aligned}$$

Por tanto a satisface las dos ecuaciones con respecto a $\overline{a}$ que son satisfechos por el complemento de $\overline{a}$. Del hecho de que el complemento de a es único, se concluye que $\overline{(\overline{a})} = a$.

■

Ejemplo 6.4.2 Demostración de una ley de idempotencia

Complete los espacios en blanco en la siguiente demostración que para todos los elementos a en una álgebra booleana B, $a + a = a$.

Demostración:

Suponga que B es una álgebra booleana y a es cualquier elemento de B. Entonces,

$$\begin{aligned} a &= a + 0 && \text{(a)} \\ &= a + (a \cdot \overline{a}) && \text{(b)} \\ &= (a + a) \cdot (a + \overline{a}) && \text{(c)} \\ &= (a + a) \cdot 1 && \text{(d)} \\ &= a + a && \text{(e)} \end{aligned}$$

Solución

a. porque 0 es una identidad para $+$

b. por la ley de complemento para $\cdot$

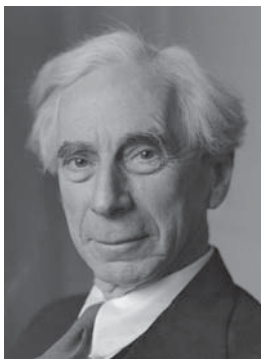
c. por la ley distributiva para $+$ sobre $\cdot$

d. por la Ley de complemento para $+$

e. porque 1 es una identidad para $\cdot$

■

Paradoja de Russell


Sylvia Salmi

Bertrand Russell (1872-1970)

A principios del siglo XX, la teoría abstracta de conjuntos había ganado tal aceptación que un gran número de matemáticos estaban trabajando duro para demostrar que todas las matemáticas podrían construirse sobre las bases de la teoría de conjuntos. En medio de esta actividad, el matemático y filósofo inglés Bertrand Russell descubrió una "paradoja" (realmente una verdadera contradicción) que parecía hacer temblar la esencia misma de las bases. La paradoja supone la definición de conjunto de Cantor como "cualquier colección en un todo de objetos definidos y separados de nuestra intuición o de nuestro pensamiento".

Paradoja de Russell: La mayoría de los conjuntos no son elementos de sí mismos. Por ejemplo, el conjunto de todos los enteros no es un entero y el conjunto de todos los caballos no es un caballo. Sin embargo, podemos imaginar la posibilidad de que un conjunto sea un elemento de sí mismo. Por ejemplo, el conjunto de todas las ideas abstractas puede ser considerado una idea abstracta. Si se nos permite utilizar cualquier descripción de una propiedad como la propiedad de definición de un conjunto, podemos hacer que S sea el conjunto de todos los conjuntos que no son elementos de sí mismos:

$$S = \{A \,|\, A \text{ es un conjunto y } A \notin A\}.$$

¿Es S un elemento de sí mismo?

La respuesta no es ni sí ni no. Porque si $S \in S$, entonces S satisface la propiedad de definición para S y por tanto $S \notin S$. Pero si $S \notin S$, entonces S es un conjunto tal que $S \notin S$ y así S satisface la propiedad de definición para S, lo que implica que $S \in S$. Por tanto, ni es $S \in S$ ni $S \notin S$, lo que es una contradicción.

Para ayudar a explicar su descubrimiento a laicos, Russell ideó un rompecabezas, el rompecabezas del barbero, cuya solución presenta la misma lógica que su paradoja.

Ejemplo 6.4.3 El rompecabezas del barbero

En una determinada ciudad hay un barbero hombre que afeita a todos esos hombres y sólo esos hombres, que no se afeitan a sí mismos. *Pregunta*: ¿El barbero se afeita a sí mismo?

Solución Ni sí ni no. Si el barbero se afeita a sí mismo, es miembro de la clase de hombres que se afeitan a sí mismos. Pero ningún miembro de esta clase es afeitado por el barbero y así el barbero *no* se afeita a sí mismo. Por otra parte, si el barbero no se afeita a sí mismo, pertenece a la clase de hombres que no se afeitan a sí mismos. Pero el barbero afeita a cada uno en esta clase, por lo que el barbero *se* afeita a sí mismo. ■

Pero ¿cómo puede la respuesta ser ni sí ni no? Sin duda cualquier barbero se afeita o no a sí mismo. Podría intentar pensar en circunstancias que harían que la paradoja desaparezca. Por ejemplo, tal vez ocurre que el barbero no tenga nada de barba y nunca se afeita. Pero una condición del rompecabezas es que el barbero es un hombre que afeita a *todos* aquellos hombres que no se afeitan a sí mismos. Si él no se afeita, entonces no se afeita a sí mismo, en cuyo caso él se afeitó con el barbero y la contradicción sigue estando presente por siempre. Similarmente están condenados al fracaso, otros intentos de resolver la paradoja considerando los detalles de la situación del barbero.

Así que vamos a aceptar el hecho de que la paradoja no tiene ninguna solución fácil y vamos a ver a dónde conduce ese pensamiento. Dado que el barbero ni se afeita a sí mismo ni no se afeita a sí mismo, la frase no afeitarse "el barbero se afeita a sí mismo" no es ni verdadera ni falsa. Pero la frase surgió de forma natural a partir de una descripción de la situación. Si realmente existió la situación, entonces la frase tendría que ser verdadera o falsa. Por tanto, nos vemos obligados a concluir que la situación descrita en el rompecabezas simplemente no puede existir en el mundo como lo conocemos.

De forma similar, la conclusión que se deduce de la misma paradoja de Russell es que el objeto S no es un conjunto. Ya que si realmente se tratara de un conjunto, en el sentido de satisfacer las propiedades generales de conjuntos que nosotros hemos estado suponiendo, entonces tampoco sería o no un elemento de sí mismo.

En los años siguientes al descubrimiento de Russell, se encontraron varias formas de definir los conceptos básicos de la teoría de conjuntos para evitar su contradicción. La forma utilizada en este libro requiere que, excepto para el conjunto potencia, cuya existencia está garantizada por un axioma, cada vez que se defina un conjunto usando un predicado como una propiedad de definición, también debe ponerse como condición que el conjunto es un subconjunto de un conjunto conocido. Este método no nos permite hablar del "conjunto de todos los conjuntos que no son elementos de sí mismos". Sólo se puede hablar del "conjunto de todos los conjuntos que son subconjuntos de algún conjunto conocido y que no son elementos de sí mismos". Cuando se hace esta restricción, la paradoja de Russell deja de ser contradictoria. Esto es lo que sucede:

Sea U un conjunto universo y suponga que todos los conjuntos bajo análisis son subconjuntos de U. Sea

$$S = \{A \mid A \subseteq U \text{ y } A \notin A\}.$$

En la paradoja de Russell, ambas implicaciones

$$S \in S \rightarrow S \notin S \quad \text{y} \quad S \notin S \rightarrow S \in S$$

se demostraron y la conclusión contradictoria

$$\text{ni } S \in S \quad \text{ni} \quad S \notin S$$

por tanto, es deducida. En la situación en la que todos los conjuntos bajo análisis sean subconjuntos de U, la implicación $S \in S \rightarrow S \notin S$ se demuestra casi del mismo modo como con la paradoja de Russell: (Suponga que $S \in S$. Entonces, por definición de S, $S \subseteq U$ y $S \notin S$. En particular, $S \notin S$.) Por otra parte, de la suposición de que $S \notin S$ podemos sólo deducir que el enunciado "$S \subseteq U$ y $S \notin S$" es falso. Por una de las leyes de De Morgan, esto significa que "$S \not\subseteq U$ o $S \in S$". Ya que $S \in S$ contradiría la suposición de que $S \notin S$, lo eliminamos y concluimos que $S \not\subseteq U$. En otras palabras, la única conclusión que podemos sacar es que la aparente "definición" de S es defectuosa, es decir, que S no es un conjunto en U.

Kurt Gödel (1906-1978)

El descubrimiento de Russell tuvo un profundo impacto en las matemáticas porque a pesar de su contradicción pudieron desaparecer por definiciones más cuidadosas, su existencia causó que la gente se preguntase si había otras contradicciones. En 1931, Kurt Gödel demostró que no es posible demostrar, de una manera matemáticamente rigurosa, que la matemática está libre de contradicciones. Se podría pensar que resultado de Gödel habría causado que los matemáticos renunciaran desesperadamente a su trabajo, pero eso no ha sucedido. Por el contrario, ha habido más actividad matemática a partir de 1931 que en cualquier otro periodo en la historia.

El problema del paro

Mucho antes de la construcción de una computadora electrónica, Alan M. Turing (1912-1954) dedujo un teorema profundo acerca de cómo tendrían que trabajar dichas computadoras. El argumento que él utilizó es similar al de la paradoja de Russell. También está relacionado con los utilizados por Gödel para demostrar su teorema y con los usados por Cantor para demostrar que es imposible escribir todos los números reales en una lista infinita, incluso considerando un intervalo infinitamente largo de tiempo (vea la sección 7.4 y el capítulo 12).

Si tiene cierta experiencia en programación de computadoras, debe saber lo mal que un bucle infinito puede bloquear a un sistema informático. Sería útil poder procesar previamente un programa y su conjunto de datos al ejecutarlo usando un programa de comprobación que determine si la ejecución del programa dado con el conjunto de datos dado dará como resultado un bucle infinito. ¿Se puede escribir un algoritmo para este programa? ¿En otras palabras, se puede escribir un algoritmo que acepte cualquier algoritmo X y cualquier conjunto de datos D como entrada y que después imprima "alto" o "bucles infinitos" para indicar ya sea que X termina en un número finito de pasos o que hay bucles infinitos cuando se ejecuta con el conjunto de datos D? En la década de 1930, Turing demostró que la respuesta a esta pregunta es no.

Teorema 6.4.2

No existe un algoritmo de cómputo que acepte cualquier algoritmo X y un conjunto de datos D como entrada y que después diga "pare" o "bucles infinitos" para indicar si X termina o no en un número finito de pasos cuando se ejecuta X con el conjunto de datos D.

Demostración (por contradicción):

Suponga que hay un algoritmo, ComprobaciónPare, tal que si se introducen en un algoritmo X y un conjunto de datos D, entonces,

ComprobaciónPare(X, D) imprime

"pare" si X termina en un número finito de pasos cuando se ejecuta con el conjunto de datos D

o

"bucles infinitos" si X no termina en un número finito de pasos cuando se ejecuta con el conjunto de datos D.

[Para demostrar que no puede existir ningún algoritmo, tal como ComprobaciónPare, se va a deducir una contradicción.]

Observe que la secuencia de caracteres que componen un algoritmo X puede considerarse en sí misma como un conjunto de datos. Por tanto, es posible considerar la ejecución de ComprobaciónPare con entrada (X, X). Se define un nuevo algoritmo, Prueba, como sigue: para cualquier entrada de algoritmo X,

Prueba(X)

bucles infinitos si ComprobaciónPare(X, X) imprime "pare"

o

para si ComprobaciónPare(X, X) imprime "bucles infinitos".

Ahora al ejecutar el algoritmo Prueba con la prueba de la entrada. Si Prueba(Prueba) termina después de un número finito de pasos, entonces, el valor de ComprobaciónPare (Prueba, Prueba) es "pare" y así Prueba(Prueba) crea un bucle infinito.

Por otra parte, si Prueba(Prueba) no termina después de un número finito de pasos, entonces ComprobaciónPare(Prueba, Prueba) imprime "bucles infinitos" y así termina Prueba(Prueba).

Los dos párrafos anteriores muestran bucles infinitos de Prueba(Prueba) y también pare. Esto es una contradicción. Pero la existencia de prueba se deduce lógicamente de la suposición de la existencia de un algoritmo de ComprobaciónPare que puede comprobar que cualquier algoritmo y conjunto de datos termina. *[Por tanto la suposición debe ser falsa y no existe dicho algoritmo.]*

En los últimos años se han encontrado axiomas de la teoría de conjuntos que garantizan que la paradoja de Russell no es insuficiente para tratar con toda la gama de forma de objetos definidos recursivamente en ciencias de la computación y se ha desarrollado una nueva teoría de conjuntos "que carece de fundamento". Además, los científicos de la computación y lógicos que trabajan con programas que permiten a las computadoras procesar el lenguaje natural han visto la importancia de explorar aún más los tipos de cuestiones semánticas planteadas por el rompecabezas del barbero y están desarrollando nuevas teorías de la lógica para tratar con ellas.

Autoexamen

1. Comparando entre la estructura del conjunto de formas de enunciado y el conjunto de subconjuntos de un conjunto universo, la operación $o \vee$ corresponde a _____, la operación $y \wedge$ corresponde a _____, una tautología **t** corresponde a _____, una contradicción **c** corresponde a _____ y la operación de negación, denota $\sim$, que corresponde a _____.

2. Las operaciones $+$ y $\cdot$ en un álgebra booleana son generalizaciones de las operaciones de _____ y _____ en el conjunto todas las formas de enunciado en un número finito dado de variables y de las operaciones de _____ y _____ en el conjunto de todos los subconjuntos de un conjunto dado.

3. Russell demostró que la siguiente proposición "definición del conjunto" podría en realidad no definir un conjunto: _____.

Conjunto de ejercicios 6.4

En los ejercicios 1 al 3 suponga que B es una álgebra booleana con operaciones $+$ y $\cdot$. Dé las razones que necesite para completar los espacios en blanco en las demostraciones, pero no utilice ninguna parte del teorema 6.4.1 a menos que ya se haya demostrado. Sin embargo, puede utilizar cualquier parte de la definición de una álgebra booleana y los resultados de los ejercicios anteriores.

1. Para toda a en B, $a \cdot a = a$.

Demostración: Sea a cualquier elemento de B. Entonces,

$$\begin{aligned} a &= a \cdot 1 && \text{(a)} \\ &= a \cdot (a + \overline{a}) && \text{(b)} \\ &= (a \cdot a) + (a \cdot \overline{a}) && \text{(c)} \\ &= (a \cdot a) + 0 && \text{(d)} \\ &= a \cdot a && \text{(e)}. \end{aligned}$$

2. Para toda a en B, $a + 1 = 1$.

Demostración: Sea a cualquier elemento de B. Entonces

$$\begin{aligned} a + 1 &= a + (a + \overline{a}) && \text{(a)} \\ &= (a + a) + \overline{a} && \text{(b)} \\ &= a + \overline{a} && \text{por el ejemplo 6.4.2} \\ &= 1 && \text{(c)}. \end{aligned}$$

3. Para todas a y b en B, $(a + b) \cdot a = a$.

Demostración: Sea a y b cualesquiera elementos de B. Entonces

$$\begin{aligned} (a + b) \cdot a &= a \cdot (a + b) && \text{(a)} \\ &= a \cdot a + a \cdot b && \text{(b)} \\ &= a + a \cdot b && \text{(c)} \\ &= a \cdot 1 + a \cdot b && \text{(d)} \\ &= a \cdot (1 + b) && \text{(e)} \\ &= a \cdot (b + 1) && \text{(f)} \\ &= a \cdot 1 && \text{por el ejercicio 2} \\ &= a && \text{(g)}. \end{aligned}$$

En los ejercicios del 4 al 10 suponga que B es una álgebra booleana con operaciones $+$ y $\cdot$. Demuestre cada enunciado sin necesidad de utilizar ninguna parte del teorema 6.4.1 a menos que ya se haya demostrado. Sin embargo, se puede utilizar cualquier parte de la definición de una álgebra booleana y los resultados de ejercicios anteriores.

4. Para toda a en B, $a \cdot 0 = 0$.

5. Para todas a y b en B, $(a \cdot b) + a = a$

6. **a.** $\overline{0} = 1$.
   b. $\overline{1} = 0$

7. **a.** Hay un único elemento de B que es una identidad para $+$.
   H b. Hay un único elemento de B que es una identidad para $\cdot$.

8. Para todas a y b en B, $\overline{a \cdot b} = \overline{a} + \overline{b}$. (*Sugerencia:* demuestre que $(a \cdot b) + (\overline{a} + \overline{b}) = 1$ y que $(a \cdot b) \cdot (\overline{a} + \overline{b}) = 0$ y utilice el hecho de que $a \cdot b$ tiene un complemento único.)

9. Para todas a y b en B, $\overline{a + b} = \overline{a} \cdot \overline{b}$.

H 10. Para todas x, y y z en B, si $x + y = x + z$ y $x \cdot y = x \cdot z$, entonces $y = z$.

11. Sea $S = \{0, 1\}$ y defina las operaciones $+$ y $\cdot$ en S con las siguientes tablas:

+	0	1
0	0	1
1	1	1

·	0	1
0	0	0
1	0	1

   a. Demuestre que los elementos de S satisfacen las siguientes propiedades:
      i) ley conmutativa para $+$
      ii) ley conmutativa para $\cdot$
      iii) ley asociativa para $+$
      iv) ley asociativa para $\cdot$
      H v) ley distributiva para $+$ sobre $\cdot$
      vi) ley distributiva para $\cdot$ sobre $+$
   H b. Demuestre que 0 es un elemento identidad para $+$ y que 1 es un elemento identidad para $\cdot$.
   c. Defina $\overline{0} = 1$ y $\overline{1} = 0$. Demuestre que para toda a en S, $a + \overline{a} = 1$ y $a \cdot \overline{a} = 0$. Se deduce de los incisos del *a*) al *c*) que S es un álgebra booleana con operaciones $+$ y $\cdot$.

H ∗ 12. Demuestre que las leyes asociativas de una álgebra booleana se pueden omitir de la definición. Es decir, demuestre que las leyes asociativas se pueden deducir de las otras leyes en la definición.

En los ejercicios del 13 al 18 determine si cada frase es un enunciado. Explique sus respuestas.

13. Esta frase es falsa.

14. Si $1 + 1 = 3$ entonces, $1 = 0$.

15. La frase en este cuadro es una mentira.

16. Todos los enteros positivos con cuadrados negativos son primos.

17. Esta frase es falsa o $1 + 1 = 3$.

18. Esta frase es falsa y $1 + 1 = 2$.

19. a. Suponiendo que la frase siguiente es un enunciado, demuestre que $1 + 1 = 3$:

si esta frase es verdadera, entonces $1 + 1 = 3$.

b. ¿qué se puede deducir del inciso *a*) acerca el estado de "esta frase es verdadera"? ¿Por qué? (En este ejemplo se conoce como **la paradoja de Löb**.)

***H* 20.** Las siguientes dos frases fueron concebidas por el lógico Saul Kripke. Si bien no son intrínsecamente paradójicas, podrían ser paradójicas bajo ciertas circunstancias. Describa tales circunstancias.

(i) La mayoría de las afirmaciones de Nixon acerca del Watergate son falsas.

(ii) Todo lo que Jones dice acerca del Watergate es verdadero.

(*Sugerencia*: Supongamos que Nixon dice *ii*) y el único enunciado que Jones hace acerca de Watergate es *i*).)

21. ¿Puede existir un programa que tenga como salida una lista de todos los programas de computadora que no liste a ellos mismos en su salida? Explique su respuesta.

22. ¿Puede existir un libro que se refiera a todos aquellos libros y sólo aquellos libros que no hagan referencia a sí mismos? Explique su respuesta.

23. Algunos adjetivos son descriptivos de sí mismos (por ejemplo, la palabra *polisilábica es* polisilábica) mientras que otros no lo son (por ejemplo, la palabra *monosilábica* no es monosilábica). La palabra heterológica se refiere a un adjetivo que no se describe por sí mismo. ¿Es *heterológica* heterológica? Explique su respuesta.

24. Por extraño que pueda parecer, es posible dar una definición verbal precisa de un entero que, de hecho, no es una definición para todos los enteros. Lo siguiente fue ideado por un bibliotecario inglés, G. G. Berry y comunicado por Bertrand Russell. Explique cómo conduce a una contradicción. Sea *n* "el entero más pequeño no descrito con menos de 12 palabras en inglés". (Note que el número total de cadenas que consiste en 11 o menos palabras en inglés es finito.)

***H* 25.** ¿Existe un algoritmo que, para una cantidad fija *a* y cualquier entrada de algoritmo *X* y el conjunto de datos *D*, pueda determinar si *X* imprime *a* cuando se ejecuta con el conjunto de datos *D*? Explique. (Este problema se llama el **problema de impresión**.)

26. Usar una técnica similar a la utilizada para deducir la paradoja de Russel para demostrar que para cualquier conjunto A, $\mathscr{P}(A) \not\subseteq A$.

Respuestas del autoexamen

1. la operación de unión $\cup$; la operación de intersección $\cap$; un conjunto universo U; el conjunto vacío $\emptyset$; la operación de complementación, que se denota con ^{c} 2. $\vee$; $\wedge$; $\cup$; $\cap$ 3. el conjunto de todos los conjuntos que no son elementos de sí mismos

CAPÍTULO 7

FUNCIONES

Las funciones están presentes en matemáticas y ciencia computacional. Esto significa que difícilmente puede caminar apenas dos pasos en estos temas sin ejecutar una función. En este libro previamente hemos analizado tablas de verdad y tablas de entrada/salida (que se pueden considerar como funciones booleanas), las sucesiones (que son funciones definidas sobre el conjunto de números enteros), *mod* y *div* (que son funciones definidas sobre productos cartesianos de números enteros) y piso y techo (que son funciones de **R** a **Z**).

En este capítulo consideramos una más amplia variedad de funciones, centrándonos en las que se definen en conjuntos discretos (como conjuntos finitos o conjuntos de enteros). Después vemos las propiedades de las funciones tales como inyectivas y sobreyectivas, la existencia de funciones inversas y la interacción de composición de funciones y las propiedades de inyectiva y sobreyectiva. Terminamos el capítulo con el sorprendente resultado de que hay diferentes tamaños de conjuntos infinitos y se da una aplicación a la computabilidad.

7.1 Funciones definidas sobre conjuntos generales

La teoría que ha tenido el mayor desarrollo en los últimos tiempos es sin duda la teoría de funciones. —Vito Volterra, 1888

Como se utiliza en lenguaje común, la palabra *función* indica la dependencia de una cantidad variable con respecto a otra. Si su profesor le dice que su calificación en el curso será una función de su rendimiento en los exámenes, usted interpreta que esto significa que el maestro tiene algunas reglas para la traducción de los puntajes en las calificaciones de los exámenes. A cada colección de puntajes de examen le corresponde una calificación dada.

En la sección 1.3 definimos una función como un cierto tipo de relación. En este capítulo nos centramos en la forma más dinámica de las funciones que se utilizan en matemáticas. Lo siguiente es un nuevo planteamiento de la definición de función que incluye terminología adicional asociada con el concepto.

• Definición

Una **función *f* de un conjunto *X* a un conjunto *Y***, se denota por $f: X \to Y$ y es una relación del **dominio** X, al **codominio** Y, que satisface dos propiedades: 1) cada elemento en X está relacionado con algún elemento en Y y 2) ningún elemento en X está relacionado con más de un elemento en Y. Por lo que, dado cualquier elemento x en X, hay un único elemento en Y que está relacionado con x por f. Si llamamos a este elemento y, entonces decimos que "f envía x a y" o "f mapea x a y" y se escribe $x \xrightarrow{f} y$ o $f: x \to y$. El único elemento con el que f envía a x se denota

$f(x)$	y se llama	**f de x** o **la salida de f para la entrada x**, o **el valor de f en x**, o **la imagen de x bajo f**.

El conjunto de todos los valores de f se llama el *rango de f* o la *imagen de X bajo f*. Simbólicamente.

$$\textbf{rango de } f = \textbf{imagen de } X \textbf{ bajo } f = \{y \in Y \mid y = f(x), \text{ para alguna } x \text{ en } X\}.$$

Dado un elemento y en Y, pueden existir elementos en X con y como su imagen. Si $f(x) = y$, entonces x se llama **una pre-imagen de *y*** o **de una imagen inversa de *y***. El conjunto de las imágenes inversas de y se llama *la imagen inversa de y*. Simbólicamente

$$\textbf{la imagen inversa de } y = \{x \in X \mid f(x) = y\}.$$

¡Precaución! Use $f(x)$ para referirse al valor de la función f en x. Generalmente evite usar $f(x)$ para referirse a la función f misma.

En el mismo contexto matemático, se usa la notación $f(x)$ para referirse tanto al valor de f en x como a la función f misma. Ya que el uso de la notación de esta manera puede conducir a la confusión, lo evitaremos cada vez que sea posible. En este libro, a menos que se establezca explícitamente de otra manera, el símbolo $f(x)$ siempre se referirá al valor de la función f en x y no a la función f misma.

El concepto de función se desarrolló en un periodo de varios siglos. Una definición similar apenas dada para conjuntos de números fue formulada primero por el matemático alemán Lejeune Dirichlet (DEER-ish-lay) en 1837.

Stock Montage

Johann Peter Gustav Lejeune Dirichlet (1805-1859)

Diagramas de flechas

Recuerde de la sección 1.3 que si X y Y son conjuntos finitos, se puede definir una función f de X a Y dibujando un diagrama de flechas. Realice una lista de elementos en X y una lista de elementos en Y y dibuje una flecha de cada elemento en X al elemento correspondiente en Y, como se muestra en la figura 7.1.1.

Este diagrama de flechas define una función ya que

1. Cada elemento de X tiene una flecha que sale de éste.
2. Ningún elemento de X tiene dos flechas que salen de éste y que apuntan a dos diferentes elementos de Y.

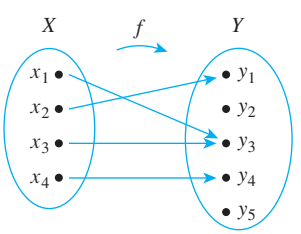
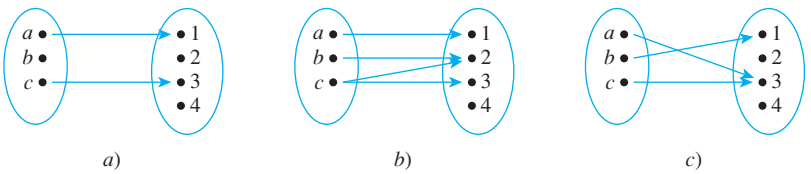


Figura 7.1.1

Ejemplo 7.1.1 Funciones y no funciones

¿Cuál de los diagramas de flechas de la figura 7.1.2 definen funciones de $X = \{a, b, c\}$ a $Y = \{1, 2, 3, 4\}$?



a) *b)* *c)*

Figura 7.1.1

Solución Sólo *c*) define una función. En *a*) hay un elemento de X, a saber, b, que no se envía a ningún elemento de Y; es decir, no hay flecha que salga de b. Y en *b*) el elemento c no envía a un *único* elemento de Y; es decir, hay dos flechas que salen de c, una apunta a 2 y la otra a 3. ■

Ejemplo 7.1.2 Una función definida por un diagrama de flechas

Sea $X = \{a, b, c\}$ y $Y = \{1, 2, 3, 4\}$. Defina una función f de X a Y por el diagrama de flechas de la figura 7.1.3.

a. Escriba el dominio y el codominio de f.

b. Determine $f(a)$, $f(b)$ y $f(c)$.

c. ¿Cuál es el rango de f?

d. ¿Es c una imagen inversa de 2? ¿es b una imagen inversa de 3?

e. Encuentre las imágenes inversas de 2, 4 y 1.

f. Represente f como un conjunto de pares ordenados.

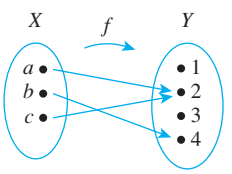


Figura 7.1.1

Solución

a. dominio de $f = \{a, b, c\}$, codominio de $f = \{1, 2, 3, 4\}$

b. $f(a) = 2$, $f(b) = 4$, $f(c) = 2$

c. rango de $f = \{2, 4\}$

d. Sí, No

e. imagen inversa de $2 = \{a, c\}$
imagen inversa de $4 = \{b\}$
imagen inversa de $1 = \emptyset$ (*ya que no hay flechas que apunten a* 1)

f. $\{(a, 2), (b, 4), (c, 2)\}$ ■

En el ejemplo 7.1.2 no hay flechas apuntando al 1 o el 3. Esto ilustra el hecho de que a pesar de que cada elemento del dominio de una función debe tener una flecha apuntando hacia afuera, puede haber elementos del codominio a los que ninguna flecha los apunte. Observe también que hay dos flechas que apuntan al 2, una proviene de a y la otra de c.

En la sección 1.3 se le dio una prueba para determinar si dos funciones con el mismo dominio y codominio son iguales, la prueba da como resultado la definición de una función como una relación binaria. Formalizamos esta justificación en el teorema 7.1.1.

Teorema 7.1.1 Una prueba para la igualdad de funciones

Si $F: X \to Y$ y $G: X \to Y$ son funciones, entonces $F = G$ si y sólo si, $F(x) = G(x)$ para toda $x \in X$.

Demostración:

Suponga que $F: X \to Y$ y $G: X \to Y$ son funciones, es decir, F y G son relaciones binarias de X a Y que satisfacen las dos propiedades adicionales de funciones. Entonces, F y G son subconjuntos de $X \times Y$ y para (x, y) que está en F significa que y es el único elemento relacionado a x con F, lo que se denota por $F(x)$. Del mismo modo, que (x, y) esté en G significa que y es el único elemento relacionando a x por G, lo que denotamos por $G(x)$.

Nota Así $(x, y) \in F \Leftrightarrow y = F(x)$ y $(x, y) \in G \Leftrightarrow y = G(x)$.

Ahora suponga que $F(x) = G(x)$ para toda $x \in X$. Entonces, si x es cualquier elemento de X,

$$(x, y) \in F \Leftrightarrow y = F(x) \Leftrightarrow y = G(x) \Leftrightarrow (x, y) \in G \qquad \text{ya que } F(x) = G(x)$$

Así F y G consisten de exactamente los mismos elementos y por tanto $F = G$.

Por otra parte, si $F = G$, entonces para toda $x \in X$,

$$y = F(x) \Leftrightarrow (x, y) \in F \Leftrightarrow (x, y) \in G \Leftrightarrow y = G(x) \qquad \text{porque } F \text{ y } G \text{ consisten en exactamente los mismos elementos}$$

Ya que tanto $F(x)$ como $G(x)$ son iguales a y, tenemos que

$$F(x) = G(x).$$

Ejemplo 7.1.3 Igualdad de funciones

a. Sea $J_3 = \{0, 1, 2,\}$ y se definen las funciones f y g, de J_3 a J_3 como sigue: Para toda x en J_3,

$$f(x) = (x^2 + x + 1) \ mod \ 3 \quad \text{y} \quad g(x) = (x + 2)^2 \ mod \ 3.$$

¿Es $f = g$?

b. Sean $F: \mathbf{R} \to \mathbf{R}$ y $G: \mathbf{R} \to \mathbf{R}$ funciones. Se definen las nuevas funciones $F + G: \mathbf{R} \to \mathbf{R}$ y $G + F: \mathbf{R} \to \mathbf{R}$ de la siguiente manera: para toda $x \in \mathbf{R}$,

$$(F + G)(x) = F(x) + G(x) \quad \text{y} \quad (G + F)(x) = G(x) + F(x).$$

¿Es $F + G = G + F$?

Solución

a. Sí, la tabla de valores muestra que $f(x) = g(x)$ para toda x en J_3.

x	$x^2 + x + 1$	$f(x) = (x^2 + x + 1) \ mod \ 3$	$(x + 2)^2$	$g(x) = (x + 2)^2 \ mod \ 3$
0	1	$1 \ mod \ 3 = 1$	4	$4 \ mod \ 3 = 1$
1	3	$3 \ mod \ 3 = 0$	9	$9 \ mod \ 3 = 0$
2	7	$7 \ mod \ 3 = 1$	16	$16 \ mod \ 3 = 1$

b. Una vez más, la respuesta es sí. Para todos los números reales x,

$$\begin{aligned} (F + G)(x) &= F(x) + G(x) && \text{por definición de } F + G \\ &= G(x) + F(x) && \text{por la ley conmutativa para la suma de números reales} \\ &= (G + F)(x) && \text{por definición de } G + F \end{aligned}$$

Por tanto, $F + G = G + F$. ■

Ejemplos de funciones

Los siguientes ejemplos ilustran algo de la amplia variedad de diferentes tipos de funciones.

Ejemplo 7.1.4 La función identidad sobre un conjunto

Dado un conjunto X, se define una función I_X de X a X por

$$I_X(x) = x \quad \text{para toda } x \text{ en } X.$$

La función I_X se llama la **función identidad sobre X** porque envía cada elemento de X al elemento que es idéntico a él mismo. Por tanto, la función identidad se puede representar como una máquina que envía cada pieza de entrada directamente al conducto de salida sin cambiarla en modo alguno.

Sea X cualquier conjunto y suponga que a_{ij}^k y $\phi(z)$ son elementos de X. Encuentre $I_X\left(a_{ij}^k\right)$ y $I_X(\phi(z))$.

Solución Todo lo que entra a la función identidad sale sin cambios, así $I_X\left(a_{ij}^k\right) = a_{ij}^k$ y $I_X(\phi(z)) = \phi(z)$. ■

Ejemplo 7.1.5 Sucesiones

La definición formal de sucesiones especifica que una sucesión infinita es una función definida en un conjunto de enteros que son mayores o iguales a un entero dado. Por ejemplo, la sucesión que se denota por

$$1, -\frac{1}{2}, \frac{1}{3}, -\frac{1}{4}, \frac{1}{5}, \ldots, \frac{(-1)^n}{n+1}, \ldots$$

puede pensarse como la función f de los enteros positivos a los números reales que asocia $0 \to 1, 1 \to -\frac{1}{2}, 2 \to \frac{1}{3}, 3 \to -\frac{1}{4}, 4 \to \frac{1}{5}$ y, en general, $n \to \frac{(-1)^n}{n+1}$. En otras palabras, $f: \mathbf{Z}^{noneg} \to \mathbf{R}$ es la función definida como sigue:

$$\text{Envía cada entero } n \geq 0 \text{ a } f(n) = \frac{(-1)^n}{n+1}.$$

De hecho, hay muchas funciones que se pueden utilizar para definir una sucesión dada. Por ejemplo, exprese la sucesión anterior como una función del conjunto de números enteros *positivos* al conjunto de números reales.

Solución Se define $g: \mathbf{Z}^+ \to \mathbf{R}$ por $g(n) = \frac{(-1)^{n+1}}{n}$, para cada $n \in \mathbf{Z}^+$. Entonces $g(1) = 1$, $g(2) = -\frac{1}{2}$, $g(3) = \frac{1}{3}$ y en general

$$g(n+1) = \frac{(-1)^{n+2}}{n+1} = \frac{(-1)^n}{n+1} = f(n).$$ ■

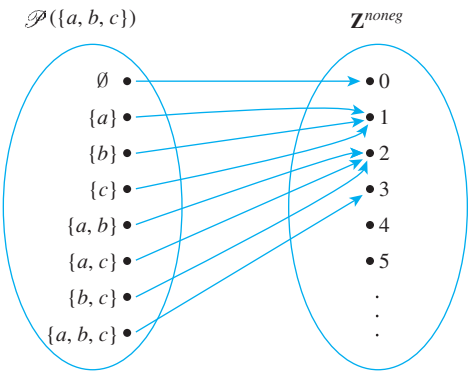
Ejemplo 7.1.6 Una función definida sobre un conjunto potencia

Recuerde de la sección 6.1 que $\mathscr{P}(A)$ denota el conjunto de todos los subconjuntos del conjunto A. Defina una función $F: \mathscr{P}(\{a, b, c\}) \to \mathbf{Z}^{noneg}$ como sigue: Para cada $X \in \mathscr{P}(\{a, b, c\})$,

$$F(X) = \text{el número de elementos en } X.$$

Dibuje un diagrama de flechas para F.

Solución



■

Ejemplo 7.1.7 Funciones definidas sobre un producto cartesiano

Se definen funciones M: $\mathbf{R} \times \mathbf{R} \to \mathbf{R}$ y R: $\mathbf{R} \times \mathbf{R} \to \mathbf{R} \times \mathbf{R}$ como sigue: Para todos los pares de reales (a, b),

$$M(a, b) = ab \quad \text{y} \quad R(a, b) = (-a, b).$$

Nota Se acostumbra omitir un conjunto de paréntesis cuando se refiere a funciones definidas en productos cartesianos. Por ejemplo, se escribe $M(a, b)$ en lugar de $M((a, b))$.

Entonces M es la función multiplicación que envía cada par de números reales al producto de los dos y R es la función de reflexión que envía cada punto en el plano que corresponde a un par de números reales a la imagen espejo del punto a través del eje vertical. Encuentre lo siguiente:

a. $M(-1, -1)$ b. $M\left(\frac{1}{2}, \frac{1}{2}\right)$ c. $M(\sqrt{2}, \sqrt{2})$
d. $R(2, 5)$ e. $R(-2, 5)$ f. $R(3, -4)$

Solución

a. $(-1)(-1) = 1$ b. $(1/2)(1/2) = 1/4$ c. $\sqrt{2} \cdot \sqrt{2} = 2$
d. $(-2, 5)$ e. $(-(-2), 5) = (2, 5)$ f. $(-3, -4)$

■

• Definición de logaritmos y funciones logarítmicas

Sea b un número real positivo con $b \neq 1$. Para cada número real positivo x; el **logaritmo con base b de x**, que se escribe $\log_b x$, es el exponente al que debe elevarse b para obtener x. Simbólicamente,

$$\log_b x = y \quad \Leftrightarrow \quad b^y = x.$$

La **función logarítmica con base b** es la función de $\mathbf{R}^+$ a $\mathbf{R}$ que envía cada número real positivo x a $\log_b x$.

Nota No es obvio, pero es verdad, que para cualquier número real positivo x hay un número real único y, tal que $b^y = x$. La mayoría de los libros de cálculo contienen un análisis de este resultado.

Ejemplo 7.1.8 La función logarítmica con base b

Encuentre lo siguiente:

a. $\log_3 9$ b. $\log_2\left(\frac{1}{2}\right)$ c. $\log_{10}(1)$ d. $\log_2(2^m)$ (m es cualquier número real)

e. $2^{\log_2 m}$ $(m > 0)$

Solución

a. $\log_3 9 = 2$ ya que $3^2 = 9$. b. $\log_2 \left(\frac{1}{2}\right) = -1$ ya que $2^{-1} = \frac{1}{2}$.

c. $\log_{10} (1) = 0$ ya que $10^0 = 1$.

d. $\log_2(2^m) = m$ ya que el exponente al que se debe elevar 2 para obtener 2^m es m.

e. $2^{\log_2 m} = m$ ya que $\log_2 m$ es el exponente al que se debe elevar 2 para obtener m. ■

Recuerde, de la sección 5.9, que si S no es un conjunto vacío y es un conjunto de caracteres finito, entonces una **cadena sobre *S*** es una sucesión finita de elementos de S. El número de caracteres de una cadena se llama la **longitud** de la cadena. La **cadena nula sobre *S*** es la "cadena" sin caracteres. Usualmente se denota por ϵ y se dice que tiene la longitud 0.

Ejemplo 7.1.9 Funciones de codificación y decodificación

Los mensajes digitales constan de sucesiones finitas de 0 y de 1. Cuando se comunican a través de un canal de transmisión, con frecuencia se codifican de forma especial para reducir la posibilidad de que sean ilegibles por ruido que interfiera en las líneas de transmisión. Por ejemplo, suponga que un mensaje consiste en una sucesión de 0 y de 1. Una forma sencilla de codificar el mensaje es escribir cada bit tres veces. Por tanto, el mensaje

$$00101111$$

podría codificarse como

$$000000111000111111111111.$$

El receptor del mensaje lo decodifica sustituyendo cada sección de tres bits idénticos por un bit que es igual a todos los tres.

Sea A el conjunto de todas las cadenas de 0 y de 1 y sea T el conjunto de todas las cadenas de 0 y de 1 que consisten de triples consecutivos bits idénticos. Los procesos de codificación y decodificación descritos anteriormente son realmente funciones de A a T y de T a A. La función de codificación E es la función de A a T se define como sigue: Para cada cadena $s \in A$,

$$E(s) = \text{cadena que se obtiene de } s \text{ al reemplazar cada bit de } s \text{ por el mismo bit escrito tres veces.}$$

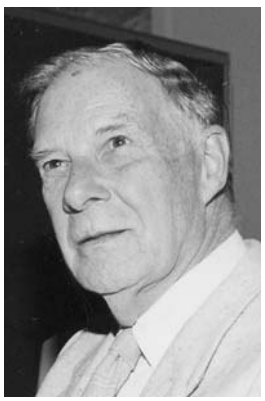
La función de decodificación D se define como sigue: Para cada cadena $t \in T$,

$$D(t) = \text{cadena que se obtiene de } t \text{ al sustituir cada triple consecutivo de tres bits idénticos de } t \text{ por una sola copia de dicho bit.}$$

La ventaja de este esquema de codificación particular es que hace posible hacer una cierta cantidad de corrección de errores cuando hay interferencia en los canales de transmisión que ha introducido errores en la sucesión de bits. Si el receptor del mensaje codificado observa que una de las secciones de tres bits consecutivos que deben ser idénticos no consisten de bits idénticos entonces, un bit difiere de los otros dos. En este caso, si los errores son raros, es probable que el único bit que es diferente es el error y este bit se cambia de acuerdo con los otros dos antes de la decodificación. ■

Ejemplo 7.1.10 La función de distancia de Hamming

La función de distancia de Hamming, nombrada así en honor del científico en computación Richard W. Hamming, es muy importante en la teoría de codificación. Da una medida de la "diferencia" entre dos cadenas de 0 y 1 que tienen la misma longitud. Sea S_n el conjunto



Cortesía de U. S. Naval Academy

Richard Hamming (1915-1998)

de todas las cadenas de 0 y de 1 de longitud n. Defina una función H: $S_n \times S_n \to \mathbf{Z}^{noneg}$ como sigue: Para cada par de cadenas $(s, t) \in S_n \times S_n$,

$$H(s, t) = \text{número de posiciones en las que } s \text{ y } t \text{ tienen valores diferentes.}$$

Por tanto, haciendo $n = 5$, $\quad H(11111, 00000) = 5$

ya que 11111 y 00000 difieren en todas las cinco posiciones, mientras que

$$H(11000, 00000) = 2$$

ya que 11000 y 00000 difieren sólo en las dos primeras posiciones.

a. Encuentre $H(00101, 0\,1\,110)$. b. Encuentre $H(10001, 01111)$.

Solución

a. 3 b. 4 ■

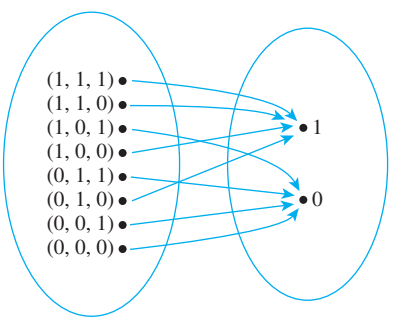
Funciones booleanas

En la sección 2.4 mostramos cómo encontrar tablas de entrada/salida para ciertos circuitos lógicos digitales. Cualquier tabla de entrada/salida define una función de la siguiente manera: Los elementos en la columna de entrada se pueden considerar como tuplas ordenadas de 0 y de 1; el conjunto de todas estas tuplas ordenadas es el dominio de la función. Los elementos en la columna de resultados son ya sea 0 o 1; por tanto {0, 1} se toma como el codominio de la función. La relación que envía cada elemento de entrada al elemento de salida en el mismo renglón. Así, por ejemplo, la tabla de entrada y salida de la figura 7.1.4*a*) define la función con el diagrama de flechas que se muestra en la figura 7.1.4*b*).

Más generalmente, la tabla de entrada/salida correspondiente a un circuito con n cables de entrada tienen n columnas de entrada. Este tipo de tabla define una función del conjunto de todas las n- tuplas de 0 y 1 como el conjunto {0, 1}.

Entrada			Salida
P	***Q***	***R***	***S***
1	1	1	1
1	1	0	1
1	0	1	0
1	0	0	1
0	1	1	0
0	1	0	1
0	0	1	0
0	0	0	0

a)



b)

Figura 7.1.2 **Dos representaciones de una función booleana**

• Definición

Una **función booleana (*n*-lugares)** f es una función cuyo dominio es el conjunto de todas las n-tuplas ordenadas de 0 y 1 y cuyo codominio es el conjunto {0, 1}. Más formalmente, el dominio de una función booleana se puede describir como el producto cartesiano de n copias del conjunto {0, 1}, que se denota por $\{0, 1\}^n$. Por tanto, f: $\{0, 1\}^n \to \{0, 1\}$.

Ejemplo 7.1.11 Una función booleana

Considere la función booleana de tres lugares definida a partir del conjunto de todas las 3-tuplas de 0 y 1 a {0, 1} como sigue: Para cada tripleta (x_1, x_2, x_3) de 0 y 1.

$$f(x_1, x_2, x_3) = (x_1 + x_2 + x_3) \ mod \ 2.$$

Describa f utilizando una tabla de entrada y salida.

Solución
$$f(1, 1, 1) = (1 + 1 + 1) \ mod \ 2 = 3 \ mod \ 2 = 1$$
$$f(1, 1, 0) = (1 + 1 + 0) \ mod \ 2 = 2 \ mod \ 2 = 0$$

Los demás valores de f se pueden calcular de forma similar para obtener la siguiente tabla.

Entrada			Salida
x_1	x_2	x_3	$(x_1 + x_2 + x_3) \ mod \ 2$
1	1	1	1
1	1	0	0
1	0	1	0
1	0	0	1
0	1	1	0
0	1	0	1
0	0	1	1
0	0	0	0

Verificación de si una función está bien definida

A veces puede ocurrir que se presente una función definida por una regla que no es realmente toda una función. Para dar un ejemplo. Suponga que se escribe: Se define una función $f: \mathbf{R} \to \mathbf{R}$ especificando que para todos los números reales x,

$$f(x) \text{ es el número real } y \text{ tal que } x^2 + y^2 = 1.$$

Hay dos razones distintas de por qué esta descripción no define una función. Para casi todos los valores de x, ya sea 1) no hay y que satisfaga la ecuación dada o 2) hay dos valores diferentes de y que satisfacen la ecuación. Por ejemplo, cuando $x = 2$, no hay ningún número real y tal que $2^2 + y^2 = 1$ y cuando $x = 0$, tanto $y = -1$ como $y = 1$ satisfacen la ecuación $0^2 + y^2 = 1$. En general, decimos que la "función" **no está bien definida** si no satisface al menos uno de los requisitos para ser una función.

Ejemplo 7.1.12 Una función que no está bien definida

Recuerde que $\mathbf{Q}$ representa el conjunto de todos los números racionales. Suponga que lee una función $f: \mathbf{Q} \to \mathbf{Z}$ que está definida por la fórmula

$$f\left(\frac{m}{n}\right) = m \quad \text{para todos los enteros } m \text{ y } n \text{ con } n \neq 0.$$

Es decir, el entero asociado por f al número $\frac{m}{n}$ es m. ¿f está bien definida? ¿Por qué?

Solución La función f no está bien definida. La razón es que las fracciones tienen más de una representación como cocientes de enteros. Por ejemplo, $\frac{1}{2} = \frac{3}{6}$. Ahora si f fuera una

función, entonces la definición de una función implicaría que $f\left(\frac{1}{2}\right) = f\left(\frac{3}{6}\right)$ ya que $\frac{1}{2} = \frac{3}{6}$. Pero aplicando la fórmula para f, se encuentra que

$$f\left(\frac{1}{2}\right) = 1 \quad \text{y} \quad f\left(\frac{3}{6}\right) = 3,$$

y por tanto

$$f\left(\frac{1}{2}\right) \neq f\left(\frac{3}{6}\right).$$

Esta contradicción muestra que f no está bien definida y, por tanto, no es una función. ■

Observe que la frase *función bien definida* es realmente redundante; que una función está bien definida realmente significa que merece llamarse una función.

Funciones actuando sobre conjuntos

Dada una función de un conjunto X a un conjunto Y, puede considerar el conjunto de imágenes en Y de todos los elementos en un subconjunto de X y el conjunto de imágenes inversas en X de todos los elementos en un subconjunto de Y.

Nota Para $y \in Y$, $f^{-1}(y) = f^{-1}(\{y\})$.

• Definición

Si $f: X \to Y$ es una función y $A \subseteq X$ y $C \subseteq Y$, entonces

$$f(A) = \{y \in Y \mid y = f(x) \text{ para alguna } x \text{ en } A\}$$

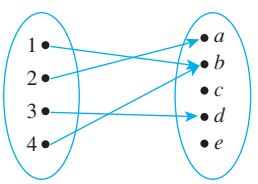
y

$$f^{-1}(C) = \{x \in X \mid f(x) \in C\}.$$

$f(A)$ se llama la **imagen de *A*** y $f^{-1}(C)$ se llama la **imagen inversa de *C***.

Ejemplo 7.1.13 La acción de una función sobre subconjuntos de un conjunto

Sea $X = \{1, 2, 3, 4\}$ y $Y = \{a, b, c, d, e\}$ y se define $F: X \to Y$ por el diagrama de flechas siguiente:



Sea $A = \{1, 4\}$, $C = \{a, b\}$ y $D = \{c, e\}$. Encuentre $F(A)$, $F(X)$, $F^{-1}(C)$ y $F^{-1}(D)$.

Solución

$$F(A) = \{b\} \quad F(X) = \{a, b, d\} \quad F^{-1}(C) = \{1, 2, 4\} \quad F^{-1}(D) = \emptyset$$ ■

Ejemplo 7.1.14 Interacción de una función con unión

Sea X y Y conjuntos, sea F una función de X a Y y sean A y B subconjuntos cualesquiera de X. Demuestre que $F(A \cup B) \subseteq F(A) \cup F(B)$.

Solución

El hecho que X, Y, F, A y B se introdujeran formalmente antes de la palabra "Demostración" le permite considerar su existencia y relaciones como parte de sus fundamentos del conocimiento. Por tanto, para demostrar que $F(A \cup B) \subseteq F(A) \cup F(B)$, sólo necesita demostrar que si y es cualquier elemento de $F(A \cup B)$ entonces, y es un elemento de $F(A) \cup F(B)$.

Demostración:

Suponga que $y \in F(A \cup B)$. *[Debemos demostrar que $y \in F(A) \cup F(B)$.]* Por definición de función, $y = F(x)$ para alguna $x \in A \cup B$. Por definición de unión, $x \in A$ o $x \in B$.

Caso 1. $x \in A$: En este caso, $y = F(x)$ para alguna x en A. Por tanto $y \in F(A)$ y así por definición de unión, $y \in F(A) \cup F(B)$.

Caso 2. $x \in B$: En este caso, $y = F(x)$ para alguna x en B. Por tanto $y \in F(B)$ y así por definición de unión, $y \in F(A) \cup F(B)$.

Por lo que, en cualquier caso $y \in F(A) \cup F(B)$ *[como se quería demostrar]*. ■

En el ejercicio 38 se le pide demostrar la contención opuesta a la del ejemplo 7.1.14. En conjunto, el ejemplo y la demostración al ejercicio establecen la total igualdad de $F(A \cup B) = F(A) \cup F(B)$.

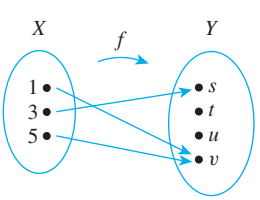
Autoexamen

Las respuestas a las preguntas del autoexamen se encuentran al final de cada sección.

1. Dada una función f de un conjunto X a un conjunto Y, $f(x)$ es _____.
2. Dada una función f de un conjunto X a un conjunto Y, si $f(x) = y$, entonces, y se llama _____ o _____ o _____.
3. Dada una función f de un conjunto X a un conjunto Y, el rango de f (o la imagen de X bajo f) es _____.
4. Dada una función f de un conjunto X a un conjunto Y, si $f(x) = y$, entonces, x se llama _____ o _____.
5. Dada una función f de un conjunto X a un conjunto Y, si $y \in Y$, entonces $f^{-1}(y) =$ _____ y se llama _____.
6. Dadas las funciones f y g de un conjunto X a un conjunto Y, $f = g$ si y sólo si, _____.
7. Dados los números reales positivos x y b con $b \neq 1$, $\log_b x =$ _____.
8. Dada una función f de un conjunto X a un conjunto Y y un subconjunto A de X, $f(A) =$ _____.
9. Dada una función f de un conjunto X a un conjunto Y y un subconjunto C de Y, $f^{-1}(C) =$ _____.

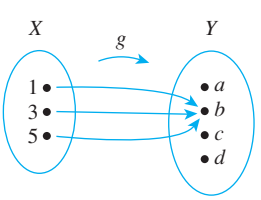
Conjuntos de ejercicios 7.1*

1. Sea $X = \{1, 3, 5\}$ y $Y = \{s, t, u, v\}$. Se define $f: X \to Y$ con el siguiente diagrama de flechas.



a. Escriba el dominio de f y el codominio de f.
b. Encuentre $f(1)$, $f(3)$ y $f(5)$.
c. ¿Cuál es el rango de f?
d. ¿Es 3 una imagen inversa de f? ¿Es 1 imagen inversa de u?
e. ¿Cuál es la imagen inversa de s?, ¿de u?, ¿de v?
f. Represente a f como un conjunto de pares ordenados.

2. Sea $X = \{1, 3, 5\}$ y $Y = \{a, b, c, d\}$. Defina $g: X \to Y$ con el siguiente diagrama de flechas.



a. Escriba el dominio de g y el codominio de g.
b. Encuentre $g(1)$, $g(3)$ y $g(5)$.
c. ¿Cuál es el rango de g?
d. ¿Es 3 una imagen inversa de a? ¿Es 1 una imagen inversa de b?
e. ¿Cuál es la imagen inversa de b?, ¿de c?
f. Represente a g como un conjunto de pares ordenados.

*Para los ejercicios con números o letras azules, las soluciones están dadas en el apéndice B. El símbolo ***H*** indica que sólo se da una sugerencia o una solución parcial. El símbolo ✶ indica que el ejercicio es más difícil de lo normal.

3. Indique si los enunciados en los incisos del *a*) al *d*) son verdaderos o falsos. Justifique sus respuestas.
   a. Si dos elementos en el dominio de una función son iguales, entonces, sus imágenes en el codominio son iguales.
   b. Si dos elementos en el codominio de una función son iguales, entonces, sus pre-imágenes en el dominio también son iguales.
   c. Una función puede tener la misma salida para más de una entrada.
   d. Una función puede tener la misma entrada para más de una salida.

4. **a.** Encuentre todas las funciones de $X = \{a, b\}$ a $Y = \{u, v\}$.
   b. Encuentre todas las funciones de $X = \{a, b, c\}$ a $Y = \{u\}$.
   c. Determine todas las funciones de $X = \{a, b, c\}$ a $Y = \{u, v\}$.

5. Sea $I_{\mathbf{Z}}$ la función identidad definida en el conjunto de todos los enteros y suponga que e, b_i^{jk}, $K(t)$ y u_{kj} todos representan enteros. Determine
   a. $I_{\mathbf{Z}}(e)$ **b.** $I_{\mathbf{Z}}\left(b_i^{jk}\right)$ c. $I_{\mathbf{Z}}(K(t))$ d. $I_{\mathbf{Z}}(u_{kj})$

6. Determine las funciones definidas en el conjunto de enteros no negativos que definen las sucesiones cuyos primeros seis términos son los siguientes.
   a. $1, -\frac{1}{3}, \frac{1}{5}, -\frac{1}{7}, \frac{1}{9}, -\frac{1}{11}$ b. $0, -2, 4, -6, 8, -10$

7. Sea $A = \{1, 2, 3, 4, 5\}$ y defina una función $F: \mathscr{P}(A) \to \mathbf{Z}$ de la siguiente manera: Para todos los conjuntos X en $\mathscr{P}(A)$,

$$F(X) = \begin{cases} 0 & \text{si } X \text{ tiene un número par de elementos} \\ 1 & \text{si } X \text{ tiene un número impar de elementos.} \end{cases}$$

   Determine lo siguiente:
   a. $F(\{1, 3, 4\})$ b. $F(\emptyset)$
   c. $F(\{2, 3\})$ d. $F(\{2, 3, 4, 5\})$

8. Sea $J_5 = \{0, 1, 2, 3, 4\}$ y defina una función $F: J_5 \to J_5$ de la siguiente manera: Para cada $x \in J_5$, $F(x) = (x^3 + 2x + 4)$ *mod* 5.
   Encuentre lo siguiente:
   a. $F(0)$ **b.** $F(1)$ c. $F(2)$ d. $F(3)$ e. $F(4)$

9. Defina una función $S: \mathbf{Z}^+ \to \mathbf{Z}^+$ como sigue: Para cada entero positivo n,
   $S(n) =$ la suma de los divisores positivos de n.
   Determine lo siguiente:
   a. $S(1)$ **b.** $S(15)$ **c.** $S(17)$
   d. $S(5)$ e. $S(18)$ f. $S(21)$

10. Sea D el conjunto de todos los subconjuntos finitos de enteros positivos. Defina una función $T: \mathbf{Z}^+ \to D$ de la siguiente manera: Para cada entero positivo n, $T(n) =$ el conjunto de divisores positivos de n.
    Determine lo siguiente:
    a. $T(1)$ **b.** $T(15)$ **c.** $T(17)$
    d. $T(5)$ e. $T(18)$ f. $T(21)$

11. Defina $F: \mathbf{Z} \times \mathbf{Z} \to \mathbf{Z} \times \mathbf{Z}$ como sigue: Para todos los pares ordenados (a, b) de enteros, $F(a, b) = (2a + 1, 3b - 2)$.
    Encuentre lo siguiente:
    a. $F(4, 4)$ **b.** $F(2, 1)$ c. $F(3, 2)$ d. $F(1, 5)$

12. Defina $G: J_5 \times J_5 \to J_5 \times J_5$ como sigue: Para todo $(a, b) \in J_5 \times J_5$,
    $G(a, b) = ((2a + 1)$ *mod* $5, (3b - 2)$ *mod* $5)$.
    Encuentre lo siguiente:
    a. $G(4, 4)$ **b.** $G(2, 1)$ c. $G(3, 2)$ d. $G(1, 5)$

13. Sea $J_5 = \{0, 1, 2, 3, 4\}$ y defina las funciones $f: J_5 \to J_5$ y $g: J_5 \to J_5$ como sigue: Para cada $x \in J_5$,
    $f(x) = (x + 4)^2$ *mod* 5 y $g(x) = (x^2 + 3x + 1)$ *mod* 5.
    ¿Es $f = g$? Explique.

14. Sea $J_5 = \{0, 1, 2, 3, 4\}$ y defina las funciones $h: J_5 \to J_5$ y $k: J_5 \to J_5$ de la siguiente manera: Para cada $x \in J_5$,
    $h(x) = (x + 3)^2$ *mod* 5 y $k(x) = (x^3 + 4x^2 + 2x + 2)$ *mod* 5.
    ¿Es $h = k$? Explique.

15. Sean F y G funciones del conjunto de todos los números reales a sí mismo. Defina el producto de funciones $F \cdot G: \mathbf{R} \to \mathbf{R}$ y $G \cdot F: \mathbf{R} \to \mathbf{R}$ de la siguiente manera: Para toda $x \in \mathbf{R}$,
    $$(F \cdot G)(x) = F(x) \cdot G(x)$$
    $$(G \cdot F)(x) = G(x) \cdot F(x)$$
    ¿Es $F \cdot G = G \cdot F$? Explique.

16. Sean F y G funciones del conjunto de todos los números reales a sí mismo. Defina las nuevas funciones $F - G: \mathbf{R} \to \mathbf{R}$ y $G - F: \mathbf{R} \to \mathbf{R}$ como sigue: Para toda $x \in \mathbf{R}$,
    $$(F - G)(x) = F(x) - G(x)$$
    $$(G - F)(x) = G(x) - F(x)$$
    ¿Es $F - G = G - F$? Explique.

17. Utilice la definición del logaritmo para completar los siguientes espacios en blanco.
    a. $\log_2 8 = 3$ ya que _____
    b. $\log_5\left(\frac{1}{25}\right) = -2$ ya que _____
    c. $\log_4 4 = 1$ ya que _____
    d. $\log_3 (3^n) = n$ ya que _____
    e. $\log_4 1 = 0$ ya que _____

18. Encuentre los valores exactos para cada una de las siguientes cantidades. No utilice una calculadora.
    a. $\log_3 81$ b. $\log_2 1024$ **c.** $\log_3\left(\frac{1}{27}\right)$ d. $\log_2 1$
    e. $\log_{10}\left(\frac{1}{10}\right)$ f. $\log_3 3$ g. $\log_2(2^k)$

19. Utilice la definición de logaritmo para demostrar que para cualquier número real positivo b con $b \neq 1$, $\log_b b = 1$.

20. Utilice la definición de logaritmo para demostrar que para cualquier número real positivo b con $b \neq 1$, $\log_b 1 = 0$.

21. Si b es cualquier número real positivo con $b \neq 1$ y x es cualquier número real, b^{-x} se define como: $b^{-x} = \frac{1}{b^x}$. Utilice esta definición y la definición de logaritmo para demostrar que $\log_b\left(\frac{1}{u}\right) = -\log_b(u)$ para todos los números reales positivos u y b, con $b \neq 1$.

***H* 22.** Utilice la factorización única del teorema de enteros (sección 4.3) y la definición de logaritmo en demostrar que $\log_3(7)$ es irracional.

23. Si b y y son números de reales positivos tales que $\log_b y = 3$, ¿A qué es igual $\log_{1/b}(y)$?¿Por qué?

24. Si b y y son números de reales positivos tales que $\log_b y = 2$, ¿A qué es igual $\log_{b^2}(y)$? ¿Por qué?

25. Sea $A = \{2, 3, 5\}$ y $B = \{x, y\}$. Sea p_1 y p_2 las **proyecciones de $A \times B$ sobre la primera y segunda coordenadas**. Es decir, para cada par $(a, b) \in A \times B$, $p_1(a, b) = a$ y $p_2(a, b) = b$.

a. Encuentre $p_1(2, y)$ y $p_1(5, x)$. ¿Cuál es el rango de p_1?
b. Encuentre $p_1(2, y)$ y $p_2(5, x)$. ¿Cuál es el rango de p_2?

26. Observe que *mod* y *div* se pueden definir como funciones de $\mathbf{Z}^{noneg} \times \mathbf{Z}^+$ a $\mathbf{Z}$. Para cada uno de los pares ordenados (n, d) consisten de un entero no negativo n y un entero positivo d, sean

$$mod(n, d) = n \bmod d \text{ (el residuo no negativo obtenido cuando se divide } n \text{ por } d).$$

$$div(n, d) = n \operatorname{div} d \text{ (el cociente de entero obtenido cuando } n \text{ se divide por } d).$$

Encuentre cada una de las siguientes expresiones:

a. *mod* (67, 10) y *div* (67, 10)
b. *mod* (59, 8) y *div* (59, 8)
c. *mod* (30, 5) y *div* (30, 5)

27. Sea S el conjunto de todas las cadenas de a y de b.

a. Defina $f: S \to Z$ como sigue: Para cada cadena s en S

$$f(s) \begin{cases} \text{el número de } b\text{'s a la izquierda de la } a \text{ que está más hacia la izquierda en } s \\ 0 \quad \text{si } s \text{ no tiene } a\text{'s.} \end{cases}$$

Encuentre $f(aba)$ y $f(bbab)$ y $f(b)$. ¿Cuál es el rango de f?
b. Defina $g: S \to S$ de la siguiente manera: para cada cadena s en S,

$$g(s) = \text{la cadena obtenida al escribir los caracteres de } s \text{ en orden inverso}$$

Determine $g(aba)$, $g(bbab)$ y $g(b)$. ¿Cuál es el rango de g?

28. Considere las funciones de codificación y decodificación E y D definidas en el ejemplo 7.1.9.

a. Encuentre $E(0110)$ y $D(111111000111)$.
b. Encuentre $E(1010)$ y $D(000000111111)$.

29. Considere la función de distancia de Hamming definida en el ejemplo 7.1.10.

a. Determine $H(10101, 00011)$
b. Encuentre $H(00110, 10111)$.

30. Dibuje diagramas de flechas para las funciones booleanas definidas por la siguiente tabla de entrada y salida.

a.

Entrada		Salida
P	***Q***	***R***
1	1	0
1	0	1
0	1	0
0	0	1

b.

Entrada			Salida
P	***Q***	***R***	***S***
1	1	1	1
1	1	0	0
1	0	1	1
1	0	0	1
0	1	1	0
0	1	0	0
0	0	1	0
0	0	0	1

31. Complete la tabla siguiente para mostrar los valores de todas las funciones booleanas de dos lugares posibles.

Entrada	f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8	f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}	f_{16}
1 1																
1 0																
0 1																
0 0																

32. Considere la función booleana de tres lugares f que se define por la siguiente regla: para cada tripleta (x_1, x_2, x_3) de 0's y de 1's,

$$f(x_1, x_2, x_3) = (4x_1 + 3x_2 + 2x_3) \bmod 2.$$

a. Encuentre $f(1, 1, 1)$ y $f(0, 0, 1)$.
b. Describa f utilizando una tabla de entrada y salida.

33. El estudiante A intenta definir una función $g: \mathbf{Q} \to \mathbf{Z}$ por la regla

$$g\left(\frac{m}{n}\right) = m - n, \text{ para todos los enteros } m \text{ y } n \text{ con } n \neq 0.$$

El estudiante B afirma que g no está bien definida. Justifique la afirmación del estudiante B.

34. El estudiante C intenta definir una función $h: \mathbf{Q} \to \mathbf{Q}$ por la regla

$$h\left(\frac{m}{n}\right) = \frac{m^2}{n}, \text{ para todos los enteros } m \text{ y } n \text{ con } n \neq 0.$$

El estudiante D afirma que h no está bien definida. Justifique la afirmación del estudiante D.

35. Sea $J_5 = \{0, 1, 2, 3, 4\}$. Entonces $J_5 - \{0\} = \{1, 2, 3, 4\}$. El estudiante A intenta definir una función $R: J_5 - \{0\} \to J_5 - \{0\}$ de la siguiente manera: Para cada $x \in J_5 - \{0\}$,

$$R(x) \text{ es el número } y \text{ para que } (xy) \; mod \; 5 = 1.$$

El estudiante B afirma que R no está bien definida. ¿Quién tiene razón: el estudiante A o el estudiante B? Justifique su respuesta.

36. Sea $J_4 = \{0, 1, 2, 3\}$. Entonces $J_4 - \{0\} = \{1, 2, 3\}$. El estudiante C intenta definir una función de S: $J_4 - \{0\} \to J_4 - \{0\}$ como sigue: Para cada $x \in J_4 - \{0\}$,

$$S(x) \text{ es el número } y \text{ para que } (xy) \; mod \; 4 = 1.$$

El estudiante F afirma que S no está bien definida. ¿Quién tiene razón: el estudiante C o el estudiante D? Justifique su respuesta.

37. En ciertas computadoras, el tipo de datos enteros van de -2, 147, 483, 648 a 2, 147, 483, 647. Sea S el conjunto de todos los enteros de -2, 147, 483, 648 a 2, 147, 483, 647. Trate de definir una función $f: S \to S$ con la regla $f(n) = n^2$ para cada n en S. ¿Está f bien definida? ¿Por qué?

38. Sea $X = \{a, b, c\}$ y $Y = \{r, s, t, u, v, w\}$. Defina $f: X \to Y$ de la siguiente manera: $f(a) = v$, $f(b) = v$ y $f(c) = t$.
a. Dibuje un diagrama de flechas para g.
b. Sea $A = \{a, b\}$, $C = \{t\}$, $D = \{u, v\}$ y $E = \{r, s\}$. Determine $f(A)$, $f(X)$, $f^{-1}(C)$, $f^{-1}(D)$, $f^{-1}(E)$ y $f^{-1}(Y)$.

39. Sea $X = \{1, 2, 3, 4\}$ y $Y = \{a, b, c, d, e\}$. Defina $g: X \to Y$ como sigue: $g(1) = a$, $g(2) = a$, $g(3) = a$ y $g(4) = d$.
a. Dibuje un diagrama de flechas para g.
b. Sea $A = \{2, 3\}$, $C = \{a\}$ y $D = \{b, c\}$. Encuentre $g(A)$, $g(X)$, $g^{-1}(C)$, $g^{-1}(D)$ y $g^{-1}(Y)$.

***H* 40.** Sean X y Y conjuntos, sean A y B subconjuntos cualesquiera de X y sea F una función de X a Y. Complete los espacios en blanco en la siguiente demostración de que $F(A) \cup F(B) \subseteq F(A \cup B)$.

Demostración: Sea y cualquier elemento en $F(A) \cup F(B)$. *[Debemos demostrar que y está en $F(A \cup B)$.]* Por definición de unión, __(a)__.

Caso 1. $y \in F(A)$: En este caso, por definición de $F(A)$, $y = F(x)$ para __(b)__ $x \in A$. Puesto que $A \subseteq A \cup B$, se tiene por la definición de unión que $x \in$ __(c)__. Por tanto, $y = F(x)$ para algún $x \in A \cup B$ y así por definición de $F(A \cup B)$, $y \in$ __(d)__.

Caso 2. $y \in F(B)$: En este caso, por definición de $F(B)$, __(e)__ $x \in B$. Ya que $B \subseteq A \cup B$ se deduce de la definición de unión que __(f)__.

Por tanto, independientemente de si $y \in F(A)$ o $y \in F(B)$ tenemos que $y \in F(A \cup B)$ *[como se quería demostrar]*.

En los ejercicios del 41 al 49, sean X y Y conjuntos, sean A y B subconjuntos cualesquiera de X y sea C y D subconjuntos cualesquiera de Y. Determine cuáles de las propiedades son verdaderas para todas las funciones F de X a Y y cuáles son falsas para al menos una función F de X a Y. Justifique sus respuestas.

41. Si $A \subseteq B$, entonces $F(A) \subseteq F(B)$.

42. $F(A \cap B) \subseteq F(A) \cap F(B)$

43. $F(A) \cap F(B) \subseteq F(A \cap B)$

44. Para todos los subconjuntos A y B de X, $F(A - B) = F(A) - F(B)$.

45. Para todos los subconjuntos C y D de Y, si $C \subseteq D$ entonces,

$$F^{-1}(C) \subseteq F^{-1}(D).$$

***H* 46.** Para todos los subconjuntos C y D de Y,

$$F^{-1}(C \cup D) = F^{-1}(C) \cup F^{-1}(D).$$

47. Para todos los subconjuntos C y D de Y,

$$F^{-1}(C \cap D) = F^{-1}(C) \cap F^{-1}(D).$$

48. Para todos los subconjuntos C y D de Y,

$$F^{-1}(C - D) = F^{-1}(C) - F^{-1}(D).$$

49. $F(F^{-1}(C)) \subseteq C$

50. Dado un conjunto S y un subconjunto A, la **función característica de A**, que se denota χ_A, es la función definida de S a $\mathbf{Z}$ con la propiedad que por toda $u \in S$,

$$\chi_A(u) = \begin{cases} 1 & \text{si } u \in A \\ 0 & \text{si } u \notin A. \end{cases}$$

Demuestre que cada una de las siguientes afirmaciones se cumple para todos los subconjuntos A y B de S y para toda $u \in S$.
a. $\chi_{A \cap B}(u) = \chi_A(u) \cdot \chi_B(u)$
b. $\chi_{A \cup B}(u) = \chi_A(u) + \chi_B(u) - \chi_A(u) \cdot \chi_B(u)$

Cada uno de los ejercicios del 51 al 53 se refiere a la función phi de Euler, que se denota por ϕ, que se define como sigue: para cada entero $n \geq 1$, $\phi(n)$ es el número de enteros positivos menores o iguales a n que no tienen ningún factor común con n excepto ± 1. Por ejemplo, $\phi(10) = 4$ ya que hay cuatro enteros positivos menores o iguales a 10 que no tienen ningún factor común con 10 excepto ± 1: a saber, 1, 3, 7 y 9.

51. Encuentre cada uno de los siguientes:
a. $\phi(15)$ **b.** $\phi(2)$ **c.** $\phi(5)$
d. $\phi(12)$ e. $\phi(11)$ f. $\phi(1)$

***⋆* 52.** Demuestre que si p es un número primo y n es un entero con $n \geq 1$, entonces $\phi(p^n) = p^n - p^{n-1}$.

***H* 53.** Demuestre que hay infinito de números enteros n para los que $\phi(n)$ es un cuadrado perfecto.

Respuestas del autoexamen

1. el único elemento de salida en Y que esté relacionado con x por f 2. el valor de f en x; la imagen de x bajo f; la salida de f para la entrada x 3. el conjunto de toda y en Y tal que $f(x) = y$ 4. una imagen inversa de y bajo f; un preimagen de y 5. $\{x \in X \mid f(x) = y\}$; la imagen inversa de y 6. $f(x) = g(x)$ para toda $x \in X$ 7. el exponente al que hay que elevar a b para obtener x (O: el número real y tal que $x = b^y$) 8. $\{y \in Y \mid y = f(x)$ para alguna $x \in A\}$ (O: $\{f(x) \mid x \in A\}$) 9. $\{x \in X \mid f(x) \in C\}$

7.2 Inyectiva y sobreyectiva, funciones inversas

No acepte un enunciado sólo porque está impreso. —Anna Pell Wheeler, 1883-1966

En esta sección se analizan dos propiedades importantes que pueden satisfacer las funciones: la propiedad de ser *inyectiva* y la propiedad de ser *sobreyectiva*. A las funciones que satisfacen ambas propiedades se les llama funciones con *correspondencia inyectiva* o *funciones inyectivas sobreyectivas*. Cuando una función tiene una correspondencia inyectiva, los elementos de su dominio y de su codominio corresponden perfectamente y se puede definir una *función inversa* del codominio al dominio que "deshace" la acción de la función.

Funciones inyectivas

En la sección 7.1 se observó que una función puede enviar varios elementos de su dominio a un mismo elemento de su codominio. En términos de diagramas de flechas, esto significa que dos o más flechas que inician en el dominio pueden apuntar al mismo elemento en el codominio. Por otra parte, si no hay dos flechas que comienzan en un punto del dominio al mismo elemento del codominio, entonces, la función se llama *inyectiva* o *uno a uno*. En una función inyectiva, cada elemento del rango es la imagen de a lo más un elemento del dominio.

• Definición

Sea F una función de un conjunto X a un conjunto Y. F es **inyectiva** (o **uno a uno**) si y sólo si, para todos los elementos x_1 y x_2 en X.

$$\text{si } F(x_1) = F(x_2), \text{ entonces } x_1 = x_2,$$

o, de forma equivalente, si $x_1 \neq x_2$, entonces $F(x_1) \neq F(x_2)$.

Simbólicamente,

$$F: X \to Y \text{ es inyectiva} \quad \Leftrightarrow \quad \forall x_1, x_2 \in X, \text{ si } F(x_1) = F(x_2) \text{ entonces } x_1 = x_2.$$

Para obtener un enunciado preciso de lo que significa que una función *no* sea inyectiva, se toma la negación de una de las versiones equivalentes de la definición anterior. De esta forma:

$$\text{Una función } F: X \to Y \textit{ no} \text{ es inyectiva} \quad \Leftrightarrow \quad \exists \text{ elementos } x_1 \text{ y } x_2 \text{ en } X \text{ con } F(x_1) = F(x_2) \text{ y } x_1 \neq x_2.$$

Es decir, si se encuentra que los elementos x_1 y x_2 tienen el mismo valor de la función pero no son iguales, entonces F no es inyectiva.

En términos de diagramas de flechas, una función inyectiva puede pensarse como una función que separa puntos. Es decir, manda puntos distintos del dominio a puntos distintos puntos del codominio. Una función que no es inyectiva no puede separar puntos. Es decir, al menos dos puntos del dominio se mandan al mismo punto del codominio. Esto se ilustra en la figura 7.2.1, en la página siguiente.

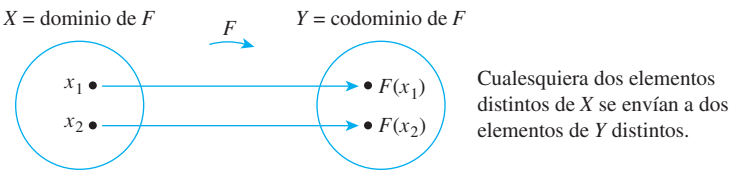


Figura 7.2.1*a*) **Una función inyectiva separa puntos**

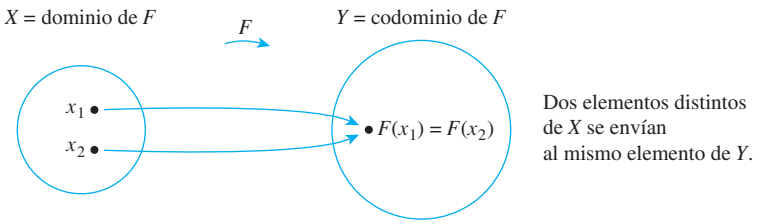


Figura 7.2.1*b*) **Una función que no es inyectiva colapsa puntos juntos**

Ejemplo 7.2.1 Identificación de funciones inyectivas definidas sobre conjuntos finitos

a. ¿Cualquiera de los diagramas de flechas en la figura 7.2.2 define funciones inyectivas?

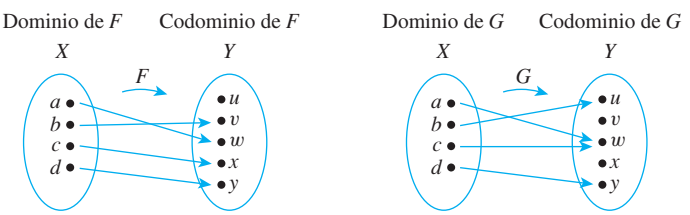


Figura 7.2.2

b. Sea $X = \{1, 2, 3\}$ y $Y = \{a, b, c, d\}$. Se define $H: X \to Y$ como sigue: $H(1) = c$, $H(2) = a$ y $H(3) = d$. Se define $K: X \to Y$ como sigue: $K(1) = d$, $K(2) = b$ y $K(3) = d$. ¿Es H o K inyectiva?

Solución

a. F es inyectiva, pero G no. F es inyectiva, ya que no hay dos elementos diferentes de X que se envían con F al mismo elemento de Y. G no es inyectiva ya que los elementos a y c son ambos enviados con G al mismo elemento de Y: $G(a) = G(c) = w$, pero $a \neq c$.

b. H es inyectiva, pero K no lo es. H es inyectiva, ya que cada uno de los tres elementos del dominio de H se envía con H a un elemento diferente del codominio: $H(1) \neq H(2)$, $H(1) \neq H(3)$ y $H(2) \neq H(3)$. Sin embargo, K, no es inyectiva porque $K(1) = K(3) = d$, pero $1 \neq 3$. ■

Considere el problema de escribir un algoritmo de computadora para comprobar si una función F es inyectiva. Si F se define sobre un conjunto finito y hay un algoritmo independiente para calcular valores de F, entonces un algoritmo para comprobar si F es inyectiva puede escribirse de la siguiente manera: Represente el dominio de F como un arreglo unidimensional $a[1], a[2], \ldots, a[n]$ y utilice el bucle anidado para examinar todos los pares posibles $(a[i], a[j])$, donde $i < j$. Si hay un par $(a[i], a[j])$ para el que $F(a[i]) = F(a[j])$ y $a[i] \neq a[j]$, entonces F no es inyectiva. Sin embargo, si se han examinado todos los pares sin encontrar dicho par, entonces F es inyectiva. Se le pide que escriba dicho algoritmo en el ejercicio 57 al final de esta sección.

Funciones inyectivas sobre conjuntos infinitos

Ahora suponga que f es una función definida en un conjunto infinito de X. Por definición, f es inyectiva si y sólo si, el siguiente enunciado universal es verdadero:

$$\forall x_1, x_2 \in X, \text{ si } f(x_1) = f(x_2) \text{ entonces } x_1 = x_2.$$

Por lo que, para demostrar que f es inyectiva, por lo general se utiliza el método de demostración directa:

suponga que x_1 y x_2 son elementos de X tal que $f(x_1) = f(x_2)$

y **demuestre** que $x_1 = x_2$.

Para demostrar que f *no* es inyectiva, comúnmente

encuentre elementos x_1 y x_2 en X tales que $f(x_1) = f(x_2)$, pero $x_1 \neq x_2$.

Ejemplo 7.2.2 Demostración o refutación de que las funciones son inyectivas

Se definen $f: \mathbf{R} \to \mathbf{R}$ y $g: \mathbf{Z} \to \mathbf{Z}$ con las reglas

$$f(x) = 4x - 1 \quad \text{para toda} \quad x \in \mathbf{R}$$

y

$$g(x) = n^2 \quad \text{para toda} \quad n \in \mathbf{Z}.$$

a. ¿Es f uno a uno? Demuestre o dé un contraejemplo.

b. ¿Es g uno a uno? Demuestre o dé un contraejemplo.

Solución Normalmente es mejor empezar por adoptar un enfoque positivo para responder a preguntas como estas. Intente demostrar que las funciones dadas son inyectiva y vea si no se presentan problemas. Si termina sin problemas, entonces tendrá una demostración. Si encuentra un problema, entonces, analizar el problema le puede conducir a descubrir un contraejemplo.

a. La función $f: \mathbf{R} \to \mathbf{R}$ se define por la regla

$$f(x) = 4x - 1 \quad \text{para todos los números reales } x.$$

Para demostrar que f es inyectiva, se necesita demostrar que

$$\forall \text{ números reales } x_1 \text{ y } x_2, \text{ si } f(x_1) = f(x_2), \text{ entonces, } x_1 = x_2.$$

Sustituyendo la definición de f en el diseño de una demostración directa, usted

suponga que x_1 y x_2 son números reales tales que $4x_1 - 1 = 4x_2 - 1$,

y **demuestre** que $x_1 = x_2$.

¿Puede demostrar a partir de la suposición? Por supuesto. Simplemente debe sumar 1 a ambos lados de la ecuación de la suposición y después dividir ambos lados por 4.

Este análisis se resume en la siguiente respuesta formal.

Respuesta a *a*):

Si la función f: $\mathbf{R} \to \mathbf{R}$ se define por la regla $f(x) = 4x - 1$, para todos los números reales x, entonces f es inyectiva.

Demostración:

Suponga que x_1 y x_2 son números reales tales que $f(x_1) = f(x_2)$. *[Debemos demostrar que $x_1 = x_2$.]* Por definición de f,

$$4x_1 - 1 = 4x_2 - 1.$$

Sumando 1 en ambos miembros se obtiene

$$4x_1 = 4x_2,$$

y dividiendo ambos lados entre 4 se obtiene

$$x_1 = x_2,$$

que es lo que se quería demostrar.

b. La función g: $\mathbf{Z} \to \mathbf{Z}$ se define con la regla

$$g(n) = n^2 \quad \text{para todos los enteros } n.$$

Como ya se indicó, se comienza demostrando que g es inyectiva. Se sustituye la definición de g en el diseño de una demostración directa, usted

suponga que n_1 y n_2 son enteros tales que $n_1^2 = n_2^2$,

e **intente demostrar** que $n_1 = n_2$.

¿Lo puede demostrar a partir de la suposición? ¡No! Es bastante posible que dos números tengan los mismos cuadrados y sean diferentes. Por ejemplo, $2^2 = (-2)^2$, pero $2 \neq -2$.

Por tanto, al tratar de demostrar que g es inyectiva, se encuentra una dificultad. Y el analizar esta dificultad conduce al descubrimiento de un contraejemplo, que muestra que g no es inyectiva.

Este análisis se resume como sigue:

Respuesta a *b*):

Si la función g: $\mathbf{Z} \to \mathbf{Z}$ se define con la regla $g(n) = n^2$, para toda $n \in \mathbf{Z}$, entonces g no es inyectiva.

Contraejemplo:

Sean $n_1 = 2$ y $n_2 = -2$. Entonces, por definición de g,

$$g(n_1) = g(2) = 2^2 = 4 \quad \text{y también}$$

$$g(n_2) = g(-2) = (-2)^2 = 4,$$

Por tanto $\quad g(n_1) = g(n_2) \quad \text{pero} \quad n_1 \neq n_2,$

y así g no es inyectiva.

■

Aplicación: Funciones Hash

Imagine un conjunto de registros de los estudiantes, que incluye número de seguro social y suponga que los registros se pueden almacenar en una tabla en la que se puede encontrar un registro si se conoce el número de seguridad social. Una manera de hacer esto sería colocar el registro con el número de seguro social n en la posición n de la tabla. Sin embargo, como los números de seguro social tienen nueve dígitos, este método requeriría una tabla con 999 999 999 posiciones. El problema es que la creación de este tipo de tabla para un pequeño conjunto de registros sería un desperdicio de espacio de memoria de la computadora. Las **funciones Hash** son funciones definidas de conjuntos de enteros de mayores a menores, con frecuencia se utiliza la función *mod*, que constituye parte de la solución a este problema. Mostramos cómo definir y utilizar una función *hash* con un ejemplo muy sencillo.

Ejemplo 7.2.3 Una función Hash

Suponga que no hay más registros que los de siete estudiantes. Defina una función *Hash* del conjunto de todos los números de seguridad social (ignorando los guiones) al conjunto $\{0, 1, 2, 3, 4, 5, 6\}$ como sigue:

$$Hash(n) = n \bmod 7 \quad \text{para todos los } n \text{ números de seguridad social.}$$

Utilice la calculadora para encontrar $n \bmod 7$, utilice la fórmula $n \bmod 7 = n - 7 \cdot (n \operatorname{div} 7)$. (Consulte la sección 4.4.) En otras palabras, divida n entre 7, multiplique la parte entera del resultado por 7 y reste ese número de n. Por ejemplo, ya $328343419/7 = 46906202.71\ldots$,

$$Hash(328\text{-}34\text{-}3419) = 328343419 - (7 \cdot 46906202) = 5.$$

Como una primera aproximación para resolver el problema de almacenar los registros, intente colocar el registro con el número de seguro social n en la posición $Hash(n)$. Por ejemplo. Si los números de seguridad social son 328-34-3419, 356-63-3102, 223-79-9061 y 513-40-8716, las posiciones de los registros son como se muestra en la tabla 7.2.1.

Tabla 7.2.1

0	356-63-3102
1	
2	513-40-8716
3	223-79-9061
4	
5	328-34-3419
6	

El problema con este enfoque es que la función *Hash* no sea inyectiva; la función *Hash* podría asignar la misma posición en la tabla a registros con diferentes números de seguridad social. A dicha asignación se le llama una **colisión**. Cuando se producen colisiones, se utilizan diversos **métodos de resolución de colisión**. Uno de los más simples es el siguiente: Si, cuando el registro con número de seguro social n se debe colocar, la posición $Hash(n)$ ya está ocupada, inicie desde esa posición y busque hacia abajo para colocar el registro en la primera posición vacía que se presente, regrese al comienzo de la tabla si es necesario. Para localizar un registro en la tabla de su número de seguro social, n, calcule $Hash(n)$ y busque hacia abajo desde esa posición para encontrar el registro con número de seguro social n. Si no hay demasiadas colisiones, esta es una forma muy eficiente para almacenar y localizar registros.

Suponga que almacena otro número de seguro social para otro registro 908-37-1011. Determine la posición en la tabla 7.2.1 en que se pondría este registro.

Solución Cuando calcula *Hash* encuentra que $Hash(908\text{-}31\text{-}1011) = 2$, que ya está ocupado por el registro con el número de seguro social 513-40-8716. Buscando hacia abajo desde la posición 2, encontrará que la posición 3 también está ocupada pero la posición 4 está libre.

$$908\text{-}37\text{-}1011 \xrightarrow{Hash} \underset{\text{ocupada}}{2} \rightarrow \underset{\text{ocupada}}{3} \rightarrow \underset{\text{libre}}{4}$$

Por tanto, coloque el registro con el número de seguro social n en la posición 4. ■

Funciones sobreyectivas

Como se indicó en la sección 7.1 puede haber un elemento del codominio de una función que no es la imagen de cualquier elemento en el dominio. Por otra parte, *cada* elemento del codominio de una función puede ser la imagen de algún elemento de su dominio. Esta función se llama *sobreyectiva*. Cuando una función es sobreyectiva su rango es igual a su codominio.

• Definición

Sea F una función de un conjunto X a un conjunto Y. F es **sobreyectiva** si y sólo si, dado cualquier elemento y en Y, es posible encontrar un elemento x en X con la propiedad de que $y = F(x)$.

Simbólicamente:

$$F: X \to Y \text{ es sobreyectiva} \quad \Leftrightarrow \quad \forall y \in Y, \exists x \in X \text{ tal que } F(x) = y.$$

Para obtener un enunciado preciso de lo que significa que una función *no* sea sobreyectiva, tome la negación de la definición de sobreyectiva:

$$F: X \to Y \textit{ no} \text{ es sobreyectiva} \quad \Leftrightarrow \quad \exists y \text{ en } Y \text{ tal que } \forall x \in X, F(x) \neq y.$$

Es decir, hay algún elemento en Y que *no* es la imagen de *ningún* elemento en X.

En términos de diagramas de flechas, una función es sobreyectiva, si cada elemento del codominio tiene una flecha apuntando al mismo elemento del dominio. Una función no es sobreyectiva, si al menos un elemento en su codominio no tiene una flecha apuntándolo. En la figura 7.2.3, se muestra esto.

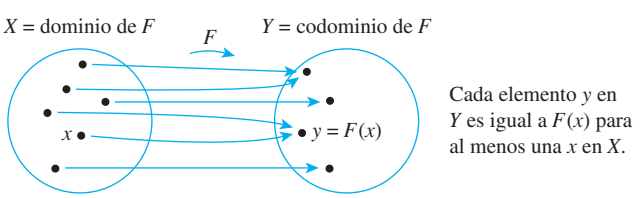


Figura 7.2.3*a*) **Una función que es sobreyectiva**

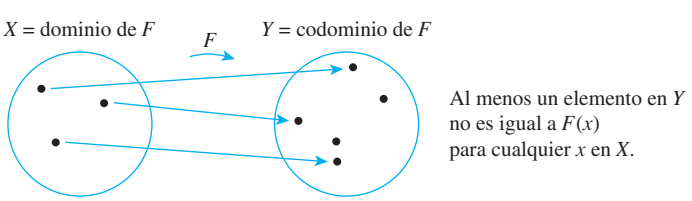


Figura 7.2.3*b*) **Una función que no es sobreyectiva**

Ejemplo 7.2.4 Identificación de funciones sobreyectivas definidas sobre conjuntos finitos

a. ¿Alguno de los diagramas de flechas de la figura 7.2.4 define funciones sobreyectivas?

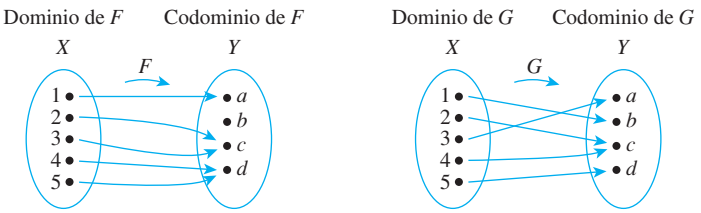


Figura 7.2.4

b. Sea $X = \{1, 2, 3, 4\}$ y $Y = \{a, b, c\}$. Se define $H: X \to Y$ como sigue: $H(1) = c$, $H(2) = a$, $H(3) = c$, $H(4) = b$. Se define $K: X \to Y$ como sigue: $K(1) = c$, $K(2) = b$, $K(3) = b$ y $K(4) = c$. ¿Es ya sea H o K sobreyectiva?

Solución

a. F no es sobreyectiva porque $b \neq F(x)$ para cualquier x en X. G es sobreyectiva porque cada elemento de Y es igual a $G(x)$ para alguna x en X: $a = G(3)$, $b = G(1)$, $c = G(2) = G(4)$ y $d = G(5)$.

b. H es sobreyectiva pero K no lo es. H es sobreyectiva porque cada uno de los tres elementos del codominio de H es la imagen de algún elemento del dominio de H: $a = H(2)$, $b = H(4)$ y $c = H(1) = H(3)$. Sin embargo, K, no es sobreyectiva porque $a \neq K(x)$ para cualquier x en $\{1, 2, 3, 4\}$. ■

Es posible escribir un algoritmo de computadora para comprobar si una función F es sobreyectiva suponiendo que F se define de un conjunto finito X a un conjunto finito Y y hay un algoritmo independiente para calcular valores de F. Represente a X y Y como arreglos unidimensionales $a[1], a[2], \ldots, a[n]$ y $b[1], b[2], \ldots, b[m]$, respectivamente y utilice un bucle anidado para tomar un elemento y de Y a la vez y buscar en los elementos de X para encontrar una x tal que y es la imagen de x. Si alguna búsqueda no tiene éxito entonces F no es sobreyectiva. Si toda búsqueda tiene éxito, entonces F es sobreyectiva. Se le pide que escriba dicho algoritmo en el ejercicio 58 al final de esta sección.

Funciones sobreyectivas sobre conjuntos infinitos

Ahora suponga que F es una función de un conjunto X a un conjunto Y y suponga que Y es infinito. Por definición, F es sobreyectiva si y sólo si, el siguiente enunciado universal es verdadero:

$$\forall y \in Y, \exists x \in X \text{ tal que } F(x) = y.$$

Por tanto para demostrar que F es sobreyectiva, normalmente se utiliza el método de la generalización de lo particular a lo general:

suponga que y es cualquier elemento de Y

y **demuestre** que hay un elemento x de X tal que $F(x) = y$.

Para demostrar que F *no* es sobreyectiva, generalmente

encuentre un elemento y de Y tal que $y \neq F(x)$ para *cualquier* x *en* X.

Ejemplo 7.2.5 Demostración o refutación de qué funciones son sobreyectivas

Se define $f: \mathbf{R} \to \mathbf{R}$ y $h: \mathbf{Z} \to \mathbf{Z}$ con las reglas

$$f(x) = 4x - 1 \quad \text{para toda} \quad x \in \mathbf{R}$$

y

$$h(n) = 4n - 1 \quad \text{para toda} \quad n \in \mathbf{Z}.$$

a. ¿Es f sobreyectiva? Demuestre o dé un contraejemplo.

b. ¿Es h sobreyectiva? Demuestre o dé un contraejemplo.

Solución

a. El mejor enfoque es comenzar tratando de demostrar que f es sobreyectiva y estar alerta con las dificultades que pueden indicar que no lo es. Ahora $f: \mathbf{R} \to \mathbf{R}$ es la función definida por la regla

$$f(x) = 4x - 1 \quad \text{para todos los números reales } x.$$

Para demostrar que f es sobreyectiva, deberá demostrarse

$$\forall y \in Y, \exists x \in X \text{ tal que } f(x) = y.$$

Sustituyendo la definición de f en el diseño de demostración por el método de la generalización de lo particular a lo general, usted

supone que y es un número real

y **demuestre** que existe un número real x tal que $y = 4x - 1$.

¡Precaución! Este trabajo de preparación sólo demuestra lo que tiene que ser x *si* es que existe. El trabajo de preparación no demuestra que x existe.

Trabajo de preparación: **Si** existe tal número real x, entonces

$$\begin{aligned} 4x - 1 &= y \\ 4x &= y + 1 && \text{sumando 1 a ambos lados} \\ x &= \frac{y+1}{4} && \text{dividiendo ambos lados por 4.} \end{aligned}$$

Por tanto, *si* existe un número x, éste debe ser igual a $(y+1)/4$. ¿Existe tal número? Sí. Para demostrar esto, sea $x = (y+1)/4$ y entonces aseguramos que 1) x es un número real y que 2) f realmente envía x a y. La siguiente respuesta formal resume este proceso.

Respuesta a *a*):

Si $f: \mathbf{R} \to \mathbf{R}$ es la función definida por la regla $f(x) = 4x - 1$ para todos los números reales x, entonces f es sobreyectiva.

Demostración:

Sea $y \in \mathbf{R}$. *[Debemos demostrar que* $\exists x$ *en* $\mathbf{R}$ *tal que* $f(x) = y$*.]* Sea $x = (y+1)/4$. Entonces x es un número real ya que sumas y cocientes (distintos de 0) de números reales son números reales. Se tiene que

$$\begin{aligned} f(x) &= f\left(\frac{y+1}{4}\right) && \text{por sustitución} \\ &= 4 \cdot \left(\frac{y+1}{4}\right) - 1 && \text{por definición de } f \\ &= (y+1) - 1 = y && \text{por álgebra básica} \end{aligned}$$

[Esto es lo que se quería demostrar.]

b. La función $h: \mathbf{Z} \to \mathbf{Z}$ se define por la regla

$$h(n) = 4n - 1 \quad \text{para todos los enteros } n.$$

Para demostrar que h es sobreyectiva, es necesario demostrar que

$$\forall \text{ entero } m, \exists \text{ un entero } n \text{ tal que } h(n) = m.$$

Sustituyendo la definición de h en el diseño de demostración por el método de generalización de lo particular a lo general, usted

suponga que m es cualquier número entero

y **trate de demostrar** que existe un entero n con $4n - 1 = m$.

¿Lo puede demostrar de la suposición? ¡No! Si $4n - 1 = m$, entonces

$$n = \frac{m+1}{4} \quad \text{sumando 1 y dividiendo por 4.}$$

Pero n debe ser un entero. Y cuando, por ejemplo, $m = 0$ entonces

$$n = \frac{0+1}{4} = \frac{1}{4},$$

que *no* es un entero.

Por tanto, tratando de demostrar que h es sobreyectiva, se encuentra una dificultad y ésta revela un contraejemplo que muestra que h no es sobreyectiva.

Este análisis se resume en la siguiente respuesta formal.

Respuesta a *b*):

Si la función h: $\mathbf{Z} \to \mathbf{Z}$ está definida por la regla $h(n) = 4n - 1$ para todos los enteros n, entonces h no es sobreyectiva.

Contraejemplo:

El codominio de h es $\mathbf{Z}$ y $0 \in \mathbf{Z}$. Pero $h(n) \neq 0$ para cualquier entero n. Si para $h(n) = 0$, entonces

$$4n - 1 = 0 \quad \text{por definición de } h$$

que implica que

$$4n = 1 \quad \text{sumando 1 en ambos lados}$$

y así

$$n = \frac{1}{4} \quad \text{dividiendo ambos lados por 4.}$$

Pero $1/4$ no es un entero. Por tanto, no existe ningún entero n para el que $f(n) = 0$ y por tanto, f no es sobreyectiva.

■

Relaciones entre las funciones exponenciales y logarítmicas

Nota Que la cantidad b^x es un número real para cualquier número real x se deduce de la propiedad de la menor cota superior del sistema de números reales. (Vea el apéndice A.)

Para números positivos $b \neq 1$, la **función exponencial con base *b***, que se denota $\exp_b$, la función de $\mathbf{R}$ a $\mathbf{R}^+$ se define como sigue: Para todos los números reales x,

$$\exp_b(x) = b^x$$

donde $b^0 = 1$ y $b^{-x} = 1/b^x$.

Cuando trabajamos con la función exponencial, es útil recordar las leyes de los exponentes del álgebra elemental.

Leyes de los exponentes

Si b y c son números reales positivos y u y v son números reales, se cumplen las siguientes leyes de los exponentes:

$$b^u b^v = b^{u+v} \tag{7.2.1}$$

$$(b^u)^v = b^{uv} \tag{7.2.2}$$

$$\frac{b^u}{b^v} = b^{u-v} \tag{7.2.3}$$

$$(bc)^u = b^u c^u \tag{7.2.4}$$

En la sección 7.1 se definió la función logarítmica de base b para cualquier número positivo $b \neq 1$ como la función de $\mathbf{R}^+$ a $\mathbf{R}$ con la propiedad que para cada número real positivo x,

$$\log_b(x) = \text{al exponente al que hay que elevar } b \text{ para obtener } x.$$

O, equivalentemente, para cada número real x positivo y el número real y,

$$\log_b x = y \quad \Leftrightarrow \quad b^y = x.$$

Se puede demostrar usando cálculo que tanto la función exponencial como la logarítmica son inyectivas y sobreyectivas. Por tanto, por definición de inyectiva, se cumplen las siguientes propiedades:

Para cualquier número real positivo b con $b \neq 1$,

$$\text{si } b^u = b^v \text{ entonces } u = v \quad \text{para todos los números reales } u \text{ y } v, \tag{7.2.5}$$

y

$$\text{si } \log_b u = \log_b v \text{ entonces } u = v \quad \text{para todos los números reales positivos } u \text{ y } v. \tag{7.2.6}$$

Estas propiedades se utilizan para deducir muchos hechos adicionales acerca de exponentes y logaritmos. En particular, tenemos las siguientes propiedades de los logaritmos:

Teorema 7.2.1 Propiedades de los logaritmos

Para cualesquiera números reales positivos b, c y x con $b \neq 1$ y $c \neq 1$:

a. $\log_b(xy) = \log_b x + \log_b y$

b. $\log_b\left(\frac{x}{y}\right) = \log_b x - \log_b y$

c. $\log_b(x^a) = a \log_b x$

d. $\log_c x = \dfrac{\log_b x}{\log_b c}$

El teorema 7.2.1*d*) se demuestra en el siguiente ejemplo. Deberá demostrar el resto del teorema en los ejercicios del 33 al 35 al final de esta sección.

Ejemplo 7.2.6 Uso de la inyectividad de la función exponencial

Use la definición de logaritmo y de las leyes de los exponentes y la inyectividad de la función exponencial (propiedad 7.2.5) para demostrar el inciso d) del teorema 7.2.1: Para cualesquiera números reales positivos b, c y x, con $b \neq 1$ y $c \neq 1$,

$$\log_c x = \frac{\log_b x}{\log_b c}.$$

Solución Suponga que se dan los números reales positivos b, c y x. Sea

$$1)\ u = \log_b c \qquad 2)\ v = \log_c x \qquad 3)\ w = \log_b x.$$

Entonces, por definición del logaritmo,

$$1')\ c = b^u \qquad 2')\ x = c^v \qquad 3')\ x = b^w.$$

Sustituyendo $(1')$ en $(2')$ y usando una de las leyes de los exponentes se obtiene

$$x = c^v = (b^u)^v = b^{uv} \qquad \text{por 7.2.2}$$

Pero por 3), también $x = b^w$. Por tanto

$$b^{uv} = b^w$$

y por tanto por la inyectividad de la función exponencial (propiedad 7.2.5),

$$uv = w.$$

Sustituyendo 1), 2) y 3) se obtiene que

$$(\log_b c)(\log_c x) = \log_b x.$$

Y dividiendo a ambos lados por $\log_b c$ (que es distinto de cero porque $c \neq 1$) se obtiene que

$$\log_c x = \frac{\log_b x}{\log_b c}.$$

■

Ejemplo 7.2.7 Cálculo de logaritmos de base 2 en una calculadora

En ciencia computacional a menudo es necesario calcular logaritmos de base 2. La mayoría de las calculadoras no tiene teclas para calcular logaritmos de base 2, pero tienen teclas para calcular logaritmos de base 10 (llamados **logaritmos comunes** y con frecuencia se denotan simplemente con log) y los logaritmos de base e (llamados **logaritmos naturales** y usualmente se denotan por ln). Suponga que su calculadora muestra que $\ln 5 \cong 1.609437912$ y que $\ln 2 \cong 0.6931471806$. Utilice el teorema 7.2.1d) para encontrar un valor aproximado de $\log_2 5$.

Solución Por el teorema 7.2.1d),

$$\log_2 5 = \frac{\ln 5}{\ln 2} \cong \frac{1.609437912}{0.6931471806} \cong 2.321928095.$$

■

Correspondencias inyectivas

Considere una función $F: X \to Y$ que es a la vez inyectiva y sobreyectiva. Dado cualquier elemento x en X, existe un único elemento correspondiente $y = F(x)$ en Y (ya que F es una función). También dado cualquier elemento y en Y, hay un elemento x en X tal que $F(x) = y$ (ya que F es sobreyectiva) y hay sólo una x (ya que F es inyectiva). Por tanto, una función que es inyectiva y sobreyectiva que hace un apareamiento entre los elementos de X

y los elementos de Y que coinciden con cada elemento de X con exactamente un elemento de Y y cada elemento de Y con exactamente un elemento de X. A dicho apareamiento se le llama una *correspondencia inyectiva* o *biyección* y se ilustra con el diagrama de flechas de la figura 7.2.5. Las correspondencias uno a uno se utilizan a menudo como ayuda para el conteo. Por ejemplo, el apareamiento de la figura 7.2.5, muestra que existen cinco elementos en el conjunto X.

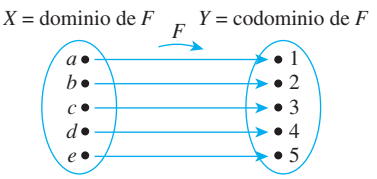


Figura 7.2.5 **Un diagrama de flechas para una correspondencia inyectiva**

• Definición

Una **correspondencia uno a uno** (o **biyección**) de un conjunto X a un conjunto Y es una función $F: X \to Y$ que es a la vez inyectiva y sobreyectiva.

Ejemplo 7.2.8 Una función de un conjunto potencia a un conjunto de cadenas

Sea $\mathscr{P}(\{a, b\})$ el conjunto de todos los subconjuntos de $\{a, b\}$ y sea S el conjunto de todas las cadenas de longitud 2 formado de 0 y 1. Entonces $\mathscr{P}(\{a, b\}) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$ y $S = \{00, 01, 10, 11\}$. Se define una función h de $\mathscr{P}(\{a, b\})$ a S como sigue: Dado cualquier subconjunto A de $\{a, b\}$, a está ya sea en A o no está en A y b está ya sea en A o no está en A. Si a está en A, se escribe un 1 en la primera posición de la cadena $h(A)$. Si a no está en A, se escribe 0 en la primera posición de la cadena $h(A)$. Del mismo modo, si b está en A, se escribe un 1 en la segunda posición de la cadena $h(A)$. Si b no está en A, se escribe 0 en la segunda posición de la cadena $h(A)$. Esta definición se resume en la tabla siguiente.

h

Subconjunto de $\{a, b\}$	Estado de a	Estado de b	Cadena en S
$\emptyset$	no está en	no está en	00
$\{a\}$	está en	no está en	10
$\{b\}$	no está en	está en	01
$\{a, b\}$	está en	está en	11

¿Es h correspondencia uno a uno?

Solución En la figura 7.2.6 se muestra el diagrama de flechas que muestra claramente que h es una correspondencia uno a uno. Es sobreyectiva porque cada elemento de S tiene una flecha apuntando al mismo. Es inyectiva debido a que cada elemento de S no tiene más de una flecha apuntando al mismo.

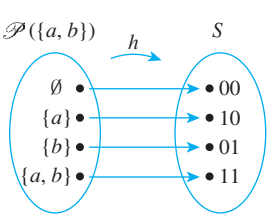


Figura 7.2.6

■

Ejemplo 7.2.9 Una función de cadena inversa

Sea T el conjunto de todas las cadenas finitas de x y y. Se define $g: T \to T$ por la regla: Para todas las cadenas $s \in T$,

$$g(s) = \text{la cadena obtenida al escribir los caracteres de } s \text{ en orden inverso.}$$

¿Es g una correspondencia inyectiva de T a sí mismo?

Solución La respuesta es sí. Para demostrar que g es una correspondencia inyectiva, es necesario demostrar que g es uno a uno y sobreyectiva.

Para ver que g es uno a uno, suponga que para algunas cadenas s_1 y s_2 en T, $g(s_1) = g(s_2)$. *[Debemos demostrar que $s_1 = s_2$.]* Ahora decir que $g(s_1) = g(s_2)$ es lo mismo que decir que la cadena que se obtiene al escribir los caracteres de s_1 en orden inverso es igual a la cadena obtenida al escribir los caracteres de s_2 en orden inverso. Pero si s_1 y s_2 son iguales cuando se escribe en orden inverso, entonces deben ser iguales desde el principio. En otras palabras, $s_1 = s_2$ *[que era lo que se quería demostrar]*.

Para demostrar que g es sobreyectiva, suponga que t es una cadena en T. *[Debemos encontrar una cadena s en T tal que $g(s) = t$.]* Sea $s = g(t)$. Por definición de g, $s = g(t)$ es la cadena en T obtenida al escribir los caracteres de t en orden inverso. Pero cuando el orden de los caracteres de una cadena se invierten una vez y después se revierten una vez más, se recupera la cadena original. Por tanto,

$$\begin{aligned} g(s) = g(g(t)) &= \text{la cadena obtenida por escribir los caracteres de } t \text{ en orden inverso y después escribir de nuevo esos caracteres en orden inverso} \\ &= t. \end{aligned}$$

Esto es lo que se quería demostrar. ■

Ejemplo 7.2.10 Función de dos variables

Se define una función $F: \mathbf{R} \times \mathbf{R} \to \mathbf{R} \times \mathbf{R}$ de la siguiente manera: Para toda $(x, y) \in \mathbf{R} \times \mathbf{R}$,

$$F(x, y) = (x + y, x - y).$$

¿Es F una correspondencia inyectiva de $\mathbf{R} \times \mathbf{R}$ a sí mismo?

Solución La respuesta es sí. Para demostrar que F es una correspondencia inyectiva, debe mostrar que F es tanto inyectiva como F es sobreyectiva.

Demostración de que F es inyectiva: Suponga que (x_1, y_1) y (x_2, y_2) pares ordenados cualesquiera en $\mathbf{R} \times \mathbf{R}$ tal que

$$F(x_1, y_1) = F(x_2, y_2).$$

[Debemos demostrar que $(x_1, y_1) = (x_2, y_2)$.] Por definición de F,

$$(x_1 + y_1, x_1 - y_1) = (x_2 + y_2, x_2 - y_2).$$

Para dos pares ordenados iguales, la primera y segunda componentes deben ser iguales. Por tanto, x_1, y_1, x_2 y y_2 satisfacen el siguiente sistema de ecuaciones:

$$x_1 + y_1 = x_2 + y_2 \tag{1}$$
$$x_1 - y_1 = x_2 - y_2 \tag{2}$$

Sumando las ecuaciones (1) y (2) se obtiene que

$$2x_1 = 2x_2, \quad \text{y así} \quad x_1 = x_2.$$

¡Precaución! Este trabajo de preparación sólo muestra lo que (r, s) deben hacer *si* es que existen. El trabajo de preparación no demuestra que (r, s) existen.

Sustituyendo $x_1 = x_2$ en la ecuación (1) se obtiene

$$x_1 + y_1 = x_1 + y_2, \quad \text{y así} \quad y_1 = y_2.$$

Por lo que, por definición de igualdad de pares ordenados, $(x_1, y_1) = (x_2, y_2)$ *[como se quería demostrar]*.

Trabajo de preparación para la demostración de que f es sobreyectiva: Para demostrar que F es sobreyectiva, suponga que cualquier par ordenado en el codominio $\mathbf{R} \times \mathbf{R}$, digamos (u, v) y después demuestre que hay un par ordenado en el dominio que envía a (u, v) por F. Para ello, suponga temporalmente que ha encontrado un par ordenado, digamos (r, s). Entonces

$$F(r, s) = (u, v) \qquad \text{ya que está suponiendo que } F \text{ envía } (r, s) \text{ a } (u, v)$$

y

$$F(r, s) = (r + s, r - s) \qquad \text{por definición de } F.$$

Igualando los lados derechos se obtiene

$$(r + s, r - s) = (u, v).$$

Por definición de igualdad de pares ordenados esto significa que

$$r + s = u \tag{1}$$
$$r - s = v \tag{2}$$

Sumando las ecuaciones (1) y (2) se obtiene

$$2r = u + v \quad \text{y así} \quad r = \frac{u+v}{2}.$$

Restando la ecuación (2) de la ecuación (1) se obtiene

$$2s = u - v \quad \text{y así} \quad s = \frac{u-v}{2}.$$

Por lo que, ***si*** F envía (r, s) a (u, v), entonces $r = (u + v)/2$ y $s = (u - v)/2$. Para convertir este trabajo de preparación en una demostración, es necesario asegurarse de que 1) $\left(\frac{u+v}{2}, \frac{u-v}{2}\right)$ está en el dominio de F y 2) que F realmente envía $\left(\frac{u+v}{2}, \frac{u-v}{2}\right)$ a (u, v).

Demostración de que F es sobreyectiva: Suponga que (u, v) es cualquier par ordenado en el codominio de F. *[Demostraremos que hay un par ordenado en el dominio de F que se envía a (u, v) por F.]* Sea

$$r = \frac{u+v}{2} \quad \text{y} \quad s = \frac{u-v}{2}.$$

Entonces (r, s) es un par ordenado de números reales y así está en el dominio de F. Además:

$$\begin{aligned} F(r, s) &= F\left(\frac{u+v}{2}, \frac{u-v}{2}\right) && \text{por definición de } F \\ &= \left(\frac{u+v}{2} + \frac{u-v}{2}, \frac{u+v}{2} - \frac{u-v}{2}\right) && \text{por sustitución} \\ &= \left(\frac{u+v+u-v}{2}, \frac{u+v-u+v}{2}\right) \\ &= \left(\frac{2u}{2}, \frac{2v}{2}\right) \\ &= (u, v) && \text{por álgebra.} \end{aligned}$$

[Esto es lo que se quería demostrar.] ■

Funciones inversas

Si F es una correspondencia inyectiva de un conjunto X a un conjunto Y, entonces hay una función de Y a X que "deshace" la acción de F; es decir, envía cada elemento de Y al elemento de X del que vino. Esta función se llama la *función inversa* de F.

Teorema 7.2.2

Suponga que $F: X \to Y$ es una correspondencia inyectiva; es decir, suponga que F es uno a uno y sobreyectiva. Entonces, hay una función $\boldsymbol{F^{-1}: Y \to X}$ que se define como sigue:

Dado cualquier elemento y en Y,

$$\boldsymbol{F^{-1}(y)} = \text{al único elemento } x \text{ en } X \text{ tal que } F(x) \text{ es igual a } y.$$

En otras palabras,

$$F^{-1}(y) = x \quad \Leftrightarrow \quad y = F(x).$$

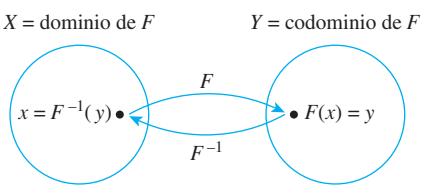
La demostración del teorema 7.2.2 se deduce inmediatamente de la definición uno a uno y sobreyectiva. Dado un elemento y en Y, hay un elemento x en X con $F(x) = y$ porque F es sobreyectiva; x es única porque F es inyectiva.

• Definición

La función F^{-1} del teorema 7.2.2 se llama **función inversa** para F.

Observe que de acuerdo con esta definición, la función logarítmica de base $b > 0$ es el inverso de la función exponencial de base b.

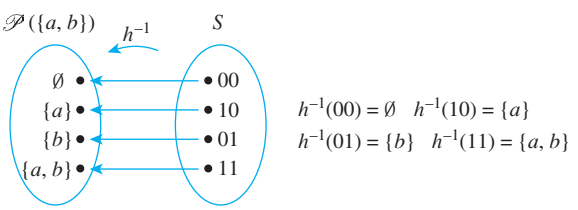
El diagrama siguiente muestra el hecho de que una función inversa envía cada elemento de regreso de donde provino.



Ejemplo 7.2.11 Determinación de una función inversa de una función dada por un diagrama de flechas

Defina la función inversa para la correspondencia inyectiva h dada en el ejemplo 7.2.8.

Solución El diagrama de flechas para h^{-1} se obtiene trazando las flechas de h de regreso de S a $\mathscr{P}(\{a, b\})$ como se muestra a continuación.



■

Ejemplo 7.2.12 Determinación de una función inversa para una función dada con palabras

Defina la función inversa para la correspondencia inyectiva g dada en el ejemplo 7.2.9.

Solución La función $g: T \to T$ está definida por la regla

Para todas las cadenas t en T,

$$g(t) = \text{cadena obtenida al escribir los caracteres de } t \text{ en orden inverso.}$$

Ahora si los caracteres de t están escritos en orden inverso y, después, una vez más, escritos en orden inverso, se recupera la cadena original. Por tanto, dada cualquier cadena t en T,

$$\begin{aligned} g^{-1}(t) &= \text{única cadena que, cuando se escribe} \\ &\quad \text{en orden inverso, es igual a } t \\ &= \text{cadena obtenida al escribir los} \\ &\quad \text{caracteres de } t \text{ en orden inverso} \\ &= g(t). \end{aligned}$$

Por tanto $g^{-1}: T \to T$ es el mismo que g, o, en otras palabras, $g^{-1} = g$. ■

Ejemplo 7.2.13 Determinación de una función inversa para una función dada por una fórmula

La función $f: \mathbf{R} \to \mathbf{R}$ se define por la fórmula

$$f(x) = 4x - 1 \quad \text{para todos los números reales } x$$

se demostró que es inyectiva en el ejemplo 7.2.2 y sobreyectiva en el ejemplo 7.2.5. Encuentre su función inversa.

Solución Para cualquier *[dada, pero arbitrariamente elegida]* y en $\mathbf{R}$, por definición de f^{-1},

$$f^{-1}(y) = \text{es el único número real } x \text{ tal que } f(x) = y.$$

Pero

$$\begin{aligned} & f(x) = y \\ \Leftrightarrow \quad & 4x - 1 = y && \text{por definición de } f \\ \Leftrightarrow \quad & x = \frac{y+1}{4} && \text{por álgebra.} \end{aligned}$$

Por tanto $f^{-1}(y) = \dfrac{y+1}{4}$. ■

El teorema siguiente se deduce fácilmente de las definiciones.

Teorema 7.2.3

Si X y Y son conjuntos y $F: X \to Y$ es inyectiva y sobreyectiva, entonces $F^{-1}: Y \to X$ es también inyectiva y sobreyectiva.

Demostración:

F^{-1} es inyectiva: Suponga que y_1 y y_2 son elementos de Y tal que $F^{-1}(y_1) = F^{-1}(y_2)$. *[Debemos demostrar que $y_1 = y_2$.]* Sea $x = F^{-1}(y_1) = F^{-1}(y_2)$. Entonces $x \in X$ y por definición de F^{-1},

$$F(x) = y_1 \quad \text{ya que } x = F^{-1}(y_1)$$

y

$$F(x) = y_2 \quad \text{ya que } x = F^{-1}(y_2).$$

En consecuencia, $y_1 = y_2$ ya que cada una es igual a $F(x)$. Esto es lo que se quería demostrar.

F^{-1} es sobreyectiva: Suponga que $x \in X$. *[Debemos demostrar que existe un elemento en Y tal que $F^{-1}(y) = x$.]* Sea $y = F(x)$. Entonces $y \in Y$ y por definición de F^{-1}, $F^{-1}(y) = x$. Esto es lo que se quería demostrar.

Ejemplo 7.2.14 Determinación de una función inversa para una función de dos variables

Defina la función inversa de $F^{-1}: \mathbf{R} \times \mathbf{R} \to \mathbf{R} \times \mathbf{R}$ para la correspondencia inyectiva dada en el ejemplo 7.2.10.

Solución

La solución del ejemplo 7.2.10 muestra que $F\left(\frac{u+v}{2}, \frac{u-v}{2}\right) = (u, v)$. Ya que F es inyectiva, lo que significa que

$\left(\frac{u+v}{2}, \frac{u-v}{2}\right)$ es el único par ordenado en el dominio de F que se envía a (u, v) por F.

Por tanto, F^{-1} se define como sigue: Para toda $(u, v) \in \mathbf{R} \times \mathbf{R}$,

$$F^{-1}(u, v) = \left(\frac{u+v}{2}, \frac{u-v}{2}\right).$$

■

Autoexamen

1. Si F es una función de un conjunto X a un conjunto Y, entonces, F es inyectiva si y sólo si, _____.
2. Si F es una función de un conjunto X a un conjunto de Y, entonces F no es inyectiva si y sólo si, _____.
3. Si F es una función de un conjunto X a un conjunto de Y, entonces F es sobreyectiva si y sólo si, _____.
4. Si F es una función de un conjunto X a un conjunto Y, entonces F no es sobreyectiva si y sólo si, _____.
5. Los siguientes dos enunciados son _____:

   $\forall\, u, v \in U$, si $H(u) = H(v)$ entonces $u = v$.

   $\forall\, u, v \in U$, si $u \neq v$ entonces $H(u) \neq H(v)$.
6. Dada una función $F: X \to Y$ y un conjunto infinito X, para demostrar que F es inyectiva, suponga que _____ y después demuestre que _____.
7. Dada una función $F: X \to Y$ y un conjunto infinito X, para demostrar que F es sobreyectiva, suponga que _____ y después demuestre que _____.
8. Dada una función $F: X \to Y$, para demostrar que F no es inyectiva, usted _____.
9. Dada una función $F: X \to Y$, para demostrar que F no es sobreyectiva, usted _____.
10. Una correspondencia inyectiva de un conjunto X a un conjunto Y es una _____ que es _____.
11. Si F es una correspondencia inyectiva de un conjunto X a un conjunto Y y y está en Y, entonces $F^{-1}(y)$ es _____.

Conjunto de ejercicios 7.2

1. La definición uno a uno se establece de dos maneras:

$\forall x_1, x_2 \in X$, si $F(x_1) = F(x_2)$ entonces $x_1 = x_2$

y $\forall x_1, x_2 \in X$, si $x_1 \neq x_2$ entonces $F(x_1) \neq F(x_2)$.

¿Por qué estos dos enunciados son lógicamente equivalentes?

2. Complete cada espacio en blanco con la palabra *más* o *menos*.

a. Una función F es uno a uno si y sólo si, cada elemento en el codominio de F es la imagen de _____ un elemento en el dominio de F.

b. Una función F es sobreyectiva si y sólo si, cada elemento en el codominio de F es la imagen de _____ un elemento en el dominio de F.

H 3. Cuando se le pide establecer la definición uno a uno, un estudiante responde: "Una función f es uno a uno si y sólo si, cada elemento de X se envía por f exactamente a un elemento de Y". Dé un contraejemplo para demostrar que su respuesta es incorrecta.

H 4. Sea $F: X \to Y$ una función. ¿Verdadera o falsa? Una condición suficiente para que f sea inyectiva, es que para todos los elementos y en Y, hay a lo más una x en X con $f(x) = y$.

H 5. Sólo dos de los siguientes enunciados son formas correctas para expresar el hecho de que una función f es sobreyectiva. Determine los dos que son incorrectos.

a. f es sobreyectiva $\Leftrightarrow$ cada elemento en su codominio es la imagen de algún elemento en su dominio.

b. f es sobreyectiva $\Leftrightarrow$ cada elemento de su dominio tiene una imagen correspondiente en su codominio.

c. f es sobreyectiva $\Leftrightarrow \forall y \in Y, \exists x \in X$ tal que $f(x) = y$.

d. f es sobreyectiva $\Leftrightarrow \forall x \in X, \exists y \in Y$ tal que $f(x) = y$.

e. f es sobreyectiva $\Leftrightarrow$ el rango de f es el mismo que el codominio de f.

6. Sea $X = \{1, 5, 9\}$ y $Y = \{3, 4, 7\}$.

a. Defina $F: X \to Y$ especificando que

$$f(1) = 4, \quad f(5) = 7, \quad f(9) = 4.$$

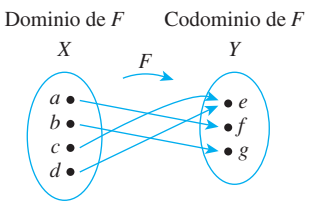
¿Es f inyectiva? ¿Es f sobreyectiva? Explique sus respuestas.

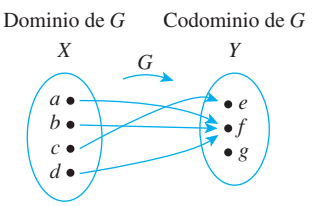
b. Defina $g: X \to Y$ para especificar que

$$g(1) = 7, \quad g(5) = 3, \quad g(9) = 4.$$

¿Es g inyectiva? ¿Es g sobreyectiva? Explique sus respuestas.

7. Sea $X = \{a, b, c, d\}$ y $Y = \{e, f, g\}$. Se definen las funciones F y G con los diagramas de flechas que se muestran a continuación.

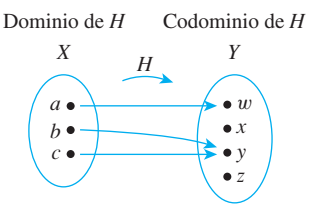


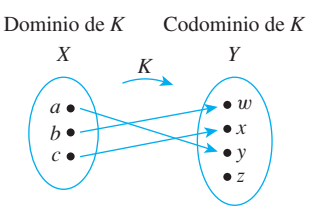


a. ¿Es F inyectiva? ¿Por qué sí o por qué no? ¿Es sobreyectiva? ¿Por qué sí o por qué no?

b. ¿Es G inyectiva? ¿Por qué sí o por qué no? ¿Es sobreyectiva? ¿Por qué sí o por qué no?

8. Sea $X = \{a, b, c\}$ y $Y = \{w, x, y, z\}$. Se definen las funciones H y K con los diagramas de flechas que se muestran a continuación.





a. ¿Es H inyectiva? ¿Por qué sí o por qué no? ¿Es sobreyectiva? ¿Por qué sí o por qué no?

b. ¿Es K inyectiva? ¿Por qué sí o por qué no? ¿Es sobreyectiva? ¿Por qué sí o por qué no?

9. Sea $X = \{1, 2, 3\}$, $Y = \{1, 2, 3, 4\}$ y $Z = \{1, 2\}$.

a. Defina una función $f: X \to Y$ que sea inyectiva, pero que no sea sobreyectiva.

b. Defina una función $g: X \to Z$ que sea sobreyectiva pero no inyectiva.

c. Defina una función $h: X \to X$ que ni sea inyectiva ni sobreyectiva.

d. Defina una función $k: X \to X$ que sea inyectiva y sobreyectiva pero que no sea la función identidad en X.

10. a. Se define $f: \mathbf{Z} \to \mathbf{Z}$ por la regla de $f(n) = 2n$, para todo entero n.

i) ¿Es f inyectiva? Demuestre o dé un contraejemplo.

ii) ¿Es f sobreyectiva? Demuestre o dé un contraejemplo.

b. Sea $2\mathbf{Z}$ denote que es el conjunto de todos los enteros pares. Es decir, $2\mathbf{Z} = \{n \in \mathbf{Z} \mid n = 2k, \text{ para algún entero } k\}$. Se define $h: \mathbf{Z} \to 2\mathbf{Z}$ con la regla $h(n) = 2n$, para todos los enteros n. ¿Es h sobreyectiva? Demuestre o dé un contraejemplo.

***H* 11.** a. Se define $g: \mathbf{Z} \to \mathbf{Z}$ por la regla de $g(n) = 4n - 5$, para todo entero n.

i) ¿Es g inyectiva? Demuestre o dé un contraejemplo.

ii) ¿Es g sobreyectiva? Demuestre o dé un contraejemplo.

b. Se define $G: \mathbf{R} \to \mathbf{R}$ con la regla de $G(x) = 4x - 5$ para todos los números reales x. ¿Es G sobreyectiva? Demuestre o dé un contraejemplo.

12. a. Se define $F: \mathbf{Z} \to \mathbf{Z}$ por la regla de $F(n) = 2 - 3n$, para todo entero n.

i) ¿Es F inyectiva? Demuestre o dé un contraejemplo.

ii) ¿Es F sobreyectiva? Demuestre o dé un contraejemplo.

b. Se define $G: \mathbf{R} \to \mathbf{R}$ con la regla $G(x) = 2 - 3x$ para todos los números reales x. ¿Es G sobreyectiva? Demuestre o dé un contraejemplo.

13. **a.** Se define $H: \mathbf{R} \to \mathbf{R}$ por la regla de $H(x) = x^2$, para todos los números reales x.

i) ¿Es H inyectiva? Demuestre o dé un contraejemplo.

ii) ¿Es H sobreyectiva? Demuestre o dé un contraejemplo.

b. Se define $K: \mathbf{R}^{noneg} \to \mathbf{R}^{noneg}$ con la regla $K(x) = x^2$ para todos los números reales x. ¿Es K sobreyectiva? Demuestre o dé un contraejemplo

14. Explique el error en la siguiente "demostración".

Teorema: La función $f: \mathbf{Z} \to \mathbf{Z}$ se define por la fórmula $f(n) = 4n + 3$, para todos los enteros n, es inyectiva.

"**Demostración:** Suponga que se da cualquier entero n. Entonces, por definición de f, hay sólo un valor posible para $f(n)$, a saber, $4n + 3$. Por tanto f es inyectiva".

En cada uno de los ejercicios del 15 al 18 se define una función f en un conjunto de números reales. Determine si es o no f inyectiva y justifique su respuesta.

15. $f(x) = \dfrac{x + 1}{x}$, para todos los números reales $x \neq 0$

16. $f(x) = \dfrac{x}{x^2 + 1}$, para todos los números reales x

17. $f(x) = \dfrac{3x - 1}{x}$, para todos los números reales $x \neq 0$

18. $f(x) = \dfrac{x + 1}{x - 1}$, para todos los números reales $x \neq 1$

19. Con referencia al ejemplo 7.2.3, suponga que los registros con los siguientes números de seguridad social se pueden colocar en una sucesión en la tabla 7.2.1. Encuentre la posición en la que se coloca cada registro.

a. 417-30-2072 b. 364-98-1703 c. 283-09-0787

20. Defina Piso: $\mathbf{R} \to \mathbf{Z}$ por la fórmula $\text{Piso}(x) = \lfloor x \rfloor$, para todos los números reales x.
a. ¿Es Piso inyectiva? Demuestre o dé un contraejemplo.
b. ¿Es Piso sobreyectiva? Demuestre o dé un contraejemplo.

21. Sea S el conjunto de todas las cadenas de 0 y 1 y defina l: $S \to \mathbf{Z}^{noneg}$ por

$$l(s) = \text{la longitud de } s, \qquad \text{para toda cadena } s \text{ en } S.$$

a. ¿Es l inyectiva? Demuestre o dé un contraejemplo.
b. ¿Es l sobreyectiva? Demuestre o dé un contraejemplo.

22. Sea S el conjunto de todas las cadenas de 0 y 1 y defina D: $S \to \mathbf{Z}$ como sigue: para toda $s \in S$,

$$D(s) = \text{número de 1 en } s \text{ menos el número de 0 en } s.$$

a. ¿Es D inyectiva? Demuestre o dé un contraejemplo.
b. ¿Es D sobreyectiva? Demuestre o dé un contraejemplo.

23. Se define F: $\mathscr{P}(\{a, b, c\}) \to \mathbf{Z}$ como sigue: Para toda A en $\mathscr{P}(\{a, b, c\})$,

$$F(A) = \text{el número de elementos en } A.$$

a. ¿Es F inyectiva? Demuestre o dé un contraejemplo.
b. ¿Es F sobreyectiva? Demuestre o dé un contraejemplo.

24. Sea S el conjunto de todas las cadenas de a y de b y se define N: $S \to \mathbf{Z}$ por

$$N(s) = \text{el número de } a \text{ en } s, \qquad \text{para toda } s \in S.$$

a. ¿Es N inyectiva? Demuestre o dé un contraejemplo.
b. ¿Es N sobreyectiva? Demuestre o dé un contraejemplo.

25. Sea S el conjunto de todas las cadenas en a y en b y se define C: $S \to S$ por

$$C(s) = as, \qquad \text{para toda } s \in S.$$

(C se llama **concatenación** por a en la izquierda.)
a. ¿Es C inyectiva? Demuestre o dé un contraejemplo.
b. ¿Es C sobreyectiva? Demuestre o dé un contraejemplo.

26. Se define S: $\mathbf{Z}^+ - \mathbf{Z}^+$ por la regla: Para todos los enteros n, $S(n) =$ la suma de los divisores positivos de n.
a. ¿Es S inyectiva? Demuestre o dé un contraejemplo.
b. ¿Es S sobreyectiva? Demuestre o dé un contraejemplo.

***H* 27.** Sea D el conjunto de todos los subconjuntos finitos de enteros positivos y se define T: $\mathbf{Z}^+ \to D$ por la regla: para todos los enteros n.
$T(n) =$ conjunto de todos los divisores positivos de n.
a. ¿Es T inyectiva? Demuestre o dé un contraejemplo.
b. ¿Es T sobreyectiva? Demuestre o dé un contraejemplo.

28. Se define G: $\mathbf{R} \times \mathbf{R} \to \mathbf{R} \times \mathbf{R}$ como sigue:
$G(x, y) = (2y, -x)$ para toda $(x, y) \in \mathbf{R} \times \mathbf{R}$.
a. ¿Es G inyectiva? Demuestre o dé un contraejemplo.
b. ¿Es G sobreyectiva? Demuestre o dé un contraejemplo.

29. Se define H: $\mathbf{R} \times \mathbf{R} \to \mathbf{R} \times \mathbf{R}$ de la siguiente manera:
$H(x, y) = (x + 1, 2 - y)$ para todo $(x, y) \in \mathbf{R} \times \mathbf{R}$.
a. ¿Es H inyectiva? Demuestre o dé un contraejemplo.
b. ¿Es H sobreyectiva? Demuestre o dé un contraejemplo.

30. Se define J: $\mathbf{Q} \times \mathbf{Q} \to \mathbf{R}$ por la regla $J(r, s) = r + \sqrt{2}s$ para toda $(r, s) \in \mathbf{Q} \times \mathbf{Q}$.
a. ¿Es J inyectiva? Demuestre o dé un contraejemplo.
b. ¿Es J sobreyectiva? Demuestre o dé un contraejemplo.

∗ 31. Se define F: $\mathbf{Z}^+ \times \mathbf{Z}^+ \to \mathbf{Z}^+$ y G: $\mathbf{Z}^+ \times \mathbf{Z}^+ \to \mathbf{Z}^+$ como sigue: Para toda $(n, m) \in \mathbf{Z}^+ \times \mathbf{Z}^+$,

$$F(n, m) = 3^n 5^m \quad \text{y} \quad G(n, m) = 3^n 6^m.$$

H **a.** ¿Es F inyectiva? Demuestre o dé un contraejemplo.
b. ¿Es G inyectiva? Demuestre o dé un contraejemplo.

32. **a.** ¿Es $\log_8 27 = \log_2 3$? ¿Por qué sí o por qué no?
b. ¿Es $\log_{16} 9 = \log_4 3$? ¿Por qué sí o por qué no?

En las secciones 11.4 y 11.5, se utilizan las propiedades de los logaritmos establecidas en los ejercicios del 33 al 35.

33. Demuestre que para todos los números reales positivos b, x y y con $b \neq 1$,

$$\log_b \left(\frac{x}{y}\right) = \log_b x - \log_b y.$$

34. Demuestre que para todos los números reales positivos b, x y y con $b \neq 1$,

$$\log_b (xy) = \log_b x + \log_b y.$$

***H* 35.** Demuestre que para todos los números reales a, b y x con b y x positivos y $b \neq 1$,

$$\log_b (x^a) = a \log_b x.$$

Los ejercicios 36 y 37 utilizan la siguiente definición: si f: $\mathbf{R} \to \mathbf{R}$ y g: $\mathbf{R} \to \mathbf{R}$ son funciones, entonces la función $(f + g)$: $\mathbf{R} \to \mathbf{R}$ se define por la fórmula $(f + g)(x) = f(x) + g(x)$ para todos los números reales x.

36. Si f: $\mathbf{R} \to \mathbf{R}$ y g: $\mathbf{R} \to \mathbf{R}$ son ambas inyectivas, ¿$f + g$ también es inyectiva? Justifique su respuesta.

37. Si f: $\mathbf{R} \to \mathbf{R}$ y g: $\mathbf{R} \to \mathbf{R}$ son ambas sobreyectivas, ¿es $f + g$ también sobreyectiva? Justifique su respuesta.

Los ejercicios de 38 y 39 utilizan la siguiente definición: si f: $\mathbf{R} \to \mathbf{R}$ es una función y c es un número distinto de cero de real, la función $(c \cdot f)$: $\mathbf{R} \to \mathbf{R}$ se define por la fórmula $(c \cdot f)(x) = c \cdot f(x)$ para todos los números reales x.

38. Sea f: $\mathbf{R} \to \mathbf{R}$ una función y c un número real distinto de cero. Si f es inyectiva, ¿$c \cdot f$ también es inyectiva? Justifique su respuesta.

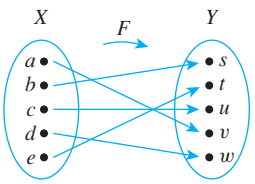
39. F: $\mathbf{R} \to \mathbf{R}$ es una función y c un número real distinto de cero. Si f es sobreyectiva ¿es también sobreyectiva $c \cdot f$? Justifique su respuesta.

***H* 40.** Suponga que F: $X \to Y$ es inyectiva.
a. Demuestre que para todos los subconjuntos $A \subseteq X$, $F^{-1}(F(A)) = A$.
b. Demuestre que para todos los subconjuntos A_1 y A_2 en X, $F(A_1 \cap A_2) = F(A_1) \cap F(A_2)$.

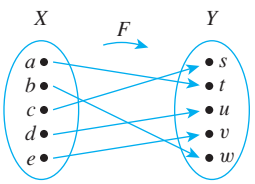
41. Suponga que $F: X \to Y$ es sobreyectiva. Demuestre que para todos los subconjuntos $B \subseteq Y$, $F(F^{-1}(B)) = B$.

Sea $X = \{a, b, c, d, e\}$ y $Y = \{s, t, u, v, w\}$. En cada uno de los ejercicios 42 y 43 se define una correspondencia inyectiva $F: X \to Y$ con un diagrama de flechas. En cada caso dibuje un diagrama de flechas para F^{-1}.

42.



43.



En los ejercicios 44 al 55 indican que las funciones en el ejercicio que se hace referencia son correspondencias inyectivas. Para cada función que sea una correspondencia inyectiva, encuentre la función inversa.

44. Ejercicio 10a

45. Ejercicio l0b

46. Ejercicio 11a

47. Ejercicio 11b

48. Ejercicio 12a

49. Ejercicio 12b

50. Ejercicio 21

51. Ejercicio 22

52. El ejercicio 15 con el codominio tomado como el conjunto de todos los números reales, no iguales a 1.

H 53. El ejercicio 16 con el codominio tomado como el conjunto de todos los números reales.

54. El ejercicio 17 con el codominio tomado como el conjunto de todos los números reales no iguales a 3.

55. El ejercicio 18 con el codominio tomado como el conjunto de todos los números reales no iguales a 1.

56. En el ejemplo 7.2.8 se definió una correspondencia inyectiva del conjunto potencia de $\{a, b\}$ para el conjunto de todas las cadenas de 0 y de 1 que tienen longitud 2. Por tanto, los elementos de estos dos conjuntos pueden coincidir exactamente y así los dos conjuntos tienen el mismo número de elementos.
   a. Sea $X = \{x_1, x_2, \ldots, x_n\}$ un conjunto con n elementos. Utilice el ejemplo 7.2.8 como modelo para definir una correspondencia inyectiva de $\mathscr{P}(X)$, el conjunto de todos los subconjuntos de X, al conjunto de todas las cadenas de 0 y de 1 que tienen longitud n.
   b. Utilice la correspondencia inyectiva del inciso *a*) para deducir que un conjunto con n elementos tiene 2^n subconjuntos. (Esto proporciona una demostración alternativa del teorema 6.3.1.)

H 57. Escriba un algoritmo de computadora para comprobar si una función de un conjunto finito a otro es inyectiva. Suponga la existencia de un algoritmo independiente para calcular los valores de la función.

H 58. Escriba un algoritmo de computadora para comprobar si una función de un conjunto finito a otro es sobreyectiva. Suponga la existencia de un algoritmo independiente para calcular los valores de la función.

Respuestas del autoexamen

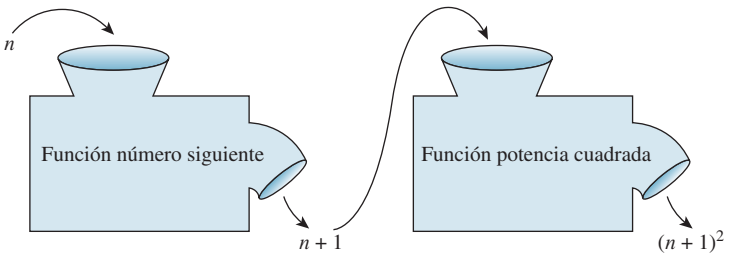
1. para toda x_1 y x_2 en X, si $F(x_1) = F(x_2)$, entonces $x_1 = x_2$ 2. existen los elementos x_1 y x_2 en X, si $F(x_1) = F(x_2)$ y $x_1 \neq x_2$ 3. para toda y en Y, existe al menos un elemento x en X tal que $f(x) = y$ 4. existe un elemento y en Y tal que para todos los elementos x en X, $f(x) \neq y$ 5. formas lógicamente equivalentes de expresar lo que significa para que una función H sea inyectiva (el segundo es la contrapositiva del primero). 6. x_1 y x_2 son elementos *[dados pero arbitrariamente elegidos]* en X con la propiedad de que $F(x_1) = F(x_2)$; $x_1 = x_2$ 7. y es cualquier elemento *[dado pero arbitrariamente elegido]* en Y; existe al menos un elemento x *en* X tal que $f(x) = y$ 8. demuestre que hay elementos concretos de x_1 y x_2 con la propiedad de que $F(x_1) = F(x_2)$ y $x_1 \neq x_2$ 9. demuestre que hay un elemento concreto de y en Y con la propiedad que $F(x) \neq y$ para cualquier elemento x en X 10. función de X a Y; tanto inyectiva como sobreyectiva 11. el único elemento x en X tal que $F(x) = y$ (en otras palabras, $F^{-1}(y)$ es la única pre-imagen de y en X)

7.3 Composición de funciones

No es paradoja decir que podemos estar más cerca de nuestras aplicaciones si nuestro estado de ánimo es más teórico. —Alfred North Whitehead

Considere dos funciones, la función número siguiente y la función potencia cuadrada, definida de $\mathbf{Z}$ (el conjunto de enteros) a $\mathbf{Z}$ e imagine que cada una está representada por una máquina. Si las dos máquinas se enganchan para que la salida de la función número siguiente se use como entrada a la función potencia cuadrada, entonces trabajan juntas para

que funcionen como una máquina más grande. En esta máquina más grande, primero un entero n se incrementa en 1 obteniéndose $n + 1$; después, la cantidad $n + 1$ se eleva al cuadrado con lo que se obtiene $(n + 1)^2$. Esto se ilustra en el dibujo siguiente.



A combinar las funciones de esta manera se le llama *componerlas*; la función resultante se llama la *composición* de las dos funciones. Observe que la composición se puede formar sólo si la salida de la primera función es entrada aceptable para la segunda función. Es decir, el rango de la primera función debe estar contenido en el dominio de la segunda función.

• Definición

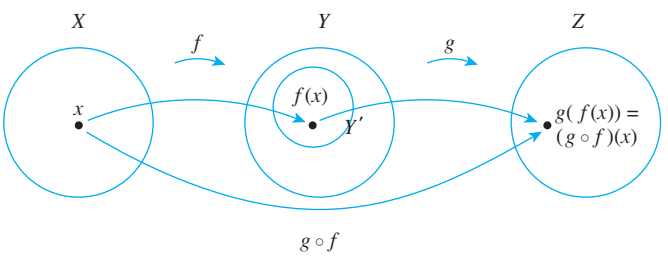
Sea $f: X \to Y'$ y $g: Y \to Z$ funciones con la propiedad de que el rango de f es un subconjunto del dominio de g. Se define una nueva función $g \circ f: X \to Z$ de la siguiente manera:

$$(g \circ f)(x) = g(f(x)) \quad \text{para toda } x \in X,$$

donde $g \circ f$ se lee "g círculo f" y $g(f(x))$ se lee "g de f de x". La función $g \circ f$ se llama la **composición de f y g**.

Nota Colocamos primero la f cuando decimos "la composición de f y g", porque sobre los elementos de x actúan primero por f y después por g.

Esta definición se muestra esquemáticamente a continuación.



Ejemplo 7.3.1 Composición de funciones definidas por fórmulas

Sea $f: \mathbf{Z} \to \mathbf{Z}$ la función número siguiente y sea $g: \mathbf{Z} \to \mathbf{Z}$ la función potencia cuadrada. Entonces, $f(n) = n + 1$ para toda $n \in \mathbf{Z}$ y $g(n) = n^2$ para toda $n \in \mathbf{Z}$.

a. Encuentre las composiciones $g \circ f$ y $f \circ g$.

b. ¿Es $g \circ f = f \circ g$? Explique.

¡Precaución! Tenga cuidado de no confundir a $g \circ f$ y $g(f(x))$: $g \circ f$ es el nombre de la función mientras que $g(f(x))$ es el valor de la función en x.

Solución

a. Las funciones $g \circ f$ y $f \circ g$ se definen como sigue:

$$(g \circ f)(n) = g(f(n)) = g(n + 1) = (n + 1)^2 \quad \text{para toda } n \in \mathbf{Z},$$

y

$$(f \circ g)(n) = f(g(n)) = f(n^2) = n^2 + 1 \quad \text{para toda } n \in \mathbf{Z}.$$

b. Dos funciones de un conjunto a otro son iguales si y sólo si, tienen siempre los mismos valores. En este caso,

$$(g \circ f)(1) = (1 + 1)^2 = 4, \text{ mientras que } (f \circ g)(1) = 1^2 + 1 = 2.$$

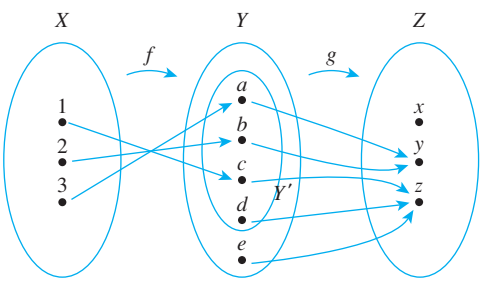
Por tanto, no son iguales las dos funciones $g \circ f$ y $f \circ g$:

$$g \circ f \neq f \circ g.$$ ■

El ejemplo 7.3.1 ilustra el hecho importante de que la composición de funciones no es una operación conmutativa: *Para funciones generales F y G, F ∘ G no se necesita que necesariamente sea igual a G ∘ F* (aunque las dos *pueden* ser iguales).

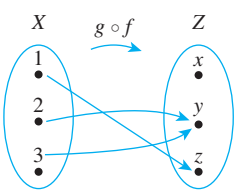
Ejemplo 7.3.2 Composición de funciones definidas sobre conjuntos finitos

Sea $X = \{1, 2, 3\}$, $Y' = \{a, b, c, d\}$, $Y = \{a, b, c, d, e\}$ y $Z = \{x, y, z\}$. Se definen las funciones $f: X \to Y'$ y $f: Y \to Z$ por los diagramas de flechas que se muestran a continuación.



Dibuje el diagrama de la flecha para $g \circ f$. ¿Cuál es el rango de $g \circ f$?

Solución Para encontrar el diagrama de la flecha para $g \circ f$, sólo trace las flechas que vayan de X a Z a través de Y. A continuación se muestra el resultado.



$$(g \circ f)(1) = g(f(1)) = g(c) = z$$
$$(g \circ f)(2) = g(f(2)) = g(b) = y$$
$$(g \circ f)(3) = g(f(3)) = g(a) = y$$

El rango de $g \circ f$ es $\{y, z\}$. ■

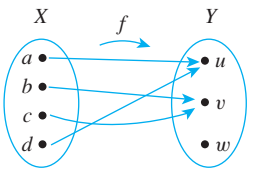
Recuerde que la función identidad en un conjunto X, I_X, es la función de X a X definida por la fórmula

$$I_X(x) = x \quad \text{para toda } x \in X.$$

Es decir, la función identidad en X envía cada elemento de X a sí mismo. ¿Qué sucede cuando una función identidad se compone con otra función?

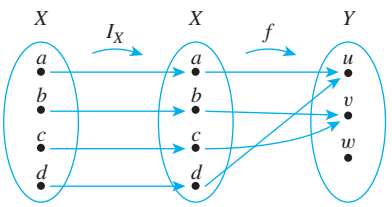
Ejemplo 7.3.3 Composición con la función identidad

Sea $X = \{a, b, c, d\}$ y $Y = \{u, v, w\}$ y suponga que $f: X \to Y$ está dada por el diagrama de flechas que se muestra en la página siguiente.



Encuentre $f \circ I_X$ y $I_Y \circ f$.

Solución Los valores de $f \circ I_X$ se obtienen dibujando el diagrama de flechas que se muestra a continuación.



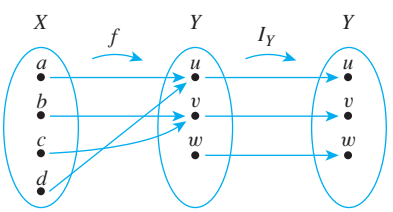
$$(f \circ I_X)(a) = f(I_X(a)) = f(a) = u$$
$$(f \circ I_X)(b) = f(I_X(b)) = f(b) = v$$
$$(f \circ I_X)(c) = f(I_X(c)) = f(c) = v$$
$$(f \circ I_X)(d) = f(I_X(d)) = f(d) = u$$

Observe que para todos los elementos x en X,

$$(f \circ I_X)(x) = f(x).$$

Por definición de igualdad de funciones, esto significa que $f \circ I_X = f$.

Del mismo modo, la igualdad $I_Y \circ f = f$ se puede comprobar siguiendo el diagrama de flechas que se muestra a continuación para cada x en X considerando que en cada caso, $(I_Y \circ f)(x) = f(x)$.



■

Más generalmente, la composición de cualquier función con una función identidad es igual a la función.

Teorema 7.3.1 Composición con una función identidad

Si f es una función de un conjunto X a un conjunto Y e I_X es la función identidad en X e I_Y es la función identidad en Y, entonces

$$a)\ f \circ I_X = f \quad \text{y} \quad b)\ I_Y \circ f = f.$$

Demostración:

Inciso a): Suponga que f es una función de un conjunto X a un conjunto Y e I_X es la función identidad en X. Entonces, para toda x en X,

$$(f \circ I_X)(x) = f(I_X(x)) = f(x).$$

Por tanto, por definición de igualdad de funciones, $f \circ I_X = f$, como se demostró.

Inciso b): Este es el ejercicio 13 del final de esta sección.

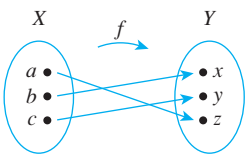
Ahora sea f una función de un conjunto X a un conjunto Y, suponga que f tiene una función inversa f^{-1}. Recuerde que f^{-1} es la función de Y a X con la propiedad de que

$$f^{-1}(y) = x \quad \Leftrightarrow \quad f(x) = y.$$

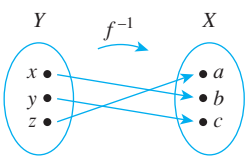
¿Qué sucede cuando f se compone con f^{-1}? ¿O cuando f^{-1} se compone con f?

Ejemplo 7.3.4 Composición de una función con su inversa

Sea $X = \{a, b, c\}$ y $Y = \{x, y, z\}$. Se define $f: X \to Y$ con el siguiente diagrama de flechas.



Entonces f es uno a uno y sobreyectiva. Por tanto, f^{-1} existe y se encuentra siguiendo las flechas hacia atrás, como se muestra a continuación.



Ahora f^{-1} o f se encuentra siguiendo las flechas de X a Y por f y regresando a X con f^{-1}. Si lo hace, se verá que

$$(f^{-1} \circ f)(a) = f^{-1}(f(a)) = f^{-1}(z) = a$$
$$(f^{-1} \circ f)(b) = f^{-1}(f(b)) = f^{-1}(x) = b$$

y

$$(f^{-1} \circ f)(c) = f^{-1}(f(c)) = f^{-1}(y) = c.$$

Por tanto, la composición de f y f^{-1} envía cada elemento a sí mismo. Por lo que por definición de la función identidad,

$$f^{-1} \circ f = I_X.$$

De forma similar, se puede ver que

$$f \circ f^{-1} = I_Y.$$ ■

Más generalmente, la composición de cualquier función con su inversa (si tiene una) es una función identidad. Intuitivamente, la función envía un elemento en su dominio a un elemento en su codominio y la función inversa se envía hacia atrás de nuevo, por lo que la composición de las dos envía cada elemento a sí mismo. Este razonamiento se ha formalizado en el teorema 7.3.2.

Teorema 7.3.2 Composición de una función con su inversa

Si $f: X \to Y$ es una función inyectiva y sobreyectiva con función inversa $f^{-1}: Y \to X$, entonces,

$$a)\ f^{-1} \circ f = I_X \quad \text{y} \quad b)\ f \circ f^{-1} = I_Y.$$

Demostración:

Inciso a): Suponga que $f: X \to Y$ es una función inyectiva y sobreyectiva con función inversa y $f^{-1}: Y \to X$. *[Para demostrar que* $f^{-1} \circ f = I_X$, *debemos demostrar que para toda* $x \in X$, $(f^{-1} \circ f)(x) = x$.*]* Sea X cualquier elemento de X. Entonces

$$(f^{-1} \circ f)(x) = f^{-1}(f(x))$$

por definición de la composición de funciones. Ahora la función inversa de f^{-1} satisface la condición

$$f^{-1}(b) = a \quad \Leftrightarrow \quad f(a) = b \quad \text{para toda } a \in X \text{ y } b \in Y. \tag{7.3.1}$$

Sea

$$x' = f^{-1}(f(x)). \tag{7.3.2}$$

Aplicando la propiedad (7.3.1) con x' jugando el papel de a y $f(x)$ jugando el papel de b. Entonces

$$f(x') = f(x).$$

Pero puesto que f es uno a uno, esto implica que $x' = x$. Sustituyendo x para x' en la ecuación (7.3.2) se obtiene

$$x = f^{-1}(f(x)).$$

Entonces por definición de composición de funciones,

$$(f^{-1} \circ f)(x) = x.$$

como se quería demostrar.

Inciso b): Es el ejercicio 14 al final de esta sección.

Composición de funciones inyectivas

La composición de funciones interactúa de maneras interesantes con las propiedades de ser inyectiva y sobreyectiva. ¿Qué ocurre, por ejemplo, cuando dos funciones inyectiva están compuestas? ¿Su composición debe ser inyectiva? Por ejemplo, sea $X = \{a, b, c\}$, $Y = \{w, x, y, z\}$ y $Z = \{1, 2, 3, 4, 5\}$ y se definen las funciones inyectiva $f: X \to Y$ y g: $Y \to$ Z, como se muestra en los diagramas de la flecha de la figura 7.3.1.

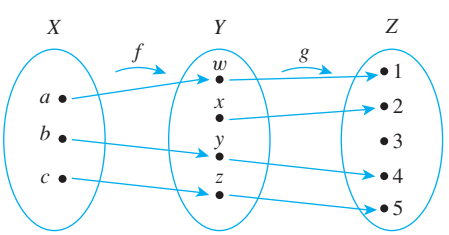


Figura 7.3.1

Entonces $g \circ f$ es la función con el diagrama de flechas que se muestra en la figura 7.3.2.

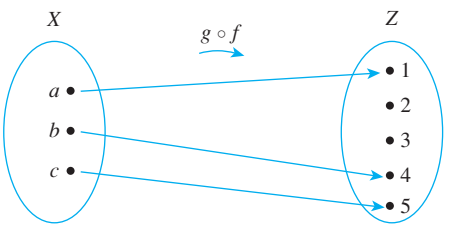


Figura 7.3.2

Del diagrama es claro que para estas funciones dadas, la composición es inyectiva. Este resultado no es casualidad. Resulta que las composiciones de dos funciones inyectivas siempre es inyectiva.

Teorema 7.3.3

Si $f: X \to Y$ y $g: Y \to Z$ ambas son funciones inyectivas, entonces $g \circ f$ es inyectiva.

Por el método de demostración directa, la demostración del teorema 7.3.3 tiene el siguiente punto de partida y la conclusión que se muestra.

Punto de partida: Suponga que f es que una función inyectiva de X a Y y g es una función inyectiva de Y a Z.

A demostrar: $g \circ f$ es una función inyectiva de X a Z.

La conclusión dice que una función dada es inyectiva. ¿Cómo se demuestra? El paso crucial es darse cuenta de que si se sustituye $g \circ f$ en la definición inyectiva, vemos que

$$g \circ f \text{ es inyectiva} \quad \Leftrightarrow \quad \forall x_1, x_2 \in X, \text{ si } (g \circ f)(x_1) = (g \circ f)(x_2) \text{ entonces } (x_1) = (x_2).$$

Después, por el método de demostración directa, demuestre que $g \circ f$ es inyectiva, usted

suponga que x_1 y x_2 son elementos de X tal que $(g \circ f)(x_1) = (g \circ f)(x_2)$,

y

demuestre que $x_1 = x_2$.

Ahora comienza el corazón de la demostración. Para demostrar que $x_1 = x_2$, trabaje a partir de la suposición de que $(g \circ f)(x_1) = (g \circ f)(x_2)$, usando el hecho de que f y g son ambas inyectivas. Por definición de composición,

$$(g \circ f)(x_1) = g(f(x_1)) \quad \text{y} \quad (g \circ f)(x_2) = g(f(x_2)).$$

Ya que los miembros izquierdos de las ecuaciones son iguales, así lo son los miembros del lado derecho. Por tanto

$$g(f(x_1)) = g(f(x_2)).$$

Ahora sólo vea la ecuación anterior por un momento. Dice que

$$g(\text{algo}) = g(\text{algo más}).$$

Ya que g es una función inyectiva, en cualquier momento g de una cosa es igual a g de otra cosa, las dos cosas son iguales. Por tanto

$$f(x_1) = f(x_2).$$

Pero f también es una función inyectiva. En cualquier momento f de una cosa es igual a f de otra cosa, las dos cosas son iguales. Por tanto,

$$x_1 = x_2.$$

¡Que es lo que se quería demostrar!

Este análisis se resume en la siguiente demostración formal.

Demostración del teorema 7.3.3:

Suponga que $f: X \to Y$ y $g: Y \to Z$ ambas son funciones inyectivas. *[Debemos demostrar que $g \circ f$ es inyectiva.]* Suponga que x_1 y x_2 son elementos de X tal que

$$(g \circ f)(x_1) = (g \circ f)(x_2).$$

[Debemos demostrar que $x_1 = x_2$.] Por definición de composición de funciones,

$$g(f(x_1)) = g(f(x_2)).$$

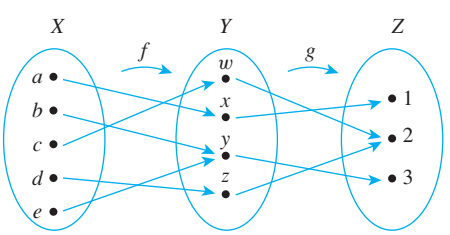
Ya que g es inyectiva, $\quad f(x_1) = f(x_2).$

Y puesto que f es inyectiva, $\quad x_1 = x_2.$

[Que es lo que se quería demostrar.] Por tanto $g \circ f$ es inyectiva.

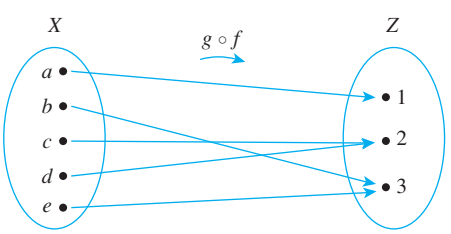
Composición de funciones sobreyectivas

Ahora considere qué sucede cuando dos funciones sobreyectivas están compuestas. Por ejemplo, sea $X = \{a, b, c, d, e\}$, $Y = \{w, x, y, z\}$ y $Z = \{1, 2, 3\}$. Los siguientes diagramas de flechas definen a las funciones f y g.



Entonces $g \circ f$ es la función con el diagrama de flechas que se muestra a continuación.

Es claro del diagrama que $g \circ f$ es sobreyectiva.



Resulta que la composición de cualesquiera dos funciones sobreyectiva (que puedan componerse) es sobreyectiva.

Teorema 7.3.4

Si $f: X \to Y$ y $g: Y \to Z$ son ambas funciones sobreyectivas, entonces $g \circ f$ es sobreyectiva.

Una demostración directa del teorema 7.3.4 tiene el siguiente punto de partida y la conclusión que se muestra:

Punto de partida: Suponga que f es una función sobreyectiva de X a Y y g es una función sobreyectiva de Y a Z.

A demostrar: $g \circ f$ es una función sobreyectiva de X a Z.

La conclusión dice que es una función sobreyectiva dada. ¿Cómo se demuestra? El paso crucial es darse cuenta de que si se sustituye $g \circ f$ en la definición de sobreyectiva, verá que

$g \circ f : X \to Z$ es sobreyectiva $\Leftrightarrow$ dado cualquier elemento z de Z, es posible encontrar un elemento x de X tal que $(g \circ f)(x) = z$.

¡Precaución! Para demostrar que una función es sobreyectiva, usted debe comenzar en el elemento arbitrario del codominio y deducir que es la imagen de un cierto elemento en el dominio.

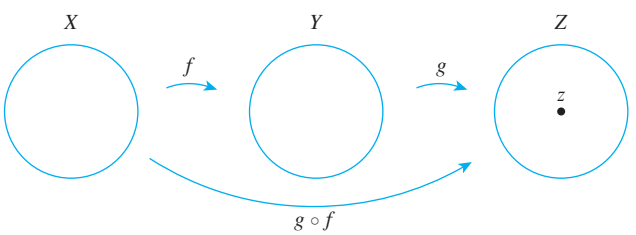
Puesto que este enunciado es universal, para demostrarlo

suponga que z es un elemento *[particular arbitrariamente elegido]* de Z

y **demuestre** que existe un elemento x en X tal que $(g \circ f)(x) = z$.

Por lo que debe iniciar la demostración suponiendo que le están dando un elemento particular arbitrariamente elegido en Z. Le llamamos z. Su trabajo consiste en encontrar un elemento x de X tal que $(g \circ f)(x) = z$.

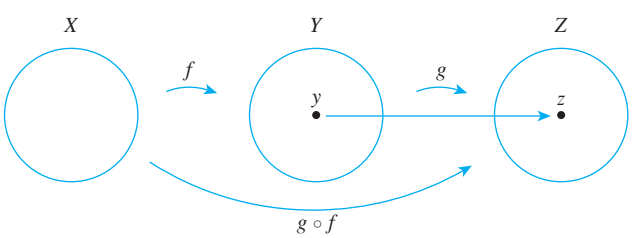
Para encontrar x, considere la suposición de que z está en Z, usando el hecho de que tanto g como f son sobreyectivas. Imagine diagramas de flechas para la funciones f y g.



Tiene un elemento particular z en Z y necesita encontrar un elemento x de X tal que cuando x se envía a Z con $g \circ f$, su imagen será z. Puesto que g es sobreyectiva, z está en la punta de alguna flecha que viene de Y. Es decir, existe un elemento y en Y tal que

$$g(y) = z. \qquad 7.3.3$$

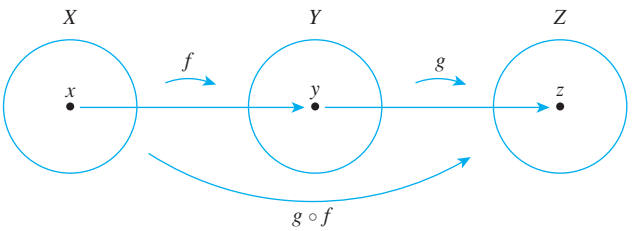
Esto significa que se pueden dibujar los diagramas de flechas siguientes:



Pero f también es sobreyectiva, por lo que cada elemento en Y está en la punta de una flecha que viene de X. En particular, y está en la punta de alguna flecha. Es decir, existe un elemento x de X tal que

$$f(x) = y. \tag{7.3.4}$$

Por tanto, el diagrama se puede dibujar como se muestra a continuación.



Ahora sólo sustituya la ecuación (7.3.4) en la ecuación (7.3.3) para obtener

$$g(f(x)) = z.$$

Pero por la definición de $g \circ f$,

$$g(f(x)) = (g \circ f)(x).$$

Por tanto

$$(g \circ f)(x) = z.$$

Por lo que x es un elemento de X, que es enviado por $g \circ f$ a z y así x es el elemento que se quería encontrar.

Este análisis se resume en la siguiente demostración formal.

Demostración del teorema 7.3.4:

Suponga que $f: X \to Y$ y $g: Y \to Z$ son ambas funciones. *[Debemos demostrar que $g \circ f$ es sobreyectiva.]* Sea z un elemento *[particular arbitrariamente elegido]* de Z. *[Debemos demostrar la existencia de un elemento x de X tal que $(g \circ f)(x) = z$.]* Como g es sobreyectiva, hay un elemento y de Y tal que $g(y) = z$. Y puesto que f es sobreyectiva, existe un elemento x en X tal que $f(x) = y$, por tanto, existe un elemento x en X tal que

$$(g \circ f)(x) = g(f(x)) = g(y) = z$$

[como se quería demostrar]. Por lo que se deduce que $g \circ f$ es sobreyectiva.

Ejemplo. 7.3.5 Una "demostración" incorrecta que es una función sobreyectiva

Para demostrar que una composición de funciones sobreyectiva es sobreyectiva, un estudiante escribió,

"Suponga que $f: X \to Y$ y $g: Y \to Z$ son ambas sobreyectivas. Entonces

$\forall y \in Y, \exists x \in X$ tal que $f(x) = y$(*)

y

$\forall z \in Z, \exists y \in Y$ tal que $f(y) = z$.

Por tanto

$$(g \circ f)(x) = g(f(x)) = g(y) = z$$

y así, $g \circ f$ es sobreyectiva".

Explique los errores en esta "demostración".

Solución Para demostrar que $g \circ f$ es sobreyectiva, debe ser capaz de hacer frente al siguiente reto: si alguien le da un elemento z en Z (sobre el que no tienen ningún control), debe ser capaz de explicar cómo encontrar un elemento x en X tal que $(g \circ f)(x) = z$. Por tanto una demostración de que $g \circ f$ es sobreyectiva debe comenzar con la suposición de que tenga un elemento particular arbitrariamente elegido de Z. Esta demostración no lo hace.

Además, observe que el enunciado (*) simplemente afirma que f es sobreyectiva. Una versión informal de (*) es la siguiente: Dado cualquier elemento en el codominio de f, existe un elemento en el dominio de f que envía a f al elemento particular. Use los símbolos x y y para denotar que dichos elementos son arbitrarios. Igualmente bien se podrían haber utilizado cualesquiera otros dos símbolos. Por tanto, si reemplazamos las x y y en (*) por u y v, obtenemos un enunciado lógicamente equivalente y la "demostración" será lo siguiente:

"Suponga que $f: X \to Y$ y $g: Y \to Z$ son ambas sobreyectivas. Entonces,

$$\forall v \in Y, \exists u \in X \text{ tal que } f(u) = v$$

y

$$\forall z \in Z, \exists y \in Y \text{ tal que } f(y) = z.$$

Por lo que (¿?¡!)

$$(g \circ f)(x) = g(f(x)) = g(y) = z$$

y por tanto $g \circ f$ es sobreyectiva".

Puesto que esta versión es lógicamente equivalente de la "demostración", puede ver que los enunciados que conducen a las palabras, *Por lo que*, no ofrecen un fundamento para el enunciado que sigue. La razón original para escribir *Por lo que* tan solo se basó en una interpretación errónea del significado de la notación. ■

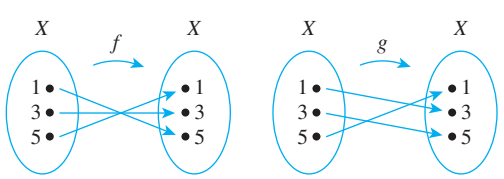
Autoexamen

1. Si f es una función de X a Y', g es una función de Y a Z y $Y' \subseteq Y$, entonces $g \circ f$ es una función de _____ a _____ y $(g \circ f)(x) =$ _____ para toda x en X.
2. Si f es una función de X a Y y I_X e I_Y son las funciones identidad de X a X y Y a Y, respectivamente, entonces, $f \circ I_x =$ _____ y $I_y \circ f =$ _____.
3. Si f es una correspondencia inyectiva de X a Y, entonces, $f^{-1} \circ f =$ _____ y $f \circ f^{-1} =$ _____.
4. Si f es una función inyectiva de X a Y y g es una función inyectiva de Y a Z, demuestre que $g \circ f$ es inyectiva suponiendo que _____ y después se demuestra que _____.
5. Si f es una en función de X a Y y g es una función sobreyectiva de Y a Z, demuestre que $g \circ f$ es sobreyectiva suponiendo que _____ y después demostrando que _____.

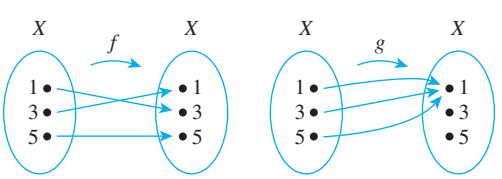
Conjunto de ejercicios 7.3

En cada uno de los ejercicios 1 y 2, las funciones f y g se definen con diagramas de flechas. Encuentre $g \circ f$ y $f \circ g$ y determine si $g \circ f$ es igual a $f \circ g$.

1.



2.



En 3 y 4, las funciones F y G se definen mediante fórmulas. Encuentre $G \circ F$ y $F \circ G$ y determine si $G \circ F$ es igual que $F \circ G$.

3. $F(x) = x^3$ y $G(x) = x - 1$ para todos los números reales x.

4. $F(x) = x^5$ y $G(x) = x^{1/5}$ para todos los números reales x.

5. Se define $f: \mathbf{R} \to \mathbf{R}$ por la regla de $f(x) = -x$ para todos los números reales x. Determine $(f \circ f)(x)$.

6. Se define $F: \mathbf{Z} \to \mathbf{Z}$ y $G: \mathbf{Z} \to \mathbf{Z}$ por las reglas $F(a) = 7a$ y $G(a) = a \bmod 5$ para todos los enteros a. Determine $(G \circ F)(0)$, $(G \circ F)(1)$, $(G \circ F)(2)$, $(G \circ F)(3)$ y $(G \circ F)(4)$.

7. Se define $H: \mathbf{Z} \to \mathbf{Z}$ y $K: \mathbf{Z} \to \mathbf{Z}$ por las reglas $H(a) = 6a$ y $K(a) = a \bmod 4$ para todos los enteros a. Determine $(K \circ H)(0)$, $(K \circ H)(1)$, $(K \circ H)(2)$ y $(K \circ H)(3)$.

8. Se define $L: \mathbf{Z} \to \mathbf{Z}$ y $M: \mathbf{Z} \to \mathbf{Z}$ por las reglas de $L(a) = a^2$ y $M(a) = a \bmod 5$ para todos los enteros a.
   a. Determine $(L \circ M)(12)$, $(M \circ L)(12)$, $(L \circ M)(9)$ y $(M \circ L)(9)$.
   b. ¿Es $L \circ M = M \circ L$?

Las funciones de cada par en los ejercicios del 9 al 11 son inversas entre sí. Para cada par, compruebe que ambas composiciones dan la función identidad.

9. $F: \mathbf{R} \to \mathbf{R}$ y $F^{-1}: \mathbf{R} \to \mathbf{R}$ están definidas por

$$F(x) = 3x + 2 \quad \text{y} \quad F^{-1}(y) = \frac{y - 2}{3},$$

para toda $y \in \mathbf{R}$.

10. $G: \mathbf{R}^+ \to \mathbf{R}^+$ y $G^{-1}: \mathbf{R}^+ \to \mathbf{R}^+$ están definidas por

$$G(x) = x^2 \quad \text{y} \quad G^{-1}(x) = \sqrt{x},$$

para toda $x \in \mathbf{R}^+$.

11. H y H^{-1} se definen ambas de $\mathbf{R} - \{1\}$ a $\mathbf{R} - \{1\}$ por la fórmula

$$H(x) = H^{-1}(x) = \frac{x + 1}{x - 1}, \quad \text{para toda } x \in \mathbf{R} - \{1\}.$$

12. Explique cómo se deduce de la definición del logaritmo que
   a. $\log_b (b^x) = x$, para todos los números reales x.
   b. $b^{\log_b x} = x$, para todos los números reales positivos x.

***H* 13.** Demuestre el teorema 7.3.1*b*): si f es cualquier función de un conjunto X a un conjunto Y, entonces $I_Y \circ f = f$, donde I_Y es la función identidad en Y.

14. Demuestre el teorema 7.3.2*b*): si $f: X \to Y$ es función inyectiva y sobreyectiva con la función inversa $f^{-1}: Y \to X$, entonces $f \circ f^{-1} = I_Y$, donde I_Y es la función identidad en Y.

15. Suponga que Y y Z son conjuntos y $g: Y \to Z$ es una función inyectiva. Esto significa que si g envía el mismo valor en dos elementos de Y, entonces esos elementos son iguales. Así, por ejemplo, si a y b son elementos de Y y $g(a) = g(b)$, entonces se puede inferir que $a = b$. ¿Qué puede deducirse en las siguientes situaciones?
   a. s_k y s_m son elementos de Y y $g(s_k) = g(s_m)$.
   b. $z/2$ y $t/2$ son elementos de Y y $g(z/2) = g(t/2)$.
   c. $f(x_1)$ y $f(x_2)$ son elementos de Y y $g(f(x_1)) = g(f(x_2))$.

16. Si $f: X \to Y$ y $g: Y \to Z$ son funciones y $g \circ f$ es inyectiva, ¿debe g ser inyectiva? Demuestre o dé un contraejemplo.

17. Si $f: X \to Y$ y $g: Y \to Z$ son funciones y $g \circ f$ es inyectiva, ¿debe f ser inyectiva? Demuestre o dé un contraejemplo.

***H* 18.** Si $f: X \to Y$ y $g: Y \to Z$ son funciones y $g \circ f$ es inyectiva, ¿debe f ser inyectiva? Demuestre o dé un contraejemplo.

***H* 19.** Si $f: X \to Y$ y $g: Y \to Z$ son funciones y $g \circ f$ es inyectiva, ¿debe g ser inyectiva? Demuestre o dé un contraejemplo.

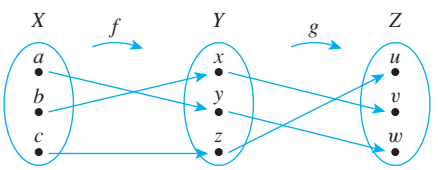
20. Sean $f: W \to X$, $g: X \to Y$ y $h: Y \to Z$ funciones. ¿Debe $h \circ (g \circ f) = (h \circ g) \circ f$? Demuestre o dé un contraejemplo.

21. ¿Verdadero o falso? Dado cualquier conjunto X y dadas las funciones cualesquiera $f: X \to X$, $g: X \to X$ y $h: X \to X$, si h es inyectiva y $h \circ f = h \circ g$, entonces $f = g$. Justifique su respuesta.

22. ¿Verdadero o falso? Dado cualquier conjunto X y dadas las funciones cualesquiera $f: X \to X$, $g: X \to X$ y $h: X \to X$, si h es inyectiva y $f \circ h = g \circ h$, entonces $f = g$. Justifique su respuesta.

En los ejercicios 23 y 24 determine $g \circ f$, $(g \circ f)^{-1}$, g^{-1}, f^{-1} y $f^{-1} \circ g^{-1}$ y establezca cómo están relacionadas $(g \circ f)^{-1}$ y $f^{-1} \circ g^{-1}$.

23. Sea $X = \{a, c, b\}$, $Y = (x, y, z\}$ y $Z = \{u, v, w\}$. Se define $f: X \to Y$ y $g: Y \to Z$ con los diagramas de flechas que se muestran a continuación.



24. Se define $f: \mathbf{R} \to \mathbf{R}$ y $g: \mathbf{R} \to \mathbf{R}$ por las fórmulas

$$f(x) = x + 3 \quad \text{y} \quad g(x) = -x \quad \text{para toda } x \in \mathbf{R}.$$

25. Demuestre o dé un contraejemplo: si $f: X \to Y$ y $g: Y \to X$ son funciones tales que $g \circ f = I_X$ y $f \circ g = I_Y$, entonces f y g son ambas funciones inyectivas y sobreyectivas y $g = f^{-1}$.

***H* 26.** Suponga que $f: X \to Y$ y $g: Y \to Z$ son tanto inyectivas como sobreyectivas. Demuestre que $(g \circ f)^{-1}$ existe y $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

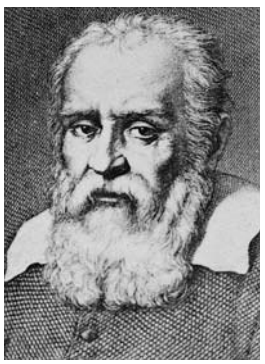
27. Sean $f: X \to Y$ y $g: Y \to Z$. ¿Es la siguiente propiedad verdadera o falsa? Para todos los subconjuntos C en Z, $(g \circ f)^{-1}(C) = (f^{-1}(g^{-1}(C))$. Justifique sus respuestas.

Respuestas del autoexamen

1. X; Z; $g(f(x))$ 2. f; f 3. I_X; I_Y, 4. x_1 y x_2 son los elementos *[particulares arbitrariamente elegidos]* de X con la propiedad que $(g \circ f)(x_1) = (g \circ f)(x_2)$; $x_1 = x_2$ 5. z es cualquier elemento *[particular arbitrariamente elegido]* en Z; existe al menos un elemento x de X tal que $(g \circ f)(x) = z$

7.4 Cardinalidad con aplicaciones a la computabilidad

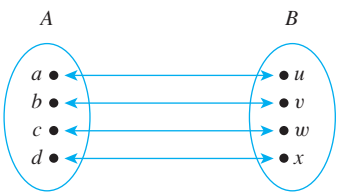
Hay tantos cuadrados como números hay ya que son exactamente tan numerosos como sus raíces. —Galileo Galilei, 1632



iStockphoto.com/Steven Wynn

Galileo Galilei (1564-1642)

Históricamente, el término *número cardinal* fue introducido para describir el tamaño de un conjunto ("Este conjunto tiene *ocho* elementos") a diferencia de un *número ordinal* que hace referencia al orden de un elemento en una sucesión. ("Este es el octavo elemento del renglón".) La definición de número cardinal se deduce de la técnica primitiva de representar números con dedos o marcas de conteo. Los niños pequeños, cuando se les pregunta qué edad tienen, a menudo responden indicando un cierto número de dedos, cada dedo está apareado con un año de su vida. Como se analizó en la sección 7.2, una pareja de elementos de los dos conjuntos se llama una correspondencia inyectiva. Decimos que dos conjuntos finitos, cuyos elementos pueden estar apareados con una correspondencia inyectiva tiene el *mismo tamaño*. Esto se ilustra en el siguiente diagrama.



Los elementos del conjunto A se pueden poner en correspondencia inyectiva con los elementos de B.

Ahora un **conjunto finito** es uno que no tiene ningún elemento o que puede ponerse en correspondencia inyectiva con un conjunto de la forma $\{1, 2, \ldots, n\}$ para un entero positivo dado. Por el contrario, un **conjunto infinito** es un conjunto no vacío que no puede ponerse en correspondencia inyectiva con $\{1, 2, \ldots, n]$ para cualquier número entero positivo n. Suponga que, como lo sugiere la cita de Galileo del principio de esta sección, ampliemos el concepto del tamaño a conjuntos infinitos diciendo que un conjunto infinito tiene el mismo tamaño que otro conjunto infinito si y sólo si, el primer conjunto se puede poner en correspondencia inyectiva con el segundo. ¿Qué consecuencias se deducen de dicha definición? ¿Todos los conjuntos infinitos tienen el mismo tamaño, o son algunos conjuntos infinitos más grandes que otros? Estas son las preguntas que abordamos en esta sección. Las respuestas son a veces sorprendentes y tienen consecuencias interesantes tal como que hay funciones definidas en el conjunto de los enteros cuyos valores no pueden calcularse con una computadora.

• Definición

Sean A y B conjuntos cualesquiera. ***A* tiene la misma cardinalidad que *B*** si y sólo si, hay una correspondencia inyectiva de A a B. En otras palabras, A tiene la misma cardinalidad que B si y sólo si, hay una función f de A a B que sea inyectiva y sobreyectiva.

El teorema siguiente da algunas propiedades básicas de cardinalidad, que la mayoría se deducen de enunciados ya demostrados acerca de funciones inyectivas sobreyectivas.

Teorema 7.4.1 Propiedades de cardinalidad

Para todos los conjuntos A, B y C:

a. **Propiedad reflexiva de cardinalidad:** A tiene la misma cardinalidad que A.

b. **Propiedad simétrica de cardinalidad:** si A tiene la misma cardinalidad que B, entonces B tiene la misma cardinalidad que A.

c. **Propiedad transitiva de cardinalidad:** si A tiene la misma cardinalidad que B y B tiene la misma cardinalidad que C, entonces A tiene la misma cardinalidad que C.

Demostración:

***Inciso a). Reflexividad*:** Suponga que A es cualquier conjunto. *[Para demostrar que A tiene la misma cardinalidad que A, debemos demostrar que hay una correspondencia inyectiva de A a A.]* Considere la función identidad I_A de A a A. Esta función es inyectiva, ya que si x_1 y x_2 son elementos cualesquiera en A con $I_A(x_1) = I_A(x_2)$, entonces, por definición de I_A, $x_1 = x_2$. La función identidad es también sobreyectiva porque si y es cualquier elemento de A, entonces $y = I_A(y)$ por definición de I_A. Por lo que I_A es una correspondencia inyectiva de A a A. *[Por lo que existe una correspondencia inyectiva de A a A, como se quería demostrar.]*

Inciso b). Simetría: Suponga que A y B son conjuntos cualesquiera y A tiene la misma cardinalidad que B. *[Debemos demostrar que B tiene la misma cardinalidad que A.]* Puesto que A tiene la misma cardinalidad que B, hay una función f de A a B que es inyectiva y sobreyectiva. Pero entonces, por los teoremas 7.2.2 y 7.2.3, hay una función f^{-1} de B a A que también es inyectiva y sobreyectiva. Por tanto B tiene la misma cardinalidad que A *[como se quería demostrar]*.

Inciso c). Transitividad: Suponga que A, B y C son conjuntos cualesquiera y que A tiene la misma cardinalidad que B y B tiene la misma cardinalidad que C. *[Debemos demostrar que A tiene la misma cardinalidad que C.]* Ya que A tiene la misma cardinalidad que B, hay una función f de A a B que es inyectiva y sobreyectiva y puesto que B tiene la misma cardinalidad que C, hay una función g de B a C, que es inyectiva y sobreyectiva. Pero entonces, por los teoremas 7.3.3 y 7.3.4, $g \circ f$ es una función de A a C, que es inyectiva y sobreyectiva. Por tanto A tiene la misma cardinalidad que C *[como se quería demostrar]*.

Observe que el teorema 7.4.1*b*), hace posible decir simplemente que dos conjuntos tienen la misma cardinalidad en lugar de tener que decir siempre que un conjunto tiene la misma cardinalidad que otro. Es decir, se puede hacer la siguiente definición.

• Definición

A y B **tienen la misma cardinalidad** si y sólo si, A tiene la misma cardinalidad que B o B tiene la misma cardinalidad que A.

El siguiente ejemplo muestra una propiedad muy importante de conjuntos infinitos: a saber, que un conjunto infinito puede tener la misma cardinalidad que un subconjunto propio del mismo. Esta propiedad se toma a veces como la definición de un conjunto infinito. El ejemplo muestra que a pesar de que parezca razonable decir que hay el doble de enteros como enteros pares hay, los elementos de los dos conjuntos pueden coincidir exactamente y por tanto, de acuerdo con la definición, los dos conjuntos tienen la misma cardinalidad.

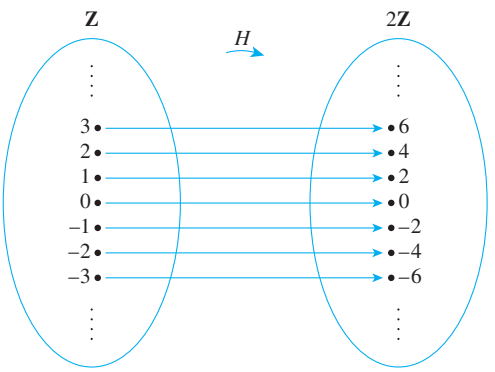
Ejemplo 7.4.1 Un conjunto infinito y un subconjunto propio pueden tener la misma cardinalidad

Sea $2\mathbf{Z}$ el conjunto de todos los enteros pares. Demuestre que $2\mathbf{Z}$ y $\mathbf{Z}$ tienen la misma cardinalidad.

Solución Considere la función H de $\mathbf{Z}$ a $2\mathbf{Z}$ que se define como sigue:

$$H(n) = 2n \quad \text{para toda } n \in \mathbf{Z}.$$

A continuación se muestra un diagrama de flechas (parcial) de H.



Para demostrar que H es inyectiva, suponga que $H(n_1) = H(n_2)$ para algunos números enteros n_1 y n_1. Entonces $2n_1 = 2n_2$ por definición de H y dividiendo ambos lados entre 2 se obtiene $n_1 = n_2$. Por tanto H es inyectiva.

Para demostrar que H es sobreyectiva, suponga que m es cualquier elemento de $2\mathbf{Z}$. Entonces m es un entero par y así $m = 2k$ para algún entero k. Lo que se deduce de que $H(k) = 2k = m$. Por tanto existe k en $\mathbf{Z}$ con $H(k) = m$ y por tanto, H es sobreyectiva.

Nota ¡Hay "tantos" enteros pares como enteros!

Por tanto, por definición de cardinalidad, $\mathbf{Z}$ y $2\mathbf{Z}$ tienen la misma cardinalidad. ■

En la sección 9.4 demostraremos que una función de un conjunto finito a otro conjunto del mismo tamaño es inyectiva si y sólo si, es sobreyectiva. Este resultado no se cumple para conjuntos infinitos. Aunque es cierto que para que dos conjuntos infinitos tengan la misma cardinalidad debe existir una función de uno a otro que sea tanto inyectiva como sobreyectiva, también siempre es el caso de que:

> Si A y B son conjuntos infinitos con la misma cardinalidad, entonces existen funciones de A a B que son inyectiva, pero no sobreyectivas y funciones de A a B que son sobreyectiva pero no inyectiva.

Por ejemplo, dado que la función H del ejemplo 7.4.1 es inyectiva y sobreyectiva, $\mathbf{Z}$ y $2\mathbf{Z}$ tienen la misma cardinalidad. Pero la "función de inclusión" I de $2\mathbf{Z}$ a $\mathbf{Z}$, dado que $I(n) = n$ para todo los enteros pares n, es inyectiva, pero no sobreyectiva. Y la función J de $\mathbf{Z}$ a $2\mathbf{Z}$ definida por $J(n) = 2\lfloor n/2 \rfloor$, para todos los enteros n, es sobreyectiva pero no inyectiva. (Vea el ejercicio 6 al final de esta sección.)

Conjuntos contables

El conjunto $\mathbf{Z}^+$ de números contables $\{1, 2, 3, 4, \ldots\}$ es, en cierto sentido, el más básico de todos los conjuntos infinitos. Un conjunto A que tiene la misma cardinalidad que este conjunto se llama *infinito contable*. La razón es que la correspondencia inyectiva entre los dos conjuntos se puede utilizar para "contar" los elementos de A: Si F es una función inyectiva y sobreyectiva de $\mathbf{Z}^+$ a A, entonces $F(1)$ pueden designarse como el primer elemento de A, $F(2)$ como el segundo elemento de A, $F(3)$ como el tercer elemento de A y así sucesivamente. Esto se ilustra gráficamente en la figura 7.4.1 en la página siguiente. Ya que F es inyectiva, nunca se cuenta algún elemento dos veces y ya que es sobreyectiva, cada elemento de A se considera eventualmente.

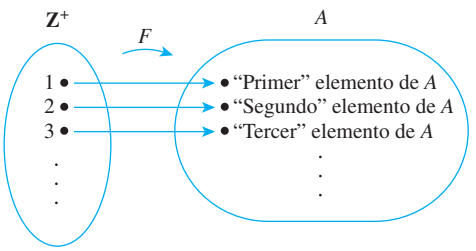


Figura 7.4.1 **"Conteo" de un conjunto infinito contable**

• Definición

Un conjunto se llama **infinito contable** si y sólo si, tiene la misma cardinalidad que el conjunto de enteros positivos $\mathbf{Z}^+$. Se llama un conjunto **contable** si y sólo si, es finito o **infinito contable**. Un conjunto que no es contable se llama **no contable**.

Ejemplo 7.4.2 Contabilidad de Z, el conjunto de todos los enteros

Demuestre que el conjunto $\mathbf{Z}$ de todos los enteros es contable.

Solución El conjunto $\mathbf{Z}$ de todos los enteros, desde luego, no es finito, por lo que, si es contable, debe ser porque es infinito contable. Para mostrar que $\mathbf{Z}$ es infinito contable, encuentre una función de los enteros positivos $\mathbf{Z}^+$ a $\mathbf{Z}$ que es inyectiva y sobreyectiva. Visto a la luz, esto contradice el sentido común; a juzgar por el diagrama siguiente, parecen ser más de dos veces como enteros positivos hay.

Pero fue alertado de que en esta sección se encontraría con sorprendentes resultados. Intente pensar en una forma de "contar" el conjunto de todos los enteros de todas formas.

El truco es comenzar en medio y trabajar hacia fuera sistemáticamente. Sea el primer entero 0, el segundo 1, el tercero -1, el cuarto 2, el quinto -2 y así sucesivamente como se muestra en la figura 7.4.2, empezando en 0 y se balancea hacia afuera en ida y vuelta en arcos desde los números positivo a los enteros negativos y viceversa, tomando un entero adicional en cada balanceo.

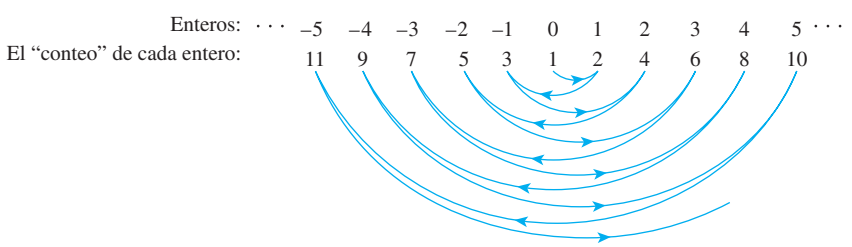


Figura 7.4.2 **"Contando" el conjunto de todos enteros**

Es claro del diagrama que ningún entero se cuenta dos veces (de modo que la función es uno a uno) y cada entero se cuenta eventualmente (por lo que la función es sobreyectiva). En consecuencia, este diagrama define una función de $\mathbf{Z}^+$ a $\mathbf{Z}$ que es inyectiva y sobreyectiva. A pesar de que en cierto sentido parecen ser números enteros más que enteros

positivos, los elementos de los dos conjuntos se pueden aparear uno a uno. Se deduce por definición de cardinalidad que $\mathbf{Z}^+$ tiene la misma cardinalidad que $\mathbf{Z}$. Por tanto, $\mathbf{Z}$ es infinito contable y por tanto contable.

La descripción diagramática de la función anterior es aceptable tal como se indica. Sin embargo, puede comprobar, que la función también puede ser descrita por la fórmula explícita

$$F(n) = \begin{cases} \dfrac{n}{2} & \text{si } n \text{ es un entero positivo par} \\ -\dfrac{n-1}{2} & \text{si } n \text{ es un número entero impar.} \end{cases}$$ ■

Ejemplo 7.4.3 Contabilidad de 2Z, el conjunto de todos los enteros pares

Demuestre que el conjunto $2\mathbf{Z}$ de todos los enteros pares es contable.

Solución El ejemplo 7.4.2 demostró que $\mathbf{Z}^+$ tiene la misma cardinalidad que $\mathbf{Z}$ y el ejemplo 7.4.1 mostró que $\mathbf{Z}$ tiene la misma cardinalidad como $2\mathbf{Z}$. Así, por la propiedad transitiva de cardinalidad, $\mathbf{Z}^+$ tiene la misma cardinalidad como $2\mathbf{Z}$. Se deduce por definición de infinito contable que $2\mathbf{Z}$ es infinito contable y por tanto contable. ■

La búsqueda de grandes infinitos: el proceso de diagonalización de Cantor

Cada conjunto infinito que hemos analizado hasta el momento ha sido infinito contable. ¿Existen algún infinito más grande? ¿Existen conjuntos no contables? A continuación se presenta un candidato.

Imagine la recta numérica como se muestra a continuación.

Como se indicó en la sección 1.2, los enteros se extienden a lo largo de la recta numérica en intervalos discretos. Los números racionales, por el contrario, son *densos*: Entre cualesquiera dos números racionales, no importa qué tan cerca, se encuentre otro número racional (por ejemplo, el promedio de dos números; vea el ejercicio 17). Esto sugiere la conjetura de que el infinito del conjunto de los números racionales es mayor que el infinito del conjunto de los enteros.

Asombrosamente, esta conjetura es falsa. A pesar del hecho de que en la recta numérica los números racionales se aglomeran, mientras que los enteros están muy separados, el conjunto de todos los números racionales puede ponerse en correspondencia inyectiva con el conjunto de los enteros. El ejemplo siguiente da parte de una demostración de este hecho. Se muestra que el conjunto de todos los números racionales positivos se puede poner en correspondencia uno a uno con el conjunto de todos los enteros positivos. En el ejercicio 16 al final de esta sección se le pide que utilice este resultado, junto con una técnica similar a la del ejemplo 7.4.2 para demostrar que el conjunto de *todos* los números racionales es contable.

Ejemplo 7.4.4 El conjunto de todos los números racionales positivos es contable

Muestre que el conjunto $\mathbf{Q}^+$ de todos los números racionales positivos es contable.

Solución Muestre los elementos del conjunto $\mathbf{Q}^+$ de números racionales positivos en una cuadrícula como se muestra en la figura 7.4.3 en la página siguiente.

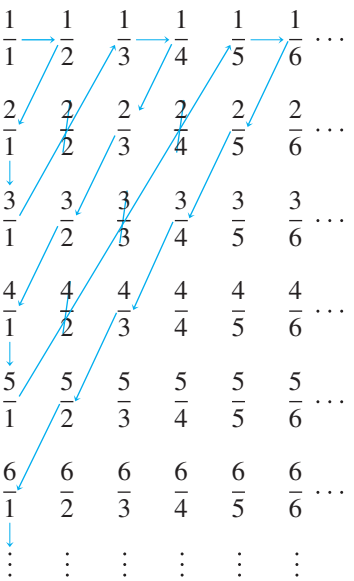


Figura 7.4.3

Definir una función f de $\mathbf{Z}^+$ a $\mathbf{Q}^+$, empezando a contar en $\frac{1}{1}$ y siguiendo las flechas como se indica, omitiendo cualquier número que ya ha sido contado.

En concreto: Sean $F(1) = \frac{1}{1}$, $F(2) = \frac{1}{2}$, $F(3) = \frac{2}{1}$ y $F(4) = \frac{3}{1}$. Pase a $\frac{2}{2}$ ya que $\frac{2}{2} = \frac{1}{1}$, que fue contado primero. Después de que se establece $F(5) = \frac{1}{3}$, $F(6) = \frac{1}{4}$, $F(7) = \frac{2}{3}$, $F(8) = \frac{3}{2}$, $F(9) = \frac{4}{1}$ y $F(10) = \frac{5}{1}$. Después se salta a $\frac{4}{2}$, $\frac{3}{3}$ y $\frac{2}{4}$ (ya que $\frac{4}{2} = \frac{2}{1}$, $\frac{3}{3} = \frac{1}{1}$ y $\frac{2}{4} = \frac{1}{2}$) y se hace $F(11) = \frac{1}{5}$. Continuando de esta manera, se define $F(n)$ para cada entero positivo n.

Observe que cada número racional positivo aparece en algún lugar en la cuadrícula y el procedimiento del conteo se configura para que cada punto de la cuadrícula se alcance finalmente. Por tanto, la función F es sobreyectiva. También, omitiendo los números que se saltan porque ya han sido contados asegura que no hay número que se cuente dos veces. Por tanto, F es uno a uno. En consecuencia, F es una función de $\mathbf{Z}^+$ a $\mathbf{Q}^+$ que es inyectiva y sobreyectiva y por tanto $\mathbf{Q}^+$ es infinito contable y por tanto contable. ■

Al Kashi
(1380-1429)

Bettmann/CORBIS

Simon Stevin
(1548-1620)

En 1874, el matemático alemán Georg Cantor logró éxito en la búsqueda de un mayor infinito, mostrando que el conjunto de todos los números reales es no contable. Sin embargo, su método de demostración es un poco complicado. Damos una demostración de la incontabilidad del conjunto de todos los números reales entre 0 y 1 usando una técnica más simple introducida por Cantor en 1891 y ahora se llama el **proceso de Diagonalización de Cantor**. En el transcurso de los años, esta técnica y variaciones se han utilizado acerca del mismo para establecer una serie de importantes resultados en lógica y la teoría de la computación.

Antes de establecer y demostrar el teorema de Cantor, observamos que cada número real, es una medida de la posición en la recta numérica se puede representar por una expansión decimal de la forma

$$a_0.a_1a_2a_3\ldots,$$

donde a_0 es un entero (positivo, negativo o cero) y para cada $i \geq 1$, a_i es un entero entre 0 y 9.

Esta manera de pensar acerca de los números se desarrolló durante varios siglos por los matemáticos en los mundos chinos, hindúes e islámicos, que culminó con la labor de Ghiyāth al-Dīn Jamshīd al-Kashi en 1427. En Europa fue donde primero se formuló claramente y se promovió con éxito por el matemático flamenco Simon Stevin en 1585. Mostramos el concepto con un ejemplo.

Considere el punto P en la figura 7.4.4. La figura 7.4.4*a*) muestra a P situado entre 1 y 2. Cuando el intervalo entre 1 y 2 se divide en diez subintervalos iguales (vea la figura 7.4.4*b*)) P se ve que se encuentra entre 1.6 y 1.7. Si el intervalo entre 1.6 y 1.7 fuese dividido en diez subintervalos iguales (vea la figura 7.4.4*c*)), P se ve que se encuentra entre 1.62 y 1.63 pero que está más cerca de 1.62 que de 1.63. Por lo que los tres primeros dígitos de la expansión decimal de P son 1.62.

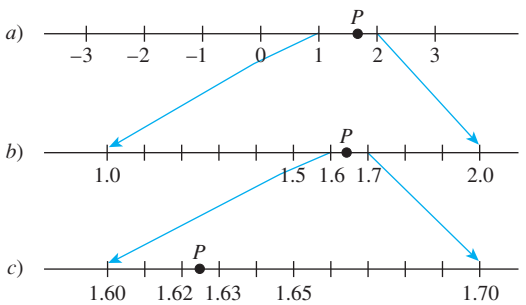


Figura 7.4.4

Suponiendo que cualquier intervalo de números reales, sin importar qué tan pequeño, se puede dividir en diez subintervalos iguales, el proceso de obtención de dígitos adicionales en la expansión decimal para P puede, en teoría, repetirse indefinidamente. Si en cualquier momento P se ve como un punto de subdivisión, entonces todos los dígitos adicionales en la expansión se pueden tomar iguales a 0. Si no, entonces el proceso da una expansión con un número infinito de dígitos.

La representación decimal resultante para P es única salvo para los números que terminan con repetición infinita del 9 o del 0. Por ejemplo (vea el ejercicio 25 al final de esta sección),

$$0.199999\ldots = 0.200000\ldots.$$

Concordamos en expresar cualquier decimal de forma que termine con todos los 0 de modo que tendremos una representación única para cada número real.

Teorema 7.4.2 (Cantor)

El conjunto de todos los números reales entre 0 y 1 es no contable.

Demostración (por contradicción):

Suponga que el conjunto de todos los números reales entre 0 y 1 es contable. Entonces las representaciones decimales de estos números se pueden escribir en una lista como sigue:

$$\begin{aligned}
&0.a_{11}a_{12}a_{13}\cdots a_{1n}\cdots\\
&0.a_{21}a_{22}a_{23}\cdots a_{2n}\cdots\\
&0.a_{31}a_{32}a_{33}\cdots a_{3n}\cdots\\
&\qquad\vdots\\
&0.a_{n1}a_{n2}a_{n3}\cdots a_{nn}\cdots\\
&\qquad\vdots
\end{aligned}$$

[Deduciremos una contradicción, al demostrar que existe un número entre 0 *y* 1 *que no aparece en esta lista.]*

Para cada par de números enteros positivos, i y j, el j-ésimo dígito decimal del i-ésimo número en la lista es a_{ij}. En particular, el primer dígito decimal del primer

número en la lista es a_{11}, el segundo dígito decimal del número segundo en la lista es a_{22} y así sucesivamente. Por ejemplo, suponga que la lista de los números reales entre 0 y 1 se inicia como sigue:

$$\begin{array}{llllllllll} 0. & \textcircled{2} & 0 & 1 & 4 & 8 & 8 & 0 & 2 \ldots \\ 0. & 1 & \textcircled{1} & 6 & 6 & 6 & 0 & 2 & 1 \ldots \\ 0. & 0 & 3 & \textcircled{3} & 5 & 3 & 3 & 2 & 0 \ldots \\ 0. & 9 & 6 & 7 & \textcircled{7} & 6 & 8 & 0 & 9 \ldots \\ 0. & 0 & 0 & 0 & 3 & \textcircled{1} & 0 & 0 & 2 \ldots \\ & & & & \vdots & & & & \end{array}$$

Los elementos de la diagonal están en un círculo: a_{11} es 2, a_{22} es 1, a_{33} es 3, a_{44} es 7, a_{55} es 1 y así sucesivamente.

Construya un nuevo número decimal $d = 0.d_1d_2d_3 \ldots d_n \ldots$ como sigue:

$$d_n = \begin{cases} 1 & \text{si } a_{nn} \neq 1 \\ 2 & \text{si } a_{nn} = 1 \end{cases}.$$

En el ejemplo anterior,

$$\begin{aligned} &d_1 \text{ es 1 porque } a_{11} = 2 \neq 1, \\ &d_2 \text{ es 2 porque } a_{22} = 1, \\ &d_3 \text{ es 1 porque } a_{33} = 3 \neq 1, \\ &d_4 \text{ es 1 porque } a_{44} = 7 \neq 1, \\ &d_5 \text{ es 2 porque } a_{55} = 1, \end{aligned}$$

y así sucesivamente. Por tanto d sería igual a 0.12112 ....

La observación crucial es que *d es diferente para cada entero n, en la enésima posición decimal del enésimo número en la lista*. Sin embargo, ¡esto implica que d no está en la lista! En otras palabras, d es un número real entre 0 y 1 que no está en la lista de *todos* los números reales entre 0 y 1. Esta contradicción muestra la falsedad de la suposición de que el conjunto de todos los números entre 0 y 1 es contable. Por tanto, el conjunto de todos los números reales entre 0 y 1 es no contable.

Junto con la demostración de la existencia de un conjunto no contable, Cantor desarrolló toda una teoría aritmética de conjuntos infinitos de varios tamaños. Uno de los teoremas más básicos de la teoría establece que cualquier subconjunto de un conjunto contable es contable.

Teorema 7.4.3

Cualquier subconjunto de cualquier conjunto contable es contable.

Demostración:

Sea A un conjunto contable dado pero arbitrariamente elegido y sea B cualquier subconjunto de A. *[Debemos demostrar que B es contable.]* B puede ser finito o infinito. Si B es finito, entonces B es contable por definición de contable y hemos acabado. Así que suponga que B es infinito. Dado que A es contable, los distintos elementos de A se pueden representar como una sucesión

$$a_1, a_2, a_3, \ldots$$

Se define una función g: $\mathbf{Z}^+ \to B$ inductivamente de la siguiente manera:

continúa en la página 436

1. Busque sucesivamente a través de los elementos de $a_1, a_2, a_3, \ldots$ hasta que encuentre un elemento de B. *[Esto debe suceder eventualmente ya que $B \subseteq A$ y $B \neq \emptyset$.]* Llame al elemento $g(1)$.
2. Para cada entero $k \geq 2$, suponga que $g(k-1)$ se ha definido. Entonces $g(k-1) = a_i$ para alguna a_i en $\{a_1, a_2, a_3, \ldots\}$. Comenzando con a_{i+1}, busque de forma sucesiva a través de $a_{i+1}, a_{i+2}, a_{i+3}, \ldots$ tratando de encontrar un elemento de B. Uno lo debe encontrar finalmente ya que B es infinito y $\{g(1), g(2), \ldots, g(k-1)\}$ es un conjunto finito. Cuando se encuentra un elemento de B, se define como $g(k)$.

Por (1) y (2) que acabamos de ver, la función g se define para cada entero positivo.

Puesto que los elementos de $a_1, a_2, a_3, \ldots$ son todos distintos, g es inyectiva. Por otra parte, las búsquedas para elementos de B son sucesivas: Cada uno recoge al anterior donde lo dejó. Por tanto, se obtiene cada elemento de A durante alguna búsqueda. Pero todos los elementos de B se encuentran en algún lugar en la sucesión $a_1, a_2, a_3, \ldots$ y así cada elemento de B finalmente se encuentra y es la imagen de algunos enteros. Por tanto g es sobreyectiva. Estas observaciones muestran que g es una correspondencia inyectiva de $\mathbf{Z}^+$ a B. Por tanto B es infinito contable y por tanto contable.

Nota Si $g(k-1) = a_i$, entonces $g(k)$ también podría ser definida al aplicarle el principio del buen-orden al sistema $\{n \in \mathbf{Z} \mid n > i \text{ y } a_i \in B\}$, para los números enteros.

Una consecuencia inmediata del teorema 7.4.3 es el siguiente corolario.

Corolario 7.4.4

Cualquier conjunto con un subconjunto no contable es no contable.

Demostración:

Considere la siguiente redacción equivalente del teorema 7.4.3: Para todos los conjuntos S y para todos los subconjuntos A de S, si S es contable, entonces A es contable. El contrapositivo de este enunciado es lógicamente equivalente a éste y establece: Para todos los conjuntos S y para todos los subconjuntos A de S, si A es no contable entonces S es no contable. Pero esta es una frase equivalente para el corolario. Por lo que se demuestra el corolario.

El corolario 7.4.4 implica que el conjunto de todos los números reales es no contable ya que el subconjunto de los números entre 0 y 1 es no contable. De hecho, como muestra el ejemplo 7.4.5, ¡el conjunto de todos los números reales tiene la misma cardinalidad que el conjunto de todos los números reales entre 0 y 1! Este hecho se explora aún más en los ejercicios 13 y 14 del final de esta sección.

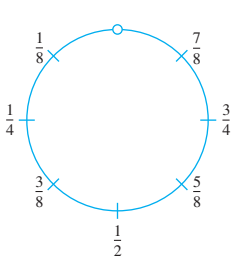
Ejemplo 7.4.5 La cardinalidad del conjunto de todos los números reales

Demuestre que el conjunto de todos los números reales tiene la misma cardinalidad que el conjunto de números reales entre 0 y 1.

Solución Sea S el intervalo abierto de números entre 0 y 1:

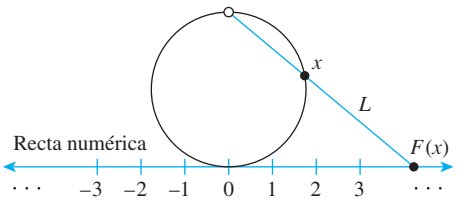
$$S = \{x \in \mathbf{R} \mid 0 < x < 1\}.$$

Imagine tomar a S y colocarlo en la circunferencia, como se muestra a continuación. Ya que S no incluye ni al punto final 0 ni al 1, el punto de la parte superior de la circunferencia se omite en el dibujo.



Se define una función $F: S \to \mathbf{R}$ como sigue:

Se dibuja una recta numérica y se coloca el intervalo, S, algo ampliado y colocado en una circunferencia, tangente a la recta de arriba del punto 0. Esto se muestra a continuación.



Para cada punto x en la circunferencia que representa a S, dibuje una línea recta L del punto de la parte superior de la circunferencia a x. Sea $F(x)$ el punto de intersección de L y la recta numérica. ($F(x)$ se llama la *proyección de* x en la recta numérica.)

Es claro de la geometría de la situación que distintos puntos de la circunferencia van a puntos distintos en la recta numérica, por lo que F es uno a uno. Además, dado cualquier punto y en la recta numérica, se puede dibujar una recta de y al punto de la parte superior de la circunferencia. Esta recta debe intersectar la circunferencia en algún punto x y, por definición $y = F(x)$. Por tanto, F es sobreyectiva. Por tanto F es una correspondencia inyectiva de S a $\mathbf{R}$ y por tanto S y $\mathbf{R}$ tienen la misma cardinalidad. ■

Usted sabe que cada entero positivo es un número real, por lo que al colocar el ejemplo 7.4.5 junto con el teorema de Cantor (teorema 7.4.2) se muestra que el infinito del conjunto de todos los números reales es "mayor" que el infinito del conjunto de todos los enteros positivos. En el ejercicio 35, deberá demostrar que cualquier conjunto y su conjunto potencia tienen cardinalidad diferente. Ya que hay una función inyectiva de cualquier conjunto con su conjunto potencia (la función que toma cada elemento a con el conjunto singleton $\{a\}$), esto implica que la cardinalidad de cualquier conjunto es "menor que" la cardinalidad de su conjunto potencia. Como resultado, puede crear una sucesión infinita de ¡infinitos más y más grandes! Por ejemplo, podría comenzar con $\mathbf{Z}$, el conjunto de todos los enteros y tomar $\mathbf{Z}$, $\mathscr{P}(\mathbf{Z})$, $\mathscr{P}(\mathscr{P}(\mathbf{Z}))$, $\mathscr{P}(\mathscr{P}(\mathscr{P}(\mathbf{Z})))$ y así sucesivamente.

Aplicación: cardinalidad y computabilidad

El conocimiento de la contabilidad y de la no-contabilidad de ciertos conjuntos pueden utilizarse para responder una pregunta de computabilidad. Comenzamos con la demostración que un cierto conjunto es contable.

Ejemplo 7.4.6 Contabilidad del conjunto de programas de computadora en un lenguaje de computadora

Demuestre que el conjunto de todos los programas de computadora en un lenguaje de programación determinado es contable.

Solución Este resultado es consecuencia del hecho de que cualquier programa de computadora en cualquier lenguaje se puede considerar como una cadena finita de símbolos en el alfabeto (finito) del lenguaje.

Dado cualquier lenguaje de programación, sea P es el conjunto de todos los programas de computadora en el lenguaje. P será finito o infinito. Si P es finito, entonces P es contable y hemos acabado. Si P es infinito, se establece un código binario para traducir, los símbolos del alfabeto de la lengua en cadenas de 0 y de 1. (Por ejemplo, podría utilizarse el Código Estadounidense Estándar para el Intercambio de Información de siete bits, conocido como ASCII (por sus siglas en inglés para American Standard Code for Information Interchange), o el Extended Binary-Coded Decimal Interchange Code de 8 bits, conocido como EBCDIC.)

Para cada programa en P, utilice el código para traducir todos los símbolos en el programa en 0 y en 1. Ordene estas cadenas de longitud, colocando la más corta antes de

la más larga y ordenar todas las cadenas de una longitud dada considerando cada cadena como un número binario y escriba los números en orden ascendente.

Se define una función $F: \mathbf{Z}^+ \to P$ especificando que

$$F(n) = \text{el enésimo programa en la lista} \quad \text{para cada } n \in \mathbf{Z}^+.$$

Por construcción, F es inyectiva y sobreyectiva, por lo que P es infinito contable y por tanto contable. Como un simple ejemplo, suponga que los siguientes números que se muestran son todos programas en P traducidos en cadenas de bits de longitud menor o igual a 5:

$$10111,\ 11,\ 0010,\ 1011,\ 01,\ 00100,\ 1010,\ 00010.$$

Ordenados por longitud,

longitud 2: 11, 01
longitud 4: 0010, 1011, 1010
longitud 5: 10111, 00100, 00010

Y ordenando cada longitud dada por el tamaño del número binario que representan se obtiene

$$\begin{aligned} 01 &= F(1) \\ 11 &= F(2) \\ 0010 &= F(3) \\ 1010 &= F(4) \\ 1011 &= F(5) \\ 00010 &= F(6) \\ 00100 &= F(7) \\ 10111 &= F(8) \end{aligned}$$

Observe que cuando sólo se ven como números, haciendo caso omiso de los ceros líderes, $0010 = 00010$. Esto muestra la necesidad de ordenar primero las cadenas por longitud antes de ordenarlas en orden numérico ascendente. ■

El ejemplo final de esta sección muestra que cierto conjunto es no contable y, por tanto, que debe existir una función no-computable.

Ejemplo 7.4.7 La cardinalidad de un conjunto de funciones y computabilidad

a. Sea T el conjunto de todas las funciones de los enteros positivos para el conjunto {0, 1, 2, 3, 4, 5. 6, 7, 8, 9}. Demuestre, que T es no contable.

b. Deduzca la consecuencia que hay funciones no-computables. En concreto, demuestre que en cualquier lenguaje de programación debe haber una función F de $\mathbf{Z}^+$ a {0, 1, 2, 3, 4, 5, 6, 7, 8, 9} con la propiedad que no se puede escribir ningún programa de computadora que se pueda escribir en lenguaje que tome valores arbitrarios como entrada y de salida a los valores correspondientes de la función.

Solución

a. Sea S es el conjunto de todos los números reales entre 0 y 1. Como se indicó antes, se puede representar cualquier número S en la forma

$$0.a_1a_2a_3 \ldots a_n \ldots,$$

donde cada a_i es un entero de 0 a 9. Esta representación es única si se omiten los decimales que terminan en 9.

Se define una función F de S a un subconjunto de T (el conjunto de todas las funciones de $\mathbf{Z}^+$ a $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$) como sigue:

$$F(0.a_1a_2a_3 \ldots a_n \ldots) = \text{la función que envía cada entero positivo } n \text{ a } a_n.$$

Se elige el codominio de F exactamente como ese subconjunto de T que hace que F sea sobreyectiva. Es decir, se define el codominio de F igual a la imagen de F. Observe que F es uno a uno porque si $F(x_1) = F(x_2)$, entonces cada dígito decimal de x_1 es igual al correspondiente dígito decimal de x_2 y así $x_1 = x_2$. Por tanto, F es una correspondencia uno a uno de S a un subconjunto de T. Pero S es no contable por el teorema 7.4.2. Por tanto T tiene un subconjunto no contable y por tanto, por el corolario 7.4.5, T es no contable.

b. El inciso *a*) muestra que el conjunto T de todas las funciones de $\mathbf{Z}^+$ a $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ es no contable. Pero el ejemplo 7.4.6 muestra que dado cualquier lenguaje de programación, el conjunto de todos los programas en ese lenguaje es contable. En consecuencia, en cualquier lenguaje de programación no hay suficientes programas para calcular los valores de cada función en T. ¡Deben existir funciones que no son computables! ■

Autoexamen

1. Un conjunto es finito si y sólo si, _____.
2. Para demostrar que un conjunto A tiene la misma cardinalidad que B debe _____.
3. La propiedad reflexiva de cardinalidad dice que dado cualquier conjunto A, _____.
4. La propiedad simétrica de cardinalidad dice que dados los conjuntos cualesquiera A y B, _____.
5. La propiedad transitiva de cardinalidad dice que dados los conjuntos cualesquiera A, B y C, _____.
6. Un conjunto se llama infinito contable si y sólo si, _____.
7. Un conjunto se llama contable si y sólo si, _____.
8. En cada una de las siguientes opciones, complete el espacio en blanco con la palabra *contable* o con la palabra *no contable*.
   a) El conjunto de todos los enteros es _____.
   b) El conjunto de todos los números racionales es _____.
   c) El conjunto de todos los números reales entre 0 y 1 es _____.
   d) El conjunto de todos los números reales es _____.
9. El proceso de diagonalización de Cantor se usa para demostrar que _____.

Conjunto de ejercicios 7.4

1. Cuando se pregunta lo que significa que el conjunto A tiene la misma cardinalidad que el conjunto B, un estudiante responde: "A y B son inyectivas y sobreyectivas". ¿Qué debería haber contestado el estudiante? ¿Por qué?
2. Demuestre que "hay tantos cuadrados como números hay" mostrando una correspondencia inyectiva de los enteros positivos, $\mathbf{Z}^+$, al conjunto S de todos los cuadrados de los enteros positivos:

   $$S = \{n \in \mathbf{Z}^+ \mid n = k^2, \text{ para algún entero positivo } k\}.$$

3. Sea $3\mathbf{Z} = \{n \in \mathbf{Z} \mid n = 3k, \text{ para algún entero } k\}$. Demuestre que $\mathbf{Z}$ y $3\mathbf{Z}$ tienen la misma cardinalidad.
4. Sea $\mathbf{O}$ el conjunto de todos los enteros impares. Demuestre que $\mathbf{O}$ tiene la misma cardinalidad que $2\mathbf{Z}$, el conjunto de todos los enteros pares.
5. Sea $25\mathbf{Z}$ el conjunto de todos los enteros que son múltiplos de 25. Demuestre que $25\mathbf{Z}$ tiene la misma cardinalidad que $2\mathbf{Z}$, el conjunto de todos los enteros pares.

H 6. Utilice las funciones I y J definidas en el párrafo siguiente al ejemplo 7.4.1 para demostrar que a pesar de que hay una correspondencia inyectiva, H, de $2\mathbf{Z}$ a $\mathbf{Z}$, hay también una función de $2\mathbf{Z}$ a $\mathbf{Z}$ que es uno a uno, pero que no es sobreyectiva y una función de $\mathbf{Z}$ a $2\mathbf{Z}$ que es sobreyectiva pero que no es inyectiva. En otras palabras, demuestre que I es inyectiva, pero que no es sobreyectiva y demuestre que J es sobreyectiva, pero que no es inyectiva.

7. a. Compruebe que la fórmula para F dada al final del ejemplo 7.4.2 produce los valores correctos para $n = 1, 2, 3$ y 4.
   b. Utilice la función piso para escribir una fórmula para F como una sola expresión algebraica para todos los enteros positivos n.

8. Utilice el resultado del ejercicio 3 para demostrar que esa $3\mathbf{Z}$ es contable.
9. Demuestre que el conjunto de todos los enteros no negativos es contable presentando una correspondencia inyectiva entre $\mathbf{Z}^+$ y $\mathbf{Z}^{noneg}$.

En los ejercicios del 10 al 14, S denota el conjunto de números reales estrictamente entre 0 y 1. Es decir, $S = \{x \in \mathbf{R} \mid 0 < x < 1\}$.

10. Sea $U = \{x \in \mathbf{R} \mid 0 < x < 2\}$. Demuestre que S y U tienen la misma cardinalidad.

***H* 11.** Sea $V = \{x \in \mathbf{R} \mid 2 < x < 5\}$. Demuestre que S y V tienen la misma cardinalidad.

12. Sean a y b números reales con $a < b$ y suponga que $W = \{x \in \mathbf{R} \mid a < x < b\}$. Demuestre que S y W tienen la misma cardinalidad.

13. Dibuje la gráfica de la función f definida por la siguiente fórmula:

Para todos los números reales x con $0 < x < 1$,

$$f(x) = \tan\left(\pi x - \frac{\pi}{2}\right).$$

Utilice la gráfica para explicar por qué S y $\mathbf{R}$ tienen la misma cardinalidad.

✶ 14. Se define una función g del conjunto de números reales a S mediante la siguiente fórmula:

Para todos los números reales x,

$$g(x) = \frac{1}{2} \cdot \left(\frac{x}{1 + |x|}\right) + \frac{1}{2}.$$

Demuestre que g es una correspondencia inyectiva. (Es posible demostrar este enunciado con o sin cálculo.) ¿Qué conclusión puede sacar de este hecho?

15. Demuestre que el conjunto de todas las cadenas de bits (cadenas de 0 y de 1) es contable.

16. Demuestre que $\mathbf{Q}$, el conjunto de todos los números racionales, es contable.

17. Demuestre que el conjunto $\mathbf{Q}$ de todos los números racionales es denso a lo largo de la recta numérica demostrando que dados cualesquiera dos números racionales r_1 y r_2 con $r_1 < r_2$ existe ahí un número racional x tal que $r_1 < x < r_2$.

***H* 18.** ¿La media de dos números irracionales siempre debe ser irracional? Demuestre o dé un contraejemplo.

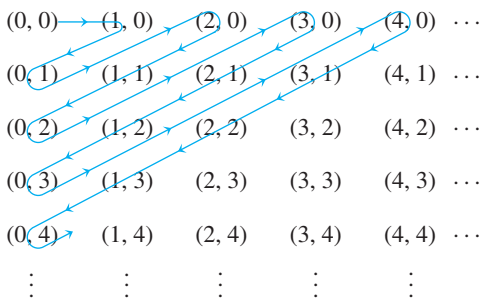
***H* ✶ 19.** Demuestre que el conjunto de todos los números irracionales es denso a lo largo de la recta numérica demostrando que dados dos números reales, hay un número irracional en medio.

20. Dé dos ejemplos de funciones de $\mathbf{Z}$ a $\mathbf{Z}$ que sean inyectivas, pero no sobreyectivas.

21. Dé dos ejemplos de funciones de $\mathbf{Z}$ a $\mathbf{Z}$ que sean sobreyectivas pero no inyectiva.

***H* 22.** Se define una función g: $\mathbf{Z}^+ \times \mathbf{Z}^+ \to \mathbf{Z}^+$ por la fórmula $g(m, n) = 2^m 3^n$ para toda $(m, n) \in \mathbf{Z}^+ \times \mathbf{Z}^+$. Demuestre que g es inyectiva y utilice este resultado para demostrar que $\mathbf{Z}^+ \times \mathbf{Z}^+$ es contable.

23. **a.** Explique cómo utilizar el diagrama siguiente para mostrar que $\mathbf{Z}^{noneg} \times \mathbf{Z}^{noneg}$ y $\mathbf{Z}^{noneg}$ tienen la misma cardinalidad.



***H* ✶ b.** Defina una función H: $\mathbf{Z}^{noneg} \times \mathbf{Z}^{noneg} \to \mathbf{Z}^{noneg}$ por la fórmula

$$H(m, n) = n + \frac{(m + n)(m + n + 1)}{2}$$

para todos los enteros no negativos m y n. Interprete la acción de H geométricamente utilizando el diagrama del inciso *a*).

✶ 24. Demuestre que la función H definida analíticamente en el ejercicio 23*b* es una correspondencia inyectiva.

***H* 25.** Demuestre que $0.1999\ldots = 0.2$.

26. Demuestre que cualquier conjunto infinito contiene un subconjunto infinito contable.

27. Si A es cualquier conjunto infinito contable, B es cualquier conjunto y g: $A \to B$ es sobreyectiva, entonces B es contable.

28. Demuestre que una unión disjunta de cualquier conjunto finito con cualquier conjunto infinito contable es infinito contable.

***H* 29.** Demuestre que la unión de dos conjuntos infinitos contables es infinito contable.

***H* 30.** Use el resultado del ejercicio 29 para demostrar que el conjunto de todos los números irracionales es no contable.

***H* 31.** Utilice los resultados de los ejercicios 28 y 29 para demostrar que la unión de dos conjuntos contables es contable.

***H* 32.** Demuestre que $\mathbf{Z} \times \mathbf{Z}$, el producto cartesiano del conjunto de enteros consigo mismo, es infinito contable.

33. Use los resultados de los ejercicios, 27, 31 y 32 para demostrar lo siguiente: Si R es el conjunto de todas las soluciones a todas las ecuaciones de la forma $x^2 + bx + c = 0$, donde b y c son enteros, entonces R es contable.

***H* 34.** Sea $\mathscr{P}(S)$ el conjunto de todos los subconjuntos del conjunto S y sea T el conjunto de todas las funciones de S a $\{0, 1\}$. Demuestre que $\mathscr{P}(S)$ y T tienen la misma cardinalidad.

***H* 35.** Sea S un conjunto y sea $\mathscr{P}(S)$ el conjunto de todos los subconjuntos de S. Demuestre que S es "más pequeño que" $\mathscr{P}(S)$ en el sentido de que hay una función inyectiva de S a $\mathscr{P}(S)$ pero no hay una función sobreyectiva de $\mathscr{P}(S)$ a S.

✶ 36. El teorema de Schroeder-Bernstein establece lo siguiente: si A y B son conjuntos cualesquiera con la propiedad que existe una función inyectiva de A a B y una función inyectiva de B a A, entonces A y B tienen la misma cardinalidad. Use este teorema para demostrar que hay tantas funciones de $\mathbf{Z}^+$ a $\{0, 1, 2, 3, 4, 5, 6, 7. 8, 9\}$ como funciones hay de $\mathbf{Z}^+$ a $\{0, 1\}$.

***H* 37.** Demuestre que si A y B son conjuntos infinitos contables cualesquiera, entonces $A \times B$ es infinito contable.

✶ 38. Suponga que $A_1, A_2, A_3, \ldots$ es una sucesión infinita de conjuntos contables. Recuerde que

$$\bigcup_{i=1}^{\infty} A_i = \{x \mid x \in A_i \text{ para algún entero positivo } i\}$$

Demuestre que $\bigcup_{i=1}^{\infty} A_i$ es contable. (En otras palabras. demuestre que una unión de conjuntos infinitos contables es contable.)

Respuestas del autoexamen

1. es el conjunto vacío o hay una correspondencia inyectiva de $\{1, 2, \ldots, n\}$ a éste, donde n es un número entero 2. demostrar que existe una función de A a B que es inyectiva y sobreyectiva (O: demostrar que existe una correspondencia inyectiva de A a B) 3. A tiene la misma cardinalidad que A. 4. si A tiene la misma cardinalidad que B, entonces B tiene la misma cardinalidad que A 5. si A tiene la misma cardinalidad que B y B tiene la misma cardinalidad que C, entonces A tiene la misma cardinalidad que C 6. tiene la misma cardinalidad que el conjunto de todos los enteros positivos 7. es finito o infinito contable 8. contable; contable; no contable; no contable 9. el conjunto de todos los números reales entre 0 y 1 es no contable

CAPÍTULO 8

RELACIONES

En este capítulo analizamos las matemáticas de las relaciones definidas sobre conjuntos, centrándonos en las formas de representar relaciones y explorando las diversas propiedades que puedan tener. El concepto de relación de equivalencia se presentó en la sección 8.3 y se aplica en la sección 8.4 a la aritmética modular y criptografía. Las relaciones de orden parcial se abordan en la sección 8.5 y se presenta una aplicación que muestra cómo utilizar estas relaciones para ayudar a coordinar y orientar el flujo de tareas individuales que se deben realizar para lograr un proyecto complejo de gran escala.

8.1 Relaciones sobre conjuntos

Por extraño que parezca, el poder de las matemáticas descansa en su evasión de todo pensamiento innecesario y en el ahorro maravilloso de operaciones mentales. —Ernst Mach, 1838-1916

Una manera más formal para referirse al tipo de relación que se define en la sección 1.3 es llamarla una **relación binaria**, porque es un subconjunto de un producto cartesiano de dos conjuntos. Al final de esta sección se establece una *relación n-aria* como un subconjunto de un producto cartesiano de n conjuntos, donde n es cualquier número entero mayor o igual a dos. Tal relación es la estructura fundamental usada en bases de datos relacionales. Sin embargo, ya que nos concentramos en relaciones binarias en este libro, cuando usamos el término *relación* por sí mismo, queremos decir una relación binaria.

Ejemplo 8.1.1 La relación menor que para números reales

Se define una relación L de $\mathbf{R}$ a $\mathbf{R}$ como sigue: Para todos los números reales x y y,

$$x \, L \, y \Leftrightarrow x < y.$$

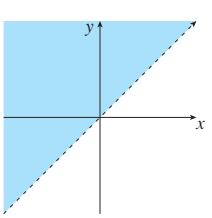
a. ¿Es $57 \, L \, 53$? b. ¿Es $(-17) \, L \, (-14)$? c. ¿Es $143 \, L \, 143$? d. ¿Es $(-35) \, L \, 1$?

e. Dibuje la gráfica de L como un subconjunto del plano cartesiano $\mathbf{R} \times \mathbf{R}$

Solución

a. No, $57 > 53$ b. Sí, $-17 < -14$ c. No, $143 = 143$ d. Sí, $-35 < 1$

e. Para cada valor de x, todos los puntos (x, y) con $y > x$ están sobre la gráfica. Por lo que la gráfica consiste de todos los puntos que están arriba de la recta $x = y$.



■

Ejemplo 8.1.2 La relación de congruencia módulo 2

Se define una relación E de $\mathbf{Z}$ a $\mathbf{Z}$ como sigue: Para todo $(m, n) \in \mathbf{Z} \times \mathbf{Z}$,

$$m \; E \; n \Leftrightarrow m - n \text{ es par.}$$

a. ¿Es $4 \; E \; 0$? ¿Es $2 \; E \; 6$? ¿Es $3 \; E \; (-3)$? ¿Es $5 \; E \; 2$?

b. Enumere cinco enteros que están relacionados por E a 1.

c. Demuestre que si n es cualquier entero impar, entonces $n \; E \; 1$.

Solución

a. Sí, $4 \; E \; 0$ ya que $4 - 0 = 4$ y 4 es par.
Sí, $2 \; E \; 6$ ya que $2 - 6 = -4$ y -4 es par.
Sí, $3 \; E \; (-3)$ porque $3 - (-3) = 6$ y 6 es par.
No, $5 \not E \; 2$ ya que $5 - 2 = 3$ y 3 no es par.

b. Hay muchas de estas listas. Una es

$$\begin{aligned} 1 &\text{ ya que } 1 - 1 = 0 \text{ es par,} \\ 3 &\text{ ya que } 3 - 1 = 2 \text{ es par,} \\ 5 &\text{ ya que } 5 - 1 = 4 \text{ es par,} \\ -1 &\text{ ya que } -1 - 1 = -2 \text{ es par,} \\ -3 &\text{ ya que } -3 - 1 = -4 \text{ es par.} \end{aligned}$$

c. **Demostración:** Suponga que n es cualquier entero impar. Entonces $n = 2k + 1$ para todo entero k. Ahora por definición de E, $n \; E \; 1$ si y sólo si, $n - 1$ es par. Pero por sustitución,

$$n - 1 = (2k + 1) - 1 = 2k,$$

y ya que k es un número entero, $2k$ es par. Por tanto $n \; E \; 1$ *[como se quería demostrar]*.

Se puede demostrar (vea el ejercicio 2 al final de esta sección) que los enteros m y n están relacionados por E si y sólo si, $m \; mod \; 2 = n \; mod \; 2$ (es decir, ambos son pares o ambos son impares). Cuando esto ocurre se dice que m y n tienen **congruencia módulo 2.** ■

Ejemplo 8.1.3 Una relación sobre el conjunto potencia

Sea $X = \{a, b, c\}$. Entonces $\mathscr{P}(X) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$. Se define una relación $\mathbf{S}$ de $\mathscr{P}(X)$ a $\mathbf{Z}$ como sigue: Para todos los conjuntos A y B en $\mathscr{P}(X)$ (es decir, para todos los subconjuntos A y B de X),

$$A \; \mathbf{S} \; B \Leftrightarrow A \text{ tiene al menos los mismos elementos que } B.$$

a. ¿Es $\{a, b\} \; \mathbf{S} \; \{b, c\}$? b. ¿Es $\{a\} \; \mathbf{S} \; \emptyset$? c. ¿Es $\{b, c\} \; \mathbf{S} \; \{a, b, c\}$? d. ¿Es $\{c\} \; \mathbf{S} \; \{a\}$?

Solución

a. Sí, ambos conjuntos tienen dos elementos.

b. Sí, $\{a\}$ tiene un elemento y $\emptyset$ tiene cero elementos y $1 \geq 0$.

c. No, $\{b, c\}$ tiene dos elementos y $\{a, b, c\}$ tiene tres elementos y $2 < 3$.

d. Sí, ambos conjuntos tienen un elemento. ■

La inversa de una relación

Si R es una relación de A a B, entonces una relación R^{-1} de B a A puede definirse intercambiando los elementos de todos los pares ordenados de R.

• Definición

Sea R una relación de A a B. Se define la relación inversa R^{-1} de B a A como sigue:

$$R^{-1} = \{(y, x) \in B \times A \mid (x, y) \in R\}.$$

Esta definición puede escribirse operacionalmente como sigue:

Para toda $x \in A$ y $y \in B$, $\quad (y, x) \in R^{-1} \quad \Leftrightarrow \quad (x, y) \in R.$

Ejemplo 8.1.4 La inversa de una relación finita

Sea $A = \{2, 3, 4)$ y $B = \{2, 6, 8\}$ y sea R la relación "divide" de A a B: Para toda $(x, y) \in A \times B$,

$$x \, R \, y \quad \Leftrightarrow \quad x \mid y \qquad\qquad x \text{ divide } y.$$

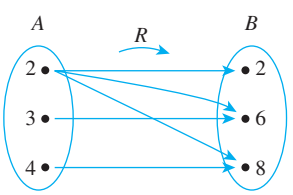
a. Establezca explícitamente qué pares ordenados están en R y R^{-1} y dibuje diagramas de flechas para R y R^{-1}.

b. Describa R^{-1} en palabras.

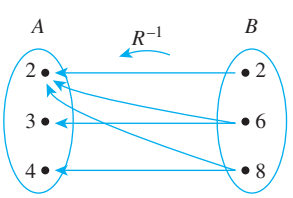
Solución

a. $R \quad = \{(2, 2), (2, 6), (2, 8), (3, 6), (4, 8)\}$

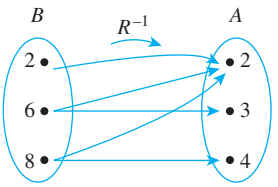
$R^{-1} = \{(2, 2), (6, 2), (8,2), (6,3), (8,4)\}$



Para dibujar el diagrama de flechas para R^{-1}, puede copiar el diagrama de flechas para R, pero invierta la dirección de las flechas.



O puede volver a dibujar el diagrama para B que está a la izquierda.



b. R^{-1} se puede describir en palabras como sigue: Para toda $(y, x) \in B \times A$,

$$y\, R^{-1}\, x \quad \Leftrightarrow \quad y \text{ es un múltiplo de } x.$$

■

Ejemplo 8.1.5 La inversa de una relación infinita

Se define una relación R de $\mathbf{R}$ a $\mathbf{R}$ como sigue: Para todas $(x, y) \in \mathbf{R} \times \mathbf{R}$,

$$x\, R\, y \quad \Leftrightarrow \quad y = 2\,|\,x\,|.$$

Dibuje las gráficas de R y R^{-1} en el plano cartesiano. ¿Es R^{-1} una función?

Solución Un punto (v, u) en la gráfica de R^{-1} si y sólo si, (u, v) está en la gráfica de R. Observe que si $x \geq 0$ entonces la gráfica de $y = 2\,|\,x\,| = 2x$ es una línea recta con pendiente 2. Y si $x < 0$ entonces, la gráfica de $y = 2\,|\,x\,| = 2(-x) = -2x$ es una línea recta con pendiente -2. Algunos valores de ejemplo están tabulados y las gráficas se muestran a continuación.

$R = \{(x, y) \mid y = 2|x|\}$

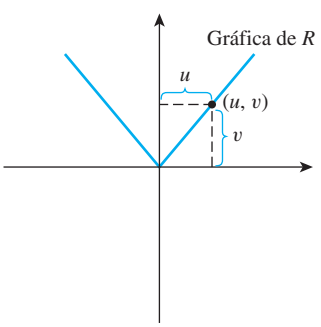
x	y
0	0
1	2
−1	2
2	4
−2	4

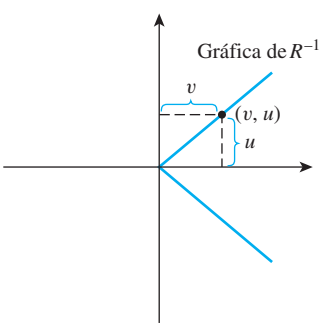
1a. coordenada — 2a. coordenada

$R^{-1} = \{(y, x) \mid y = 2|x|\}$

y	x
0	0
2	1
2	−1
4	2
4	−2

1a. coordenada — 2a. coordenada





R^{-1} no es una función, porque, por ejemplo, tanto (2, 1) y (2, − 1) están en R^{-1}. ■

Grafo dirigido de una relación

En las secciones restantes de este capítulo, se analizan las propiedades importantes de las relaciones que se definen a partir de un conjunto en sí mismo.

Nota Es importante distinguir claramente entre una relación y el conjunto en el que se define.

• Definición

Una **relación sobre un conjunto *A*** es una relación de A a A.

Cuando una relación R se define *sobre* un conjunto A, el diagrama de flechas de la relación se puede modificar para que se convierta en un **grafo dirigido**. En lugar de representar a A como dos conjuntos separados de puntos, A se representa una sola vez y se dibuja una flecha desde cada punto A a cada punto relacionado. Como un diagrama de flechas ordinario,

Para todos los puntos x y y en A,

hay una flecha de x a $y \quad \Leftrightarrow \quad x\,R\,y \quad \Leftrightarrow \quad (x, y) \in R$.

Si un punto está relacionado consigo mismo, se dibuja un bucle que sale del punto y regresa a éste.

Ejemplo 8.1.6 Grafo dirigido de una relación

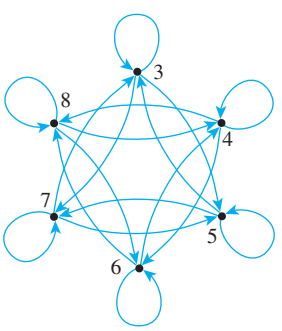
Sea $A = \{3, 4, 5, 6, 7, 8\}$ y se define una relación R sobre A como sigue: Para toda $x, y \in A$,

$$x\,R\,y \quad \Leftrightarrow \quad 2 \mid (x - y).$$

Dibuje el grafo dirigido de R.

Solución Observe que $3\,R\,3$ porque $3 - 3 = 0$ y $2 \mid 0$ ya que $0 = 2 \cdot 0$. Por tanto hay un bucle de 3 a sí mismo. Del mismo modo, hay un bucle de 4 a sí mismo, de 5 a sí mismo y así sucesivamente, ya que la diferencia de cada entero consigo mismo es 0 y $2 \mid 0$.

Observe también que $3\,R\,5$ porque $3 - 5 = -2 = 2 \cdot (-1)$. Y $5\,R\,3$ porque $5 - 3 = 2 = 2 \cdot 1$. Por tanto hay una flecha de 3 a 5 y también a una flecha de 5 a 3. Las otras flechas en el grafo dirigido, se muestran a continuación, se obtienen por razonamiento similar.



■

Relaciones n-arias y Bases de datos relacionales

Las relaciones n-arias forman la base matemática de la teoría de la base de datos relacional. Una relación binaria es un subconjunto de un producto cartesiano de dos conjuntos, asimismo, una relación n-aria es un subconjunto de un producto cartesiano de n conjuntos.

• Definición

Dados los conjuntos $A_1, A_2, \ldots, A_n$, una **relación *n*-aria** R sobre $A_1 \times A_2 \times \ldots \times A_n$ es un subconjunto de $A_1 \times A_2 \times \ldots \times A_n$. Los casos especiales de 2-arias, 3-arias y 4-arias se denominan relaciones **binarias**, **ternarias** y **cuaternarias,** respectivamente.

Ejemplo 8.1.7 Una base de datos simple

La siguiente es una versión radicalmente simplificada de una base de datos que podría utilizarse en un hospital. Sea A_1 un conjunto de enteros positivos, A_2, un conjunto de cadenas de caracteres alfabéticos, A_3 un conjunto de cadenas de caracteres numéricos y A_4 un conjunto de cadenas de caracteres alfabéticos. Se define una relación cuaternaria R sobre $A_1 \times A_2 \times A_3 \times A_4$ como sigue:

$(a_1, a_2, a_3, a_4) \in R \quad \Leftrightarrow$ un paciente con número de identificación de paciente a_1 y nombre a_2, que fue admitido en la fecha a_3, con diagnóstico primario a_4.

En un hospital particular, esta relación puede contener las siguientes 4-tuplas:

(011985, John Schmidt, 020710, asma)

(574329, Tak Kurosawa, 0114910, neumonía)

(466581, Mary Lazars, 0103910, apendicitis)

(008352, Joan Kaplan, 112409, gastritis)

(011985, John Schmidt, 021710, neumonía)

(244388, Sarah Wu, 010310, pierna rota)

(778400, Jamal Baskers, 122709, apendicitis)

En los análisis de bases de datos relacionales, normalmente las tuplas se consideran como se escriben en las tablas. Cada renglón de la tabla corresponde a una tupla y el encabezado de cada columna da el atributo descriptivo para los elementos de la columna.

Las operaciones dentro de una base de datos permiten que los datos sean manipulados de muchas maneras diferentes. Por ejemplo, en el lenguaje de base de datos SQL, si la base de datos anterior se denota por S, el resultado de la consulta es

SELECCIONE ID_Paciente#, Nombre DE S DONDE

Fecha_Admisión = 010310

podría ser una lista de los números de ID y los nombres de todos los pacientes admitidos sobre 01-03-10:

466581 Mary Lazars,

244388 Sarah Wu.

Esto se obtiene tomando la intersección del conjunto $A_1 \times A_2 \times \{010310\} \times A_4$ con la base de datos y después la proyección en las dos primeras coordenadas. (Vea el ejercicio 25 de la sección 7.1.) Del mismo modo, se puede utilizar SELECCIÓN para obtener una lista de todas las fechas de admisión de un paciente dado. Para John Schmidt, esta lista es

02-07-10 y

02-17-10

Las entradas individuales en una base de datos se pueden agregar, eliminar o actualizar y en la mayoría de las bases de datos se pueden ordenar las entradas de datos de diferentes maneras. Además, se pueden combinar todas las bases de datos y las entradas comunes a las dos bases de datos se pueden mover a una nueva base de datos. ■

Autoexamen

Las respuestas a las preguntas del autoexamen se encuentran al final de cada sección.

1. Si R es una relación de A a B, $x \in A$ y $y \in B$ la notación $x\ R\ y$ significa que _____.
2. Si R es una relación de A a B, $x \in A$ y $y \in B$, la notación $x \not R\ y$ significa que _____.
3. Si R es una relación de A a B, $x \in A$ y $y \in B$, entonces $(y, x) \in R^{-1}$ si y sólo si, _____.
4. Una relación sobre un conjunto A es una relación de _____ a _____.
5. Si R es una relación sobre un conjunto A, el grafo dirigido de R tiene una flecha de x a y si y sólo si, _____.

Conjunto de ejercicios 8.1*

1. Como en el ejemplo 8.1.2, la **congruencia módulo 2** es una relación E que se define de $\mathbf{Z}$ a $\mathbf{Z}$ como sigue: Para todos los enteros m y n,

$$m\ E\ n \quad \Leftrightarrow \quad m - n \text{ es par.}$$

   a. ¿Es $0\ E\ 0$? ¿Es $5\ E\ 2$? ¿Es $(6, 6) \in E$? ¿Es $(-1, 7) \in E$?
   b. Demuestre que para cualquier entero n, $n\ E\ 0$.

H **2.** Demuestre que para todos los enteros m y n, $m - n$ es par si y sólo si, m y n son pares o m y n son impares.

3. La relación de **congruencia módulo 3**, T, se define de $\mathbf{Z}$ a $\mathbf{Z}$ como sigue: para todos los enteros m y n,

$$m\ T\ n \quad \Leftrightarrow \quad 3 \mid (m - n).$$

   a. ¿Es $10\ T\ 1$? ¿Es $1\ T\ 10$? ¿Es $(2, 2) \in T$? ¿Es $(8, 1) \in T$?
   b. Enumere cinco enteros n tal que $n\ T\ 0$.
   c. Liste cinco enteros n tal que $n\ T\ 1$.
   d. Enumere cinco enteros n tal que $n\ T\ 2$.
H **e.** Haga y demuestre una conjetura acerca de cuáles enteros están relacionados por T a 0, cuáles enteros están relacionados por T a 1 y cuáles enteros están relacionados por T a 2.

4. Defina una relación P sobre $\mathbf{Z}$ como sigue: Para todas $m, n \in \mathbf{Z}$,

$$m\ P\ n \quad \Leftrightarrow \quad m \text{ y } n \text{ tienen un factor primo común.}$$

   a. ¿Es $15\ P\ 25$? **b.** ¿$22\ P\ 27$?
   c. ¿Es $0\ P\ 5$? d. ¿Es $8\ P\ 8$?

5. Sea $X = \{a, b, c\}$. Recuerde que $\mathscr{P}(X)$ es el conjunto potencia de X. Defina una relación $\mathbf{R}$ en $\mathscr{P}(X)$ como sigue:
   Para toda $A, B \in \mathscr{P}(X)$,

$$A\ \mathbf{R}\ B \Leftrightarrow A \text{ tiene el mismo número de elementos que } B.$$

   a. ¿Es $\{a, b\}\ \mathbf{R}\ \{b, c\}$? b. ¿Es $\{a\}\ \mathbf{R}\ \{a, b\}$?
   c. ¿Es $\{c\}\ \mathbf{R}\ \{b\}$?

6. Sea $X = \{a, b, c\}$. Se define una relación $\mathbf{J}$ sobre $\mathscr{P}(X)$ como sigue: Para todas $A, B \in \mathscr{P}(X)$

$$A\ \mathbf{J}\ B \quad \Leftrightarrow \quad A \cap B \neq \emptyset.$$

   a. ¿Es $\{a\}\ \mathbf{J}\ \{c\}$? b. ¿Es $\{a, b\}\ \mathbf{J}\ \{b, c\}$?
   c. ¿Es $\{a, b\}\ \mathbf{J}\ \{a, b, c\}$?

7. Se define una relación R sobre $\mathbf{Z}$ como sigue: Para todos los enteros m y n,

$$m\ R\ n \quad \Leftrightarrow \quad 5 \mid (m^2 - n^2).$$

   a. ¿Es $1\ R(-9)$? b. ¿Es $2\ R\ 13$?
   c. ¿Es $2\ R(-8)$? d. ¿Es $(-8)\ R\ 2$?

8. Sea A el conjunto de todas las cadenas de a y b de longitud 4. Se define una relación R sobre A como sigue: Para todas $s, t \in A$,

$$s\ R\ t \quad \Leftrightarrow \quad s \text{ tiene los mismos dos primeros caracteres que } t.$$

   a. ¿Es *abaa R abba*? **b.** ¿Es *aabb R bbaa*?
   c. ¿Es *aaaa R aaab*? d. ¿Es *baaa R abaa*?

9. Sea A el conjunto de todas las cadenas de 0 de 1 y 2 de longitud 4. Defina una relación R sobre A como sigue: Para todas $s, t \in A$,

$$s\ R\ t \quad \Leftrightarrow \quad \text{la suma de los caracteres de } s \text{ es igual a la suma de los caracteres de } t.$$

   a. ¿Es $0121\ R\ 2200$? **b.** ¿Es $1011\ R\ 2101$?
   c. ¿Es $2212\ R\ 2121$? d. ¿Es $1220\ R\ 2111$?

10. Sea $A = \{3, 4, 5\}$ y $B = \{4, 5, 6\}$ y sea R la relación "menor que". Es decir, para toda $(x, y) \in A \times B$,

$$x\ R\ y \quad \Leftrightarrow \quad x < y.$$

Establezca explícitamente que pares ordenados están en R y en R^{-1}.

11. Sea $A = \{3, 4, 5\}$ y $B = \{4, 5, 6\}$ y sea S la relación "divide". Es decir, para todo $(x, y) \in A \times B$,

$$x\ S\ y \quad \Leftrightarrow \quad x \mid y.$$

Establezca explícitamente que pares ordenados están en S y en S^{-1}.

12. **a.** Suponga una función $F: X \to Y$ inyectiva, pero no sobreyectiva. ¿Es F^{-1} (la relación inversa de F) una función? Explique su respuesta.
    b. Suponga una función $F: X \to Y$ que es sobreyectiva pero no uno a uno. ¿Es F^{-1} (la relación inversa de F) una función? Explique su respuesta.

*Para los ejercicios con números o letras azules, las soluciones están dadas en el apéndice B. El símbolo **H** indica que sólo se da una sugerencia o una solución parcial. El símbolo ✶ indica que el ejercicio es más difícil de lo normal.

Dibuje las gráficas dirigidas de las relaciones definidas en los ejercicios 13 al 18.

13. Se define una relación R sobre $A = \{0, 1, 2, 3\}$ por $R = \{(0,0), (1,2), (2, 2)\}$.

14. Se define una relación S sobre $B = \{a, b, c, d\}$ por $S = \{(a, b), (a, c), (b, c), (d, d)\}$.

15. Sea $A = \{2, 3, 4, 5, 6, 7, 8\}$ y se define una relación R sobre A como sigue: Para todas $x, y \in A$,

$$x\,R\,y \quad \Leftrightarrow \quad x \mid y.$$

H 16. Sea $A = \{5, 6, 7, 8, 9, 10\}$ y se define una relación S sobre A como sigue: Para todas $x, y \in A$,

$$x\,S\,y \quad \Leftrightarrow \quad 2 \mid (x - y).$$

17. Sea $A = \{2, 3, 4, 5, 6, 7, 8\}$ y se define una relación T sobre A como sigue: Para todas $x, y \in A$,

$$x\,T\,y \quad \Leftrightarrow \quad 3 \mid (x - y).$$

18. Sea $A = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$ y se define una relación V sobre A como sigue: Para todas $x, y \in A$,

$$x\,V\,y \quad \Leftrightarrow \quad 5 \mid (x^2 - y^2).$$

Los ejercicios 19 y 20 se refieren a las uniones y las intersecciones de las relaciones. Dado que las relaciones son subconjuntos de los productos cartesianos, sus uniones e intersecciones pueden calcularse como para cualesquier subconjunto. Dadas dos relaciones R y S de A a B,

$$R \cup S = \{(x, y) \in A \times B \mid (x, y) \in R \text{ o } (x, y) \in S\}$$
$$R \cap S = \{(x, y) \in A \times B \mid (x, y) \in R \text{ y } (x, y) \in S\}.$$

19. Sea $A = \{2, 4\}$ y $B = \{6, 8, 10\}$ y se definen las relaciones R y S de A a B como sigue: Para todo $(x, y) \in A \times B$,

$$x\,R\,y \quad \Leftrightarrow \quad x \mid y \quad \text{y}$$
$$x\,S\,y \quad \Leftrightarrow \quad y - 4 = x.$$

Establezca explícitamente cuáles pares ordenados están en $A \times B$, R, S, $R \cup S$ y $R \cap S$.

20. Sea $A = \{-1, 1, 2, 4\}$ y $B = \{1, 2\}$ y se definen las relaciones R y S de A a B como sigue: Para toda $(x, y) \in A \times B$,

$$x\,R\,y \quad \Leftrightarrow \quad |x| = |y| \quad \text{y}$$
$$x\,S\,y \quad \Leftrightarrow \quad x - y \text{ es par.}$$

Establezca explícitamente cuáles pares ordenados están en $A \times B$, R, S, $R \cup S$ y $R \cap S$.

21. Se definen las relaciones R y S sobre $\mathbf{R}$ como sigue:

$$R = \{(x, y) \in \mathbf{R} \times \mathbf{R} \mid x < y\} \quad \text{y}$$
$$S = \{(x, y) \in \mathbf{R} \times \mathbf{R} \mid x = y\}.$$

Es decir, R es la relación "menor que" y S es la relación "igual" en $\mathbf{R}$. Trace la gráfica de R, S, $R \cup S$ y $R \cap S$ en el plano cartesiano.

22. Se definen las relaciones R y S sobre $\mathbf{R}$ como sigue:

$$R = \{(x, y) \in \mathbf{R} \times \mathbf{R} \mid x^2 + y^2 = 4\} \quad \text{y}$$
$$S = \{(x, y) \in \mathbf{R} \times \mathbf{R} \mid x = y\}.$$

Trace la gráfica de R, S, $R \cup S$ y $R \cap S$ en el plano cartesiano.

23. Se definen las relaciones R y S sobre $\mathbf{R}$ como sigue:

$$R = \{(x, y) \in \mathbf{R} \times \mathbf{R} \mid y = |x|\} \quad \text{y}$$
$$S = \{(x, y) \in \mathbf{R} \times \mathbf{R} \mid y = 1\}.$$

Trace la gráfica de R, S, $R \cup S$ y $R \cap S$ en el plano cartesiano.

24. En el ejemplo 8.1.7 el resultado de la consulta SELECCIONE Paciente_ID #, Nombre DE S DÓNDE Diagnóstico_primario $= X$ es la proyección en las dos primeras coordenadas de la intersección del conjunto $A_1 \times A_2 \times A_3 \times \{X\}$ con la base de datos.
   a. Determine el resultado de la consulta SELECCIONE Paciente_ID #, Nombre DE S DÓNDE Diagnóstico_primario = pneumonía.
   b. Determine el resultado de la consulta SELECCIONE Paciente_ID #, Nombre DE S DÓNDE Diagnóstico_primario = apendicitis.

Respuestas del autoexamen

1. x está relacionada con y por R 2. x no está relacionado con y por R 3. $(x, y) \in R$ 4. A; A 5. x está relacionado con y por R

8.2 Reflexividad, simetría y transitividad

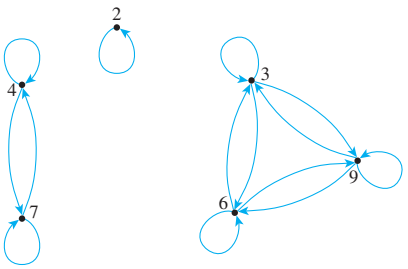
Matemáticas es la herramienta especialmente adaptada para hacer frente a los conceptos abstractos de cualquier tipo y no hay límite para su poder en este campo. —P. A. M. Dirac, 1902-1984

Sea $A = \{2, 3, 4, 6, 7, 9\}$ y se define una relación R sobre A como sigue: Para todas $x, y \in A$,

$$x\,R\,y \quad \Leftrightarrow 3 \mid (x - y).$$

Nota Para referencia:
$x\ R\ y \Leftrightarrow 3 \mid (x - y)$.

Entonces $2\ R\ 2$ ya que $2 - 2 = 0$ y $3 \mid 0$. Del mismo modo, $3\ R\ 3$, $4\ R\ 4$, $6\ R\ 6$, $7\ R\ 7$ y $9\ R\ 9$. También $6\ R\ 3$ ya que $6 - 3 = 3$ y $3 \mid 3$. Y $3\ R\ 6$ ya que $3 - 6 = -(6 - 3) = -3$ y $3 \mid (-3)$. Del mismo modo, $3\ R\ 9$, $9\ R\ 3$, $6\ R\ 9$, $9\ R\ 6$, $4\ R\ 7$ y $7\ R\ 4$. En consecuencia, el grafo dirigido para R tiene el aspecto que se muestra a continuación.



Este grafo tiene tres propiedades importantes:

1. Cada punto del grafo tiene una flecha de bucle alrededor de sí mismo.
2. En cada caso donde hay una flecha que va de un primer punto a un segundo, hay una flecha que va del segundo punto y se regresa al primero.
3. En cada caso donde hay una flecha que va de un primer punto a un segundo y del segundo punto a un tercero, hay una flecha que va del primer punto al tercero. Es decir, no hay "triángulos dirigidos incompletos" en el grafo.

Las propiedades (1), (2) y (3) corresponden a las propiedades de las relaciones generales llamadas *reflexividad*, *simetría* y *transitividad*.

• Definición

Sea R una relación sobre un conjunto A.

1. R es **reflexiva** si y sólo si, para toda $x \in A$, $x\ R\ x$.
2. R es **simétrica** si y sólo si, para toda $x, y \in A$, ***si*** $x\ R\ y$ entonces $y\ R\ x$.
3. R es **transitiva** si y sólo si, para toda $x, y, z \in A$, ***si*** $x\ R\ y$ y $y\ R\ z$ entonces $x\ R\ z$.

¡Precaución! La definición de simetría no dice que x está relacionada con y por R; sólo que si pasa que x está relacionada con y entonces y está relacionada con x.

Debido a la equivalencia de las expresiones $x\ R\ y$ y $(x, y) \in R$ para toda x y y en A, las propiedades reflexivas, simétricas y transitivas también pueden escribirse como sigue:

1. R es reflexiva $\Leftrightarrow$ para toda x en A, $(x, x) \in R$.
2. R es simétrica $\Leftrightarrow$ para toda x y y en A, ***si*** $(x, y) \in R$ entonces $(y, x) \in R$.
3. R es transitiva $\Leftrightarrow$ para toda x, y y z en A, ***si*** $(x, y) \in R$ y $(y, z) \in R$ entonces $(x, z) \in R$.

¡Precaución! El "primer", "segundo" y "tercer" elementos en las versiones informales no necesitan ser diferentes. Esta es una desventaja de informalidad: Se pueden enmascarar matices que se aclaran con una definición formal.

En términos informales, las propiedades de la (l) a la (3) dicen lo siguiente:

1. **Reflexiva:** Cada elemento está relacionado consigo mismo.
2. **Simétrica:** Si cualquier elemento está relacionado con cualquier otro elemento entonces, el segundo elemento está relacionado con el primero.
3. **Transitiva:** Si cualquier elemento está relacionado con el segundo y el segundo elemento está relacionado con el tercero entonces, el primer elemento está relacionado con el tercero.

Observe que las definiciones de reflexividad, simetría y transitividad son enunciados universales. Esto significa que para demostrar que una relación tiene una de las propiedades, utilice el método de agotamiento o el método de generalización de lo particular a lo general.

Ahora, considere lo que significa que una relación *no* tenga una de las propiedades definidas previamente. Recuerde que la negación de un enunciado universal es existencial. Por tanto si R es una relación en un conjunto A, entonces

1. R **no** es **reflexiva** $\Leftrightarrow$ hay un elemento x en A tal que $x \not R\, x$ *[es decir, tal que* $(x, x) \notin R$*]*.
2. R **no** es **simétrica** $\Leftrightarrow$ existen los elementos x y y en A tal que $x\, R\, y$ pero $y \not R\, x$ *[es decir, tal que* $(x, y) \in R$ *pero* $(y, x) \notin R$*]*.
3. R **no** es **transitiva** $\Leftrightarrow$ existen elementos x, y y z en A tal que $x\, R\, y$ y $y\, R\, z$, pero $x \not R\, z$ *[es decir, tal que* $(x, y) \in R$ y $(y, z) \in R$*, pero* $(x, z) \notin R$*]*.

Se tiene que se puede demostrar que una relación *no* tiene una de las propiedades al encontrar un contraejemplo.

Ejemplo 8.2.1 Propiedades de las relaciones sobre conjuntos finitos

Sea $A = \{0, 1, 2, 3\}$ y se definen las relaciones R, S y T sobre A como sigue:

$$R = \{(0, 0), (0, 1), (0, 3), (1, 0), (1, 1), (2, 2), (3, 0), (3, 3)\},$$
$$S = \{(0, 0), (0, 2), (0, 3), (2, 3)\},$$
$$T = \{(0, 1), (2, 3)\}.$$

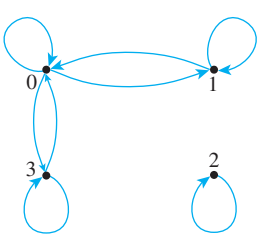
a. ¿Es R reflexiva?, ¿simétrica?, ¿transitiva?

b. ¿Es S reflexiva?, ¿simétrica?, ¿transitiva?

c. ¿Es T reflexiva?, ¿simétrica?, ¿transitiva?

Solución

a. El grafo dirigido de R tiene el aspecto que se muestra a continuación.

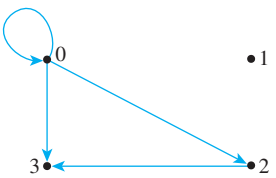


R es reflexiva: Hay un bucle en cada punto del grafo dirigido. Esto significa que cada elemento de A está relacionado consigo mismo, por lo que R es reflexiva.

R es simétrica: En cada caso donde hay una flecha que va de un punto del grafo a un segundo punto, hay una flecha que va del segundo punto hacia el primero. Esto significa que cada vez que uno de los elementos de A está relacionado con R con un segundo, entonces el segundo está relacionado con el primero. Por tanto, R es simétrica.

R no es transitiva: Hay una flecha que va de 1 a 0 y una flecha que va de 0 a 3, pero no hay ninguna flecha que vaya de 1 a 3. Esto significa que hay elementos de A — 0, 1 y 3, tales que $1\, R\, 0$ y $0\, R\, 3$, pero $1 \not R\, 3$. Por tanto, R no es transitiva.

b. El grafo dirigido de S tiene el aspecto que se muestra a continuación.

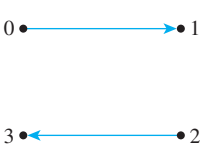


S no es reflexiva: Por ejemplo, no existe ningún bucle en 1. Por tanto $(1, 1) \notin S$ y por tanto S no es reflexiva.

S no es simétrica: Hay una flecha de 0 a 2, pero no de 2 a 0. Por tanto $(0, 2) \in S$, pero $(2, 0) \notin S$, por lo que S no es simétrica.

S es transitiva: Hay tres casos para los cuales hay una flecha que va de un punto del grafo a un segundo y del segundo punto a un tercero: a saber, hay flechas que van de 0 a 2 y de 2 a 3; hay flechas que van de 0 a 0 y de 0 a 2; y hay flechas que van de 0 a 0 y de 0 a 3. En cada caso hay una flecha que va del primer punto al tercero. (Note de nuevo una vez más que el "primer", "segundo" y "tercer" puntos no necesitan ser distintos). Esto significa que cada vez que $(x, y) \in S$ y $(y, z) \in S$, entonces $(x, z) \in S$, para todas $x, y, z \in \{0, 1, 2, 3\}$, por lo que S es transitiva.

c. El grafo dirigido de T tiene el aspecto que se muestra a continuación.



T no es reflexiva: No hay ningún bucle en 0, por ejemplo. Por tanto $(0, 0) \notin T$, así T no es reflexivo.

T no es simétrica: Hay una flecha de 0 a 1, pero no de 1 a 0. Por tanto $(0, 1) \in T$, pero $(1, 0) \notin T$ y así T no es simétrica.

Nota ¡T es transitiva por defecto ya que es *no* transitiva!

T es transitiva: La condición de transitividad es vacuamente verdadera para T. Para ver esto, observe que la condición de transitividad dice que

$$\text{Para todas } x, y, z \in A, \quad \text{si } (x, y) \in T \text{ y } (y, z) \in T \quad \text{entonces } (x, z) \in T.$$

La única manera de que esto sea falso sería que existen elementos de A que hacen verdadera la hipótesis y la conclusión sea falsa. Es decir, tendría que haber elementos x, y y z tales que

$$(x, y) \in T \quad \text{y} \quad (y, z) \in T \quad \text{y} \quad (x, z) \notin T.$$

En otras palabras, tendrían que existir dos pares ordenados en T que tienen el potencial para "vincular" al tener que el *segundo* elemento de un par es el *primer* elemento del otro par. Pero los únicos elementos en T son (0, 1) y (2, 3) y no tienen potencial para enlazar. Por tanto, la hipótesis nunca es verdadera. Por lo que es imposible para T *no* ser transitiva y así T es transitiva. ■

Cuando una relación R se define sobre un conjunto finito A, es posible escribir algoritmos de computadora para comprobar si R es reflexiva, simétrica y transitiva. Una forma de hacer esto es representar a A como un arreglo unidimensional, $(a[1], a[2], \ldots, a[n])$ y usando una modificación del algoritmo del ejercicio 38 en la sección 6.1 para comprobar si un par ordenado en $A \times A$ está en R. La comprobación de que R es reflexiva se puede hacer con un bucle que examina a su vez cada elemento $a[i]$ de A. Si, para alguna i, $(a[i], a[i]) \notin R$, entonces R no es reflexiva. De lo contrario, R es reflexiva. La comprobación de simetría se puede realizar con un bucle anidado que examina su vez cada par $(a[i], a[j])$ de $A \times A$. Si, para algún i y j, $(a[i], a[j]) \in R$ y $(a[j], a[i]) \notin R$, entonces R no es simétrica. En caso contrario, R es simétrica. La comprobación de si R es transitiva se puede hacer con un bucle triplemente anidado que examina a su vez cada tripleta $(a[i], a[j], a[k])$ de $A \times A \times A$. Si, para alguna tripleta, $(a[i], a[j]) \in R$, $(a[j], a[k]) \in R$ y $(a[i], a[k]) \notin R$ entonces, R no es transitiva. De lo contrario, R es transitiva. En los ejercicios de esta sección, deberá formalizar estos algoritmos.

Propiedades de las relaciones sobre conjuntos infinitos

Suponga una relación R que se define en un conjunto infinito A. Para demostrar que la relación es reflexiva, simétrica o transitiva, primero escriba lo que quiere demostrar. Por ejemplo, para la simetría necesita demostrar que

$$\forall x, y \in A, \text{ si } x \, R \, y \text{ entonces } y \, R \, x.$$

Después, utilice las definiciones de A y R al reescribir el enunciado para el caso particular de que se trate. Por ejemplo, para la relación de "igualdad" en el conjunto de números reales, el enunciado reescrito es

$$\forall x, y \in \mathbf{R}, \text{ si } x = y \text{ entonces } y = x.$$

A veces la veracidad del enunciado reescrito será inmediatamente evidente (como aquí). Otras veces necesitará demostrarla usando el método de la generalización de lo particular a lo general. Damos ejemplos de ambos casos en esta sección. Empezamos con la relación de igualdad, una de las relaciones más simples y aún más importantes.

Ejemplo 8.2.2 Propiedades de igualdad

Se define una relación R en $\mathbf{R}$ (el conjunto de todos los números reales) como sigue: Para todos los números reales x y y.

$$x \, R \, y \quad \Leftrightarrow \quad x = y.$$

a. ¿R es reflexiva? b. ¿R es simétrica? c. ¿R es transitiva?

Solución

a. ***R es reflexiva:*** R es reflexiva si y sólo si, el siguiente enunciado es verdadero:

$$\text{Para toda } x \in \mathbf{R}, \quad x \, R \, x.$$

Puesto que $x \, R \, x$ esto significa que $x = x$, esto es lo mismo que decir

$$\text{Para toda } x \in \mathbf{R}, \quad x = x.$$

Pero este enunciado es verdadero; cada número real es igual a sí mismo.

b. ***R es simétrica:*** R es simétrica si y sólo si, el siguiente enunciado es verdadero:

$$\text{Para todas } x, y \in \mathbf{R}, \quad \textbf{si } x \, R \, y, \text{ entonces } y \, R \, x.$$

Por definición de R, $x\,R\,y$ significa que $x = y$ y $y\,R\,x$ significa que $y = x$. Por tanto R es simétrica si y sólo si,

$$\text{Para toda } x, y \in \mathbf{R}, \quad \textbf{si } x = y, \text{ entonces } y = x.$$

Pero este enunciado es verdadero; si un número es igual a un segundo entonces, el segundo es igual al primero.

c. ***R es transitiva:*** R es transitiva si y sólo si, el siguiente enunciado es verdadero:

$$\text{Para toda } x, y, z \in \mathbf{R}, \quad \textbf{si } x\,R\,y \text{ y } y\,R\,z, \text{ entonces } x\,R\,z.$$

Por definición de R, $x\,R\,y$ significa que $x = y$, $y\,R\,z$ significa que $y = z$ y $x\,R\,z$ significa que $x = z$. Por tanto, R es transitiva si y sólo si, el siguiente enunciado es verdadero:

$$\text{Para toda } x, y, z \in \mathbf{R}, \quad \textbf{si } x = y \text{ y } y = z \text{ entonces } x = z.$$

Pero este enunciado es seguramente verdadero: Si un número real es igual a un segundo y el segundo es igual a un tercero, entonces, el primero es igual al tercero. ■

Ejemplo 8.23 Propiedades de "menor que"

Se define una relación R sobre $\mathbf{R}$ (el conjunto de todos los números reales) como sigue: Para toda $x, y \in R$,

$$x\,R\,y \quad \Leftrightarrow \quad x < y.$$

a. ¿Es R reflexiva? b. ¿Es R simétrica? c. ¿Es R transitiva?

Solución

a. ***R no es reflexiva:*** R es reflexiva si y sólo si, $\forall x \in \mathbf{R}$, $x\,R\,x$. Por definición de R, esto significa que $\forall x \in \mathbf{R}$, $x < x$. Pero esto es falso: $\exists x \in \mathbf{R}$ tal que $x \not< x$. Como un contraejemplo, sea $x = 0$ y observe que $0 \not< 0$. Por tanto, R no es reflexiva.

b. ***R no es simétrica:*** R es simétrica si y sólo si, $\forall x, y \in \mathbf{R}$, si $x\,R\,y$ entonces $y\,R\,x$. Por definición de R, esto significa que $\forall x, y \in \mathbf{R}$, si $x < y$ entonces $y < x$. Pero esto es falso: $\exists x, y \in \mathbf{R}$ tal que $x < y$ y $y \not< x$. Como un contraejemplo, sea $x = 0$ y $y = 1$ y observe que $0 < 1$ pero $1 \not< 0$. Por tanto R no es simétrica.

c. ***R es transitiva:*** R es transitiva si y sólo si, para toda $x, y, z \in \mathbf{R}$, si $x\,R\,y$ y $y\,R\,z$ entonces $x\,R\,z$. Por definición de R, esto significa que para toda $x, y, z \in \mathbf{R}$, si $x < y$ y $y < z$, entonces $x < z$. Pero este enunciado es verdadero por la ley transitiva del orden de los números reales (apéndice A, T18). Por tanto R es transitiva. ■

A veces una propiedad es "universalmente falsa" en el sentido de que es falso para *cada* elemento de su dominio. Por supuesto, se deduce inmediatamente, que la propiedad es falsa para cada elemento en particular del dominio y por tanto abundan contraejemplos. En tal caso, puede parecer más natural demostrar la falsedad universal de la propiedad, en lugar de dar un único contraejemplo. Por ejemplo, en el caso anterior, le puede resultar natural responder a (a) y a (b) como sigue:

Respuesta alternativa a (a): R no es reflexiva ya que $x \not< x$ para todos los números reales x (por la ley de la tricotomía: apéndice A, T17).

Respuesta alternativa a (b): R no simétrica ya que para toda x y y en A, si $x < y$ entonces $y \not< x$ (por ley de la tricotomía).

Ejemplo 8.2.4 Propiedades de congruencia módulo 3

Se define una relación T sobre $\mathbf{Z}$ (el conjunto de todos los enteros) como sigue: Para todos los enteros m y n,

$$m\ T\ n \quad \Leftrightarrow \quad 3 \mid (m - n).$$

Esta relación se llama **congruencia módulo 3**.

a. ¿T es reflexiva? b. ¿T es simétrica? c. ¿T es transitiva?

Solución

a. ***T es reflexiva:*** Para demostrar que T es reflexiva, es necesario demostrar que

$$\text{Para toda } m \in \mathbf{Z}, \quad m\ T\ m.$$

Por definición de T, esto significa que

$$\text{Para toda } m \in \mathbf{Z}, \quad 3 \mid (m - m).$$

O, puesto que $m - m = 0$, Para toda $m \in \mathbf{Z}$, $3 \mid 0$.

Pero esto es verdadero: $3 \mid 0$ ya que $0 = 3 \cdot 0$. Por tanto T es reflexiva. Este razonamiento se formaliza en la demostración siguiente.

Demostración de reflexividad: Suponga que m es un entero particular arbitrariamente elegido. *[Debemos demostrar que m T m.]* Ahora $m - m = 0$. Pero $3 \mid 0$ ya que $0 = 3 \cdot 0$. Por tanto $3 \mid (m - m)$. Por tanto, por definición de T, $m\ T\ m$ *[como se quería demostrar]*.

b. ***T es simétrica:*** Para demostrar que T es simétrica, es necesario demostrar que

$$\text{Para todas } m, n \in Z, \quad \textbf{si } m\ T\ n \text{ entonces } n\ T\ m.$$

Por definición de T esto significa que

$$\text{Para todas } m, n \in Z, \quad \textbf{si } 3 \mid (m - n) \text{ entonces } 3 \mid (n - m).$$

¿Es esto verdadero? Suponga que m y n son enteros particulares arbitrariamente elegidos tal que $3 \mid (m - n)$. ¿Se debe deducir que $3 \mid (n - m)$? *[En otras palabras, ¿podemos encontrar un entero tal que $n - m = 3 \cdot$ (ese número entero)?]* Por definición de "divide", ya que

$$3 \mid (m - n)$$

entonces $\qquad m - n = 3k$ para algún entero k.

La observación crucial es que $n - m = -(m - n)$. Por tanto, puede multiplicar ambos lados de esta ecuación por -1 para obtener

$$-(m - n) = -3k$$

que es equivalente a

$$n - m = 3(-k).$$

[Así nos hemos encontrado un número entero, a saber: $-k$, tal que $n - m = 3 \cdot$ (ese número entero).] Puesto que $-k$ es un entero, esta ecuación demuestra que

$$3 \mid (n - m)$$

De lo que se tiene que T es simétrica.

El razonamiento anterior se formaliza en la demostración siguiente.

Demostración de simetría: Suponga que m y n son enteros particulares arbitrariamente elegidos que cumplen la condición $m\ T\ n$. *[Debemos demostrar que $n\ T\ m$.]* Por definición de T ya que $m\ T\ n$ entonces $3 \mid (m - n)$. Por definición de "divide", esto significa que $m - n = 3k$, para algún entero k. Multiplicando ambos lados por -1 se obtiene $n - m = 3(-k)$. Puesto que, $-k$ es un entero, esta ecuación muestra que $3 \mid (n, m)$. Por tanto, por definición de T, $n\ T\ m$ *[como se quería demostrar]*.

c. ***T es transitiva:*** Para demostrar que T es transitiva, es necesario demostrar que

$$\text{Para todas } m, n, p \in \mathbf{Z}, \quad \textbf{si } m\ T\ n \text{ y } n\ T\ p \text{ entonces } m\ T\ p.$$

Por definición de T esto significa que

$$\text{Para todas } m, n \in \mathbf{Z}, \quad \textbf{si } 3 \mid (m, n) \text{ y } 3 \mid (n - p) \text{ entonces } 3 \mid (m - p).$$

¿Es esto verdadero? Supongamos que m, n y p son enteros particulares arbitrariamente elegidos tal que $3 \mid (m - n)$ y $3 \mid (n - p)$. ¿Se debe deducir que $3 \mid (m - p)$? *[En otras palabras, ¿podemos encontrar un entero tal que $m - p = 3 \cdot$ (ese entero)?]* Por definición de "divide", ya que

$$3 \mid (m - n) \quad \text{y} \quad 3 \mid (n - p),$$

entonces $m - n = 3r$ para algún entero r

y $n - p = 3s$ para algún entero s.

La observación crucial es que $(m - n) + (n - p) = m - p$. Al sumar estas dos ecuaciones juntas se obtiene

$$(m - n) + (n - p) = 3r + 3s,$$

lo que equivale a $$m - p = 3(r + s).$$

[Por tanto, hemos encontrado un entero tal que $m - p = 3 \cdot$ (ese entero).]
Ya que r y s son enteros, $r + s$ es un entero. Por lo que esta ecuación demuestra que

$$3 \mid (m - p).$$

De lo que se deduce que T es transitiva.

El razonamiento de arriba se formaliza en la demostración siguiente.

Demostración de transitividad: Suponga que m, n y p son enteros particulares arbitrariamente elegidos que satisfacen la condición $m\ T\ n$ y $n\ T\ p$. *[Debemos demostrar que $m\ T\ p$.]* Por definición de T, ya que $n\ T\ m$ y $n\ T\ p$, entonces $3 \mid (m - n)$ y $3 \mid (n - p)$. Por definición de "divide", esto significa que $m - n = 3r$ y $n - p = 3s$, para algunos enteros r y s. Sumando las dos ecuaciones se obtiene $(m - n) + (n - p) = 3r + 3s$ y simplificando se obtiene que $m - p = 3(r + s)$. Ya que $r + s$ es un entero, esta ecuación demuestra que $3 \mid (m - p)$. Por tanto, por definición de T, $m\ T\ p$ *[como se quería demostrar]*.

■

La cerradura transitiva de una relación

Generalmente hablando, una relación no puede ser transitiva porque no contienen ciertos pares ordenados. Por ejemplo, si (1, 3) y (3, 4) están en una relación R, entonces el par (1, 4) *debe* estar en R si R es transitiva. Para obtener una relación transitiva de una que no es transitiva, es necesario agregar pares ordenados. En términos generales, a la relación que se obtiene al sumar el número menor de pares ordenados para garantizar la transitividad se le llama la *cerradura transitiva* de la relación. En un sentido preciso por la definición

formal, la cerradura transitiva de una relación es la relación transitiva más pequeña que contiene la relación.

• Definición

Sea A un conjunto y R una relación sobre A. La **cerradura transitiva** de R es la relación R^t sobre A que satisface las tres siguientes propiedades:

1. R^t es transitiva.
2. $R \subseteq R^t$.
3. Si S es cualquier otra relación transitiva que contiene a R, entonces $R^t \subseteq S$.

Ejemplo 8.2.5 Cerradura transitiva de una relación

Sea $A = \{0, 1, 2, 3\}$ y considere la relación R definida sobre A como sigue:

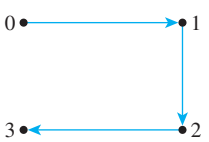
$$R = \{(0, 1), (1, 2), (2, 3)\}.$$

Encuentre la cerradura transitiva de R.

Solución Cada par ordenado en R está en R^t, por lo que

$$\{(0, 1), (1, 2), (2, 3)\} \subseteq R^t.$$

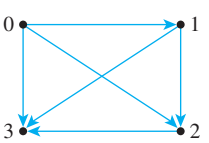
Por lo que el grafo dirigido de R contiene las flechas que se muestran a continuación.



Puesto que hay flechas que van de 0 a 1 y de 1 a 2, R^t debe tener una flecha que va de 0 a 2. Por tanto $(0, 2) \in R^t$. Entonces $(0, 2) \in R^t$ y $(2, 3) \in R^t$, por lo que puesto que R^t es transitiva $(0, 3) \in R^t$. También, puesto que $(1, 2) \in R^t$ y $(2, 3) \in R^t$, entonces $(1, 3) \in R^t$. Por tanto R^t contiene, al menos, los siguientes pares ordenados:

$$\{(0, 1), (0, 2), (0, 3), (1, 2), (1, 3), (2, 3)\}.$$

Pero esta relación *es* transitiva; por tanto es igual a R^t. Observe que el grafo dirigido de R^t es como se muestra a continuación.



■

Autoexamen

1. Que una relación R sobre un conjunto A sea reflexiva significa que _____.
2. Que una relación R sobre un conjunto A sea simétrica significa que _____.
3. Para una relación R sobre un conjunto A sea transitiva significa que _____.
4. Para demostrar que una relación R sobre un conjunto infinito A es reflexiva, suponga que _____ y demuestre que _____.
5. Para demostrar que una relación R sobre un conjunto infinito A es simétrica, suponga que _____ y demuestre que _____.
6. Para demostrar que una relación R sobre un conjunto infinito A es transitiva, suponga que _____ y demuestre que _____.
7. Para demostrar que una relación R sobre un conjunto A no es reflexiva, _____.
8. Para demostrar que una relación R sobre un conjunto A no es simétrica, _____.

9. Para demostrar que una relación R sobre un conjunto A no es transitiva, _____.

10. Dada una relación R sobre un conjunto A, la cerradura transitiva de R es la relación R^t sobre A con las siguientes tres propiedades: _____, _____ y_____.

Conjunto de ejercicios 8.2

En los ejercicios del 1 al 8, se definen una serie de relaciones en el conjunto $A = \{0, 1, 2, 3\}$. Para cada relación:
a. Dibuje el grafo dirigido.
b. Determine si la relación es reflexiva.
c. Determine si la relación es simétrica.
d. Determine si la relación es transitiva.
Dé un contraejemplo en cada caso en el que la relación no satisface una de las propiedades.

1. $R_1 = \{(0, 0), (0, 1), (0, 3), (1, 1), (1, 0), (2, 3), (3, 3)\}$

2. $R_2 = \{(0, 0), (0, 1), (1, 1), (1, 2), (2, 2), (2, 3)\}$

3. $R_3 = \{(2, 3), (3, 2)\}$

4. $R_4 = \{(1, 2), (2, 1), (1, 3), (3, 1)\}$

5. $R_5 = \{(0, 0), (0, 1), (0, 2), (1, 2)\}$

6. $R_6 = \{(0, 1), (0, 2)\}$

7. $R_7 = \{(0, 3), (2, 3)\}$

8. $R_8 = \{(0, 0), (1, 1)\}$

En los ejercicios del 9 al 33 determine si la relación dada es reflexiva, simétrica, transitiva o ninguna de las anteriores. Justifique sus respuestas.

9. R es la relación de "mayor o igual a" en el conjunto de los números reales: Para toda $x, y \in \mathbf{R}$, $x\ R\ y \Leftrightarrow x \geq y$.

10. C es la relación de la circunferencia sobre el conjunto de números reales: Para todos $x, y \in \mathbf{R}$, $x\ C\ y \Leftrightarrow x^2 + y^2 = 1$.

11. D es la relación definida sobre $\mathbf{R}$ como sigue: Para todos $x, y \in \mathbf{R}$, $x\ D\ y \Leftrightarrow xy \geq 0$.

12. E es la relación de congruencia módulo 2 sobre $\mathbf{Z}$: Para todos $m, n \in \mathbf{Z}$, $m\ E\ n \Leftrightarrow 2 \mid (m - n)$.

13. F es la relación de congruencia módulo 5 sobre $\mathbf{Z}$: Para todos $m, n \in \mathbf{Z}$, $m\ F\ n \Leftrightarrow 5 \mid (m - n)$.

14. O es la relación definida sobre $\mathbf{Z}$ como sigue: Para todos $m, n \in \mathbf{Z}$, $m\ O\ n \Leftrightarrow m - n$ es impar.

15. D es la relación "divide" sobre $\mathbf{Z}^+$: Para todos los enteros positivos m y n, $m\ D\ n \Leftrightarrow m \mid n$.

16. A es la relación "valor absoluto" sobre $\mathbf{R}$: para todos los números de reales x y y, $x\ A\ y \Leftrightarrow |\ x\ | = |\ y\ |$.

17. Recuerde que un número primo es un entero que es mayor que 1 y no tienen divisores enteros positivos excepto el 1 y a sí mismo. (En particular, 1 no es primo.) Se define una relación P sobre $\mathbf{Z}$ como sigue: para todos $m, n \in \mathbf{Z}$, $m\ P\ n \Leftrightarrow \exists$ un número primo p tal que $p \mid m$ y $p \mid n$.

***H* 18.** Se define una relación Q sobre $\mathbf{R}$ como sigue: Para todos los números reales x y y, $x\ Q\ y \Leftrightarrow x - y$ es racional.

19. Se define una relación I sobre R como sigue: Para todos los números reales x y y, $x\ I\ y \Leftrightarrow x - y$ es irracional.

20. Sea $X = \{a, b, c\}$ y $\mathscr{P}(X)$ es el conjunto potencia de X (el conjunto de todos los subconjuntos de X). Se define una relación $\mathbf{E}$ en $\mathscr{P}(X)$ como sigue: para todo A, B $\in \mathscr{P}(X)$, A $\mathbf{E}$ B $\Leftrightarrow$ el número de elementos en A es igual al número de elementos en B.

21. Sea $X = \{a, b, c\}$ y $\mathscr{P}(X)$ es el conjunto potencia de X. Se define una relación $\mathbf{L}$ en $\mathscr{P}(X)$ como sigue: Para todos A, B $\in \mathscr{P}(X)$, A $\mathbf{L}$ B $\Leftrightarrow$ el número de elementos en A es menor que el número de elementos en B.

22. Sea $X = \{a, b, c\}$ y $\mathscr{P}(X)$ es el conjunto potencia de X. Se define una relación $\mathbf{N}$ en $\mathscr{P}(X)$ como sigue: Para todos A, B $\in \mathscr{P}(X)$, A $\mathbf{N}$ B $\Leftrightarrow$ el número de elementos en A es menor que el número de elementos en B.

23. Sea X un conjunto no vacío y $\mathscr{P}(X)$ el conjunto potencia de X. Se define la relación "subconjunto" $\mathbf{S}$ en $\mathscr{P}(X)$ como sigue: para todos A, B $\in \mathscr{P}(X)$, A $\mathbf{S}$ B $\Leftrightarrow$ A $\subseteq$ B.

24. Sea X un conjunto no vacío y $\mathscr{P}(X)$ el conjunto potencia de X. Se define la relación "no igual a" $\mathbf{U}$ en $\mathscr{P}(X)$ como sigue: para todos A, B $\in \mathscr{P}(X)$, A $\mathbf{U}$ B $\Leftrightarrow$ A $\neq$ B.

25. Sea A el conjunto de todas las cadenas de a y b de longitud 4. Se define una relación R en A como sigue: para todos $s, t \in A$, $s\ R\ t \Leftrightarrow s$ tiene los mismos dos primeros caracteres que t.

26. Sea A el conjunto de todas las cadenas de 0 y 1 de longitud 4. Se define una relación R en A como sigue: para todos $s, t \in A$, $s\ R\ t \Leftrightarrow$ la suma de caracteres en s es igual a la suma de los caracteres en t.

27. Sea A el conjunto de todos los enunciados en inglés. Una relación $\mathbf{I}$ se define en A como sigue como: Para todos $p, q \in A$,

$$p\ \mathbf{I}\ q \Leftrightarrow p \rightarrow q \text{ es verdadero.}$$

28. Sea $A = \mathbf{R} \times \mathbf{R}$. Se define una relación $\mathbf{F}$ sobre A como sigue: Para todos (x_1, y_1) y (x_2, y_2) en A,

$$(x_1, y_1)\ \mathbf{F}\ (x_2, y_2) \Leftrightarrow x_1 = x_2.$$

29. Sea $A = \mathbf{R} \times \mathbf{R}$. Una relación $\mathbf{S}$ se define sobre A como sigue: Para todos (x_1, y_1) y (x_2, y_2) en A,

$$(x_1, y_1)\ \mathbf{S}\ (x_2, y_2) \Leftrightarrow y_1 = y_2.$$

30. Sea A el "plano perforado"; es decir, A es el conjunto de todos los puntos en el plano cartesiano excepto el origen (0, 0). Una relación R se define en A como sigue: Para todos p_1 y p_2 en A, $p_1 \, R \, p_2 \Leftrightarrow p_1$ y p_2, se encuentran en la misma semirrecta que sale del origen.

31. Sea A el conjunto de personas viviendo en el mundo hoy. Una relación R se define en A como sigue: Para todos $p, q \in A$,
$$p \, R \, q \Leftrightarrow p \text{ vive dentro de 100 millas de } q.$$

32. Sea A el conjunto de todas las rectas en el plano. Una relación R se define sobre A como sigue: Para todos l_1 y l_2 en A, $l_1 \, R \, l_2 \Leftrightarrow l_1$ es paralela a l_2. (Suponiendo que una recta es paralela consigo misma.)

33. Sea A el conjunto de todas las rectas en el plano. Una relación R se define sobre A como sigue: Para todas l_1 y l_2 en A,
$$l_1 \, R \, l_2 \Leftrightarrow l_1 \text{ es perpendicular a } l_2.$$

En los ejercicios del 34 al 36, suponga que R es una relación sobre un conjunto de A. Demuestre o refute cada enunciado.

34. Si R es reflexiva, entonces R^{-1} es reflexiva.

35. Si R es simétrica, entonces R^{-1} es simétrica.

36. Si R es transitiva, entonces R^{-1} es transitiva.

En los ejercicios del 37 al 42, suponga que R y S son relaciones sobre un conjunto de A. Demuestre o refute cada enunciado.

37. Si R y S son reflexivas, ¿es $R \cap S$ reflexiva? ¿Por qué?

***H* 38.** Si R y S son simétricas, ¿es $R \cap S$ simétrica? ¿Por qué?

39. Si R y S son transitivas, ¿es $R \cap S$ transitiva? ¿Por qué?

40. Si R y S son reflexivas, ¿es $R \cup S$ reflexiva? ¿Por qué?

41. Si R y S son simétricas, ¿es $R \cup S$ simétrica? ¿Por qué?

42. Si R y S son transitivas, ¿es $R \cup$ S transitiva? ¿Por qué?

En los ejercicios del 43 al 50 se utilizan las siguientes definiciones: Una relación sobre un conjunto A se define como

irreflexiva si y sólo si, para toda $x \in A$, $x \not R \, x$.

asimétrica si y sólo si, para todos $x, y \in A$, si $x \, R \, y$ entonces $y \not R \, x$.

intransitiva si y sólo si, para todos $x, y, z \in A$, si $x \, R \, y$ y $y \, R \, z$ entonces $x \not R \, z$.

Para cada una de las relaciones en el ejercicio de referencia, determine si la relación es irreflexiva, asimétrica, intransitiva o ninguno de estos.

43. Ejercicio 1

44. Ejercicio 2

45. Ejercicio 3

46. Ejercicio 4

47. Ejercicio 5

48. Ejercicio 6

49. Ejercicio 7

50. Ejercicio 8

En los ejercicios del 51 al 53. R, S y T son relaciones definidas sobre $A = \{0, 1, 2, 3\}$.

51. Sea $R = \{(0, 1), (0, 2), (1, 1), (1, 3), (2, 2), (3, 0)\}$. Determine R^t, la cerradura transitiva de R.

52. Sea $S = \{(0, 0), (0, 3), (1, 0), (1, 2), (2, 0), (3, 2)\}$. Determine S^t, la cerradura transitiva de S.

53. Sea $T = \{(0, 2), (1, 0), (2, 3), (3, 1)\}$. Determine T^t, la cerradura transitiva de T.

54. Escriba un algoritmo de computadora para comprobar si una relación R definida sobre un conjunto finito A es reflexiva, donde $A = \{a[1], a[2], \ldots, a[n]\}$.

55. Escriba un algoritmo de computadora para comprobar si una relación R definida sobre un conjunto finito A es simétrica, donde $A = \{a[1], a[2], \ldots, a[n]\}$.

56. Escriba un algoritmo de computadora para comprobar si una relación R definida sobre un conjunto finito A es transitiva, donde $A = \{a[1], a[2], \ldots, a[n]\}$.

Respuestas del autoexamen

1. para toda x en A, $x \, R \, x$ 2. para todos x y y en A, si $x \, R \, y$ entonces $y \, R \, x$ 3. para todos x, y y z en A, si $x \, R \, y$ y $y \, R \, z$ entonces $x \, R \, z$ 4. x es cualquier elemento de A; $x \, R \, x$ 5. x y y son los elementos de A tal que $x \, R \, y$; $y \, R \, x$ 6. x, y y z son elementos cualesquiera de A tal que $x \, R \, y$ y $y \, R \, z$; $x \, R \, z$ 7. se demuestra que hay un elemento x en A tal que $x \not R \, x$ 8. se demuestra que hay elementos x y y en A tal que $x \, R \, y$ pero $y \not R \, x$ 9. se demuestra que hay elementos x, y y z en A tal que $x \, R \, y$ y $y \, R \, z$ pero $x \not R \, z$ 10. R^t es transitiva; $R \subseteq R^t$; si S es cualquier otra relación transitiva que contiene a R, entonces $R^t \subseteq S$

8.3 Relaciones de equivalencia

"Estás triste", dijo el Caballero con tono de preocupación: "déjame cantarte una canción para consolarte".

"¿Es muy larga?", preguntó Alicia, ya que ella había escuchado mucha poesía ese día.

"Es larga", dijo el Caballero, "pero es muy, muy hermosa. Todos los que me escuchan cantarla —se le llenan de lágrimas los ojos, o bien—".

"¿O bien qué?", dijo Alicia, al Caballero que se había callado repentinamente.

"O bien no, sabes. El nombre de la canción es 'Ojos de merluza' ".

"Oh, ese es el nombre de la canción ¿no?", dijo Alicia tratando de parecer interesada.

"No, no comprendes", le dijo el Caballero pareciendo un poco molesto "Este es como se llama *el nombre. El nombre en realidad es 'El hombre viejo viejo'".*

"Entonces debería haber dicho 'Así es como se llama la canción'?", rectificó Alicia.

"No, en absoluto: ¡eso es otra cosa! La canción *se llama 'Modos y medios': ¡pero así es sólo como se* llama*, usted sabe!*

"Bueno, ¿qué es la canción, entonces?", dijo Alicia, quien estaba en ese momento completamente desconcertada.

"A eso iba", dijo el Caballero. "La canción realmente es 'Sentado sobre una cerca': y la melodía es de mi propia invención".

Y diciendo esto, detuvo su caballo y dejó caer las riendas sobre el cuello: luego, lentamente, siguiendo el compás con una mano y con una débil sonrisa iluminando su suave cara de tonto, como si le gustara la música de su canción, comenzó.

—Lewis Carroll, *A través del espejo*, 1872

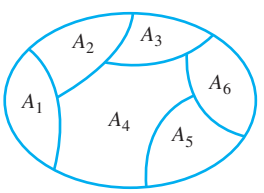
De su estudio de fracciones sabe que cada fracción tiene muchas formas equivalentes. Por ejemplo,

$$\frac{1}{2}, \frac{2}{4}, \frac{3}{6}, \frac{-1}{-2}, \frac{-3}{-6}, \frac{15}{30}, \ldots, \text{ y así sucesivamente}$$

son todas diferentes formas de representar el mismo número. Pueden verse diferentes; se les puede llamar con nombres diferentes; pero son todos iguales. La idea de agrupación de cosas que "un aspecto diferente, pero realmente son los mismos" es la idea central de las relaciones de equivalencia.

La relación inducida por una partición

Una **partición** de un conjunto A es un conjunto finito o infinito de subconjuntos no vacíos, mutuamente disjuntos, cuya unión es A. El diagrama de la figura 8.3.1 ilustra una partición de un conjunto A por subconjuntos $A_1, A_2, \ldots, A_6$.



$A_i \cap A_j = \emptyset$, siempre que $i \neq j$
$A_i \cup A_2 \cup \cdots \cup A_6 = A$

Figura 8.3.1 **Una partición de un conjunto**

• Definición

Dada una partición de un conjunto A, la **relación inducida por la partición,** R, se define en A como sigue: Para toda $x, y \in A$,

$$x \, R \, y \quad \Leftrightarrow \quad \text{hay un subconjunto } A_i \text{ de la partición tal que tanto } x \text{ como } y \text{ están en } A_i.$$

Ejemplo 8.3.1 Relación inducida por una partición

Sea $A = \{0, 1, 2, 3, 4\}$ y considere la siguiente partición de A:

$$\{0, 3, 4\}, \{1\}, \{2\}$$

Determine la relación inducida R por esta partición

Solución Puesto que $\{0, 3, 4\}$ es un subconjunto de la partición,

$$\begin{aligned} 0\ R\ 3 &\quad \text{ya que tanto 0 como 3 están en } \{0, 3, 4\}, \\ 3\ R\ 0 &\quad \text{ya que tanto 3 como 0 están en } \{0, 3, 4\}, \\ 0\ R\ 4 &\quad \text{ya que tanto 0 como 4 están en } \{0, 3, 4\}, \\ 4\ R\ 0 &\quad \text{ya que tanto 4 como 0 están en } \{0, 3, 4\}, \\ 3\ R\ 4 &\quad \text{ya que tanto 3 como 4 están en } \{0, 3, 4\} \quad \text{y} \\ 4\ R\ 3 &\quad \text{ya que tanto 4 como 3 están en } \{0, 3, 4\}. \end{aligned}$$

También,

$$\begin{aligned} 0\ R\ 0 &\quad \text{ya que tanto 0 como 0 están en } \{0, 3, 4\}, \\ 3\ R\ 3 &\quad \text{ya que tanto 3 como 3 están en } \{0, 3, 4\} \quad \text{y} \\ 4\ R\ 4 &\quad \text{ya que tanto 4 como 4 están en } \{0, 3, 4\}. \end{aligned}$$

Nota Estos enunciados pueden parecer extraños, pero, después de todo, ¡no son falsos!

Ya que $\{1\}$ es un subconjunto de la partición,

$$1\ R\ 1 \quad \text{ya que tanto 1 como 1 están en } \{1\},$$

y puesto que $\{2\}$ es un subconjunto de la partición,

$$2\ R\ 2 \quad \text{ya que tanto 2 como 2 están en } \{2\}.$$

Por tanto

$$R = \{(0, 0), (0, 3), (0, 4), (1, 1), (2, 2), (3, 0), (3, 3), (3, 4), (4, 0), (4, 3), (4, 4)\}. \quad \blacksquare$$

El hecho es que una relación inducida por una partición de un conjunto cumple con todas las tres propiedades estudiadas en la sección 8.2: reflexividad, simetría y transitividad.

Teorema 8.3.1

Sea A un conjunto con una partición y sea R la relación inducida por la partición. Entonces R es reflexiva, simétrica y transitiva.

Demostración:

Suponga que A es un conjunto con una partición. Para simplificar la notación, supongamos que la partición se compone de un número finito de conjuntos. La demostración para una partición infinita es idéntica a la excepción de la notación. Denote la partición de los subconjuntos por

$$A_1, A_2, \ldots, A_n.$$

Entonces $A_i \cap A_j = \emptyset$ siempre que $i \neq j$ y $A_1 \cup A_2 \cup \cdots \cup A_n = A$. La relación inducida R por la partición se define como sigue: Para todos $x, y \in A$,

$$x\ R\ y \quad \Leftrightarrow \quad \text{Hay un conjunto } A_i \text{ de la partición tal que } x \in A_i \text{ y } y \in A_i.$$

*[**Idea para la demostración de reflexividad:** Que R sea reflexiva significa que cada elemento de A está relacionado por R consigo mismo. Pero por definición de R, que un elemento x esté relacionado consigo mismo significa que x está en el mismo subconjunto de la partición como el mismo. Bueno, si x está en algún subconjunto de la partición, entonces es, sin duda, el mismo subconjunto como el mismo. Pero que x*

continúa en la página 462

esté en algún subconjunto de la partición ya que la unión de los subconjuntos de la partición es toda A. Este razonamiento se formaliza como sigue.]

Demostración de que R es reflexiva: Suponga que $x \in A$. Ya que $A_1, A_2, \ldots, A_n$ es una partición de A, de lo que se deduce que $x \in A_i$ para alguna i. Pero entonces el enunciado

hay un conjunto A_i, de la partición tal que $x \in A_i$ y $x \in A_i$

es verdadero. Por tanto, por definición de R, $x \; R \; x$.

Nota El hecho de que $x \in A_i$ y $x \in A_i$ se sigue de la equivalencia lógica de la forma de enunciado p y $p \wedge p$.

*[**Idea para la demostración de simetría:** Que R sea simétrica significa que en cualquier momento un elemento está relacionado con un segundo, entonces el segundo está relacionado con el primero. Ahora que un elemento x esté relacionado con un segundo elemento y significa que x y y están en el mismo subconjunto de la partición. Pero si este es el caso, entonces y está en el mismo subconjunto de la partición que x, por lo que y está relacionado con x por definición de R. Este razonamiento se formaliza como sigue.]*

Demostración de que R es simétrica: Suponga que x y y son elementos de A tal que $x \; R \; y$. Entonces

hay un subconjunto de A_i de la partición tal que $x \in A_i$ y $y \in A_i$

por definición de R. Se deduce que el enunciado

hay un subconjunto A_i de la partición tal que $y \in A_i$ y $x \in A_i$

es también verdadero. Por tanto, por definición de R, $y \; R \; x$.

Nota El hecho de que $y \in A_i$ y $x \in A_i$ se sigue de la equivalencia lógica de la forma de enunciado $p \wedge q$ y $q \wedge p$.

*[**Idea para la demostración de transitividad:** Que R sea transitiva significa que cualquier tiempo un elemento de A está relacionado por R con un segundo y el segundo está relacionado con un tercero, entonces el primer elemento está relacionado con el tercero. Pero que un elemento esté relacionado con otro significa que hay un subconjunto de la partición que contiene a ambos. Así que supongamos que x, y y z son elementos tales que x esté en el mismo subconjunto como y y y está en el mismo subconjunto que z. ¿x debe estar en el mismo subconjunto que z? Sí, porque los subconjuntos de la partición son mutuamente disjuntos. Ya que el subconjunto que contiene a x y a y tiene un elemento en común con el subconjunto que contiene y y z (a saber y), los dos subconjuntos son iguales. Pero esto significa que x, y y z están todos en el mismo subconjunto y por tanto, en particular, x y z están en el subconjunto de la misma. Por tanto x está relacionada por R a z. Este razonamiento se formaliza como sigue.]*

Demostración de que R es transitiva: Suponga que x, y y z están en A y $x \; R \; y$ y $y \; R \; z$. Por definición de R, existen los subconjuntos A_i y A_j de la partición tales que

x y y están en A_i y y y z están en A_j.

Supongamos que $A_i \neq A_j$. *[Deduciremos una contradicción.]* Entonces $A_i \cap A_j = \emptyset$ ya que $\{A_1, A_2, A_3, \ldots, A_n\}$ es una actualización de A. Pero y está en A_i y también y está en A_j. Por tanto $A_i \cap A_j \neq \emptyset$. *[Esto contradice el hecho de que $A_i \cap A_j \neq \emptyset$]* así $A_i = A_j$. De lo que se deduce que x y y z están todos en A_i y así en particular,

x y z están en A_i.

Por tanto, por definición de R, $x \; R \; z$**.**

Definición de una relación de equivalencia

Una relación en un conjunto que satisface las tres propiedades de reflexividad, simetría y transitividad se llama una *relación de equivalencia*.

• Definición

Sea A un conjunto y R una relación sobre A. R es una **relación de equivalencia** si y sólo si, R es reflexiva, simétrica y transitiva.

Así, de acuerdo con el teorema 8.3.1, la relación inducida por una partición es una relación de equivalencia. A continuación se presenta una variedad de ejemplos adicionales de las relaciones de equivalencia y en los ejercicios.

Ejemplo 8.3.2 Una relación de equivalencia sobre un conjunto de subconjuntos

Sea X el conjunto de todos los subconjuntos no vacíos de $\{1, 2, 3\}$. Entonces

$$X = \{\{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$$

Se define una relación $\mathbf{R}$ en X como sigue: Para todos A y B en X,

$$A \mathbf{R} B \Leftrightarrow \text{el elemento mínimo de } A \text{ es igual al elemento mínimo de } B.$$

Demuestre que $\mathbf{R}$ es una relación de equivalencia en X.

Solución

$\mathbf{R}$ ***es reflexiva:*** Suponga que A es un subconjunto no vacío de $\{1, 2, 3\}$. *[Debemos demostrar que* $A \mathbf{R} A$*.]* Es verdadero decir que el menor elemento de A es igual al menor elemento de A. Por tanto, por definición de R, $A \mathbf{R} A$.

$\mathbf{R}$ ***es simétrica:*** Suponga que A y B son subconjuntos no vacíos de $\{1, 2, 3\}$ y $A \mathbf{R} B$. *[Debemos demostrar que* $B \mathbf{R} A$*.]* Ya que $A \mathbf{R} B$, el elemento mínimo de A es igual al elemento mínimo de B. Pero esto implica que el elemento mínimo de B es igual a la del elemento mínimo de A y así, por definición de $\mathbf{R}$, $B \mathbf{R} A$.

$\mathbf{R}$ ***es transitiva:*** Suponga que A, B y C son subconjuntos no vacíos de $\{1, 2, 3\}$, $A \mathbf{R} B$ y $B R C$. *[Debemos demostrar que* $A \mathbf{R} C$*.]* Ya que $A \mathbf{R} B$, el elemento mínimo de A es igual a la del elemento mínimo de B y puesto $B \mathbf{R} C$, el elemento mínimo de B es igual a la del elemento mínimo de C. Por tanto, el elemento mínimo de A es igual al elemento mínimo de C y así, por definición de $\mathbf{R}$, $A \mathbf{R} C$. ■

Ejemplo 8.3.3 La equivalencia de circuitos de lógica digital es una relación de equivalencia

Sea S el conjunto de todos los circuitos lógicos digitales con un número fijo n de entradas. Se define una relación $\mathbf{E}$ sobre S como sigue: Para todos los circuitos C_1 y C_2 en S,

$$C_1 \mathbf{E} C_2 \quad \Leftrightarrow \quad C_1 \text{ tiene la misma tabla de entrada/salida que } C_2.$$

Si $C_1 \mathbf{E} C_2$, entonces se dice que el circuito C_1 es *equivalente* al circuito C_2. Demuestre que $\mathbf{E}$ es una relación de equivalencia en S.

Solución

$\mathbf{E}$ ***es reflexiva:*** Supongamos que C es un circuito lógico digital en S. *[Debemos demostrar que* $C \mathbf{E} C$*.]* Por supuesto que C tiene la misma tabla de entrada/salida. Por tanto, por definición de $\mathbf{E}$, $C \mathbf{E} C$ *[como se quería demostrar]*.

$\mathbf{E}$ ***es simétrica:*** Supongamos que C_1 y C_2 son circuitos lógicos digitales en S tales que $C_1 \mathbf{E} C_2$. *[Debemos demostrar que* $C_2 \mathbf{E} C_1$*.]* Por definición de $\mathbf{E}$, ya que $C_1 \mathbf{E} C_2$, entonces C_1 tiene la misma tabla de entrada y salida que C_2. De lo que se deduce que C_2 tiene la misma tabla de entrada y salida que C_1. Por tanto, por definición de $\mathbf{E}$, $C_2 \mathbf{E} C_1$ *[como se quería demostrar]*.

E ***es transitiva:*** Suponga que C_1, C_2 y C_3 son circuitos lógicos digitales en S tales que C_1 **E** C_2 y C_2 **E** C_3. *[Debemos demostrar que* C_1 **E** C_3*.]* Por definición de **E**, ya que C_1 **E** C_2 y C_2 **E** C_3, entonces

C_1 tiene la misma tabla de entrada/salida que C_2

y C_2 tiene la misma tabla de entrada/salida que C_3.

De lo que se deduce que C_1 tiene la misma tabla de entrada/salida que C_3.

Por tanto, por definición de **E**, C_1 **E** C_3 *[como se quería demostrar]*.

Ya que **E** es reflexiva, simétrica y transitiva, **E** es una relación de equivalencia en S. ■

Algunas implementaciones de lenguajes de programación no colocan un límite en la longitud permitida de un identificador. Esto permite a un programador ser tan preciso como sea necesario en la asignación de nombres de variables sin tener que preocuparse por exceder limitaciones de longitud. Sin embargo, los compiladores para estos lenguajes a menudo ignoran todos pero algunos especifican el número inicial de caracteres: en cuanto al compilador se trata de dos identificadores que son lo mismo si tienen los mismos caracteres iniciales, a pesar de que pueden verse diferentes para un lector humano del programa. Por ejemplo, para un compilador que ignora todo excepto los ocho primeros caracteres de un identificador, los siguientes identificadores serían lo mismo:

NumerodeTornillos NumerodePernos.

Obviamente, en el uso de dicho lenguaje, el programador tiene sin duda que evitar dar dos identificadores distintos de los ocho primeros caracteres mismos. Cuando se juntan identificadores voluminosos de un compilador de esta manera, se establece una relación de equivalencia en el conjunto de todos los identificadores posibles en el lenguaje. Tal relación se describe en el siguiente ejemplo.

Ejemplo 8.3.4 Una relación sobre un conjunto de identificadores

Sea L el conjunto de todos los identificadores permitidos en cierto lenguaje de computadora y se define una relación R sobre L como sigue: Para todas las cadenas s y t en L,

$$s\ R\ t \iff \text{los ocho primeros caracteres de } s \text{ son iguales a los ocho primeros caracteres de } t.$$

Demuestre que R es una relación de equivalencia sobre L.

Solución

R es reflexiva: Sea $s \in L$. *[Debemos demostrar que* $s\ R\ s$*.]* Claramente s tiene los mismos ocho primeros caracteres mismos. Por tanto, por definición de R, $s\ R\ s$ *[como se quería demostrar]*.

R es simétrica: Sean s y t que están en L y suponga que $s\ R\ t$. *[Debemos demostrar que* $t\ R\ s$*.]* Por definición de R, ya que $s\ R\ t$, los ocho primeros caracteres de s son iguales a los ocho primeros caracteres de t. Pero entonces los ocho primeros caracteres de t son iguales a los ocho primeros caracteres de s. Y Por tanto, por definición de R, $t\ R\ s$ *[como se quería demostrar]*.

R es transitiva: Sea s, t y u que están en L y suponga que $s\ R\ t$ y $t\ R\ u$. *[Debemos demostrar que $s\ R\ u$.]* Por definición de R, ya que $s\ R\ t$ y $t\ R\ u$, los ocho primeros caracteres de la igualdad de los ocho primeros caracteres de s, son iguales a los primeros ocho caracteres de t y a los primeros ocho caracteres de u. Por tanto los primeros ocho caracteres de s son iguales a los ocho primeros caracteres de u. Por tanto, por definición de R, $s\ R\ u$ *[como se quería demostrar]*.

Ya que R es reflexiva, simétrica y transitiva, R es una relación de equivalencia sobre L. ■

Clases de equivalencia de una relación de equivalencia

Suponga que hay una relación de equivalencia sobre un cierto conjunto. Si a es cualquier elemento particular del conjunto, entonces uno se puede preguntar, ¿cuál es el subconjunto de todos los elementos que están relacionados con a? Este subconjunto se llama la *clase de equivalencia* de a.

Nota Tenga cuidado al distinguir entre lo siguiente: una relación sobre un conjunto, el conjunto (subyacente) mismo y la clase de equivalencia para un elemento del conjunto (subyacente).

• Definición

Supongamos que A es un conjunto y R es una relación de equivalencia de A. Para cada elemento a en A, la **clase de equivalencia de *a***, que se denota $[\boldsymbol{a}]$ y se llama la clase de ***a***, es el conjunto de todos los elementos x en A tales que x está relacionado con a por R.

En símbolos:

$$[a] = \{x \in A \mid x\ R\ a\}$$

Cuando varias relaciones de equivalencia en un conjunto están bajo análisis, la notación $[a]_R$ a menudo se utiliza para denotar la clase de equivalencia de a bajo R.

La versión procedimental de esta definición es

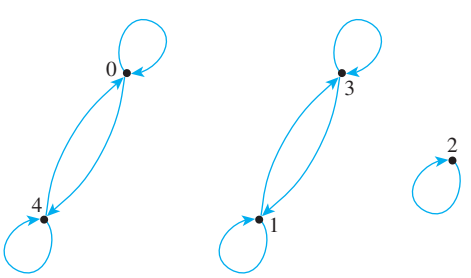
$$\text{para toda } x \in A, \quad x \in [a] \quad \Leftrightarrow \quad x\ R\ a.$$

Ejemplo 8.3.5 Clases de equivalencia de una relación dada como un conjunto de pares ordenados

Sea $A = \{0, 1, 2, 3, 4\}$ y se define una relación R sobre A como sigue:

$$R = \{(0, 0), (0, 4), (1,1), (1, 3), (2, 2), (3, 1), (3, 3), (4, 0), (4, 4)\}.$$

El grafo dirigido para R es como se muestra a continuación. Como puede verse por inspección, R es una relación de equivalencia sobre A. Determine las clases de equivalencia distintas de R.



Solución Primero encuentre la clase de equivalencia de cada elemento de A.

$$[0] = \{x \in A \mid x\, R\, 0\} = \{0,4\}$$
$$[1] = \{x \in A \mid x\, R\, 1\} = \{1,3\}$$
$$[2] = \{x \in A \mid x\, R\, 2\} = \{2\}$$
$$[3] = \{x \in A \mid x\, R\, 3\} = \{1, 3\}$$
$$[4] = \{x \in A \mid x\, R\, 4\} = \{0, 4\}$$

Observe que $[0] = [4]$ y $[1] = [3]$, Por tanto las *distintas* clases de equivalencia de la relación

$$\{0, 4\},\ \{1, 3\} \text{ y } \{2\}.$$ ■

Cuando un problema le pide encontrar las distintas clases de equivalencia de una relación de equivalencia, generalmente se solucionará el problema en dos pasos. En el primer paso se le pide explícitamente construir (como en el ejemplo 8.3.5) o imaginarse la construcción (como en los casos infinitos) de la clase de equivalencia para cada elemento del dominio A de la relación. En general varias clases contienen exactamente los mismos elementos, así en el segundo paso, usted debe revisar cuidadosamente las clases para determinar que son las mismas. Usted entonces indicará las distintas clases de equivalencia para describirlas sin duplicación.

Ejemplo 8.3.6 Clases de equivalencia de una relación sobre un conjunto de subconjuntos

En el ejemplo 8.3.2 se demostró que la relación **R** era una relación de equivalencia, donde los subconjuntos no vacíos A y B de $\{1, 2, 3\}$ relacionados por **R** significa que tienen el mismo elemento menor. Describa las distintas clases de equivalencia de **R**.

Solución La clase de equivalencia de $\{1\}$ es el conjunto de todos los subconjuntos no vacíos de $\{1, 2, 3\}$ cuyo elemento menor es 1. Por tanto,

$$[\{1\}] = \{\{1\}, \{1, 2\}, \{1, 3\}, \{1, 2, 3\}\}.$$

La clase de equivalencia de $\{2\}$ es el conjunto de todos los subconjuntos no vacíos de $\{1, 2, 3\}$ cuyo elemento menor es 2. Por tanto,

$$[\{2\}] = \{\{2\}, \{2, 3\}\}.$$

La clase de equivalencia de $\{3\}$ es el conjunto de todos los subconjuntos no vacíos de $\{1, 2, 3\}$ cuyo elemento menor es 3. Hay sólo uno de tales conjuntos, es decir, $\{3\}$ mismo. Por tanto,

$$[\{3\}] = \{\{3\}\}.$$

Puesto que todos los subconjuntos no vacíos de $\{1, 2, 3\}$ están en una de las clases de equivalencia, esta es una lista completa. Además, estas clases son todas distintas. ■

Ejemplo 8.3.7 Clases de equivalencia de identificadores

En el ejemplo 8.3.4 se demostró que la relación R que tiene los mismos ocho primeros caracteres es una relación de equivalencia sobre el conjunto L de identificadores permitidos en un lenguaje de programación. Describa las distintas clases de equivalencia de R.

Solución Por definición de R, dos cadenas en L están relacionados por R si y sólo si, tienen los mismos ocho primeros caracteres. Dando cualquier cadena s en L,

$$\begin{aligned}[\mathrm{s}] &= \{t \in L \mid t\, R\, s\} \\ &= \{t \in L \mid \text{los ocho primeros caracteres de la igualdad de los ocho primeros caracteres de } s\}.\end{aligned}$$

Por tanto, las clases de equivalencia distintas de R son conjuntos de cadenas tales que 1) cada clase consiste enteramente en cadenas, todas las cuales tienen los mismos primeros ocho caracteres y 2) cualquiera de dos clases distintas contienen cadenas que difieren en algún lugar en sus primeros ocho caracteres. ■

Ejemplo 8.3.8 Clases de equivalencia de la relación identidad

Sea A cualquier conjunto y se define una relación R como sigue: Para toda x y y en A,

$$x \, R \, y \quad \Leftrightarrow \quad x = y.$$

Entonces R es una relación de equivalencia. *[Para demostrar esto, sólo generalice el argumento que se utiliza en el ejemplo 8.2.2.]* Describa las distintas clases de equivalencia de R.

Solución Dado que cualquier a en A, la clase de a es

$$[a] = \{x \in A \mid x \, R \, a\}.$$

Pero por definición de R, $a \, R \, x$ si y sólo si, $a = x$. Así

$$\begin{aligned} [a] &= \{x \in A \mid x = a\} \\ &= \{a\} \qquad \text{ya que el único elemento de } A \text{ que es igual a } a \text{ es } a. \end{aligned}$$

Por tanto, dado cualquier a en A,

$$[a] = \{a\},$$

y si $x \neq a$, entonces $\{x\} \neq \{a\}$. En consecuencia, todas las clases de todos los elementos de A son distintas y las clases de equivalencia distintas de R son todos los subconjuntos de un solo elemento de A. ■

En cada uno de los ejemplos 8.3.5, 8.3.6, 8.3.7 y 8.3.8, el conjunto de clases distintas de equivalencia de la relación consiste en subconjuntos mutuamente disjuntos, cuya unión es el dominio completo de la relación. Esto significa que el conjunto de clases de equivalencia de la relación consiste de subconjuntos mutuamente disjuntos cuya unión es todo el dominio A de la relación. Esto significa que el conjunto de clases de equivalencias de la relación forma una partición del dominio A. De hecho, siempre es el caso de que las clases de equivalencia de la relación de equivalencia particionan el dominio de la relación en una unión de subconjuntos disjuntos mutuamente. Establecemos la verdad de este enunciado en etapas, primero se demuestran dos lemas y después se demuestra el teorema principal.

El primer lema dice que si dos elementos de A están relacionados por una relación de equivalencia R, entonces sus clases de equivalencia son las mismas.

Lema 8.3.2

Suponga que A es un conjunto, R es una relación de equivalencia sobre A y a y b son elementos de A.
Si $a \, R \, b$, entonces $[a] = [b]$.

Este lema dice que si se cumple una condición dada, entonces $[a] = [b]$. Ahora $[a]$ y $[b]$ son *conjuntos* y dos conjuntos son iguales si y sólo si, cada uno es un subconjunto del otro. Por tanto, la demostración del lema consta de dos partes: primera, una demostración de que $[a] \subseteq [b]$ y segunda, una demostración de que $[b] \subseteq [a]$. Para demostrar la relación de cada subconjunto, es necesario demostrar que cada elemento en el conjunto de la izquierda es un elemento del conjunto de la derecha.

Demostración del lema 8.3.2:

Sea A un conjunto y sea R una relación de equivalencia sobre A y suponga que

$$a \text{ y } b \text{ son elementos de } A \text{ tales que } a \; R \; b.$$

[Debemos demostrar que $[a] = [b]$*.]*

Demostración de que $[a] \subseteq [b]$**:** Sea $x \in [a]$. *[Debemos demostrar que* x e $[b]$*.]* Ya que

$$x \in [a]$$

entonces $x \; R \; a$

por definición de clase. Pero $a \; R \; b$

por hipótesis. Así, por transitividad de R,

$$x \; R \; b.$$

Por tanto $x \in [b]$

por definición de clase. *[Esto es lo que se quería demostrar.]*

Demostración de que $[b] \subseteq [a]$**:** Sea $x \in [b]$. *[Debemos demostrar que* $x \in [a]$*.]* Puesto que

$$x \in [b]$$

entonces

$$x \; R \; b$$

por definición de clase. Ahora $a \; R \; b$

por hipótesis. Así, también puesto que R es simétrica,

$$b \; R \; a$$

Entonces, puesto que R es transitiva y $x \; R \; b$ y $b \; R \; a$,

$$x \; R \; a.$$

Por tanto, $x \in [a]$

por definición de clase. *[Esto es lo que se quería demostrar.]*

Puesto que $[a] \subseteq [b]$ y $[b] \subseteq [a]$, por lo que se deduce que $[a] = [b]$ por definición de igualdad de conjuntos.

El segundo lema dice que cualesquiera dos clases de equivalencia de una relación de equivalencia son ya sea mutuamente disjuntas o idénticas.

Lema 8.3.3

Si A es un conjunto, R es una relación de equivalencia sobre A y a y b son elementos de A, entonces

$$\text{ya sea} \quad [a] \cap [b] = \emptyset \quad \text{o} \quad [a] = [b].$$

El enunciado del lema 8.3.3 tiene la forma

$$\text{si } p \text{ entonces } (q \text{ o } r),$$

Nota Usted siempre puede demostrar una declaración de la forma "si p entonces (q o r)", demostrando una de las declaraciones lógicamente equivalentes: "si (p y no q) entonces r" o "si (p y no r) entonces q".*

donde p es el enunciado "A es un conjunto, R es una relación de equivalencia sobre A y a y b son elementos de A", q es el enunciado "$[a] \cap [b] = \emptyset$" y r es el enunciado "$[a] = [b]$". Para demostrar el lema, demostraremos el enunciado lógicamente equivalente

$$\text{si } (p \text{ y no } q) \text{ entonces } r.$$

Es decir, demostraremos lo siguiente:

> Si A es un conjunto, R es una relación de equivalencia sobre A, a y b son elementos de A y $[a] \cap [b] \neq 0$, entonces $[a] = [b]$.

Demostración del lema 8.3.3:

Suponga que A es un conjunto, R es una relación de equivalencia sobre A, a y b son elementos de A, y

$$[a] \cap [b] \neq 0.$$

[Debemos demostrar que $[a] = [b]$.] Puesto que $[a] \cap [b] \neq 0$, existe un elemento x en A tal que $x \in [a] \cap [b]$. Por definición de intersección,

$$x \in [a] \quad \text{y} \quad x \in [b]$$

y así

$$x \, R \, a \quad \text{y} \quad x \, R \, b$$

por definición de clase. Puesto que R es simétrica *[es una relación de equivalencia]* y $x \, R \, a$, entonces $a \, R \, x$. Pero R es también transitiva *[puesto que esta es una relación de equivalencia] y* así, ya que $a \, R \, x$ y $x \, R \, b$,

$$a \, R \, b.$$

Ahora a y b satisfacen la hipótesis del lema 8.3.2. Por tanto, por este lema,

$$[a] = [b].$$

[Esto es lo que se quería demostrar.]

Teorema 8.3.4 Partición inducida por una relación de equivalencia

Si A es un conjunto y R es una relación de equivalencia sobre A, entonces las clases distintas de equivalencia de R forman una partición de A; es decir, la unión de las clases de equivalencia es toda de A y la intersección de cualesquiera dos clases distintas es vacía.

La demostración del teorema 8.3.4 se divide en dos partes: primera, una demostración de que A es la unión de las clases de equivalencias de R y segunda, una demostración de que la intersección de cualesquiera dos distintas clases de equivalencia es vacía. La demostración de la primera parte se deduce del hecho de que la relación es reflexiva. La demostración de la segunda parte se deduce del lema 8.3.3.

Demostración del teorema 8.3.4:

Suponga que A es un conjunto y R es una relación de equivalencia sobre A. Por simplicidad de la notación, suponemos que R tiene sólo un número finito de distintas clases de equivalencia, que se denota por

$$A_1, A_2, \ldots, A_n$$

continúa en la página 470

* Vea el ejercicio 14 en la sección 2.2.

donde n es un entero positivo. (Cuando el número de clases es infinito, la demostración es idéntica excepto para la notación).

Demostración de que $A = A_1 \cup A_2 \cup \ldots \cup A_n$: *[Debemos demostrar que $A \subseteq A_1 \cup A_2 \cup \ldots \cup A_n$ y que $A_1 \cup A_2 \cup \ldots \cup A_n \subseteq A$.]*

Para demostrar que $A \subseteq A_1 \cup A_2 \cup \ldots \cup A_n$, suponga que x es cualquier elemento de A. *[Debemos demostrar que $x \in A_1 \cup A_2 \cup \ldots \cup A_n$.]* Por reflexividad de R, $x\,R\,x$. Pero esto implica que $x \in [x]$ por definición de clase. Puesto que x está en *alguna* clase de equivalencia, debe estar en una de las distintas clases de equivalencia $A_1, A_2, \ldots,$ o A_n. Así $x \in A_i$ para algún índice i y por tanto $x \in A_1 \cup A_2 \cup \ldots \cup A_n$ por definición de unión *[como se quería demostrar]*.

Para demostrar que $A_1 \cup A_2 \cup \cdots \cup A_n \subseteq A$, suponga que $x \in A_1 \cup A_2 \cup \ldots \cup A_n$. *[Debemos demostrar que $x \in A$.]* Entonces $x \in A_i$ para algún $i = 1, 2,..., n$, por definición de unión. Pero cada A_i es una clase de equivalencia de R. Y las clases de equivalencia son subconjuntos de A. Por tanto $A_i \subseteq A$ y así $x \in$ *[como se quería demostrar]*.

Puesto que $A \subseteq A_l \cup A_2 \cup \ldots \cup A_n$ y $A_l \cup A_2 \cup \ldots \cup A_n \subseteq A$, entonces por definición de igualdad de conjuntos, $A = A_1 \cup A_2 \cup \ldots \cup A_n$.

Demostración de que las distintas clases de R son mutuamente disjuntas: Suponga que A_i y A_j son cualesquiera dos clases distintas de equivalencia de R. *[Debemos demostrar que A_i y A_j son disjuntas.]* Puesto que A_i y A_j son distintas, entonces $A_i \neq A_j$. Y puesto que A_i y A_j son clases de equivalencia de R, deben existir los elementos a y b en A tales que $A_i = [a]$ y $A_j = [b]$. Por el lema 8.3.3,

$$\text{ya sea } [a] \cap [b] = \emptyset \quad \text{o} \quad [a] = [b].$$

Pero $[a] \neq [b]$ porque $A_i \neq A_j$. Por tanto $[a] \cap [b] = \emptyset$. Así $A_i \cap A_j = \emptyset$ y así $A_i \cap A_j$ son disjuntas *[como se quería demostrar]*.

Ejemplo 8.3.9 Clases de equivalencia de los circuitos lógicos digitales

En el ejemplo 8.3.3 se demostró que la relación de equivalencia entre circuitos es una relación de equivalencia. Sea S el conjunto de todos los circuitos lógicos digitales con exactamente dos entradas y una salida. La relación binaria **E** se define sobre S como sigue: Para todos C_1 y C_2 en S,

$$C_1 \,\mathbf{E}\, C_2 \quad \Leftrightarrow \quad C_1 \text{ tiene la misma tabla de entrada/salida que } C_2.$$

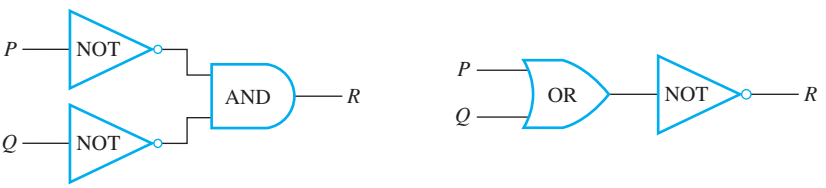
Describe las clases de equivalencias de esta relación. ¿Cuántas clases distintas de equivalencia hay? Encuentre dos circuitos diferentes que estén en una de las clases.

Solución Dado un circuito C, la clase de equivalencia de C es el conjunto de todos los circuitos con dos señales de entrada y una señal de salida que tienen la misma tabla de entrada/salida como C. Ahora cada tabla de entrada/salida tiene exactamente cuatro renglones, correspondiendo a cuatro posibles combinaciones de entradas: 11, 10, 01 y 00. Una tabla de entrada/salida típica es la siguiente:

Entrada		Salida
P	***Q***	***R***
1	1	0
1	0	0
0	1	0
0	0	1

Hay exactamente tantas tablas como cadenas binarias de longitud 4. La razón es que las distintas tablas de entrada/salida se pueden formar cambiando el patrón de los cuatro 0 y 1 en la columna de salida y hay tantas maneras de formarlas como cadenas de cuatro 0 y 1 hay. Pero el número de cadenas binarias de longitud 4 es $2^4 = 16$. Por tanto hay 16 tablas distintas de entrada/salida.

Esto implica que hay exactamente 16 clases de equivalencia de circuitos, una para cada tabla distinta de entrada/salida. Sin embargo, hay un infinito de circuitos que dan lugar a cada tabla. Por ejemplo a continuación se muestran dos circuitos para la tabla anterior de entrada/salida.



■

Congruencia módulo n

En el ejemplo 8.2.4 se muestra que la relación de congruencia módulo 3 es reflexiva, simétrica y transitiva. Por tanto, está es una relación de equivalencia.

Ejemplo 8.3.10 Clases de equivalencia de congruencia módulo 3

Sea R la relación de congruencia módulo 3 sobre el conjunto $\mathbf{Z}$ de todos los enteros. Es decir, para todos los enteros m y n,

$$m \, R \, n \quad \Leftrightarrow \quad 3 \mid (m - n) \quad \Leftrightarrow \quad m \equiv n \pmod 3.$$

Describe las distintas clases de equivalencia de R.

Solución Para cada entero a,

$$\begin{aligned}[a] &= \{x \in \mathbf{Z} \mid x \; R \; a\} \\ &= \{x \in \mathbf{Z} \mid 3 \mid (x - a)\} \\ &= \{x \in \mathbf{Z} \mid x - a = 3k, \text{ para algún entero } k\}.\end{aligned}$$

Por tanto,

$$[a] = \{x \in \mathbf{Z} \mid x = 3k + a, \text{ para algún entero } k\}.$$

En particular,

$$\begin{aligned}[0] &= \{x \in \mathbf{Z} \mid x = 3k + 0, \text{ para algún entero } k\} \\ &= \{x \in \mathbf{Z} \mid x = 3k, \text{ para algún entero } k\} \\ &= \{\ldots -9, -6, -3, 0, 3, 6, 9, \ldots\}, \\ [1] &= \{x \in \mathbf{Z} \mid x = 3k + 1, \text{ para algún entero } k\} \\ &= \{\ldots -8, -5, -2, 1, 4, 7, 10, \ldots\}, \\ [2] &= \{x \in \mathbf{Z} \mid x = 3k + 2, \text{ para algún entero } k\} \\ &= \{\ldots -7, -4, -1, 2, 5, 8, 11, \ldots\}.\end{aligned}$$

Ahora puesto que 3 R 0, entonces por el lema 8.3.2,

$$[3] = [0].$$

Más generalmente, por el mismo razonamiento,

$$[0] = [3] = [-3] = [6] = [-6] = \ldots \text{ y así sucesivamente.}$$

Similarmente,

$$[1] = [4] = [-2] = [7] = [-5] = \ldots \text{ y así sucesivamente.}$$

Y

$$[2] = [5] = [-1] = [8] = [-4] = \ldots \text{ y así sucesivamente.}$$

Observe que cada entero está en la clase [0], [1] o [2]. Por tanto las clases distintas de equivalencia son

$$\{x \in \mathbf{Z} \mid x = 3k, \text{ para algún entero } k\},$$
$$\{x \in \mathbf{Z} \mid x = 3k + 1, \text{ para algún entero } k\} \quad \text{y}$$
$$\{x \in \mathbf{Z} \mid x = 3k + 2, \text{ para algún entero } k\}.$$

En palabras, las tres clases de congruencia módulo 3 son 1) el conjunto de todos los enteros que son divisibles por 3, 2) el conjunto de todos los enteros que dejan un residuo de 1 cuando se divide por 3 y 3) el conjunto de todos los enteros que dejan un residuo de 2 cuando se divide por 3. ■

El ejemplo 8.3.10 muestra una propiedad muy importante de clases de equivalencia, a saber que una clase de equivalencia puede tener muchos nombres diferentes. En el ejemplo 8.3.10, por ejemplo, la clase de 0, [0], también se puede *llamar* la clase de 3, [3], o la clase de − 6, [−6]. Pero de qué clase *es* el conjunto

$$\{x \in \mathbf{Z} \mid x = 3k, \text{ para algún entero } k\}.$$

(La cita al comienzo de esta sección hace referencia en una forma humorística a la distinción filosóficamente interesante entre qué se *llaman* y qué *son*).

Bettmann/CORBIS

Carl Friedrich Gauss (1777-1855)

• Definición

Suponga que R es una relación de equivalencia sobre un conjunto A y S es una clase de equivalencia de R. *Un* **representativo** de la clase S es cualquier elemento a tal que $[a] = S$.

En los ejercicios del 36 al 41 al final de esta sección, se le pide demostrar en efecto, que si a es cualquier elemento de una clase de equivalencia S, entonces $S = [a]$. Por tanto *cualquier* elemento de una clase de equivalencia es un representativo de dicha clase.

La notación siguiente se utiliza con frecuencia cuando se refiere a las relaciones de congruencia. Fue introducida por Carl Friedrich Gauss en el primer capítulo de su libro *Disquisitiones Arithmeticae*. Esta obra, fue publicada cuando Gauss tenía sólo 24 años y sentó las bases para la moderna teoría de números.

• Definición

Sean m y n enteros y sea d un entero positivo. Se dice que ***m* es congruente a *n* módulo *d*** y se escribe

$$m \equiv n \pmod{d}$$

si y sólo si, $d \mid (m - n)$.

Simbólicamente: $m \equiv n \pmod{d} \Leftrightarrow d \mid (m - n)$

En el ejercicio 17*b*) al final de esta sección se le pide demostrar que $m \equiv n \pmod{d}$ si y sólo si, $m \bmod d = n \bmod d$, donde m, n y d son enteros y d es positivo.

Ejemplo 8.3.11 Evaluación de congruencias

Determine cuáles de las siguientes congruencias son verdaderas y cuáles son falsas.

a. $12 \equiv 7 \pmod 5$ b. $6 \equiv -8 \pmod 4$ c. $3 \equiv 3 \pmod 7$

Solución

a. Verdadero. $12 - 7 = 5 = 5 \cdot 1$. Por tanto $5 \mid (12 - 7)$ y así $12 \equiv 7 \pmod 5$.

b. Falso. $6 - (-8) = 14$ y $4 \nmid 14$ ya que $14 \neq 4 \cdot k$ para cualquier entero k. En consecuencia, $6 \not\equiv -8 \pmod 4$.

c. Verdadero. $3 - 3 = 0 = 7 \cdot 0$. Por tanto $7 \mid (3 - 3)$ y así $3 \equiv 3 \pmod 7$. ■

Una definición de números racionales

Por un momento, olvide lo que sabe acerca de la aritmética de fracciones y vea los números

$$\frac{1}{3} \quad \text{y} \quad \frac{2}{6}$$

como *símbolos*. Consideradas como expresiones simbólicas, *parecen* bastante diferentes. En realidad, si se escribieran como pares ordenados

$$(1, 3) \quad \text{y} \quad (2, 6)$$

serían diferentes. El hecho de que las consideramos como "lo mismo" es una instancia específica de nuestro acuerdo general de considerar cualesquiera dos números

$$\frac{a}{b} \quad \text{y} \quad \frac{c}{d}$$

como iguales si los *productos cruzados* son iguales: $ad = bc$. Esto se puede formalizar como sigue, usando el lenguaje de las relaciones de equivalencia.

Ejemplo 8.3.12 Los números racionales son en realidad clases de equivalencia

Sea A el conjunto de todos los pares ordenados de enteros para los que el segundo elemento del par es distinto de cero. Simbólicamente,

$$A = \mathbf{Z} \times (\mathbf{Z} - \{0\}).$$

Se define una relación R sobre A como sigue: Para todos $(a, b), (c, d) \in A$,

$$(a, b)\ R\ (c, d) \quad \Leftrightarrow \quad ad = bc.$$

El hecho es que R es una relación de equivalencia.

a. Demuestre que R es transitiva. (Las demostraciones de que R es reflexiva y simétrica se dejan en el ejercicio 42 al final de la sección).

b. Describa las clases distintas de equivalencia de R.

Solución

a. *[Debemos demostrar que para todos* $(a, b), (c, d), (e, f) \in A$, *si* $(a, b)\ R\ (c, d)$ *y* $(c, d)\ R\ (e, f)$, entonces $(a, b)\ R\ (e, f)$. Suponga que $(a, b), (c, d)$ y (e, f) son elementos particulares elegidos arbitrariamente de A tales que $(a, b)\ R\ (c, d)$ y $(c, d)\ R\ (e, f)$. *[Debemos demostrar que* $(a, b)\ R\ (e, f)$*.]* Por definición de R,

$$(1)\ ad = bc \quad \text{y} \quad (2)\ cf = de.$$

Puesto que los segundos elementos de todos los pares ordenados en A son distintos de cero, $b \neq 0$, $d \neq 0$ y $f \neq 0$. Multiplicando ambos lados de la ecuación (1) por f y ambos miembros de la ecuación (2) por b se obtiene

$$(1')\ adf = bcf \quad \text{y} \quad (2')\ bcf = bde.$$

Así

$$adf = bde$$

y, puesto que $d \neq 0$, se deduce de la ley de cancelación de multiplicación (T7 en el apéndice A) que

$$af = be.$$

Se sigue, por definición de R, que $(a, b)\ R\ (e, f)$ *[como se quería demostrar]*.

b. Hay una clase de equivalencia para cada número racional diferente. Cada clase de equivalencia consiste de todos los pares ordenados (a, b) que, si se escriben como fracciones a/b, serían iguales entre sí. La razón de esto es que la condición para que dos números racionales sean iguales es la misma que la condición para que dos pares ordenados estén relacionados. Por ejemplo, la clase de (1, 2) es

$$[(1, 2)] = \{(1, 2), (-1, -2), (2, 4), (-2, -4), (3, 6), (-3, -6), \ldots\}$$

puesto que $\dfrac{1}{2} = \dfrac{-1}{-2} = \dfrac{2}{4} = \dfrac{-2}{-4} = \dfrac{3}{6} = \dfrac{-3}{-6}$ y así sucesivamente. ■

Es posible ampliar el resultado del ejemplo 8.3.12 para definir las operaciones de suma y multiplicación en las clases de equivalencias de R que satisfacen las mismas propiedades que la suma y multiplicación de los números racionales. (Consulte el ejercicio 43.) Se deduce que los números racionales se pueden definir como clases de equivalencia de pares ordenados de enteros. Similarmente (vea el ejercicio 44), se puede demostrar que todos los enteros, incluyendo los negativos y el cero, se pueden definir como clases de equivalencia de pares ordenados de enteros positivos. Pero a finales del siglo XIX, F. L. G. Frege y Giuseppe Peano demostraron que los enteros positivos se pueden definir totalmente en términos de conjuntos. Y poco antes, Richard Dedekind (1848-1916) mostró que todos los números reales se pueden definir como conjuntos de números racionales. Juntando todos estos resultados se muestra que los números reales se pueden definir usando sólo teoría de conjuntos y lógica.

Autoexamen

1. Para que una relación sobre un conjunto sea una relación de equivalencia, debe ser _____.
2. La notación $m \equiv n \pmod{d}$ se lee "_____" y significa que _____.
3. Dada una relación de equivalencia R sobre un conjunto A y dado un elemento a en A, la clase de equivalencia de a se denota _____ y se define como_____.
4. Si A es un conjunto, R es una relación de equivalencia sobre A y a y b son elementos de A, entonces ya sea $[a] = [b]$ o _____.
5. Si A es un conjunto y R es una relación de equivalencia sobre A, entonces las distintas clases de equivalencia de R de _____.
6. Sea $A = \mathbf{Z} \times (\mathbf{Z} - \{0\})$ y se define una relación R sobre A al especificar que para todos (a, b) y (c, d) en A, $(a, b)\ R\ (c, d)$ si y sólo si, $ad = bc$. Entonces hay exactamente una clase de equivalencia de R para cada _____.

Conjunto de ejercicios 8.3

1. Suponga que $S = \{a, b, c, d, e\}$ y R es una relación sobre S tal que $a\ R\ b$, $b\ R$ c y $d\ R\ e$. Enumere cuáles de las expresiones siguientes son verdaderas si R es *a*) reflexiva (pero no simétrica o transitiva), *b*) simétrica (pero no reflexiva o transitiva), *c*) transitiva (pero no reflexiva o simétrica) y *d*) una relación de equivalencia.

$$c\ R\ b \quad c\ R\ c \quad a\ R\ c \quad b\ R\ a \quad a\ R\ d \quad e\ R\ a \quad e\ R\ d \quad c\ R\ a$$

2. Cada una de las siguientes particiones de $\{0, 1, 2, 3, 4\}$ induce una relación R sobre $\{0, 1, 2, 3, 4\}$. En cada caso, encuentre los pares ordenados en R.
   a. $\{0, 2\}, \{1\}, \{3, 4\}$ b. $\{0\}, \{1, 3, 4\}, \{2\}$
   c. $\{0\}, \{1, 2, 3, 4\}$

En cada uno de los ejercicios del 3 al 14, la relación R es una relación de equivalencia sobre el conjunto A. Encuentre las clases distintas de equivalencia de R.

3. $A = \{0, 1, 2, 3, 4\}$
$R = \{(0, 0), (0, 4), (1, 1), (1, 3), (2, 2), (3, 1), (3, 3), (4,0), (4, 4)\}$

4. $A = \{a, b, c, d\}$
$R = \{(a, a), (b, b), (b, d), (c, c), (d, b), (d, d)\}$

5. $A = \{1, 2, 3, 4, \ldots, 20\}$. R se define sobre A como sigue:

$$\text{Para todos } x, y \in \text{A}, \quad x\ R\ y \quad \Leftrightarrow \quad 4 \mid (x - \text{y}).$$

6. $A = \{-4, -3, -2, -1, 0, 1, 2, 3, 4, 5\}$. R se define sobre A como sigue:

$$\text{Para todos } x, y \in A, \quad x\ R\ y \quad \Leftrightarrow \quad 3 \mid (x - y).$$

7. $A = \{(1, 3), (2, 4), (-4, -8), (3, 9), (1, 5), (3, 6)\}$. R se define sobre A como sigue: Para todos $(a, b), (c, d) \in A$,

$$(a, b)\ R\ (c, d) \quad \Leftrightarrow \quad ad = bc.$$

8. $X = \{a, b, c\}$ y $A = \mathscr{P}(X)$. R se define sobre A como sigue: Para todos los conjuntos U y V en $\mathscr{P}(X)$,

$$U\ R\ V \quad \Leftrightarrow \quad N(U) = N(V).$$

(Es decir, el número de elementos en U es igual al número de elementos en V).

9. $X = \{-1, 0, 1\}$ y $A = \mathscr{P}(X)$. R se define sobre $\mathscr{P}(X)$ como sigue: Para todos los conjuntos S y T en $\mathscr{P}(X)$,

$$S\ R\ T \quad \Leftrightarrow \quad \text{la suma de los elementos en } S \text{ es igual a la suma de los elementos en } T.$$

10. $A = \{-5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5\}$. R está definida sobre A como sigue: Para todos $m, n \in \mathbf{Z}$,

$$m\ R\ n \quad \Leftrightarrow \quad 3 \mid (m^2 - n^2).$$

11. $A = \{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$. R se define sobre A como sigue: Para todo $(m, n) \in A$,

$$m\ R\ n \quad \Leftrightarrow \quad 4 \mid (m^2 - n^2).$$

12. $A = \{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$. R se define sobre A como sigue: Para todo $(m, n) \in A$,

$$m\ R\ n \quad \Leftrightarrow \quad 5 \mid (m^2 - n^2).$$

13. A es el conjunto de todas las cadenas de longitud 4 con a y b. R se define sobre A como sigue: Para todas las cadenas s y t en A,

$$s\ R\ t \quad \Leftrightarrow \quad s \text{ tiene los mismos primeros dos caracteres que } t.$$

14. A es el conjunto de todas las cadenas de longitud 2 en 0, 1 y 2. R se define sobre A como sigue: Para todas las cadenas s y t en A,

$$s\ R\ t \quad \Leftrightarrow \quad \text{la suma de caracteres en } s \text{ es igual a la suma de caracteres en } t.$$

15. Determine cuáles de las siguientes relaciones de congruencia son verdaderas y cuáles son falsas.
   a. $17 \equiv 2 \pmod 5$ b. $4 \equiv -5 \pmod 7$
   c. $-2 \equiv -8 \pmod 3$ d. $-6 \equiv 22 \pmod 2$

16. **a.** Sea R la relación de congruencia módulo 3. ¿Cuáles de las siguientes clases de equivalencia son iguales?

$$[7], [-4], [-6], [17], [4], [27], [19]$$

   b. Sea R la relación de congruencia módulo 7. ¿Cuáles de las siguientes clases de equivalencia son iguales?

$$[35], [3], [-7], [12], [0], [-2], [17]$$

17. **a.** Demuestre que para todos los enteros m y n, $m \equiv n \pmod 3$ si y sólo si, $m \bmod 3 = n \bmod 3$.
    b. Demuestre que para todos los enteros m y n y cualquier entero positivo d, $m \equiv n \pmod d$ si y sólo si, $m \bmod d = n \bmod d$.

18. **a.** Dé un ejemplo de dos conjuntos que son distintos pero no disjuntos.
    b. Encuentre los conjuntos A_1 y A_2 y los elementos x, y y z tal que x y y están en A_1 y y y z están en A_2 pero x y z no están ambos en cualquiera de los conjuntos A_1 o A_2.

En los ejercicios del 19 al 31, 1) demuestre que la relación es una relación de equivalencia y 2) describa las clases distintas de equivalencia de cada relación.

19. A es el conjunto de todos los estudiantes de su universidad.
    a. R es la relación definida sobre A como sigue: Para todos x y y en A,

$$x \, R \, y \quad \Leftrightarrow \quad x \text{ tiene la misma especialidad (o doble especialidad) que } y.$$

    (Suponga que "no definido" es una especialidad).
    b. S es la relación definida sobre A como sigue: Para todos x, $y \in$ A,

$$x \, S \, y \quad \Leftrightarrow \quad x \text{ es la misma edad que } y.$$

H 20. E es la relación definida sobre $\mathbf{Z}$ como sigue:

$$\text{Para todo } m, n \in \mathbf{Z}, \quad m \, E \, n \quad \Leftrightarrow \quad 2 \mid (m - n).$$

21. F es la relación definida sobre $\mathbf{Z}$ como sigue:

$$\text{Para todo } m, n \in \mathbf{Z}, \quad m \, F \, n \quad \Leftrightarrow \quad 4 \mid (m - n).$$

22. Sea A el conjunto de todas las formas de enunciado con tres variables p, q y r. $\mathbf{R}$ es la relación definida sobre A como sigue: Para todo P y Q en A,

$$\text{P } \mathbf{R} \text{ Q} \quad \Leftrightarrow \quad \text{P y Q tienen la misma tabla de verdad.}$$

23. Sea P el conjunto de partes enviadas a una empresa de diversos proveedores. S es la relación definida sobre P como sigue: Para todos x, $y \in P$,

$$x \, S \, y \quad \Leftrightarrow \quad x \text{ tiene la misma parte numérica y es enviada por el mismo proveedor que } y.$$

24. Sea A el conjunto de identificadores en un programa de cómputo. Es común usar identificadores durante una pequeña parte del tiempo de ejecución de un programa y no se usan de nuevo al ejecutar otras partes del programa. En dichos casos, se arreglan los identificadores para compartir localizaciones de memoria para hacer eficiente el uso de la capacidad de memoria de una computadora. Se define una relación R sobre A como sigue: Para todos los identificadores x y y,

$$x \, R \, y \quad \Leftrightarrow \quad \text{los valores } x \text{ y } y \text{ se almacenan en la misma ubicación de memoria durante la ejecución de programa.}$$

25. A es la relación "valor absoluto" definida sobre $\mathbf{R}$ como sigue:

$$\text{Para todos } x, y \in \mathbf{R}, \quad x \, A \, y \quad \Leftrightarrow \quad |x| = |y|.$$

H 26. D es la relación definida sobre $\mathbf{Z}$ como sigue: Para todos m, $n \in \mathbf{Z}$,

$$m \, D \, n \quad \Leftrightarrow \quad 3 \mid (m^2 - n^2).$$

27. R es la relación definida sobre $\mathbf{Z}$ como sigue: Para todo $(m, n) \in \mathbf{Z}$,

$$m \, R \, n \quad \Leftrightarrow \quad 4 \mid (m^2 - n^2).$$

28. I es la relación definida sobre $\mathbf{R}$ como sigue:

$$\text{Para todos } x, y \in \mathbf{R}, \quad x \, I \, y \quad \Leftrightarrow \quad x - y \text{ es un entero.}$$

29. Se define P sobre el conjunto $\mathbf{R} \times \mathbf{R}$ de pares ordenados de números reales como sigue: Para todos (w, x), $(y, z) \in \mathbf{R} \times \mathbf{R}$,

$$(w, x) \, P \, (y, z) \quad \Leftrightarrow \quad w = y.$$

30. Se define Q sobre el conjunto $\mathbf{R} \times \mathbf{R}$ como sigue: Para todos (w, x), $(y, z) \in \mathbf{R} \times \mathbf{R}$,

$$(w, x) \, Q \, (y, z) \quad \Leftrightarrow \quad x = z.$$

31. Sea P el conjunto de todos los puntos en el plano cartesiano excepto el origen. R es la relación definida sobre P como sigue: Para todo p_1 y p_2 en P,

$$p_1 \, R \, p_2 \quad \Leftrightarrow \quad p_1 \text{ y } p_2 \text{ se encuentran en la misma semirrecta que sale del origen.}$$

H 32. Sea A el conjunto de todas las líneas rectas en el plano cartesiano. Se define una relación $\|$ sobre A como sigue:

$$\text{Para todo } l_1 \text{ y } l_2 \text{ en } A, \quad l_1 \parallel l_2 \quad \Leftrightarrow \quad l_1 \text{ es paralelo a } l_2.$$

Entonces $\|$ es una relación de equivalencia sobre A. Describa las clases de equivalencias de esta relación.

33. Sea A el conjunto de puntos en el rectángulo con coordenadas x y y entre 0 y 1. Es decir,

$$A = \{(x, y) \in \mathbf{R} \times \mathbf{R} \mid 0 \le x \le 1 \quad \text{y} \quad 0 \le y \le 1\}.$$

Se define una relación R sobre A como sigue: Para todos (x_1, y_1) y (x_2, y_2) en A,

$$(x_1, y_1) \, R \, (x_2, y_2) \Leftrightarrow$$
$$\begin{array}{llllll} (x_1, y_1) = (x_2, y_2); & \text{o} & & & & \\ x_1 = 0 & \text{y} & x_2 = 1 & \text{y} & y_1 = y_2; & \text{o} \\ x_1 = 1 & \text{y} & x_2 = 0 & \text{y} & y_1 = y_2; & \text{o} \\ y_1 = 0 & \text{y} & y_2 = 1 & \text{y} & x_1 = x_2; & \text{o} \\ y_1 = 1 & \text{y} & y_2 = 0 & \text{y} & x_1 = x_2. & \end{array}$$

En otras palabras, todos los puntos a lo largo del borde superior del rectángulo están relacionados con los puntos a lo largo del borde inferior directamente por debajo de ellos y todos los puntos justo en frente de cada otro a lo largo de los extremos izquierdo y derecho, están relacionados entre sí. Los puntos en el interior del rectángulo no están relacionados con otra cosa que no sea ellos mismos. Entonces R es una relación de equivalencia sobre A. Imagine colocar juntos todos los puntos que están en la misma clase de equivalencia. Describa la figura resultante.

34. La documentación para el lenguaje de programación Java recomienda que, cuando un "método equivale a" se define para un objeto, es una relación de equivalencia. Es decir, si R está definida como sigue:

$$x\ R\ y \quad \Leftrightarrow \quad x.igual(y) \quad \text{para todos los objetos en la clase,}$$

entonces R debe ser una relación de equivalencia. Suponga que al tratar de optimizar algunas de las matemáticas de una aplicación gráfica, un programador crea un objeto denominado punto, que consta de dos coordenadas en el plano. El programa define un método igual como sigue: Si p y q son puntos cualesquiera, entonces

$$p.igual(q) \quad \Leftrightarrow \quad \text{la distancia entre } p \text{ y } q \text{ es menor o igual a } c$$

donde c es un pequeño número positivo que depende de la resolución de la pantalla del equipo. ¿Es igual el método del programador en una relación de equivalencia? Justifique su respuesta.

35. Encuentre un circuito adicional representante para la tabla de entrada/salida del ejemplo 8.3.9.

Sea R una relación de equivalencia sobre un conjunto A. Demuestre cada uno de los enunciados en los ejercicios del 36 al 41 directamente provienen de las definiciones de relación de equivalencia y clase de equivalencia sin utilizar los resultados del lema 8.3.2, lema 8.3.3, o teorema 8.3.4.

36. Para toda a en A, $a \in [a]$.

37. Para todas a y b en A, si $b \in$ [a] entonces $a\ R\ b$.

38. Para todas a, b y c en A, si $b\ R\ c$ y $c \in [a]$ entonces $b \in [a]$.

39. Para todas a y b en A, si $[a] = [b]$ entonces $a\ R\ b$.

40. Para todas a, b y x en A, si $a\ R\ b$ y $x \in [a]$, entonces $x \in [b]$.

***H* 41.** Para todas a y b en A, si $a \in [b]$ entonces $[a] = [b]$.

42. Sea R la relación definida en el ejemplo 8.3.12.
   a. Demuestre que R es reflexiva.
   b. Demuestre que R es simétrica.
   c. Enumere cuatro elementos distintos en $[(1, 3)]$.
   d. Enumere cuatro elementos distintos en $[(2, 5)]$.

✶ 43. En el ejemplo 8.3.12, se definen operaciones de adición $(+)$ y multiplicación $(\cdot)$ como sigue: Para todos (a, b), $(c, d) \in A$,

$$[(a, b)] + [(c, d)] = [(ad + be, bd)]$$
$$[(a, b)] \cdot [(c, d)] = [(ac, bd)].$$

   a. Demuestre que esta adición está bien definida. Es decir, demuestre que si $[(a, b)] = [(a', b')]$ y $[(c, d)] = [(c', d')]$, entonces $[(ad + bc, bd)] = [(a'd' + b'c', b'd')]$.
   b. Demuestre que esta multiplicación está bien definida. Es decir, demuestre que si $[(a, b)] = [(a', b')]$ y $[(c, d)] = [c', d')]$, entonces $[(ac, bd)] = [(a'c', b'd')]$.
   c. Demuestre que $[(0, 1)]$ es un elemento identidad para la adición. Es decir, demuestre que para cualquier $(a, b) \in A$,

$$[(a, b)] + [(0, 1)] = [(0, 1)] + [(a, b)] = [(a, b)].$$

   d. Encuentre un elemento identidad para la multiplicación. Es decir, encuentre (i, j) en A tal que para todo (a, b) en A. $[(a, b)] \cdot [(i, j)] = [(i, j)] \cdot [(a, b)] = ((a, b)]$.
   e. Para cualquier $(a, b) \in A$, demuestre que $[(-a, b)]$ es una inversa para $[(a, b)]$ para la adición. Es decir, demuestre que $[(-a, b)] + [(a, b)] = [(a, b)] + [(-a, b)] = [(0, 1)]$.
   f. Dado cualquier $(a, b) \in A$ con $a \neq 0$, encuentre una inversa para $[(a, b)]$ para la multiplicación. Es decir, encuentre (c, d) en A así que $[(a, b)] \cdot [(c, d)] = [(c, d)] - [(a, b)] = [(i, j)]$, donde $[(i, j)]$ es el elemento identidad que encontró en el inciso d).

44. Sea $A = \mathbf{Z}^+ \times \mathbf{Z}^+$. Se define una relación R sobre A como sigue: Para todos (a, b) y (c, d) en A,

$$(a, b)\ R\ (c, d) \quad \Leftrightarrow \quad a + d = c + b.$$

   a. Demuestre que R es reflexiva.
   b. Demuestre que R es simétrica.
***H* c.** Demuestre que R es transitiva.
   d. Enumere cinco elementos en $[(1, 1)]$.
   e. Enumere cinco elementos en $[(3, 1)]$.
   f. Enumere cinco elementos en $[(1, 2)]$.
   g. Describa las clases distintas de equivalencia de R.

45. El siguiente argumento afirma que para demostrar el requisito de que una relación de equivalencia debe ser reflexiva es redundante. En otras palabras, afirma que para demostrar si una relación es simétrica y transitiva, entonces es reflexiva. Encuentre el error en el argumento.

"**Demostración:** Sea R una relación en el conjunto A y suponga que R es simétrica y transitiva. Para cualesquiera dos elementos x y y en A, si $x\ R\ y$ entonces $y\ R\ x$ puesto que R es simétrica. Pero entonces se deduce por transitividad que $x\ R\ x$. Por tanto R es reflexiva".

46. Sea R una relación sobre un conjunto A y suponga que R es simétrica y transitiva. Demuestre lo siguiente: Si para cada x en A existe una y en A tal que $x\ R\ y$, entonces R es una relación de equivalencia.

47. Consulte la cita al inicio de esta sección para responder a las preguntas siguientes.
   a. ¿Cuál es el nombre de la canción de la llamada canción del Caballero?
   b. ¿Cuál es el nombre de la canción del Caballero?
   c. ¿Qué es la llamada canción del Caballero?
   d. ¿Cuál *es* la canción del Caballero?
   e. ¿Cuál es su nombre completo?
   f. ¿Cómo le llaman?
   g. ¿Qué *es* usted? (No responda por escrito; sólo piénselo).

Respuestas del autoexamen

1. reflexiva, simétrica y transitiva 2. m es congruente con n módulo d; d divide a $m - n$ 3. $[a]$; el conjunto de toda x en A tal que $x\ R\ a$ 4. $[a] \cap [b] = \emptyset$ 5. una partición de A 6. número racional

8.4 Aritmética modular con aplicaciones a la criptografía

Las matemáticas "reales" de los matemáticos "reales", la matemática de Fermat, Euler, Gauss, Abel y Riemann, es casi enteramente "inútil"... . No es posible justificar la vida de cualquier matemático profesional verdadero en el terreno de la "utilidad" de su trabajo. —G. H. Hardy, *Apología de un matemático*, 1941

La criptografía es el estudio de métodos para enviar mensajes secretos. Se trata de la **encriptación**, en la que un mensaje, denominado **texto simple**, se convierte en la forma, llamada **texto cifrado**, que se puede enviar a través de canales que posiblemente se abren para ver por fuera de las partes. El receptor del texto cifrado utiliza **descifrado** para convertir el texto cifrado en texto simple.

En el pasado el uso principal de la criptografía fue en el gobierno y en inteligencia militar y este uso sigue siendo importante. En realidad, la Agencia de Seguridad Nacional, cuya actividad principal es la criptografía, es el mayor empleador de matemáticos en Estados Unidos. Sin embargo, con el surgimiento de sistemas de comunicación electrónicos, especialmente el internet, un uso actual extremadamente importante de la criptografía es enviar información privada, como números de tarjeta de crédito, bancos de datos, registros médicos y así sucesivamente, a través de canales electrónicos.

Muchos de los sistemas para enviar mensajes secretos requiere que tanto el remitente como el receptor conozcan el cifrado y los procedimientos de descifrado. Por ejemplo, un sistema de cifrado que una vez utilizó Julio César y que ahora es llamado el **cifrado César**, cifra los mensajes recorriendo cada letra del alfabeto tres lugares hacia la derecha, recorriendo a X al lugar de A, a Y al de B y a Z al lugar de C. En otras palabras, se dice que cada letra del alfabeto se codifica por su posición con respecto a las demás, así A = 01, B = 02, . . . , Z = 26. Si la versión numérica del texto plano para una letra se denota con M y si la versión numérica del texto cifrado se denota con C, entonces

$$C = (M + 3) \bmod 26.$$

El receptor de un mensaje puede fácilmente ser descifrado utilizando la fórmula

$$M = (C - 3) \bmod 26.$$

Para referencia, a continuación se presentan las letras del alfabeto con su equivalente numérico:

A	B	C	D	E	F	G	H	I	J	K	L	M
01	02	03	04	05	06	07	08	09	10	11	12	13
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
14	15	16	17	18	19	20	21	22	23	24	25	26

Ejemplo 8.4.1 Encriptando y descrifando con el cifrado César

a. Utilice el cifrado César para cifrar el mensaje CÓMO ESTÁ USTED.

b. Utilice el cifrado César para descifrar el mensaje PH VLHQWR ELHQ.

Solución

a. Primero traduzca las letras de CÓMO ESTÁ USTED por sus equivalentes numéricos:

03 15 13 15 05 19 20 01 21 19 20 05 04.

Después encripte el mensaje sumando 3 a cada número. El resultado es

06 18 16 18 08 22 23 04 24 22 23 08 07.

Por último, sustituya las letras que corresponden a estos números. El mensaje cifrado se convierte en

FRPR HVWD XVWHG.

b. Primero traduzca las letras PH VLHQWR ELHQ a sus equivalentes numéricos:

16 08 22 12 08 17 23 18 05 12 08 17.

Después descifre el mensaje restando 3 de cada número:

13 05 19 09 05 14 20 15 02 09 05 14.

Después traduzca en letras para obtener el mensaje original: ME SIENTO BIEN. ■

Un problema con el cifrado César es que dando una cantidad suficiente de texto cifrado una persona con conocimientos de frecuencias de las letras en el lenguaje puede averiguar fácilmente el cifrado. En parte por esta razón, incluso el propio César no hizo uso extensivo del mismo. Otro problema con un sistema como el cifrado César es que conociendo cómo cifrar un mensaje automáticamente se conoce cómo descifrarlo. Cuando un posible destinatario de mensajes pasa la información de codificación a un potencial remitente de los mensajes, el canal mismo que pasa la información puede ser inseguro. Así puede perder la información fuera, lo que permite a una parte exterior descifrar mensajes destinados a mantenerse en secreto.

En la criptografía con clave pública, un receptor potencial de mensajes encriptados abiertamente distribuye una clave pública que contiene la información de codificación. Sin embargo, el conocimiento de la clave pública no ofrece prácticamente ninguna pista sobre cómo descifrar mensajes. Sólo el receptor tiene ese conocimiento. Independientemente de cuántas personas pueden obtener la información de codificación, sólo el destinatario debe ser capaz de descifrar los mensajes que le son enviados.

El primer sistema de cifrado con clave pública se desarrolló en 1976-1977 por tres jóvenes científicos de ciencia computacional y matemáticos que trabajan en el M.I.T.:

Cortesía de Leonard Adleman

De izquierda a derecha: Ronald Rivest (nació en 1948), Adi Shamir (nació en 1952) y Leonard Adleman (nació en 1945).

Ronald Rivest, Adi Shamir y Leonard Adleman. En su honor se llama cifrado RSA. Para que aprenda cómo funciona, debe conocer algunas propiedades adicionales de la congruencia módulo n.

Propiedades de congruencia módulo n

El primer teorema de esta sección reúne una variedad de formas equivalentes de expresar el mismo hecho aritmético básico. A veces una forma es más conveniente; a veces otra forma es mejor. Debe sentirse cómodo al pasar de una a otra, dependiendo de la naturaleza del problema que está tratando de resolver.

Teorema 8.4.1 Equivalencias modulares

Sean a, b y n enteros cualesquiera y suponga que $n > 1$. Los siguientes enunciados son todos equivalentes:

1. $n \mid (a - b)$
2. $a \equiv b \pmod{n}$
3. $a = b + kn$ para algún entero k
4. a y b tienen el mismo residuo (no negativo) cuando se divide entre n
5. $a \bmod n = b \bmod n$

Demostración:

Demostraremos que (1) $\Rightarrow$ (2) $\Rightarrow$ (3) $\Rightarrow$ (4) $\Rightarrow$ (5) $\Rightarrow$ (1). Se sigue por transitividad de si-entonces que todos los cinco enunciados son equivalentes.

Así sean a, b y n enteros cualesquier con enteros $n > 1$.

***Demostración de que* (1) $\Rightarrow$ (2):** Suponga que $n \mid (a - b)$. Por definición de congruencia módulo n, podemos inmediatamente concluir que $a \equiv b \pmod{n}$.

***Demostración de que* (2) $\Rightarrow$ (3):** Suponga que $a \equiv b \pmod{n}$. Por definición de congruencia módulo n, $n \mid (a - b)$. Así, por definición de divisibilidad, $a - b = kn$, para algún entero k. Sumando b a ambos miembros se obtiene que $a = b + kn$.

***Demostración de que* (3) $\Rightarrow$ (4):** Suponga que $a = b + kn$, para algún entero k. Use el teorema del cociente-residuo para dividir a por n para obtener

$$a = qn + r \quad \text{donde } q \text{ y } r \text{ son enteros y } 0 \leq r < n.$$

Sustituyendo $b + kn$ por a en esta ecuación se obtiene

$$b + kn = qn + r$$

y restando kn de ambos miembros y factorizando n se obtiene

$$b = (q - k)n + r.$$

Pero puesto que $0 \leq r < n$, la propiedad de unicidad del teorema del cociente residuo garantiza que r es también el residuo que se obtiene cuando se divide b por n. Así a y b tienen el mismo residuo cuando se dividen por n.

***Demostración de que* (4) $\Rightarrow$ (5):** Suponga que a y b tienen el mismo residuo cuando se dividen por n. Se sigue inmediatamente de la definición de la función *mod* que $a \bmod n = b \bmod n$.

***Demostración de que* (5) ⇒ (1):** Suponga que $a \bmod n = b \bmod n$. Por definición de la función *mod*, a y b tienen el mismo residuo cuando se dividen por n. Así, por el teorema del cociente-residuo, podemos escribir

$$a = q_1 n + r \quad \text{y} \quad b = q_2 n + r \quad \text{donde } q_1, q_2 \text{ y } r \text{ son enteros y } 0 \leq r < n.$$

Se sigue que

$$a - b = (q_1 n + r) - (q_2 n + r) = (q_1 - q_2)n.$$

Por tanto, puesto que $q_1 - q_2$ es un entero, $n \mid (a - b)$.

Otra consecuencia del teorema del cociente-residuo es que: Cuando un entero a se divide por un entero positivo n, se obtiene un único cociente q y el residuo con la propiedad de que $a = nq + r$ y $0 \leq r < n$. Porque hay exactamente n enteros que satisfacen la desigualdad $0 \leq r < n$ (los números van de 0 a $n - 1$), hay exactamente n residuos posibles que pueden ocurrir. Estos se llaman los *menores residuos no negativos módulo n* o simplemente los *residuos módulo n*.

• Definición

Dados los enteros a y n con $n > 1$, **el residuo de *a* módulo *n*** es $a \bmod n$, el residuo no negativo obtenido cuando a se divide entre n. Los números 0, 1, 2, . . . , $n - 1$ se llaman un **conjunto completo de residuos módulo *n*. Reducir un número módulo *n*** significa hacerlo igual a su residuo módulo n. Si se fija un módulo $n > 1$ durante un análisis y se da un entero a, las palabras "módulo n" con frecuencia son eliminadas y simplemente hablamos del **residuo de *a***.

El siguiente teorema generaliza varios ejemplos de la sección 8.3.

Teorema 8.4.2 Congruencia módulo *n* es una relación de equivalencia

Si n es cualquier entero con $n > 1$, la congruencia módulo n es una relación de equivalencia sobre el conjunto de todos los enteros. Las clases distintas de equivalencia de la relación son el conjunto [0], [1], [2], . . . , [$n - 1$], donde para cada $a = 0, 1, 2, \ldots, n - 1$,

$$[a] = \{m \in Z \mid m \equiv a \pmod{n}\},$$

o, equivalentemente,

$$[a] = \{m \in Z \mid m = a + kn \text{ para algún entero } k\}.$$

Demostración:

Suponga que n es cualquier entero con $n > 1$. Debemos demostrar que la congruencia módulo n es reflexiva, simétrica y transitiva.

Demostración de reflexividad: Suponga que a es cualquier entero. Para demostrar que $a \equiv a \pmod{n}$, debemos demostrar que $n \mid (a - a)$. Pero $a - a = 0$ y $n \mid 0$ ya que $0 = n \cdot 0$. Por tanto $a \equiv a \pmod{n}$.

continúa en la página 482

Demostración de simetría: Suponga que a y b son enteros cualesquiera tales que $a \equiv b \pmod{n}$. Debemos demostrar que $b \equiv a \pmod{n}$. Pero puesto que $a \equiv b \pmod{n}$, entonces $n \mid (a - b)$. Así, por definición de divisibilidad, $a - b = nk$, para algún entero k. Multiplicando ambos lados de esta ecuación por -1 se obtiene

$$-(a - b) = -nk,$$

o, equivalentemente,

$$b - a = n(-k).$$

Así, por definición de divisibilidad $n \mid (b - a)$ y así, por definición de congruencia módulo n, $b \equiv a \pmod{n}$.

Demostración de transitividad: Ésta se deja como en el ejercicio 5 al final de la sección.

***Demostración de que las clases distintas de equivalencia son* [0], [1], [2], . . . , [*n* − 1]:** Ésta se deja como en el ejercicio 6 al final de la sección.

Observe que hay una correspondencia uno a uno entre las clases distintas de equivalencia para la congruencia módulo n y los elementos de un conjunto completo de residuos módulo n.

Aritmética modular

Un hecho fundamental acerca de la congruencia módulo n es que si primero realiza una suma, resta o multiplicación con enteros y después reduce el módulo n resultante, obtiene la misma respuesta que si primero reduce cada uno de los números módulo n, realiza la operación y después reduce el módulo n resultante. Por ejemplo, en lugar de calcular

$$(5 \cdot 8) = 40 \equiv 1 \pmod{3}$$

obtendrá la misma respuesta si calcula

$$(5 \bmod 3)(8 \bmod 3) = 2 \cdot 2 = 4 \equiv 1 \pmod{3}.$$

El hecho de que este proceso funcione es un resultado del teorema siguiente.

Teorema 8.4.3 Aritmética modular

Sean a, b, c, d y n enteros con $n > 1$ y suponga que

$$a \equiv c \pmod{n} \text{ y } b \equiv d \pmod{n}.$$

Entonces

1. $(a + b) \equiv (c + d) \pmod{n}$[-2pt]
2. $(a - b) \equiv (c - d) \pmod{n}$[-2pt]
3. $ab \equiv cd \pmod{n}$
4. $a^m \equiv c^m \pmod{n}$ para todos los enteros m.

Demostración:

Ya que haremos mayor uso del punto 3 de este teorema, lo demostraremos aquí y dejaremos las demostraciones de las partes restantes del teorema a los ejercicios del 9 al 11 al final de la sección.

Demostración del inciso 3: Suponga que a, b, c, d y n son enteros con $n > 1$ y suponga que $a \equiv b \pmod{n}$ y $c \equiv d \pmod{n}$. Por el teorema 8.4.1, existen enteros s y t tales que

$$a = c + sn \quad \text{y} \quad b = d + tn.$$

Entonces

$$\begin{aligned} ab &= (c + sn)(d + tn) && \text{por sustitución} \\ &= cd + ctn + snd + sntn \\ &= cd + n(ct + sd + stn) && \text{por álgebra.} \end{aligned}$$

Sea $k = ct + sd + stn$. Entonces k es un entero y $ab = cd + nk$. Así por el teorema 8.4.1, $ab \equiv cd \pmod{n}$.

Ejemplo 8.4.2 Iniciando con la aritmética modular

El uso más práctico de la aritmética modular es reducir los cálculos que implican grandes enteros a cálculos que implican pequeños. Por ejemplo, observe que $55 \equiv 3 \pmod 4$ ya que $55 - 3 = 52$, es divisible por 4 y $26 \equiv 2 \pmod 4$ ya que $26 - 2 = 24$, que es también divisible por 4. Compruebe los siguientes enunciados.

a. $55 + 26 \equiv (3 + 2) \pmod 4$
b. $55 - 26 \equiv (3 - 2) \pmod 4$
c. $55 \cdot 26 \equiv (3 \cdot 2) \pmod 4$
d. $55^2 \equiv 3^2 \pmod 4$

Solución

a. Calcule $55 + 26 = 81$ y $3 + 2 = 5$. Por definición de congruencia módulo n, para demostrar que $81 \equiv 5 \pmod 4$, necesita demostrar que $4 \mid (81 - 5)$. Pero esto es verdadero ya que $81 - 5 = 76$ y $4 \mid 76$ puesto que $76 = 4 \cdot 19$.

b. Calcule $55 - 26 = 29$ y $3 - 2 = 1$. Por definición de congruencia módulo n, para demostrar que $29 \equiv 1 \pmod 4$, necesita demostrar que $4 \mid (29 - 1)$. Pero esto es verdadero ya que $29 - 1 = 28$ y $4 \mid 28$ puesto que $28 = 4 \cdot 7$.

c. Calcule $55 \cdot 26 = 1430$ y $3 \cdot 2 = 6$. Por definición de congruencia módulo n, para demostrar que $1430 \equiv 6 \pmod 4$, necesita demostrar que $4 \mid (1430 - 6)$. Pero esto es verdadero ya que $1430 - 6 = 1424$ y $4 \mid 1424$ puesto que $1424 = 4 \cdot 356$.

d. Calcule $55^2 = 3025$ y $3^2 = 9$. Por definición de congruencia módulo n, para demostrar que $3025 \equiv 9 \pmod 4$, necesita demostrar que $4 \mid (3025 - 9)$. Pero esto es verdadero ya que $3025 - 9 = 3016$ y $4 \mid 3016$ puesto que $3016 = 4 \cdot 754$. ■

Para facilitar los cálculos que se realizan en esta sección, es conveniente expresar el inciso 3 del teorema 8.4.3 en una forma ligeramente diferente.

Corolario 8.4.4

Sean a, b y n enteros con $n > 1$. Entonces

$$ab \equiv [(a \bmod n)(b \bmod n)] \pmod n,$$

o, equivalentemente,

$$ab \bmod n = [(a \bmod n)(b \bmod n)] \bmod n.$$

En particular, si m es un entero positivo, entonces

$$a^m \equiv [(a \bmod n)^m] \pmod n.$$

Ejemplo 8.4.3 Cálculo de un producto módulo *n*

Como en el ejemplo 8.4.2, observe que $55 \equiv 3 \pmod 4$ y $26 \equiv 2 \pmod 4$. Ya que ambos 3 y 2 son menores que 4, cada uno de estos números es un residuo no negativo mínimo módulo 4. Por tanto, $55 \; mod \; 4 = 3$ y $26 \; mod \; 4 = 2$. Use la notación del corolario 8.4.4 para encontrar el residuo de $55 \cdot 26$ módulo 4.

Solución Recuerde que al utilizar una calculadora para cuantificar residuos, puede utilizar la fórmula $n \; mod \; d = n - d \cdot \lfloor n/d \rfloor$. Si se utiliza una calculadora de mano con una característica de "parte entera" y tantos n como d son positivos, entonces $\lfloor n/d \rfloor$ es la parte entera de la división de n entre d. Cuando se divide un entero positivo n entre un entero positivo d con una calculadora más básica, se puede ver $\lfloor n/d \rfloor$ en la presentación de la calculadora simplemente haciendo caso omiso de los dígitos que siguen al punto decimal.

Por el corolario 8.4.4,

$$\begin{aligned} (55 \cdot 26) \; mod \; 4 &= \{(55 \; mod \; 4)(26 \; mod \; 4)\} \; mod \; 4 \\ &\equiv (3 \cdot 2) \; mod \; 4 && \text{ya que } 55 \bmod 4 = 3 \text{ y } 26 \bmod 4 = 2 \\ &\equiv 6 \; mod \; 4 \\ &\equiv 2 && \text{ya que } 4 \mid (6-2) \text{ y } 2 < 4. \end{aligned}$$

■

Cuando se realiza aritmética modular con un gran número, como es el caso de la criptografía RSA, los cálculos se facilitan utilizando dos propiedades de exponentes. La primera es

$$\boxed{X^{2a} = (x^a)^2 \quad \text{para todos los números reales } x \text{ y } a \text{ con } x \geq 0.} \qquad 8.4.1$$

Así, por ejemplo, si x es cualquier número real positivo, entonces

$$\begin{aligned} x^4 \; mod \; n &= (x^2)^2 \; mod \; n && \text{ya que } (x^2)^2 = x^4 \\ &= (x^2 \; mod \; n)^2 \; mod \; n && \text{por el corolario 8.4.4.} \end{aligned}$$

Por tanto puede reducir x^4 módulo n reduciendo x^2 módulo n y después reduciendo el cuadrado del módulo n resultante. Ya que todos los residuos son menores que n, este proceso limita el tamaño de los cálculos a números que son menores que n^2, lo que hace más fácil trabajar con ellos, tanto para los seres humanos (cuando los números son relativamente pequeños) y para computadoras (cuando los números son muy grandes).

Una segunda propiedad útil de los exponentes es

$$\boxed{x^{a+b} = x^a \, x^b \quad \text{para todos los números reales } x, a \text{ y } b \text{ con } x \geq 0.} \qquad 8.4.2$$

Por ejemplo, ya que $7 = 4 + 2 + 1$,

$$x^7 = x^4 \, x^2 \, x^1$$

Así, por el corolario 8.4.4,

$$x^7 \; mod \; n = \{(x^4 \; mod \; n)(x^2 \; mod \; n)(x^1 \; mod \; n)\} \; mod \; n.$$

Primero damos un ejemplo que muestra la aplicación de la fórmula (8.4.1) y después un ejemplo que utiliza tanto a la (8.4.1) como a la (8.4.2).

Ejemplo 8.4.4 Cálculo de $a^k \bmod n$ cuando k es una potencia de 2

Determine $144^4 \bmod 713$.

Solución Use la propiedad (8.4.1) para escribir $144^4 = (144^2)^2$. Entonces

$$\begin{aligned}
144^4 \bmod 713 &= (144^2)^2 \bmod 713 \\
&= (144^2 \bmod 713)^2 \bmod 713 \\
&= (20736 \bmod 713)^2 \bmod 713 && \text{ya que } 144^2 = 20736 \\
&= 59^2 \bmod 713 && \text{ya que } 20736 \bmod 713 = 59 \\
&= 3481 \bmod 713 && \text{ya que } 59^2 = 3481 \\
&= 629 && \text{ya que } 3481 \bmod 713 = 629.
\end{aligned}$$

■

Ejemplo 8.4.5 Cálculo de $a^k \bmod n$ cuando k no es una potencia de 2

Determine $12^{43} \bmod 713$.

Solución Primero escriba al exponente como una suma de potencias de 2:

$$43 = 2^5 + 2^3 + 2 + 1 = 32 + 8 + 2 + 1.$$

Ahora calcule 12^{2^k} para $k = 1, 2, 3, 4, 5$.

$$\begin{aligned}
12 \bmod 713 &= 12 \\
12^2 \bmod 713 &= 144 \\
12^4 \bmod 713 &= 144^2 \bmod 713 = 59 && \text{por ejemplo 8.4.4} \\
12^8 \bmod 713 &= 59^2 \bmod 713 = 629 && \text{por ejemplo 8.4.4} \\
12^{16} \bmod 713 &= 629^2 \bmod 713 = 639 && \text{por el método del ejemplo 8.4.4} \\
12^{32} \bmod 713 &= 639^2 \bmod 713 = 485 && \text{por el método del ejemplo 8.4.4}
\end{aligned}$$

Por la propiedad (8.4.2),

$$12^{43} = 12^{32+8+2+1} = 12^{32} \cdot 12^8 \cdot 12^2 \cdot 12^1.$$

Así, por el corolario 8.4.4,

$$\begin{aligned}
&12^{43} \bmod 713 \\
&\quad = \{(12^{32} \bmod 713) \cdot (12^8 \bmod 713) \cdot (12^2 \bmod 713) \cdot (12 \bmod 713)\} \bmod 713.
\end{aligned}$$

Por sustitución,

$$\begin{aligned}
12^{43} \bmod 713 &= (485 \cdot 629 \cdot 144 \cdot 12) \bmod 713 \\
&= 527152320 \bmod 713 \\
&= 48.
\end{aligned}$$

■

Es importante entender cómo hacer los cálculos a mano del ejemplo 8.4.5 utilizando sólo una simple calculadora electrónica, pero si está calculando muchos residuos, especialmente los relacionados con números grandes, puede que desee escribir un programa de calculadora de computadora pequeña para hacer los cálculos personales.

Extensión del algoritmo de Euclides

Una versión extendida del algoritmo de Euclides puede utilizarse para determinar una expresión concreta para el máximo común divisor de los enteros a y b.

• Definición

Un entero d se dice que es una **combinación lineal de enteros** a y b si y sólo si, existen enteros s y t tales que $as + bt = d$.

Teorema 8.4.5 Representación del máximo común divisor como una combinación lineal

Para todos los enteros a y b, no ambos cero, si $d = \text{MCD}(a, b)$, entonces existen enteros s y t tales que $as + bt = d$.

Demostración:

Dados enteros a y b, no ambos cero y dada $d = \text{MCD}(a, b)$, sea

$$S = \{x \mid x \text{ es un entero positivo y } x = as + bt \text{ para algunos enteros } s \text{ y } t\}.$$

Observe que S es un conjunto no vacío ya que 1) si $a > 0$ entonces $1 \cdot a + 0 \cdot b \in S$, 2) si $a < 0$ entonces $(-1) \cdot a + 0 \cdot b \in S$ y 3) si $a = 0$, entonces por suposición $b \neq 0$ y por tanto $0 \cdot a + 1 \cdot b \in S$ o $0 \cdot a + (-1) \cdot b \in S$. Así, ya que S es un subconjunto no vacío de enteros positivos, por el principio del buen orden para los enteros hay un elemento mínimo c en S. Por definición de S,

$$c = as + bt \quad \text{para algunos enteros } s \text{ y } t. \qquad 8.4.3$$

Demostraremos que 1) $c \geq d$ y 2) $c \leq d$ y podremos por tanto concluir que $c = d = \text{MCD}(a, b)$.

1) *Demostración de que $c \geq d$:*
[En esta parte de la prueba demuestre que d es un divisor de c y así que $d \leq c$.] Ya que $d = \text{MCD}(a, b)$, por definición de máximo común divisor, $d \mid a$ y $d \mid b$. Por tanto $a = dx$ y $b = dy$ para algunos enteros x y y. Entonces

$$\begin{aligned} c &= as + bt && \text{por (8.4.3)} \\ &= (dx)s + (dy)t && \text{por sustitución} \\ &= d(xs + yt) && \text{factorizando la } d. \end{aligned}$$

Pero $xs + yt$ es un entero ya que éste es una suma de productos de enteros. Así, por definición de divisibilidad, $d \mid c$. Tanto c como d son positivas y por tanto, por el teorema 4.3.1, $c \geq d$.

2) *Demostración de que $c \leq d$:*
[En esta parte de la prueba, demuestre que c es un divisor de a y de b y por tanto que c es menor que o igual al máximo común divisor de a y b, que es d.] Aplicando el teorema del cociente residuo a la división de a por c para obtener

$$a = cq + r \quad \text{para algunos enteros } q \text{ y } r \text{ con } 0 \leq r < c. \qquad 8.4.4$$

Así para algunos enteros q y r con $0 \leq r < c$,

$$r = a - cq$$

Ahora $c = as + bt$. Por tanto, para algunos enteros q y r con $0 \leq r < c$,

$$\begin{aligned} r &= a - (as + bt)q && \text{por sustitución} \\ &= a(1 - sq) - btq. \end{aligned}$$

Así r es una combinación lineal de a y b. Si $r > 0$, entonces r estaría en S y así r sería un elemento más pequeño de S que c, que estaría en contradicción con el hecho de que c es el elemento mínimo de S. Por tanto $r = 0$. Sustituyendo en (8.4.4),

$$a = cq$$

y por tanto $c \mid a$.

Un argumento casi idéntico establece que $c \mid b$ y se deja como ejercicio 30 del final de la sección.

Ya que $c \mid a$ y $c \mid b$, c es un común divisor de a y b. Por tanto es menor que o igual al máximo común divisor de a y b. En otras palabras, $c \leq d$.

De 1) y 2), concluimos que $c = d$. Se deduce que d, el máximo común divisor de a y b, es igual a $as + bt$.

El siguiente ejemplo muestra un método práctico para expresar el máximo común divisor de dos enteros como una combinación lineal de los dos.

Ejemplo 8.4.6 Expresando un máximo común divisor como una combinación lineal

En el ejemplo 4.8.6 mostramos cómo utilizar el algoritmo euclideano para determinar que el máximo común divisor de 330 y 156 es 6. Utilice los resultados de los cálculos para expresar el MCD(330, 156) como una combinación lineal de 330 y 156.

Solución Los primeros cuatro pasos de la solución expresan y amplían los resultados del ejemplo 4.8.6, que fueron obtenidos por aplicaciones sucesivas del teorema del cociente residuo. El quinto paso muestra cómo determinar los coeficientes de la combinación lineal sustituyendo hacia atrás a través de los resultados de los pasos anteriores.

Paso 1: $330 = 156 \cdot 2 + 18$, que implica que $18 = 330 - 156 \cdot 2$.

Paso 2: $156 = 18 \cdot 8 + 12$, que implica que $12 = 156 - 18 \cdot 8$.

Paso 3: $18 = 12 \cdot 1 + 6$, que implica que $6 = 18 - 12 \cdot 1$.

Paso 4: $12 = 6 \cdot 2 + 0$, que implica que el MCD(330, 156) $= 6$.

Paso 5: Sustituyendo hacia atrás los pasos del 3 al 1:

$$\begin{aligned} 6 &= 18 - 12 \cdot 1 && \text{del paso 3} \\ &= 18 - (156 - 8 \cdot 18) \cdot 1 && \text{por sustitución del paso 2} \\ &= 9 \cdot 18 + (-1) \cdot 156 && \text{por álgebra} \\ &= 9 \cdot (330 - 156 \cdot 2) + (-1) \cdot 156 && \text{por sustitución del paso 1} \\ &= 9 \cdot 330 + (-19) \cdot 156 && \text{por álgebra.} \end{aligned}$$

Así el MCD(330, 156) $= 9 \cdot 330 + (-19) \cdot 156$. (Siempre es una buena idea comprobar el resultado de un cálculo como este para asegurarse que no cometió un error. En este caso, usted determina que $9 \cdot 330 + (-19) \cdot 156$ de hecho es igual a 6.) ■

El algoritmo de Euclides dado en sección 4.8 se puede adaptar para calcular los coeficientes de la combinación lineal del MCD al mismo tiempo, que calcula el MCD mismo. Este algoritmo de Euclides extendido es descrito en los ejercicios al final de la sección.

Determinación de un inverso módulo n

Suponga que desea resolver la siguiente congruencia para x:

$$2x \equiv 3 \pmod 5$$

Observe que $3 \cdot 2 = 6 \equiv 1 \pmod 5$. Así puede considerar a 3 como una clase de módulo inverso 2 módulo 5 y multiplicando ambos lados de la congruencia para resolver por 3 se obtiene

$$6x = 3 \cdot 2x \equiv 3 \cdot 3 \pmod 5 \equiv 9 \pmod 5 \equiv 4 \pmod 5.$$

Pero $6 \equiv 1 \pmod 5$ y así por el teorema 8.4.3(3), $6x \equiv 1x \pmod 5 \equiv x \pmod 5$. Así, por las propiedades simétricas y transitivas de la congruencia modular,

$$x \equiv 4 \pmod 5,$$

y por tanto una solución es $x = 4$. (Podemos comprobar que $2 \cdot 4 = 8 \equiv 3 \pmod 5$).

Lamentablemente, no siempre es posible determinar un módulo "inverso" de un entero n. Por ejemplo, observe que

$$2 \cdot 1 \equiv 2 \pmod 4$$
$$2 \cdot 2 \equiv 0 \pmod 4$$
$$2 \cdot 3 \equiv 2 \pmod 4.$$

Por el teorema 8.4.3, estos cálculos son suficientes para concluir que el número 2 no tiene un inverso módulo 4.

La descripción de las circunstancias en que existen los inversos en aritmética modular requiere el concepto de número primo relativo.

• Definición

Los enteros a y b son **primos relativos** si y sólo si, MCD$(a, b) = 1$. Los enteros a_1, a_2, $a_3, \ldots, a_n$ son **primos relativos en pares** si y sólo si, el MCD$(a_i, a_j) = 1$ para todos los enteros i y j con $1 \leq i, j \leq n$ e $i \neq j$.

Dada la definición de primos relativos enteros, el corolario siguiente es una consecuencia inmediata del teorema 8.4.5.

Corolario 8.4.6

Si a y b son primos relativos enteros, entonces existen los enteros s y t tal que $as + bt = 1$.

Ejemplo 8.4.7 Expresión de 1 como una combinación lineal de enteros primos relativos

Demuestre que 660 y 43 son primos relativos y determine una combinación lineal de 660 y 43 que es igual a 1.

Solución

Paso 1: Divida 660 entre 43 para obtener $660 = 43 \cdot 15 + 15$, lo que implica que $15 = 660 - 43 \cdot 15$.

Paso 2: Divida 43 entre 15 para obtener $43 = 15 \cdot 2 + 13$, lo que implica que $13 = 43 - 15 \cdot 2$.

Paso 3: Divida 15 entre 13 para obtener $15 = 13 \cdot 1 + 2$, lo que implica que $2 = 15 - 13$.

Paso 4: Divida 13 por 2 para obtener $13 = 2 \cdot 6 + 1$, lo que implica que $1 = 13 - 2 \cdot 6$.

Paso 5: Divida 2 por 1 para obtener $2 = 1 \cdot 2 + 0$, lo que implica que MCD(660, 43) = 1 y así 660 y 43 son primos relativos.

Paso 6: Para expresar a 1 como una combinación lineal de 660 y 43, sustituya hacia atrás de los pasos 4 al 1:

$$\begin{aligned} 1 &= 13 - 2\cdot 6 && \text{del paso 4} \\ &= 13 - (15 - 13)\cdot 6 && \text{sustituyendo del paso 3} \\ &= 7\cdot 13 - 6\cdot 15 && \text{por álgebra} \\ &= 7\cdot(43 - 15\cdot 2) - 6\cdot 15 && \text{sustituyendo del paso 2} \\ &= 7\cdot 43 - 20\cdot 15 && \text{por álgebra} \\ &= 7\cdot 43 - 20\cdot(660 - 43\cdot 15) && \text{sustituyendo del paso 1} \\ &= 307\cdot 43 - 20\cdot 660 && \text{por álgebra.} \end{aligned}$$

Así el MCD(660, 43) = $1 = 307 \cdot 43 - 20 \cdot 660$. (Y una comprobación por cálculo directo confirma que $307 \cdot 43 - 20 \cdot 660$ es realmente igual a 1). ■

Una consecuencia del corolario 8.4.6 es que bajo ciertas circunstancias, es posible encontrar el inverso para un entero módulo n.

Corolario 8.4.7 Existencia del inverso módulo *n*

Para todos los enteros a y n, si MCD(a, n) = 1, entonces existe un entero s tal que $as \equiv 1 \pmod{n}$. El entero s se llama el **inverso de *a* módulo *n***.

Demostración:

Suponga que a y n son enteros y MCD(a, n) = 1. Por el corolario 8.4.6, existen los enteros s y t tales que

$$as + nt = 1.$$

Restando nt de ambos miembros se obtiene

$$as = 1 - nt = 1 + (-t)n.$$

Así, por definición de congruencia módulo n,

$$as \equiv 1 \pmod{n}.$$

Ejemplo 8.4.8 Determinación de un inverso módulo *n*

a. Determine un inverso para 43 módulo 660. Es decir, determine un entero s tal que $43s \equiv 1 \pmod{660}$.

b. Determine un inverso positivo para 3 módulo 40. Es decir, determine un entero positivo s tal que $3s \equiv 1 \pmod{40}$.

Solución

a. Por el ejemplo 8.4.7,

$$307 \cdot 43 - 20 \cdot 660 = 1.$$

Sumando $20 \cdot 660$ a ambos miembros se obtiene

$$307 \cdot 43 = 1 + 20 \cdot 660.$$

Así, por definición de congruencia módulo 660,

$$307 \cdot 43 \equiv 1 \pmod{660},$$

así 307 es un inverso para 43 módulo 660.

b. Use la técnica del ejemplo 8.4.7 para determinar una combinación lineal de 3 y 40 que sea igual a 1.

Paso 1: Divida 40 por 3 para obtener $40 = 3 \cdot 13 + 1$. Esto implica que $1 = 40 - 3 \cdot 13$.

Paso 2: Divida 3 por 1 para obtener $3 = 3 \cdot 1 + 0$. Esto implica que MCD(3, 40) = 1.

Paso 3: Utilice el resultado del paso 1 para escribir

$$3 \cdot (-13) = 1 + (-1)40.$$

Este resultado implica que -13 es un inverso para 3 módulo 40. En símbolos, $3 \cdot (-13) \equiv 1 \pmod{40}$. Para determinar un inverso positivo, calcule $40 - 13$. El resultado es 27, y

$$27 \equiv -13 \pmod{40}$$

ya que $27 - (-13) = 40$. Así, por el teorema 8.4.3(3),

$$3 \cdot 27 \equiv 3 \cdot (-13) \equiv 1 \pmod{40},$$

y así por la propiedad transitiva de congruencia módulo n, 27 es un entero positivo es decir un inverso para 3 módulo 40. ■

Criptografía RSA

En este punto hemos desarrollado suficiente teoría de números para explicar cómo cifrar y descifrar mensajes mediante el cifrado RSA. La efectividad del sistema se basa en el hecho que aunque los algoritmos de las computadoras modernas hacen bastante fácil determinar dos enteros grandes distintos p y q —digamos del orden de varios cientos de dígitos cada uno— es prácticamente seguro que son primos, incluso las computadoras más rápidas hasta el momento no pueden factorizar sus productos, un entero con aproximadamente el doble del número de dígitos. Para cifrar un mensaje utilizando criptografía RSA, una persona necesita conocer el valor de pq y de otro entero e, ambos están a la disposición del público. Pero sólo una persona que conoce los valores individuales de p y q puede descifrar un mensaje cifrado.

Primero, damos un ejemplo para mostrar *cómo* funciona el cifrado y después analizaremos algo de teoría para explicar *por qué* funciona. El ejemplo es poco realista en el sentido de que puesto que p y q son muy pequeños, sería fácil averiguar quiénes son exactamente, conociendo su producto. Pero trabajar con pequeñas cantidades nos da la idea del sistema, mientras se mantengan los cálculos en un rango que se puede realizar con una calculadora de mano.

Suponga que Alicia decide establecer un algoritmo de cifrado RSA. Ella elige dos primos, digamos $p = 5$ y $q = 11$ y calcula $pq = 55$. Después elige un entero positivo e que es primo relativo de $(p - 1)(q - 1)$. En este caso, $(p - 1)(q - 1) = 4 \cdot 10 = 40$, así que ella hace $e = 3$ ya que 3 es primo relativo de 40. (En la práctica, hacer a e pequeño podría poner en peligro el secreto del cifrado, por lo que tendría una cantidad mayor que 3. Sin embargo, las matemáticas del cifrado funcionan tanto para 3 como para un número mayor y el número menor hace los cálculos más fáciles).

Los dos números $pq = 55$ y $e = 3$ son las **claves públicas**, que ella puede distribuir ampliamente. Ya que el cifrado RSA sólo funciona con números, Alicia también informa a las personas cómo interpretará los números en los mensajes que le envían. Suponga que ella codifica las letras del alfabeto del mismo modo que se hizo para el cifrado César:

$$A = 1, B = 2, C = 3, \ldots, Z = 26.$$

También supone que los mensajes que recibe Alicia constan de bloques, cada uno de los que, por simplicidad, se toma como una letra única del alfabeto numéricamente codificada.

Alguien que quiera enviar un mensaje de Alicia divide el mensaje en bloques, cada uno consiste de una sola letra y encuentra equivalente numérico de cada bloque. El texto plano, M, en un bloque se convierte en el texto cifrado, C, de acuerdo con la siguiente fórmula:

$$C = M^e \bmod pq. \tag{8.4.5}$$

Observe que ya que ambos pq y e son claves públicas, cualquier persona a la que se le dan la claves y sabe aritmética modular puede cifrar un mensaje para enviárselo a Alicia.

Ejemplo 8.4.9 Cifrado de un mensaje utilizando criptografía RSA

Bob quiere enviar el mensaje HOLA a Alicia. ¿Cuál es el texto cifrado para su mensaje?

Solución Bob enviará sus mensaje en cuatro bloques, para la H, para la O, para la L y para la A. Puesto que H es la octava letra en el alfabeto, se codifica como 08, o 8. El texto cifrado correspondiente se calcula mediante la fórmula (8.4.5) como sigue:

$$\begin{aligned} C &= 8^3 \bmod 55 \\ &= 512 \bmod 55 \\ &= 17. \end{aligned}$$

Ya que O es la quinceava letra del alfabeto, se codifica como 15. El texto cifrado correspondiente es

$$\begin{aligned} C &= 15^3 \bmod 55 \\ &= 3375 \bmod 55 \\ &= 20. \end{aligned}$$

L es la doceava letra del alfabeto, se codifica como 12. El texto cifrado correspondiente es

$$\begin{aligned} C &= 12^3 \bmod 55 \\ &= 1728 \bmod 55 \\ &= 23. \end{aligned}$$

A es la primera letra del alfabeto, se codifica como 01 o 1. El texto cifrado correspondiente es

$$\begin{aligned} C &= 1^3 \bmod 55 \\ &= 1 \bmod 55 \\ &= 1. \end{aligned}$$

En consecuencia, Bob envía a Alicia el mensaje: 17 20 23 01. ■

Para descifrar el mensaje, Alicia necesita calcular la clave de descifrado, un número d que es un inverso positivo al e módulo $(p - 1)(q - 1)$. Ella obtiene el texto plano M del texto cifrado C usando la fórmula 8.4.6

$$M = C^d \bmod pq. \tag{8.4.6}$$

Observe que ya que $M + kpq \equiv M \pmod{pq}$, M debe ser menor que pq, como en el ejemplo anterior, para que el descifrado garantice producir el mensaje original. Pero puesto que p y q normalmente se toman muy grandes, este requisito no causa problemas. Los mensajes grandes se dividen en bloques de símbolos para satisfacer la restricción y se incluyen varios símbolos en cada bloque para presentar el descifrado en base al conocimiento de las frecuencias de las letras.

Ejemplo 8.4.10 Descifrando un mensaje utilizando criptografía RSA

Imagine que Alicia lo ha contratado para ayudarle a descifrar mensajes y comparte con usted los valores de p y q. Descifre el siguiente párrafo de texto cifrado para ella: 17 20 23 01.

Solución Ya que $p = 5$ y $q = 11$, $(p-1)(q-1) = 40$ y así primero debe determinar la clave de descifrado, que es un inverso positivo para 3 módulo 40. Conociendo que podría necesitar este número, se calculó en el ejemplo 8.4.8*b*) y encontró 27. Así necesita calcular $M = 17^{27} mod\ 55$. Para hacerlo, considere que $27 = 16 + 8 + 2 + 1 = 2^4 + 2^3 + 2 + 1$. Así determinará los residuos obtenidos cuando 17 es elevado a potencias sucesivamente mayores de 2, a $2^4 = 16$.

$$\begin{aligned}
17\ mod\ 55 &= 17\ mod\ 55 = 17\\
17^2\ mod\ 55 &= 17^2\ mod\ 55 = 14\\
17^4\ mod\ 55 &= (17^2)^2\ mod\ 55 = 14^2\ mod\ 55 = 31\\
17^8\ mod\ 55 &= (17^4)^2\ mod\ 55 = 31^2\ mod\ 55 = 26\\
17^{16}\ mod\ 55 &= (17^8)^2\ mod\ 55 = 26^2\ mod\ 55 = 16
\end{aligned}$$

Entonces usamos el hecho de que

$$17^{27} = 17^{16+8+2+1} = 17^{16} \cdot 17^8 \cdot 17^2 \cdot 17^1$$

Para escribir

$$\begin{aligned}
17^{27}\ mod\ 55 &= (17^{16} \cdot 17^8 \cdot 17^2 \cdot 17)\ mod\ 55\\
&\equiv [(17^{16}\ mod\ 55)(17^8\ mod\ 55)(17^2\ mod\ 55)(17\ mod\ 55)]\ (\text{mod } 55)\\
&\qquad \text{por el corolario 8.4.4}\\
&\equiv (16 \cdot 26 \cdot 14 \cdot 17)\ (\text{mod } 55)\\
&\equiv 99008\ (\text{mod } 55)\\
&\equiv 8\ (\text{mod } 55).
\end{aligned}$$

Por tanto $17^{27}\ mod\ 55 = 8$ y así el texto plano de la primera parte del mensaje de Bob es 8 o 08. En el último paso, se determina la letra correspondiente a 08, es *H*. En los ejercicios 14 y 15 al final de esta sección, se le pide demostrar que cuando descifra 20, el resultado es 15, que corresponde a la letra O y que cuando descifra 23, el resultado es 12, que corresponde a la letra L y que cuando descifra 01, el resultado es 1, que corresponde a la letra A así puede decir que el mensaje que le envío Bob a Alicia es HOLA. ■

Lema de Euclides

Otra consecuencia del teorema 8.4.5 se conoce como el *lema de Euclides*. Es el hecho fundamental detrás del teorema de la factorización única de enteros y es también de gran importancia en muchas otras partes de la teoría de números.

Teorema 8.4.8 Lema de Euclides

Para todos los enteros a, b y c, si MCD$(a, c) = 1$ y $a \mid bc$, entonces $a \mid b$.

Demostración:

Suponga que a, b y c son enteros, MCD$(a, c) = 1$ y $a \mid bc$. *[Debemos demostrar que* $a \mid b$*.]* Por el teorema 8.4.5, existen enteros s y t por lo que

$$as + ct = 1.$$

Multiplicando ambos lados de esta ecuación por b se obtiene

$$bas + bct = b. \tag{8.4.7}$$

Puesto que $a \mid bc$, por definición de divisibilidad existe un entero k tal que

$$bc = ak. \tag{8.4.8}$$

Sustituyendo (8.4.8) en (8.4.7), reescribiendo y factorizando a se obtiene

$$b = bas + (ak)t = a(bs + kt).$$

Sea $r = bs + kt$. Entonces r es un entero (ya que b, s, k y t son todos enteros) y $b = ar$. Así $a \mid b$ por definición de divisibilidad.

El único teorema de factorización para los enteros afirma que cualquier entero mayor que 1 tiene una representación única como un producto de números primos, excepto posiblemente por el orden en el que se escriben los números. La sugerencia del ejercicio 13 de la sección 3.4 esbozó una demostración de la parte de existencia de la demostración y la unicidad de la representación se deduce rápidamente del lema de Euclides. En el ejercicio 41 al final de esta sección, describimos una demostración que debe completar.

Otra aplicación del lema de Euclides es un teorema de cancelación para la congruencia módulo n. Este teorema nos permite, bajo ciertas circunstancias: dividir por un factor común a una relación de congruencia.

Teorema 8.4.9 Teorema de cancelación para congruencia modular

Para todos los enteros a, b, c y n con $n > 1$, si $\text{MCD}(c, n) = 1$ y $ac \equiv bc \pmod{n}$, entonces $a \equiv b \pmod{n}$.

Demostración:

Suponga que a, b, c y n son enteros cualesquiera, si $\text{MCD}(c, n) = 1$ y $ac \equiv bc \pmod{n}$. *[Debemos demostrar que $a \equiv b \pmod{n}$.]* Por definición de congruencia módulo n,

$$n \mid (ac - bc),$$

y así, puesto que

$$ac - bc = (a - b)c,$$
$$n \mid (a - b)c.$$

Ya que $\text{MCD}(c, n) = 1$, podemos aplicar el lema de Euclides para obtener

$$n \mid (a - b),$$

y así, por definición de congruencia módulo n,

$$a \equiv b \pmod{n}.$$

Una demostración alternativa del teorema 8.4.9 usa el corolario 8.4.7. Ya que $\text{MCD}(c, n) = 1$, el corolario garantiza un inverso para c módulo n. En la demostración del teorema 8.4.9, sea d un inverso para c. Aplique el teorema 8.43(3) repetidamente, primero multiplicando ambos lados de $ac \equiv bc \pmod{n}$ por d se obtiene $(ac)d \equiv (bd)d \pmod{n}$ y después se utiliza el hecho de que $cd \equiv 1 \pmod{n}$ para simplificar la congruencia y la conclusión de que $a \equiv b \pmod{n}$.

Pequeño teorema de Fermat

Se le dio el nombre del pequeño teorema de Fermat para distinguirlo del último teorema de Fermat, que se analizó en la sección 4.1. Éste proporciona a la criptografía RSA la fundamentación teórica.

Teorema 8.4.10 Pequeño teorema de Fermat

Si p es cualquier número primo y a es cualquier entero tal que $p \nmid a$, entonces $a^{p-1} \equiv 1 \pmod{p}$.

Demostración:

Suponga que p es cualquier número primo y a es cualquier entero tal que $p \nmid a$. Observe que $a \neq 0$ ya que de lo contrario p dividiría a a. Considere el conjunto de enteros

$$S = \{a, 2a, 3a, \ldots, (p-1)a\}.$$

Afirmamos que ninguno de los dos elementos de S son congruentes módulo p. Suponiendo que $sa \equiv ra \pmod{p}$ para algunos enteros s y r con $1 \leq r < s \leq p-1$. Entonces, por la definición de congruencia módulo p,

$$p \mid (sa - ra), \quad \text{o, equivalentemente,} \quad p \mid (s-r)a.$$

Ahora $p \nmid a$ por hipótesis y ya que p es primo, MCD$(a, p) = 1$. Así, por el lema de Euclides, $p \mid (s-r)$. Pero esto es imposible ya que $0 < s - r < p$.

Considere la función F de S para el conjunto $T = \{1, 2, 3, \ldots, (p-1)\}$ que envía cada elemento de S a su residuo módulo p. Entonces F es inyectiva ya que no hay dos elementos de S que sean congruentes módulo p. En la sección 9.4 demostramos que si una función de un conjunto finito a otro es inyectiva, entonces es también sobreyectiva. Por tanto F es sobreyectiva y así los $p-1$ residuos de los $p-1$ elementos de S son exactamente los números $1, 2, 3, \ldots, (p-1)$.

Se deduce del teorema 8.4.3(3) que

$$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv [1 \cdot 2 \cdot 3 \cdots (p-1)] \pmod{p},$$

o de forma equivalente,

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}.$$

Pero puesto que p es primo, p y $(p-1)!$ son primos relativos. Así, por el teorema de cancelación teorema para la congruencia modular (teorema 8.4.9),

$$a^{p-1} \equiv 1 \pmod{p}.$$

¿Por qué funciona el cifrado RSA?

Para el método de criptografía RSA, la fórmula

$$M = C^d \bmod pq$$

se supone produce el texto plano mensaje original, M, cuando el mensaje cifrado es C. ¿Cómo puede estar seguro de que no siempre es así? Recuerde que requerimos que $M < pq$ y sabemos que $C = M^e \bmod pq$. Así, por sustitución,

$$C^d \bmod pq = (M^e \bmod pq)^d \bmod pq.$$

Por teorema 8.4.3(4),

$$(M^e \bmod pq)^d \equiv M^{ed} \pmod{pq}.$$

Así $C^d \bmod pq \equiv M^{ed} \pmod{pq}$ y así es suficiente para demostrar que

$$M \equiv M^{ed} \pmod{pq}.$$

Recuerde que d se eligió como un inverso positivo para módulo e, $(p-1)(q-1)$, que existe ya que MCD$(e, (p-1)(q-1)) = 1$. En otras palabras,

$$ed \equiv 1 \pmod{(p-1)(q-1)},$$

o, equivalentemente,

$$ed = 1 + k(p-1)(q-1) \quad \text{para algún entero positivo } k.$$

Por tanto,

$$M^{ed} = M^{1+k(p-1)(q-1)} = M(M^{p-1})^{k(q-1)} = M(M^{q-1})^{k(p-1)}$$

Si $p \nmid M$, entonces por el pequeño teorema de Fermat, $M^{p-1} \equiv 1 \pmod{p}$ y así

$$M^{ed} = M(M^{p-1})^{k(q-1)} \equiv M(1)^{k(q-1)} \pmod{p} = M \pmod{p}.$$

Similarmente, si $q \nmid M$, entonces por el pequeño teorema de Fermat, $M^{q-1} \equiv 1 \pmod{q}$ y así

$$M^{ed} = M(M^{q-1})^{k(p-1)} \equiv M(1)^{k(p-1)} = M \pmod{q}.$$

Así, si M es primo relativo a pq,

$$M^{ed} \equiv M \pmod{p} \quad \text{y} \quad M^{ed} \equiv M \pmod{q}.$$

Si M no es primo relativo a pq, entonces ya sea $p \mid M$ o $q \mid M$. Sin perder generalidad, suponga que $p \mid M$. Se deduce que $M^{ed} \equiv 0 \equiv M \pmod{p}$. Además, ya que $M < pq$, $q \mid M$ y así, como anteriormente, $M^{ed} \equiv M \pmod{q}$. Por tanto, en este caso también,

$$M^{ed} \equiv M \pmod{p} \quad \text{y} \quad M^{ed} \equiv M \pmod{q}.$$

Por el teorema 8.4.1,

$$p \mid (M^{ed} - M) \quad \text{y} \quad q \mid (M^{ed} - M),$$

y, por definición de divisibilidad,

$$M^{ed} - M = pt \text{ para algún entero } t.$$

Por sustitución,

$$q \mid pt,$$

y puesto que q y p son números primos distintos, aplicando el lema de Euclides se obtiene

$$q \mid t.$$

Así

$$t = qu \text{ para algún entero } u$$

por definición de divisibilidad. Por sustitución,

$$M - M^{ed} = pt = p(qu) = (pq)u,$$

donde u es un entero y así,

$$pq \mid (M - M^{ed})$$

por definición de divisibilidad. Así

$$M - M^{ed} \equiv 0 \pmod{pq}$$

por definición de congruencia, o, equivalentemente,

$$M \equiv M^{ed} \ (mod\ pq).$$

Ya que $M < pq$, esta última congruencia implica que

$$M = M^{ed} \ mod\ pq,$$

y así el cifrado RSA obtiene el resultado correcto.

Observaciones adicionales de la teoría de números y de la criptografía

El famoso matemático británico G. H. Hardy (1877-1947) se aficionó a la comparación de las matemáticas puras, con la belleza del arte. De hecho, los teoremas en esta sección tienen muchas y bellas consecuencias más allá de los que hemos tenido el espacio para describir y el tema de la teoría de los números que va mucho más allá de estos teoremas. Hardy también disfrutó describir a las matemáticas puras como inútil. Por tanto, resulta irónico que existan libros enteros dedicados a las aplicaciones de la teoría de números de aplicaciones a las ciencias de la computación, la criptografía RSA es sólo una aplicación. Además, como la necesidad de criptografía de clave pública se ha desarrollado, se han utilizado técnicas en otras áreas de las matemáticas, tales como álgebra y geometría algebraica, para desarrollar sistemas adicionales.

Autoexamen

1. Cuando las letras del alfabeto son cifradas usando el cifrado César, la versión encriptada de una letra es _____.
2. Si a, b y n son enteros con $n > 1$, todas de las siguientes formas son diferentes maneras para expresar el hecho de que $n \mid (a - b)$: _____, _____, _____, _____.
3. Si a, b, c, d, m y n son enteros con $n > 1$ y si $a \equiv c \pmod n$ y $b \equiv d \pmod n$, entonces $a + b \equiv$ _____, $a - b \equiv$ _____, $ab \equiv$ _____ y $a^m \equiv$ _____.
4. Si a, n y k son enteros positivos con $n > 1$, una forma eficiente de calcular $a^k \pmod n$ es escribir k como una _____ y use los hechos acerca del cálculo de productos y potencias módulo n.
5. Para expresar un máximo común divisor de dos enteros como una combinación lineal de los enteros, use el algoritmo ampliado _____.
6. Para determinar un inverso para un entero positivo a módulo de un entero n con $n > 1$, exprese el número 1 como _____.
7. Para encriptar un mensaje M usando criptografía RSA con clave pública pq y e, utilice la fórmula _____ y para descifrar un mensaje C, utilice la fórmula _____, donde _____.
8. El lema de Euclides dice que para todos los enteros a, b y c si MCD$(a, c) = 1$ y $a \mid bc$, entonces _____.
9. El pequeño teorema de Fermat dice que si p es cualquier número primo y a es cualquier entero tal que $p \mid a$ entonces _____.
10. Lo crucial de la demostración de que el cifrado RSA funcione es que si 1) p y q son números primos grandes distintos, 2) $M < pq$, 3) M es primo relativo a pq, 4) e es primo relativo a $(p - 1)(q - 1)$ y 5) d es un inverso positivo para e módulo $(p - 1)(q - 1)$, entonces $M =$ _____.

Conjunto de ejercicios 8.4

1. a. Use el cifrado César para codificar el mensaje DÓNDE NOS ENCONTRAREMOS.
   b. Utilice el cifrado César para descifrar el mensaje H Q OD FDIHWHULD.

2. a. Utilice el cifrado César para codificar el mensaje UNA MANZANA AL DÍA.
   b. Utilice el cifrado César para descifrar el mensaje PDQWL HQH OHMRV DO PHGLFR

3. Sea $a = 25$, $b = 19$ y $n = 3$.
   a. Compruebe que $3 \mid (25 - 19)$.
   b. Explique por qué $25 \equiv 19 \pmod 3$.
   c. ¿Qué valor de k tiene la propiedad de que $25 = 19 + 3k$?

d. ¿Cuál es el residuo (no negativo) obtenido cuando 25 se divide entre 3? ¿Cuando 19 se divide entre 3?
e. Explique por qué 25 *mod* 3 = 19 *mod* 3.

4. Sea $a = 67$, $b = 32$ y $n = 7$.
a. Compruebe que $7 \mid (68 - 33)$.
b. Explique por qué $68 \equiv 33 \pmod 7$.
c. ¿Qué valor de k tiene la propiedad de que $68 = 33 + 7k$?
d. ¿Cuál es el residuo (no negativo) que se obtiene cuando 68 se divide entre 7? ¿Cuando 33 se divide entre 7?
e. Explique por qué 68 *mod* 7 = 33 *mod* 7.

5. Demuestre la transitividad de la congruencia modular. Es decir, demuestre que para todos los enteros a, b, c y n con $n > 1$, si $a \equiv b \pmod n$ y $b \equiv c \pmod n$ entonces $a \equiv c \pmod n$.

H 6. Demuestre que las clases distintas de equivalencia de la relación de congruencia módulo n son los conjuntos [0], [1], [2], . . . , $[n - 1]$, donde para cada $a = 0, 1, 2, \ldots, n - 1$,

$$[a] = \{m \in Z \mid m \equiv a \pmod n\}.$$

7. Compruebe los siguientes enunciados.
a. $128 \equiv 2 \pmod 7$ y $61 \equiv 5 \pmod 7$
b. $(128 + 61) \equiv (2 + 5) \pmod 7$
c. $(128 - 61) \equiv (2 - 5) \pmod 7$
d. $(128 \cdot 61) \equiv (2 \cdot 5) \pmod 7$
e. $128^2 \equiv 2^2 \pmod 7$

8. Compruebe los siguientes enunciados.
a. $45 \equiv 3 \pmod 6$ y $104 \equiv 2 \pmod 6$
b. $(45 + 104) = (3 + 2) \pmod 6$
c. $(45 - 104) = (3 - 2) \pmod 6$
d. $(45 \cdot 104) = (3 \cdot 2) \pmod 6$
e. $45^2 = 3^2 \pmod 6$

En los ejercicios del 9 al 11, demuestre cada uno de los enunciados dados, suponiendo que a, b, c, d y n son enteros con $n > 1$ y que $a \equiv c \pmod n$ y $b \equiv d \pmod n$.

9. **a.** $(a + b) \equiv (c + d) \pmod n$
b. $(a - b) \equiv (c - d) \pmod n$

10. $a^2 \equiv c^2 \pmod n$

11. $a^m \equiv c^m \pmod n$ para todos los enteros $m \geq 1$ (Utilice inducción matemática sobre m.)

12. **a.** Demuestre que para todos los enteros $n \geq 0$, $10^n \equiv 1 \pmod 9$.
b. Use el inciso *a*) para demostrar que un entero positivo es divisible entre 9 si y sólo si, la suma de sus dígitos es divisible entre 9.

13. a. Demuestre que para todos los enteros $n \geq 1$, $10^n \equiv (-1)^n \pmod{11}$.
b. Use el inciso *a*) para demostrar que un entero positivo es divisible entre 11 si y sólo si, la suma alternando sus dígitos es divisible por 11. (Por ejemplo, la suma alternando los dígitos de 82 379 es $8 - 2 + 3 - 7 + 9 = 11$ y $82\,379 = 11 \cdot 7489$.)

14. Utilice la técnica del ejemplo 8.4.4 para determinar 14^2 *mod* 55, 14^4 *mod* 55, 14^8 *mod* 55 y 14^{16} *mod* 55.

15. Use el resultado del ejercicio 14 y la técnica del ejemplo 8.4.5 para determinar 14^{27} *mod* 55.

En los ejercicios 16 al 18, utilice la técnica del ejemplo 8.4.4 y del ejemplo 8.4.5 para determinar los números dados.

16. 675^{307} *mod* 713 17. 89^{307} *mod* 713

18. 48^{307} *mod* 713

En los ejercicios 19 al 24, utilice la criptografía RSA de los ejemplos 8.4.9 y 8.4.10. En los ejercicios 19 al 21, traduzca el mensaje en su equivalente numérico y codifíquelo. En los ejercicios 22 al 24, descifre el texto cifrado y traduzca el resultado a letras del alfabeto para descubrir el mensaje.

19. HOLA 20. BIENVENIDO 21. EXCELENTE

22. 08 21 15 49 20 23. 01 09 14 20 39 24. 51 14 49 20

H 25. Use el teorema 5.2.3 para demostrar que si a y n son enteros positivos y $a^n - 1$ es primo, entonces $a = 2$ y n es primo.

En los ejercicios 26 y 27, use el algoritmo euclidiano ampliado para determinar el máximo común divisor de los números dados y exprese éste como una combinación lineal de los dos números.

26. 6664 y 765 27. 4158 y 1568

Los ejercicios 28 y 29 se refieren a la siguiente versión formal del algoritmo euclidiano ampliado.

Algoritmo 8.4.1 Algoritmo euclidiano ampliado

[Dados los enteros A y B con $A > B > 0$, este algoritmo calcula el MCD(A, B) y encuentra los enteros s y t tal que $sA + tB =$ MCD(A, B).]

Entrada: *A, B [enteros con $A > B > 0$]*

Cuerpo del algoritmo:

$a := A$, $b := B$, $s := 1$, $t := 0$, $u := 0$, $v := 1$,
[pre-condición: $a = sA + tB$ y $b = u\,A + vB$]

while $(b \neq 0)$

[invariante del bucle: $a = sA + tB$ y $b = uA + vB$, MCD(a, b) = MCD(A,B)]

$r := a \bmod b$, $q := a \operatorname{div} b$

$a := 6$, $b :=$ r

$newu := s - uq$, $newv := t - vq$

$s := u$, $t := v$

$u := newu$, $v := newv$

end while

MCD $:= a$

[post-condición: MCD(A, B) = $a = sA + tB$]

Salida: *MCD[a entero positivo], s, t [enteros]*

En los ejercicios 28 y 29, para los valores dados de A y B, realice una tabla que muestre el valor de s, t y $sA + tB$ antes del inicio del bucle while y después de cada iteración del bucle.

28. $A = 330$, $B = 156$ 29. $A = 284$, $B = 168$

30. Finalice la demostración del teorema 8.4.5 al demostrar que si, a, b y c son como en la demostración, entonces $c \mid b$.

31. a. Determine un inverso para 210 módulo 13.
b. Determine un inverso positivo para 210 módulo 13.
c. Determine una solución positiva para la congruencia $210x \equiv 8 \pmod{13}$.

32. a. Determine un inverso para 41 módulo 660.
b. Determine la solución positiva mínima para la siguiente congruencia: $41x \equiv 125 \pmod{660}$.

H 33. Use el teorema 8.4.5 para demostrar que para todos los enteros a, b y c, si MCD$(a, b) = 1$ y $a \mid c$ y $b \mid c$, entonces $ab \mid c$.

34. Dé un contraejemplo para demostrar que el recíproco del ejercicio 33 es falso.

35. El corolario 8.4.7 garantiza la existencia del inverso módulo n para un entero a cuando a y n son primos relativos. Use el lema de Euclides para demostrar que el inverso es el único módulo n. En otras palabras, demuestre que cualesquiera dos enteros cuyo producto con a es congruente a 1 módulo n son congruentes uno con el otro módulo n.

En 36, 37, 39 y 40, use la criptografía RSA con clave pública $n = 713 = 23 \cdot 31$ y $e = 43$. En los ejercicios 36 y 37, codifique los mensajes en sus valores numéricos equivalentes y codifíquelos. En 39 y 40, descifre el texto cifrado dado y determine los mensajes originales.

36. AYUDA 37. VIENE

38. Determine el menor inverso positivo para 43 módulo 660.

39. 533 423 018 089

40. 293 425 129 423 129

H 41. **a.** Utilice el lema de Euclides e inducción matemática para demostrar que para todos los enteros positivos s, si p y q_1, $q_2, \ldots, q_s$ son números primos y $p \mid q_1, q_2, \ldots, q_s$ entonces $p = q_i$ para algún i con $1 \le i \le s$.

b. La parte de unicidad del teorema de factorización única para los enteros dice que dado cualquier entero n, si

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

para algunos enteros positivos r y s y los números primos $p_1 \le p_2 \le \cdots \le p_r$ y $q_1 \le q_2 \le \cdots \le q_s$, entonces $r = s$ y $p_i = q_i$ para todos los enteros i con $1 \le i \le r$.

Use el resultado del inciso *a*) para completar los detalles del siguiente bosquejo de una demostración: Suponga que n es un entero con dos diferentes factorizaciones de primos: $n = p_1 p_2 \cdots p_t = q_1 q_2 \cdots q_u$. Todos los factores primos que aparecen en ambos miembros pueden eliminarse (tantas veces como aparezcan en ambos miembros) para llegar a la situación donde $p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$, $p_1 \le p_2 \le \cdots \le p_r$ y $q_1 \le q_2 \le \cdots \le q_s$ y $p_i \ne q_j$ para cualesquier enteros i y j. Entonces use el inciso *a*) para deducir una contradicción y así la factorización de primos de n es única excepto, posiblemente, por el orden en el que se escriben los factores primos.

42. De acuerdo con el pequeño teorema de Fermat, si p es un número primo y a y p son primos relativos, entonces $a^{p-1} \equiv 1 \pmod{p}$. Compruebe que este teorema da los resultados correctos para
a. $a = 15$ y $p = 7$ b. $a = 8$ y $p = 11$

43. El pequeño teorema de Fermat se puede usar para demostrar que un número es no primo encontrando un número a de primos relativos a p con la propiedad de que $a^{p-1} \not\equiv 1 \pmod{p}$. Sin embargo, no se puede utilizar para demostrar que un número *es* primo. Determine un ejemplo para ilustrar este hecho. Es decir, determine los enteros a y p tales que a y p son primos relativos y $a^{p-1} \equiv 1 \pmod{p}$ pero p no es primo.

Respuestas del autoexamen

1. tres lugares a la derecha de la letra en el alfabeto, con X correspondiendo a A, Y a B y Z a C 2. $a \equiv b \pmod{n}$; $a = b + kn$ para algún entero k; a y b tienen el mismo residuo no negativo cuando se divide entre n; $a \bmod n = b \bmod n$ 3. $(c + d) \pmod{n}$; $(c - d) \pmod{n}$; $(cd) \pmod{n}$; $c^m \pmod{n}$ 4. suma de potencias de 2 5. versión de Euclides 6. una combinación lineal de a y n 7. $C = M^c \bmod pq$; $M = C^d \bmod pq$; d es un inverso positivo para e módulo $(p - 1)(q - 1)$ 8. $a \mid b$ 9. $a^{p-1} \equiv 1 \pmod{p}$ 10. $M^{ed} \bmod pq$

8.5 Relaciones de orden parcial

No hay ninguna rama de la matemática, abstracta sin embargo, que pueda algún día no aplicarse a fenómenos del mundo real. —Nicolai Ivanovitch Lobachevsky, 1792-1856

Para obtener un grado en informática en una Universidad dada, un estudiante debe tomar un conjunto específico de cursos requeridos, algunos deben completarse antes de que se puedan iniciar otros. Dada la estructura de los pre-requisitos del programa, uno podría preguntarse cuál es el número mínimo de periodos que se necesita para cumplir con los requisitos del grado, o cuál es el máximo números de cursos que se pueden realizar en el mismo periodo, o si hay una secuencia en la que un estudiante de tiempo parcial pueda tomar uno de los cursos por periodo. Más adelante en esta sección, mostramos cómo se representa la estructura de los requisitos previos del programa como una relación de orden parcial lo que hace relativamente fácil responder a dichas preguntas.

Antisimetría

En la sección 8.2 definimos tres propiedades de las relaciones: reflexividad, simetría y transitividad. Una cuarta propiedad de las relaciones se llama *antisimetría*. En términos del diagrama de flechas de una relación, decimos que una relación antisimétrica es lo mismo que decir que siempre hay una flecha que va de un elemento a otro elemento *distinto*, *no* hay una flecha que vaya del segundo al primero.

• Definición

Sea R una relación sobre un conjunto A. R es **antisimétrica** si y sólo si,

$$\text{para todos } a \text{ y } b \text{ en } A, \quad \text{si } a\,R\,b \text{ y } b\,R\,a \text{ entonces } a = b.$$

Tomando la negación de la definición, puede ver que una relación R ***no*** es **antisimétrica** si y sólo si,

$$\text{existen los elementos } a \text{ y } b \text{ en } A \text{ tales que } a\,R\,b \text{ y } b\,R\,a \text{ pero } a \neq b.$$

Ejemplo 8.5.1 Demostración de antisimetría de relaciones finitas

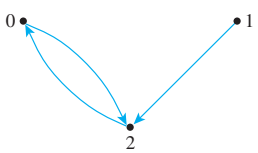
Sean R_1 y R_2 las relaciones sobre $\{0, 1, 2\}$ que se definen como sigue: Dibuje los grafos dirigidos para R_1 y R_2 e indique qué relaciones son antisimétricas.

a. $R_1 = \{(0, 2), (1, 2), (2, 0)\}$

b. $R_2 = \{(0, 0), (0, 1), (0, 2), (1, 1), (1, 2)\}$

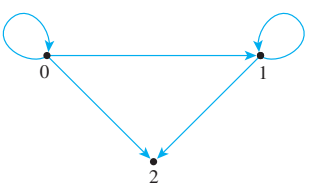
Solución

a. R_1 no es antisimétrica.



Puesto que $0\,R_1\,2$ y $2\,R_1\,0$ pero $0 \neq 2$, R_1 no es antisimétrica.

b. R_2 es antisimétrica.



Para que R_2 no sea antisimétrica, tendrían que existir un par de elementos distintos de A tal que cada uno está relacionado con el otro por R_2. Pero se puede ver por inspección que no existe ningún tal par.

■

Ejemplo 8.5.2 Demostración de antisimetría de la relación de "divide"

Sea R_1 la relación "divide" en el conjunto de todos los enteros positivos y sea R_2 la relación "divide" sobre el conjunto de todos los enteros.

$$\begin{array}{lll} \text{Para todos } a, b \in Z^+, & a\,R_1\,b & \Leftrightarrow \quad a \mid b. \\ \text{Para todos } a, b \in Z, & a\,R_2\,b & \Leftrightarrow \quad a \mid b. \end{array}$$

a. ¿Es R_1 antisimétrica? Demuestre o dé un contraejemplo.

b. ¿Es R_2 antisimétrica? Demuestre o dé un contraejemplo.

Solución

a. R_1 es antisimétrica.

Demostración:
Suponga que a y b son enteros positivos tal que $a\ R_1\ b$ y $b\ R_1\ a$. *[Debemos demostrar que $a = b$.]* Por definición de R_1, $a \mid b$ y $b \mid a$. Así, por definición de divide, existen los enteros k_1 y k_2 con $b = k_1 a$ y $a = k_2 b$. De lo que se deduce que

$$b = k_1 a = k_1(k_2 b) = (k_1 k_2)b.$$

Dividiendo ambos miembros entre b se obtiene

$$k_1 k_2 = 1.$$

Ahora puesto que a y b son ambos enteros positivos k_1 y k_2 son también ambos enteros positivos. Pero el único producto de dos enteros positivos que es igual a 1 es $1 \cdot 1$. Así

$$k_1 = k_2 = 1$$

y así $$a = k_2 b = 1 \cdot b = b.$$

[Esto es lo que se quería demostrar.]

b. R_2 no es antisimétrica.

Contraejemplo:
Sea $a = 2$ y $b = -2$. Entonces $a \mid b$ *[puesto que* $-2 = (-1) \cdot 2$*]* y $b \mid a$ *[puesto que* $2 = (-1)(-2)$*]*. Por tanto $a\ R_2\ b$ y $b\ R_2\ a$ pero $a \neq b$. ■

El ejemplo 8.5.2 muestra el hecho de que una relación puede ser antisimétrica sobre un subconjunto de un conjunto pero no antisimétrica en el conjunto mismo.

Relaciones de orden parcial

Una relación que es reflexiva, antisimétrica y transitiva se llama de *orden parcial*.

• Definición

Sea R una relación definida sobre un conjunto A. R es una **relación de orden parcial** si y sólo si, R es reflexiva, antisimétrica y transitiva.

Dos relaciones fundamentales de orden parcial son las relaciones "menor que o igual a" en un conjunto de números reales y la relación "subconjunto" en un conjunto de conjuntos. Éstas se pueden pensar como modelos o paradigmas, para relaciones generales de orden parcial.

Ejemplo 8.5.3 La relación "subconjunto"

Sea $\mathscr{A}$ cualquier colección de conjuntos y se define a la relación "subconjunto", $\subseteq$, sobre $\mathscr{A}$ como sigue: Para todos $U, V \in \mathscr{A}$,

$$U \subseteq V \quad \Leftrightarrow \quad \text{para toda } x, \text{ si } x \in U \text{ entonces } x \in V.$$

Por un argumento casi idéntico al de la solución para el ejercicio 23 de la sección 8.2, $\subseteq$ es reflexiva y transitiva. Se termina la demostración de que $\subseteq$ es una relación de orden parcial suponiendo que $\subseteq$ es antisimétrica.

Solución Que $\subseteq$ sea antisimétrica significa que para todos los conjuntos U y V en $\mathscr{A}$ si $U \subseteq V$ y $V \subseteq U$ entonces $U = V$. Pero esto es verdadero por definición de igualdad de conjuntos. ■

Ejemplo 8.5.4 La relación "divide" sobre el conjunto de enteros positivos

Sea $|$ la relación "divide" sobre el conjunto A de enteros positivos. Es decir, para todos $a, b \in A$,

$$a \mid b \quad \Leftrightarrow \quad b = ka \text{ para algún entero } k.$$

Demuestre que $|$ es una relación de orden parcial sobre A.

Solución

$|$ *es reflexiva:* *[Debemos demostrar que para todo $a \in A$, $a \mid a$.]* Suponga que $a \in A$. Entonces $a = 1 \cdot a$, así $a \mid a$ por definición de divisibilidad.

$|$ *es antisimétrica:* *[Debemos demostrar que para todo $a, b \in A$, si $a \mid b$ y $b \mid a$ entonces $a = b$.]* La demostración de esto es prácticamente idéntica a la del ejemplo 8.5.2*a*).

$|$ *es transitiva:* Demostrar transitividad significa demostrar que para todos $a, b, c \in$ A, si $a \mid b$ y $b \mid c$ entonces $a \mid c$. Pero esto se demostró como el teorema 4.3.3.

Puesto que $|$ es reflexiva, antisimétrica y transitiva, $|$ es una relación de orden parcial sobre A.

■

Ejemplo 8.5.5 La relación "menor que o igual a"

Sea S un conjunto de números reales y se define la relación "menor que o igual a", $\leq$, sobre S como sigue: Para todos los números reales x y y en S,

$$x \leq y \quad \Leftrightarrow \quad x < y \text{ o } x = y.$$

Demuestre que $\leq$ es una relación de orden parcial.

Solución

$\leq$ *es reflexiva:* Que $\leq$ sea reflexiva significa que $x \leq x$ para todos los números reales x en S. Pero $x \leq x$ significa que $x < x$ o $x = x$ y $x = x$ siempre es verdadero.

$\leq$ *es antisimétrica:* Que $\leq$ sea antisimétrica significa que para todos los números reales x y y en S, si $x \leq y$ y $y \leq x$ entonces $x = y$. Se deduce inmediatamente de la definición de $\leq$ y de la propiedad de tricotomía (vea el apéndice A, T17), que dice que dados cualesquiera números reales, x y y, exactamente se cumple uno de los siguientes enunciados: $x < y$ o $x = y$ o $x > y$.

$\leq$ *es transitiva:* Que $\leq$ sea transitiva significa que para todos los números reales x, y y z en S si $x \leq y$ y $y \leq z$ entonces $x \leq z$. Se deduce de la definición de $\leq$ y de la transitividad de la propiedad de orden (vea el apéndice A, TI8), que dice que dados cualesquiera números reales x, y y z, si $x < y$ y $y < z$ entonces $x < z$.

Ya que $\leq$ es reflexiva, antisimétrica y transitiva, ésta es una relación de orden parcial. ■

• Notación

Debido al papel paradigmático especial que juega la relación $\preceq$ en el estudio de las relaciones de orden parcial, el símbolo $\preceq$ se utiliza a menudo para hacer referencia a una relación parcial de orden general y la notación $x \preceq y$ se lee "x es menor que o igual a y" o "y es mayor que o igual a x".

Orden lexicográfico

Para averiguar cuál de las dos palabras aparece primero en un diccionario de inglés, usted compara sus letras una por una de izquierda a derecha. Si todas las letras son iguales a una determinada palabra la palabra sale de las letras, esa palabra aparece primero en el diccionario. Para ejemplo, la palabra *play* aparece antes que *playhouse*. Si todas las letras hasta un cierto punto son iguales y las siguientes letras difieren, entonces la palabra cuya letra siguiente se ubica antes en el alfabeto aparece primero en el diccionario. Por ejemplo, *playhouse* aparece antes que *playmate*.

Más generalmente, si A es cualquier conjunto con una relación de orden parcial, entonces un *diccionario* u orden *lexicográfico* se puede definir sobre un conjunto de cadenas sobre A como se indica en el siguiente teorema.

Teorema 8.5.1

Sea A un conjunto con una relación de orden parcial R y sea S un conjunto de cadenas sobre A. Se define una relación $\preceq$ sobre S como sigue:

Para cualesquiera dos cadenas en S, $a_1a_2 \cdots a_m$ y $b_1b_2 \cdots b_n$, donde m y n son enteros positivos,

1. Si $m \leq n$ y $a_i = b_i$ para toda $i = 1, 2, \ldots, m$, entonces
$$a_1a_2 \cdots a_m \preceq b_1b_2 \cdots b_n.$$
2. Si para algún entero k con $k \leq m$, $k \leq n$ y $k \geq 1$, $a_i = b_i$ para toda $i = 1, 2, \ldots, k-1$ y $a_k \neq b_k$ pero $a_k \, R \, b_k$ entonces
$$a_1a_2 \cdots a_m \preceq b_1b_2 \cdots b_n.$$
3. Si ε es la cadena nula y s es cualquier cadena en S, entonces $\varepsilon \preceq s$.

Si ninguna cadena está relacionada con otras por estas tres condiciones, entonces $\preceq$ es una relación de orden parcial.

La demostración del teorema 8.5.1 es técnica pero directa. Ésta se deja para los ejercicios.

• Definición

A la relación de orden parcial del teorema 8.5.1 se le llama el **orden lexicográfico para S** que corresponde al orden parcial R sobre A.

Ejemplo 8.5.6 Un orden lexicográfico

Sea $A = \{x, y\}$ y sea R la siguiente relación de orden parcial sobre A:

$$R = \{(x, x), (x, y), (y, y)\}.$$

Sea S el conjunto de todas las cadenas sobre A y se denota por $\preceq$ el orden lexicográfico para S que corresponde a R.

a. ¿Es $x \preceq xx$? $x \preceq xy$? $xx \preceq xxx$? $yxy \preceq yxyxxx$?

b. ¿Es $x \preceq y$? $xx \preceq xyx$? $xxxy \preceq xy$? $yxyxxyy \preceq yxyxy$?

c. ¿Es $\epsilon \preceq x$? $\epsilon \preceq xy$? $\epsilon \preceq yyxy$?

Solución

a. Sí en todos los casos, por la propiedad (1) de la definición de $\preceq$.

b. Sí en todos los casos, por la propiedad (2) de la definición de $\preceq$.

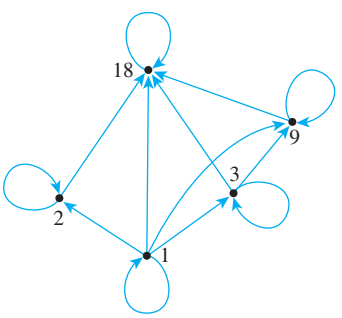
c. Sí en todos los casos, por propiedad (3) de la definición de $\preceq$. ■

Diagramas de Hasse

Sea $A = \{1, 2, 3, 9, 18\}$ y considere la relación "divide" sobre A: Para todos $a, b \in$ A,

$$a \mid b \quad \Leftrightarrow \quad b = ka \text{ para algún entero } k.$$

El grafo dirigido de esta relación tiene la siguiente apariencia:

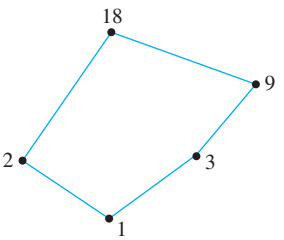


Observe que hay un bucle en cada vértice, todas las otras flechas apuntan en la misma dirección (hacia arriba) y en cualquier tiempo hay una flecha de un punto a un segundo y del segundo punto a un tercero, hay una flecha del primer punto al tercero. Dada cualquier relación de orden parcial, definida en un conjunto finito, es posible extraer el grafo dirigido de tal forma que de todas estas son propiedades satisfechas. Esto hace posible asociar un grafo algo más sencillo, llamado un **diagrama de Hasse** (debido a Helmut Hasse, un alemán teórico de números del siglo XX), con una relación de orden parcial definida en un conjunto finito. Después de obtener un diagrama de Hasse, proceda como sigue:

Iniciando con un grafo dirigido de la relación, colocando los vértices en la página así todas las flechas apuntan hacia arriba. Entonces eliminando

1. los bucles en todos los vértices,
2. todas las flechas cuya existencia es implícita por la propiedad transitiva,
3. los indicadores de dirección de las flechas.

Para la relación dada previamente, el diagrama de Hasse es el siguiente:



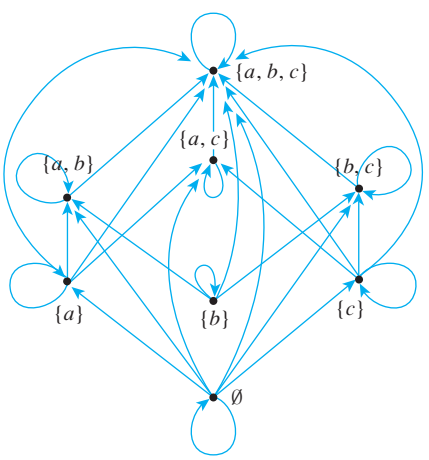
Ejemplo 8.5.7 Construcción de un diagrama de Hasse

Considere la relación "subconjunto", $\subseteq$, sobre el conjunto $\mathscr{P}(\{a, b, c\})$. Es decir, para todos los conjuntos U y V en $\mathscr{P}(\{a, b, c\})$,

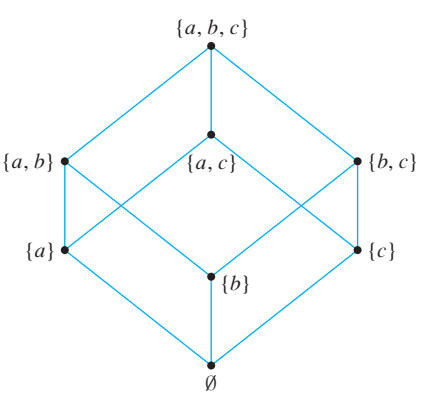
$$U \subseteq V \quad \Leftrightarrow \quad \forall x, \text{ si } x \in U \text{ entonces } x \in V.$$

Construya el diagrama de Hasse para esta relación.

Solución Dibuje el grafo dirigido de la relación de tal manera que todas las flechas excepto los bucles apunten hacia arriba.



Después se quitan todos los bucles, las flechas innecesarias, los indicadores de dirección y se obtiene el diagrama de Hasse.

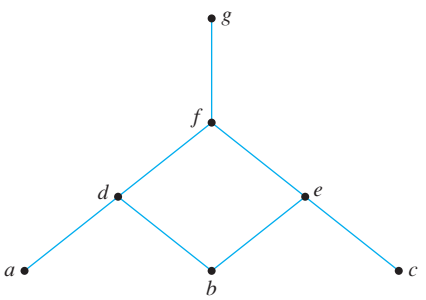


Para recuperar el grafo dirigido de una relación del diagrama de Hasse, sólo invierta las instrucciones dadas previamente, usando el conocimiento que el grafo dirigido original fue bosquejada de tal forma que todas las flechas apuntan hacia arriba:

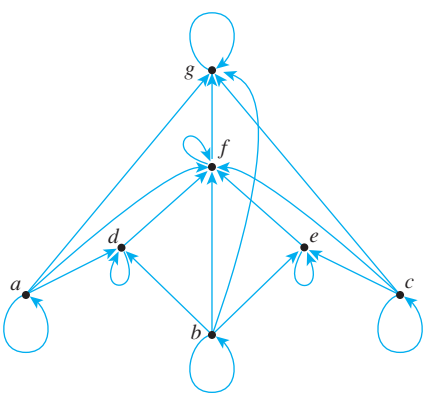
1. Vuelva a colocar los marcadores de la dirección de las flechas haciendo que todas las flechas apunten hacia arriba.
2. Agregue los bucles en cada vértice.
3. Para cada secuencia de flechas desde un punto a un segundo y desde el segundo punto a la tercera, añada una flecha del primer punto al tercero.

Ejemplo 8.5.8 Obtención del grafo dirigido de una relación de orden parcial del diagrama de Hasse de la relación

Una relación de orden parcial R tiene el siguiente diagrama de Hasse. Determine el grafo dirigido de R.



Solución



■

Conjuntos ordenados parcial y totalmente

Dados cualesquiera dos números reales x y y, ya sea $x \leq y$ o $y \leq x$. En una situación como esta, se dice que los elementos x y y son *comparables*. Por otra parte, dados dos subconjuntos A y B de $\{a, b, c\}$, puede darse el caso de que ni $A \subseteq B$ ni $B \subseteq A$. Por ejemplo, sea $A = \{a, b\}$ y $B = \{b, c\}$. Entonces $A \nsubseteq B$ y $B \nsubseteq A$. En tal caso, se dice que A y B son *no comparables*.

• Definición

Suponga que $\preceq$ es una relación de orden parcial sobre un conjunto A. Se dice que los elementos a y b de A son **comparables** si y sólo si, ya sea $a \preceq b$ o $b \preceq a$. De otra manera, a y b son llamados **no comparables.**

Cuando todos los elementos de una relación de orden parcial son comparables, la relación se llama *orden total*.

• Definición

Si R es una relación de orden parcial sobre un conjunto A y para cualesquiera dos elementos a y b en A ya sea $a\ R\ b$ o $b\ R\ a$, entonces R es una **relación de orden total** sobre A.

Tanto la relación "menor que o igual a" sobre conjuntos de números reales y el orden lexicográfico del conjunto de palabras en un diccionario son relaciones de orden total. Observe que el diagrama de Hasse para una relación de orden total se puede dibujar como una sola "cadena" vertical.

Muchas relaciones de orden parcial importantes tienen elementos que no son comparables y por tanto, no son relaciones de orden total. Por ejemplo, la relación subconjunto sobre $\mathscr{P}(\{a, b, c\})$ no es una relación de orden total ya que, como se demuestra previamente, los subconjuntos $\{a, b\}$ y $\{a, c\}$ de $\{a, b, c\}$ no son comparables. Además, una relación "divide" no es una relación de orden total a menos que los elementos sean todos potencias de un único entero. (Vea el ejercicio 21 al final de esta sección.)

Un conjunto A se llama un **conjunto parcialmente ordenado** (o **poset**) con respecto a una relación $\preceq$ si y sólo si, $\preceq$ es una relación de orden parcial sobre A. Por ejemplo, el conjunto de números reales es un conjunto parcialmente ordenado con respecto a la relación "menor que o igual a" $\leq$ y un conjunto de conjuntos está parcialmente ordenado con respecto a la relación "subconjunto" $\subseteq$. Se puede fácilmente demostrar que *cualquier subconjunto de un conjunto parcialmente ordenado está parcialmente ordenado*. (Vea el ejercicio 35 al final de esta sección.) Éste, por supuesto, supone la "misma definición" para la relación sobre el subconjunto como para el conjunto como un todo. Un conjunto A se llama un **conjunto totalmente ordenado** con respecto a una relación $\preceq$ si y sólo si, A está parcialmente ordenado con respecto a $\preceq$ y $\preceq$ está totalmente ordenado.

Un conjunto que está parcialmente ordenado, pero no totalmente ordenado puede tener subconjuntos totalmente ordenados. Dichos subconjuntos se llaman *cadenas*.

• Definición

Sea A un conjunto que es parcialmente ordenado con respecto a una relación $\preceq$. Un subconjunto B de A se llama una **cadena** si y sólo si, los elementos en cada par de elementos en B es comparable. En otras palabras, $a \preceq b$ o $b \preceq a$ para todos a y b en A. La **longitud de una cadena** es uno menos que el número de elementos en la cadena.

Observe que si B es una cadena en A, entonces B es un conjunto totalmente ordenado con respecto a la "restricción" de $\preceq$ a B.

Ejemplo 8.5.9 Una cadena de subconjuntos

El conjunto $\mathscr{P}(\{a, b, c\})$ es parcialmente ordenado con respecto a la relación subconjunto. Determine una cadena de longitud 3 en $\mathscr{P}(\{a, b, c\})$.

Solución Puesto que $\emptyset \subseteq \{a\} \subseteq \{a, b, \} \subseteq \{a, b, c\}$, el conjunto

$$S = \{\emptyset, \{a\}, \{a, b\}, \{a, b, c\}\}$$

es una cadena de longitud 3 en $\mathscr{P}(\{a, b, c\})$. ■

En el ejercicio 39 al final de esta sección, se le pide demostrar que un conjunto que es parcialmente ordenado con respecto a una relación $\preceq$ es totalmente ordenado con respecto a $\preceq$ si y sólo si, esta es una cadena.

Un *elemento máximo* en un conjunto parcialmente ordenado es un elemento, que es mayor que o igual a cada elemento con el *cual es comparable*. (Puede haber muchos elementos para los cuales este es *no* comparable). El *elemento mayor* en un conjunto parcialmente ordenado es un elemento que es mayor que o igual a *cada* elemento en el conjunto (así éste es comparable con cada elemento en el conjunto). Los elementos mínimos o menores se definen similarmente.

• Definición

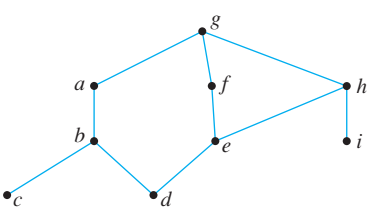
Sea un conjunto A parcialmente ordenado con respecto a una relación $\preceq$.

1. Un elemento a en A se llama un **elemento máximo de A** si y sólo si, para todo b en A, ya sea $b \preceq a$ o b y a son no comparables.
2. Un elemento a en A se llama un **elemento mayor de A** si y sólo si, para todo b en A, $b \preceq a$.
3. Un elemento a en A se llama un **elemento mínimo de A** si y sólo si, para todo b en A, ya sea $a \preceq b$ o b y a son no comparables.
4. Un elemento a en A se llama un **elemento menor de A** si y sólo si, para todo b en A, $a \preceq b$.

Un elemento mayor es máximo, pero un elemento máximo necesita no ser un elemento mayor. Sin embargo, cada subconjunto finito de un conjunto totalmente ordenado tiene tanto un elemento menor como un elemento mayor. (Vea el ejercicio 40 al final de la sección.) Similarmente, un elemento menor es mínimo, pero un elemento mínimo no necesita ser un elemento menor. Además, un conjunto que es parcialmente ordenado con respecto a una relación puede tener a lo más un elemento mayor y un elemento menor (vea el ejercicio 42 al final de la sección), pero puede tener más de un elemento máximo o mínimo. El siguiente ejemplo muestra algunos de estos hechos.

Ejemplo 8.5.10 Elementos máximo, mínimo, mayor y menor

Sea que $A = \{a, b, c, d, e, f, g, h, i\}$ tenga el ordenamiento parcial $\preceq$ definido por el siguiente diagrama de Hasse. Determine todos los elementos máximo, mínimo, mayor y menor de A.



Solución Hay exactamente un elemento máximo, g, que es también el elemento mayor. Los elementos mínimos son c, d e i y no hay elemento menor. ■

Ordenamiento topológico

¿Es posible introducir los conjuntos de $\mathscr{P}(\{a, b, c\})$ en una computadora en una forma que es *compatible* con la relación subconjunto $\subseteq$ en el sentido que si el conjunto U es un subconjunto del conjunto V, entonces U se introduce antes de V? La respuesta, lo que resulta, es sí. Por ejemplo, el siguiente orden de entrada satisface la condición dada:

$$\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}.$$

Otro orden de entrada que satisface la condición es

$$\emptyset, \{a\}, \{b\}, \{a, b\}, \{c\}, \{b, c\}, \{a, c\}, \{a, b, c\}.$$

• Definición

Dadas las relaciones de orden parcial $\preceq$ y $\preceq'$ en un conjunto A, $\preceq'$ es **compatible** con $\preceq$ si y sólo si, para todo a y b en A, si $a \preceq b$ entonces $a \preceq' b$.

Dada una relación arbitraria de orden parcial $\preceq$ sobre un conjunto A, ¿existe un orden total $\preceq'$ sobre A que es compatible con $\preceq$? Si el conjunto en el que se define el orden parcial es finito, entonces la respuesta es sí. Un orden total que es compatible con un orden dado se llama *ordenamiento topológico*.

• Definición

Dadas las relaciones de orden parcial $\preceq$ y $\preceq'$ sobre un conjunto A, $\preceq'$ es un **ordenamiento topológico** para $\preceq$ si y sólo si, $\preceq'$ es un orden total que es compatible con $\preceq$.

La construcción de un ordenamiento topológico para un conjunto finito general parcialmente ordenado se basa en el hecho de que *cualquier conjunto parcialmente ordenado que es finito y no vacío tiene un elemento mínimo*. (Vea el ejercicio 41 al final de la sección). Para crear un orden total para un conjunto parcialmente ordenado, simplemente elija cualquier elemento mínimo y hágalo el número uno. Después considere el conjunto que se obtiene cuando se quita este elemento. Puesto que el nuevo conjunto es un subconjunto de un conjunto parcialmente ordenado, es parcialmente ordenado. Si es vacío, pare el proceso. Si no, elija un elemento mínimo de éste y llame a ese elemento el número dos. Entonces considere el conjunto que se obtiene cuando se elimina este elemento. Si este conjunto es vacío, pare el proceso. Si no, elija un elemento mínimo y llámelo el número tres. Continúe de este modo hasta que todos los elementos del conjunto se hayan utilizado.

A continuación se presenta una versión un poco más formal del algoritmo:

Construcción de un ordenamiento topológico

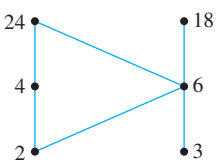
Sea $\preceq$ una relación de orden parcial sobre un conjunto finito no vacío A. Para construir un ordenamiento topológico,

1. Elija cualquier elemento mínimo x en A. *[Dicho elemento existe puesto que A es no vacío.]*
2. Sea $A' := A - \{x\}$.
3. Repita los pasos *a-c* en tanto $A' \neq \emptyset$.
   a. Elija cualquier elemento mínimo y en A'.
   b. Defina $x \preceq' y$.
   c. Sea $A' := A' - \{y\}$ y $x := y$.

[La terminación de los pasos 1-3 de este algoritmo proporciona suficiente información para construir el diagrama de Hasse para el ordenamiento total; $\preceq'$. Ya hemos demostrado cómo utilizar el diagrama de Hasse para obtener una gráfica dirigida completa para la relación.]

Ejemplo 8.5.11 Un ordenamiento topológico

Considere el conjunto $A = \{2, 3, 4, 6, 18, 24\}$ ordenado por la relación "divide" $|$. El diagrama de Hasse de esta relación es el siguiente:

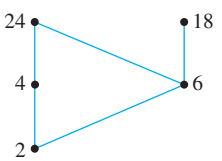


La relación común "menor que o igual a" $\leq$ en este conjunto es un ordenamiento topológico para este puesto que para los enteros positivos a y b, si $a \mid b$ entonces $a \leq b$. Determine otro ordenamiento topológico para este conjunto.

Solución El conjunto tiene dos elementos mínimos: 2 y 3. Ya sea que se elija uno; digamos que elija 3. El inicio del orden total es

$$\text{orden total: } 3.$$

Sea $A' = A - \{3\}$. Puede indicar esto eliminando 3 del diagrama de Hasse como se muestra a continuación.



Ahora elija un elemento mínimo de $A' - \{3\}$. Sólo 2 es mínimo, por lo que lo debe elegir. El orden total hasta aquí es

$$\text{orden total: } 3 \preceq 2.$$

Sea $A' = (A - \{3\}) - \{2\} = A - \{3, 2\}$. Puede indicarlo eliminando el 2 del diagrama de Hasse, como se muestra a continuación.

Elija un elemento mínimo de $A' - \{3, 2\}$. De nuevo tiene dos elecciones: 4 y 6. Digamos que elije 6. El orden total para los elementos elegidos hasta aquí es

$$\text{orden total: } 3 \preceq 2 \preceq 6.$$

Continúe de esta manera hasta que cada elemento de A se haya elegido. Una posible secuencia de elecciones da

$$\text{orden total: } 3 \preceq 2 \preceq 6 \preceq 18 \preceq 4 \preceq 24.$$

Puede comprobar que este orden es compatible con la relación de orden parcial "divide" al comprobar que para cada par de elementos a y b en A tal que $a \mid b$, entonces $a \preceq b$. Observe que éste *no es* el caso de que si $a < b$ entonces $a \mid b$. ■

Una aplicación

Regresando al ejemplo que se introdujo en esta sección, observe que la siguiente expresión define una relación de orden parcial sobre el conjunto de cursos requeridos para una carrera universitaria: Para todos los cursos requeridos x y y,

$$x \preceq y \quad \Leftrightarrow \quad x = y \quad \text{o} \quad x \text{ es un prerrequisito para } y$$

Si se dibuja el diagrama de Hasse para la relación, entonces las preguntas que se hacen al principio de esta sección se pueden responder fácilmente. Por ejemplo, considere el diagrama de Hasse para los requisitos en una universidad particular, que se muestra en la figura 8.5.1.

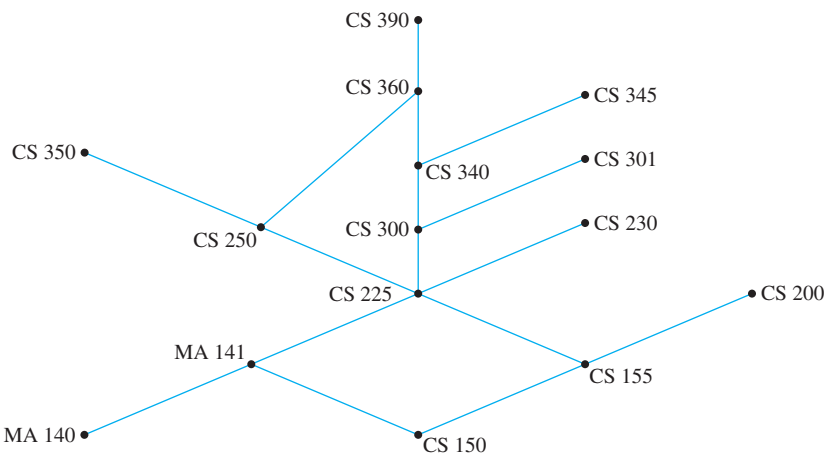


Figura 8.5.1

El número mínimo de ciclos escolares necesarios para completar los requisitos es el tamaño de una gran cadena, que es 7 (150, 155, 225, 300, 340, 360, 390, por ejemplo). El número máximo de cursos que se podrían tomar en el mismo ciclo (suponiendo que la universidad lo permita) es el número máximo de cursos no comparable, que es 6 (350, 360, 345, 301, 230, 200, por ejemplo). Un estudiante de tiempo parcial podría tomar los cursos en una secuencia dada construyendo un ordenamiento topológico para el conjunto. (Uno de dichos ordenamientos es 140, 150, 141, 155, 200, 225, 230, 300, 250, 301, 340, 345, 350, 360, 390. Hay muchos otros.)

PERT y CPM

Dos aplicaciones importantes y ampliamente usadas en las relaciones de orden parcial son **PERT** (Programa de evaluación y revisión técnica) y **CPM** (Método de trayectoria crítica). Estas técnicas surgieron en la década de 1950 y provienen de planificadores que se enfrentan con las complejidades de programación de las actividades individuales necesarias para completar proyectos muy grandes y aunque son muy similares, sus desarrollos fueron independientes. PERT fue desarrollado por la Armada de Estados Unidos para ayudar a organizar la construcción del submarino Polaris y el CPM fue desarrollado por la compañía E. I. Du Pont de Nemours para la programación de mantenimiento de la planta química. A continuación se presenta un ejemplo simplificado de la forma en que funcionan las técnicas.

Ejemplo 8.5.12 Un problema de programación de trabajo

En una planta de ensamblaje de automóviles, el trabajo de montaje de un automóvil puede desglosarse en estas tareas:

1. Construcción del marco.
2. Instalación de motor, componentes de la unidad de energía, tanque de gasolina.
3. Instalación de frenos, llantas, neumáticos.
4. Instalación del tablero de mandos, piso, asientos.
5. Instalación de las líneas eléctricas.
6. Instalación de líneas de gas.
7. Instalación de líneas de freno.
8. Acople del cuerpo a los paneles de la carrocería.
9. Pintado del cuerpo.

Algunas de estas tareas pueden llevarse a cabo al mismo tiempo, mientras que algunas no se pueden iniciar hasta que se han terminado las tareas. La tabla 8.5.1 resume el orden en las tareas que se pueden realizar y el tiempo necesario para realizar cada tarea.

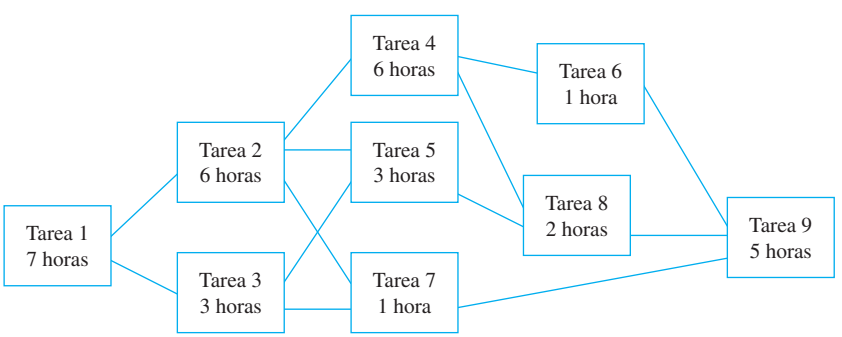
Tabla 8.5.1

Tarea	Tareas inmediatamente precedentes	Tiempo necesario para realizar una tarea
1		7 horas
2	1	6 horas
3	1	3 horas
4	2	6 horas
5	2, 3	3 horas
6	4	1 hora
7	2, 3	1 hora
8	4, 5	2 horas
9	6, 7, 8	5 horas

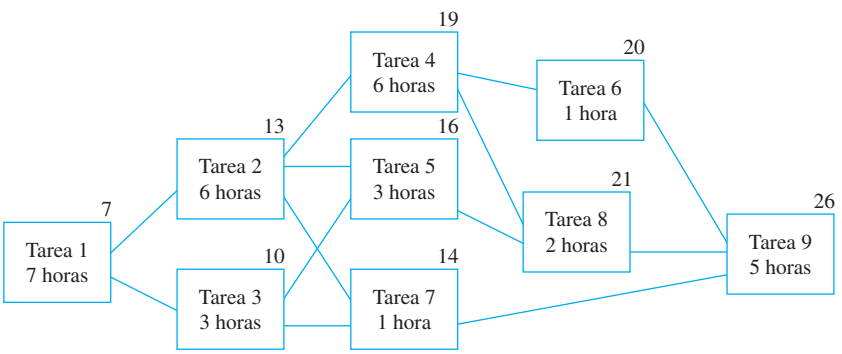
Sea T el conjunto de todas las tareas y considere la relación de orden parcial $\preceq$ que se define sobre T como sigue: Para todas las tareas x y y en T,

$$x \preceq y \quad \Leftrightarrow \quad x = y \text{ o } x \text{ precede a } y.$$

Si el diagrama de Hasse de esta relación es lateral (como se acostumbra en PERT y en el análisis CPM), tiene la apariencia que se muestra a continuación.



¿Cuál es el tiempo mínimo necesario para ensamblar un auto? Puede determinarlo trabajando de izquierda a derecha en el diagrama, observando para cada tarea (por ejemplo, justo arriba del cuadro se representa esa tarea) el tiempo mínimo necesario para completar esta tarea desde el principio del proceso de montaje. Por ejemplo, puede poner un 7 arriba del cuadro ya que la tarea 1 requiere 7 horas. La tarea 2 requiere la terminación de la tarea 1 (7 horas) más 6 horas para sí misma, así el tiempo mínimo necesario para completar la tarea 2, empezando desde comienzo del proceso ensamblaje, es de $7 + 6 = 13$ horas. Puede colocar un 13 arriba del cuadro para la tarea 2. Similarmente, puede poner un 10 arriba del cuadro para la tarea 3 ya que $7 + 3 = 10$. Ahora considere qué número debe escribir arriba del cuadro para la tarea 5. El mínimo de veces para completar las tareas 2 y 3, desde el comienzo del proceso ensamblaje, son 13 y 10 horas respectivamente. Puesto que *ambas* tareas deben completarse antes de que inicie la tarea 5, el tiempo mínimo para completar la tarea 5, desde el principio, es el tiempo mínimo para la tarea 5 misma (3 horas) más el tiempo máximo de los tiempos para completar las tareas 2 y 3 (13 horas) y esto es igual a $3 + 13 = 16$ horas. Así se debe colocar el número 16, arriba del cuadro de la tarea 5. El mismo razonamiento le lleva a colocar un 14 arriba de la tarea 7. Similarmente, se puede colocar un 19 arriba de la tarea 4, un 20 arriba la tarea 6, un 21 arriba de la tarea 8 y un 26 arriba de la tarea 9, como se muestra a continuación.



Este análisis muestra que se requieren al menos de 26 horas para completar la tarea 9 desde el comienzo del proceso de ensamblaje. Una vez finalizada la tarea 9, el ensamblaje es completo, así 26 horas es el tiempo mínimo necesario para realizar todo el proceso.

Observe que el tiempo mínimo necesario para completar las tareas 1, 2, 4, 8 y 9 en secuencia es exactamente 26 horas. Esto significa que un retraso en la realización de cualquiera de estas tareas causa un retraso en el tiempo total requerido para el ensamblaje del auto. Por esta razón, la ruta de acceso a través de las tareas 1, 2, 4, 8 y 9 se llama una **ruta crítica**. ■

Autoexamen

1. Que una relación R sobre un conjunto A sea antisimétrica significa que _____.
2. Para demostrar que una relación R en un conjunto infinito A es antisimétrica, suponga que _____ y demuestre que _____.
3. Para demostrar que una relación R sobre un conjunto A es no antisimétrica, usted _____.
4. Para construir un diagrama de Hasse para una relación de orden parcial, inicie con una gráfica dirigida de la relación en la que todas las flechas apuntan hacia arriba y elimine _____, _____ y _____.
5. Si A es un conjunto que es parcialmente ordenado con respecto a un relación $\preceq$ y si a y b son elementos de A, decimos que a y b son comparables si y sólo si, _____ o _____.
6. Una relación $\preceq$ en un conjunto A es de orden total si y sólo si, _____.
7. Si A es un conjunto que es parcialmente ordenado con respecto a una relación $\preceq$ y si B es un subconjunto de A, entonces B es una cadena si y sólo si, para todos a y b en B, _____.

8. Sea A un conjunto que es parcialmente ordenado con respecto a una relación $\preceq$ y sea a un elemento de A.
   a. a es máximo si y sólo si, _____.
   b. a es un elemento mayor de A si y sólo si, _____.
   c. a es mínimo si y sólo si, _____.
   d. a es un elemento menor de A si y sólo si, _____.

9. Dado un conjunto A que es parcialmente ordenado con respecto a una relación $\preceq$, la relación $\preceq'$ es un ordenamiento topológico para $\preceq$, si y sólo si, $\preceq'$ es un _____ y para todos a y b en A si $a \preceq b$ entonces _____.

10. PERT y CPM son utilizados para producir _____eficientes.

Conjunto de ejercicios 8.5

1. Cada una de las siguientes es una relación sobre $\{0, 1, 2, 3\}$. Dibuje los grafos dirigidos para cada relación, e indique qué relaciones son antisimétricas.
   a. $R_1 = \{(0, 0), (0, 2), (1, 0), (1, 3), (2, 2), (3, 0), (3, 1)\}$
   b. $R_2 = \{(0, 1), (0, 2), (1, 1), (1, 2), (1, 3), (2, 2), (3, 2)\}$
   c. $R_3 = \{(0, 0), (0, 3), (1, 0), (1, 3), (2, 2), (3, 3), (3, 2)\}$
   d. $R_4 = \{(0, 0), (1, 0), (1, 2), (1, 3), (2, 0), (2, 1), (3, 2), (3, 0)\}$

2. Sea P el conjunto de todas las personas en el mundo y se define una relación R sobre P como sigue: Para todos $x, y \in P$,

$$x\ R\ y \quad \Leftrightarrow \quad x \text{ no tiene más edad que } y.$$

¿Es R antisimétrica? Demuestre o dé un contraejemplo.

3. Sea S el conjunto de todas las cadenas de a y b. Se define una relación R sobre S como sigue: Para toda $t \in S$,

$$s\ R\ t \quad \Leftrightarrow \quad l(s) \leq l(t),$$

donde $l(x)$ denota la longitud de una cadena x. ¿Es R antisimétrica? Demuestre o dé un contraejemplo.

4. Sea R la relación "menor que" sobre el conjunto $\mathbf{R}$ de todos los números reales: Para todos $x, y \in \mathbf{R}$,

$$x\ R\ y \quad \Leftrightarrow \quad x < y.$$

¿Es R antisimétrica? Demuestre o dé un contraejemplo.

5. Sea $\mathbf{R}$ el conjunto de todos los números reales y se define una relación R sobre $\mathbf{R} \times \mathbf{R}$ como sigue: Para todos (a, b) y (c, d) en $\mathbf{R} \times \mathbf{R}$,

$$(a, b)\ R\ (c, d) \quad \Leftrightarrow \quad \text{ya sea } a < c \text{ o ambas } a = c \text{ y } b \leq d.$$

¿Es R una relación de orden parcial? Demuestre o dé un contraejemplo.

6. Sea P el conjunto de todas las personas que han vivido y se define una relación R sobre P como sigue: Para toda $r, s \in P$,

$$r\ R\ s \quad \Leftrightarrow \quad r \text{ es un antepasado de } s \text{ o } r = s.$$

¿Es R una relación de orden parcial? Demuestre o dé un contraejemplo.

7. Se define una relación R sobre el conjunto $\mathbf{Z}$ de todos los enteros como sigue: Para todos $m, n \in \mathbf{Z}$,

$$m\ R\ n \quad \Leftrightarrow \quad \text{cada factor primo de } m \text{ es un factor primo de } n.$$

¿Es R una relación de orden parcial? Demuestre o dé un contraejemplo.

8. Se define una relación R sobre el conjunto $\mathbf{Z}$ de todos los enteros como sigue: Para todos $m, n \in \mathbf{Z}$,

$$m\ R\ n \quad \Leftrightarrow \quad m + n \text{ es par.}$$

¿Es R una relación de orden parcial? Demuestre o dé un contraejemplo.

9. Se define una relación R sobre el conjunto de todos los números reales $\mathbf{R}$ como sigue: Para todos $x, y \in \mathbf{R}$,

$$x\ R\ y \quad \Leftrightarrow \quad x^2 \leq y^2.$$

¿Es R una relación de orden parcial? Demuestre o dé un contraejemplo.

10. Suponga que R y S son relaciones antisimétricas sobre un conjunto A. ¿Debe $R \cup S$ también ser antisimétrica? Explique.

11. Sea $A = \{a, b\}$ y suponga que A tiene la relación de orden parcial R donde $R = \{(a, a), (a, b), (b, b)\}$. Sea S el conjunto de todas las cadenas de a y de b y sea $\preceq$ el correspondiente orden lexicográfico sobre S. Indique cuáles de los siguientes enunciados son verdaderos y para cada enunciado verdadero cite como una razón los incisos 1), 2) o 3) de la definición de orden lexicográfico dada en el teorema 8.5.1.
   a. $aab \preceq aaba$
   b. $bbab \preceq bba$
   c. $\epsilon \preceq aba$
   d. $aba \preceq abb$
   e. $bbab \preceq bbaa$
   f. $ababa \preceq ababaa$
   g. $bbaba \preceq bbabb$

12. Demuestre el teorema 8.5.1.

13. Sea $A = \{a, b\}$. Describa todas las relaciones de orden parcial sobre A.

14. Sea $A = \{a, b, c\}$.
   a. Describa todas las relaciones de orden parcial sobre A para las que a es un elemento máximo.
   b. Describa todas las relaciones de orden parcial sobre A para las que a es un elemento mínimo.

***H* 15.** Suponga que una relación R sobre un conjunto A es reflexiva, simétrica, transitiva y antisimétrica. ¿Qué puede concluir acerca de R? Demuestre su respuesta.

16. Considere la relación "divide" en cada uno de los siguientes conjuntos A. Dibuje el diagrama de Hasse para cada relación.
   a. $A = \{1, 2, 4, 5, 10, 15, 20\}$
   b. $A = \{2, 3, 4, 6, 8, 9, 12, 18\}$

17. Considere la relación "subconjunto" sobre $\mathscr{P}(S)$ para cada uno de los siguientes conjuntos S. Dibuje el diagrama de Hasse para cada relación.
   a. $S = \{0, 1\}$
   b. $S = \{0, 1, 2\}$

18. Sea $S = \{0, 1\}$ y considere la relación de orden parcial R definida en $S \times S$ como sigue: Para todos los pares ordenados (a, b) y (c, d) en $S \times S$,

$$(a, b)\ R\ (c, d) \quad \Leftrightarrow \quad \text{ya sea } a < c \text{ o ambos } a = c \text{ y } b \leq d,$$

donde $<$ denota la relación usual "menor que" y $\leq$ denota la relación común "menor que o igual a" para números reales. Dibuje el diagrama de Hasse para R.

19. Sea $S = \{0, 1\}$ y considere la relación de orden parcial R, defina sobre $S \times S$ como sigue: Para todos los pares ordenados (a, b) y (c, d) en $S \times S$,

$$(a, b)\ R\ (c, d) \quad \Leftrightarrow \quad a \leq c \text{ y } b \leq d,$$

donde $\leq$ denota la relación usual "menor que o igual a" para números reales. Dibuje el diagrama de Hasse para R.

20. Sea $S = \{0, 1\}$ y considere la relación de orden parcial R definida sobre $S \times S \times S$ como sigue: Para todas las tripletas ordenadas (a, b, c) y (d, e, f) en $S \times S \times S$,

$$(a, b, c)\ R\ (d, e, f) \quad \Leftrightarrow \quad a \leq d, b \leq e \text{ y } c \leq f,$$

donde $\leq$ denota la relación usual "menor que o igual a" para números reales. Dibuje el diagrama de Hasse para R.

21. Considere la relación "divide" que se define en el conjunto $A = \{1, 2, 2^2, 2^3, \ldots, 2^n\}$, donde n es un entero no negativo.
a. Demuestre que esta relación es una relación de orden total sobre A.
b. Dibuje el diagrama de Hasse para esta relación para $n = 4$.

En los ejercicios 22 al 29, determine el elemento mayor, el menor, el máximo y el mínimo para las relaciones en cada uno de los ejercicios mencionados.

22. Ejercicio 16*a*)
23. Ejercicio 16*b*)
24. Ejercicio 17*a*)
25. Ejercicio 17*b*)
26. Ejercicio 18
27. Ejercicio 19
28. Ejercicio 20
29. Ejercicio 21

30. Cada uno de los siguientes conjuntos está parcialmente ordenado con respecto a la relación "menor que o igual a", $\leq$, para números reales. En cada clase, determine si el conjunto tiene un elemento mayor o menor.
a. $\mathbf{R}$
b. $\{x \in \mathbf{R} \mid 0 \leq x \leq 1\}$
c. $\{x \in \mathbf{R} \mid 0 < x < 1\}$
d. $\{x \in \mathbf{Z} \mid 0 < x < 10\}$

31. Sea $A = \{a, b, c, d\}$ y sea R la relación

$$R = \{(a, a), (b, b), (c, c), (d, d), (c, a), (a, d), (c, d), (b, c), (b, d), (b, a)\}.$$

¿Es R una relación de orden total sobre A? Justifique su respuesta.

32. Sea $A = \{a, b, c, d\}$ y sea R la relación

$$R = \{(a, a), (b, b), (c, c), (d, d), (c, b), (a, d), (b, a), (b, d), (c, d), (c, a)\}.$$

¿Es R una relación de orden total sobre A? Justifique su respuesta.

33. Considere el conjunto $A = \{12, 24, 48, 3, 9\}$ ordenado por la relación "divide". ¿Está A totalmente ordenado con respecto a la relación? Justifique su respuesta.

H* 34.** Suponga que R es una relación de orden parcial sobre un conjunto A y que B es un subconjunto de A. La **restricción de *R* a *B se define como sigue:

La restricción de R a B

$$= \{(x, y) \mid x \in B, y \in B \text{ y } (x, y) \in R\}.$$

En otras palabras, dos elementos de B están relacionados por la restricción de R a B si y sólo si, están relacionados por R. Demuestre que la restricción de R a B es una relación de orden parcial sobre B. (En lenguaje menos formal, se dice que un subconjunto de un conjunto parcialmente ordenado es parcialmente ordenado).

35. El conjunto $\mathscr{P}(\{w, x, y, z\})$ es parcialmente ordenado con respecto a la relación "subconjunto" $\subseteq$. Determine una cadena de longitud 4 en $\mathscr{P}(\{w, x, y, z\})$.

36. El conjunto $A = \{2, 4, 3, 6, 12, 18, 24\}$ es parcialmente ordenado con respecto a la relación "divide". Determine la cadena de longitud 3 en A.

37. Determine la cadena de longitud 2 para la relación definida en el ejercicio 19.

38. Demuestre que un conjunto parcialmente ordenado es totalmente ordenado si y sólo si, es una cadena.

39. Suponga que A es un conjunto totalmente ordenado. Use inducción matemática para demostrar que para cualquier entero $n \geq 1$, cada subconjunto de A con n elementos tiene tanto un elemento menor como un elemento mayor.

40. Demuestre que un conjunto finito no vacío parcialmente ordenado tiene
a. al menos un elemento mínimo,
b. al menos un elemento máximo.

41. Demuestre que un conjunto finito parcialmente ordenado tiene
a. a lo más un elemento mayor,
b. a lo más un elemento menor.

42. Dibuje un diagrama de Hasse para un conjunto parcialmente ordenado que tiene dos elementos máximos y dos elemento mínimos y es tal que cada elemento es comparable con exactamente otros dos elementos.

43. Dibuje un diagrama de Hasse para un conjunto parcialmente ordenado que tiene tres elementos máximos y tres elementos mínimos y es tal que cada elemento es, ya sea mayor que o menor, que exactamente otros dos elementos.

44. Use el algoritmo dado en el libro para determinar un ordenamiento topológico para la relación del ejercicio 16*a*) que es diferente de la relación "menor que o igual a" $\leq$.

45. Use el algoritmo dado en el libro para determinar un ordenamiento topológico para la relación del ejercicio 16*b*) que es diferente de la relación "menor que o igual a" $\leq$.

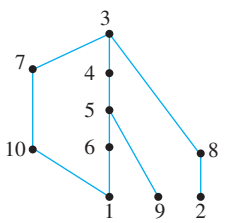
46. Use el algoritmo dado en el libro para determinar un ordenamiento topológico para la relación del ejercicio 19.

47. Use el algoritmo dado en el libro para determinar un ordenamiento topológico para la relación del ejercicio 20.

48. Use el algoritmo dado en el libro para determinar un ordenamiento topológico para la relación "subconjunto" sobre $\mathscr{P}(\{a, b, c, d\})$.

49. Consulte la estructura de prerrequisitos que se muestra en la figura 8.5.1.
    a. Determine una lista de seis cursos no comparables que es diferente de la lista dada en el texto.
    b. Determine dos ordenamientos topológicos que sean diferentes del dado en el libro.

50. Un conjunto de trabajos S se pueden ordenar y escribir $x \preceq y$ que significa que ya sea $x = y$ o x debe estar hecho antes de y, para todos x y y en S. El siguiente es un diagrama de Hasse para esta relación para un conjunto de trabajos dado S.



a. Si una persona realiza todos los trabajos, uno después de otro determine un orden en el que se deben realizar los trabajos.

b. Suponga que hay bastantes personas disponibles para realizar cualquier número de trabajos simultáneamente.
   (i) Si cada trabajo requiere un día para realizarse, ¿cuál es el menor número de días necesarios para realizar todos los trabajos?
   (ii) ¿Cuál es el número máximo de trabajos que se pueden realizar al mismo tiempo?

51. Suponga que las tareas descritas en el ejemplo 8.5.12 requieren los siguientes tiempos de realización:

Tarea	Tiempo necesario para realizar las tareas
1	9 horas
2	7 horas
3	4 horas
4	5 horas
5	7 horas
6	3 horas
7	2 horas
8	4 horas
9	6 horas

a. ¿Cuál es el tiempo mínimo requerido para ensamblar un auto?
b. Determine una trayectoria crítica para el proceso de ensamble.

Respuestas del autoexamen

1. para todos a y b en A, si $a\ R\ b$ y $b\ R\ a$ entonces $a = b$ 2. a y b son cualesquier elementos de A con $a\ R\ b$ y $b\ R\ a$; $a = b$ 3. demuestre que hay elementos a y b en A tal que $a\ R\ b$ y $b\ R\ a$ y $a \neq b$ 4. todos los bucles; todas las flechas cuya existencia es implicada por la propiedad transitiva; los indicadores de dirección en las flechas 5. $a \preceq b$; $b \preceq a$ 6. para cualesquiera dos elementos a y b en A, ya sea $a \preceq b$ o $b \preceq a$ 7. a y b son comparables 8. *a*) para toda b en A ya sea $b \preceq a$ o b y a no son comparables *b*) para toda b en A, $b \preceq a$ *c*) para toda b en A ya sea $a \preceq b$ o b y a no son comparables *d*) para toda b en A, $a \preceq' b$ 9. orden total; $a \preceq' b$ 10. programación de tareas

CAPÍTULO 9

CONTEO Y PROBABILIDAD

"Es tan fácil como 1-2-3".

Esto es lo que se dice. Y en cierta forma, el conteo *es* fácil. Pero otros aspectos del conteo no son tan simples. ¿Ha quedado de acuerdo de encontrarse con un amigo "en tres días" y ¿entonces se dio cuenta que para usted y para su amigo esto puede significar cosas diferentes? Por ejemplo, en el continente europeo, reunirse en ocho días significa encontrarse el mismo día que el día de hoy pero una semana después; por otro lado, en países de habla inglesa encontrarse en siete días significa encontrarse una semana después. La diferencia es que en el continente, todos los días incluyendo el primero y el último se cuentan. En el mundo de habla inglesa, es el número de periodos de 24 horas los que se cuentan.

Países continentales	1	2	3	4	5	6	7	8
	↕	↕	↕	↕	↓	↕	↕	↕
	Dom	Lun	Mar	Miér	Jue	Vie	Sáb	Dom
Países de habla inglesa		1	2	3	4	5	6	7

La convención inglesa para el conteo de días sigue la convención casi universal del conteo de horas. Si son las 9 de la mañana y dos personas en algún lugar del mundo concuerdan con reunirse en tres horas, significa que se encontrarán de nuevo a las 12 del mediodía.

Por otro lado, los intervalos musicales, universalmente se calculan de la manera que se hace el conteo continental de los días de la semana. Un intervalo de un tercer consta de dos tonos con un único tono entre ellos y un intervalo de un segundo consta de dos tonos adyacentes. (Vea la figura 9.1.1.)

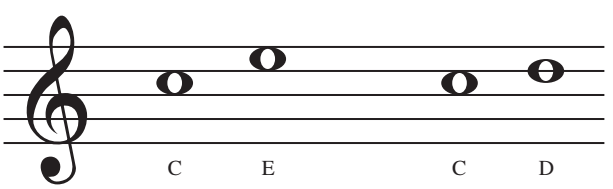


Figura 9.1.1

Por supuesto, el factor que se complicaba en todos estos ejemplos no es cómo contar sino más bien lo que se cuenta. Y, de hecho, en los problemas matemáticos de conteo más complejos analizados en este capítulo, lo que se cuenta es la cuestión central. Una vez que uno sabe exactamente qué contar, el conteo en sí mismo es tan fácil como 1-2-3.

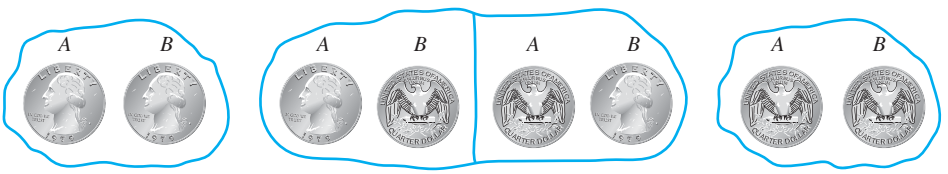
9.1 Introducción

Imagine que se lanzan dos monedas y observa si se obtienen 0, 1 o 2 caras. Sería natural intuir que cada uno de estos eventos se produce en un tercio de las veces, pero en realidad no es así. La tabla 9.1.1 que se muestra a continuación se obtuvo con datos reales obtenidos al lanzar dos monedas de 25 centavos 50 veces.

Tabla 9.1.1 Datos experimentales obtenidos del lanzamiento 50 veces de dos monedas de 25 centavos

Evento	Conteo	Frecuencia (número de veces que se ha producido el evento)	Frecuencia relativa (fracción de veces que se ha producido el evento)
2 caras obtenidas	𝍸 𝍸 |	11	22%
1 cara obtenida	𝍸 𝍸 𝍸|𝍸 𝍸 ||	27	54%
0 caras obtenidas	𝍸 𝍸 ||	12	24%

Como puede ver, la frecuencia relativa de obtener exactamente 1 cara fue aproximadamente dos veces mayor que la de obtener 2 caras o 0 caras. Resulta que la teoría matemática de la probabilidad puede utilizarse para predecir que casi siempre se producirá un resultado así. Para ver cómo, llame a las dos monedas *A* y *B* y suponga que cada una está perfectamente balanceada. Entonces, cada una tiene la misma probabilidad de obtener caras o cruces y cuando se lanzan las dos juntas, se obtienen los cuatro resultados que se muestran en la figura 9.1.2 que son equiprobables.



se obtienen 2 caras se obtiene 1 cara se obtienen 0 caras

Figura 9.1.2 Resultados equiprobables del lanzamiento de dos monedas balanceadas

La figura 9.1.2 muestra que hay 1 de cada 4 posibilidades de obtener dos caras y 1 de 4 posibilidades de no obtener caras. Sin embargo, la posibilidad de obtener una cara, es de 2 en 4 ya que *A* podría ser cara y *B* cruz o *B* podría ser cara y *A* cruz. Así que si repetidamente se lanzan dos monedas balanceadas y se registra el número de caras, se deben esperar frecuencias similares a las que se muestran en la tabla 9.1.1.

Para formalizar este análisis y extenderlo a situaciones más complejas, presentamos los conceptos de proceso aleatorio, espacio muestral, evento y probabilidad. Decir que el proceso es **aleatorio** significa que cuando se realiza, es seguro que se produzca un resultado de un conjunto de resultados, pero es imposible predecir con certeza qué resultado será. Por ejemplo, si una persona común realiza el experimento de lanzar al aire una moneda común y la deja caer al suelo, se puede predecir con certeza que cuando caiga la moneda será cara o cruz (así el conjunto de resultados se puede ser denotar como {cara, cruz}), pero no se sabe con certeza si se producirá cara o cruz. Hemos restringido este experimento a gente común porque un mago hábil puede lanzar una moneda de una forma que parece aleatoria, pero que no lo es y un físico equipado con dispositivos de medición de primer nivel puede ser capaz de analizar todas las fuerzas de la moneda y predecir correctamente su posición al caer. Algunos de los muchos ejemplos de procesos aleatorios o experimentos son la opción para los ganadores de la lotería, la selección de entrevistados en una encuesta de opinión pública y la elección de temas para recibir tratamientos o servir como control en experimentos médicos. El conjunto de resultados que puede dar como resultado un proceso aleatorio o experimento se llama un *espacio muestral*.

• Definición

Un **espacio muestral** es el conjunto de todos los posibles resultados de un proceso aleatorio o experimento. Un **evento** es un subconjunto de un espacio muestral.

En caso de que un experimento tenga muchos resultados finitos y todos los resultados son equiprobables, la *probabilidad* de un evento (conjunto de resultados) es exactamente la razón entre el número de resultados en el evento y el número total de resultados. Estrictamente hablando, este resultado se puede deducir de un conjunto de axiomas de probabilidad formulados en 1933 por el matemático ruso A. N. Kolmogorov. En la sección 9.8 analizamos los axiomas y mostramos cómo deducir sus consecuencias formalmente. En la actualidad, tomamos un enfoque ingenuo de la probabilidad y simplemente establecemos el resultado como un principio.

Fórmula de probabilidad de eventos equiprobables

Si S es un espacio muestral finito en el que todos los resultados son equiprobables y E es un evento en S, entonces la **probabilidad de *E***, se denota por ***P*(*E*)**, es

$$P(E) = \frac{\text{el número de resultados en } E}{\text{el número total de resultados en } S}.$$

• Notación

Para cualquier conjunto finito A, $N(A)$ indica el número de elementos en A.

Con esta notación, la fórmula de probabilidad de eventos equiprobables será

$$P(E) = \frac{N(E)}{N(S)}.$$

Ejemplo 9.1.1 Probabilidades en una baraja de cartas

Una baraja ordinaria de cartas contiene 52 cartas divididas en cuatro *palos*. Los *palos rojos* son diamantes (♦) y corazones (♥) y los *palos negros* son tréboles (♣) y espadas (♠). Cada palo contiene 13 tarjetas de las *denominaciones* siguientes: 2, 3, 4, 5, 6, 7, 8, 9, 10, J (sota), Q (reina), K (rey) y *A* (as). Las cartas J, Q y K se llaman *cartas de cara*.

El matemático Persi Diaconis, trabajando con David Aldous en 1986 y Dave Bayer en 1992, demostraron que se necesitan siete barajeadas para "mezclar completamente" las cartas de una baraja normal. En el 2000 el matemático Nick Trefethen, al trabajar con su padre, Lloyd Trefethen, un ingeniero mecánico, utilizaba una definición diferente para "mezclar completamente" al demostrar que seis barajeadas serán casi siempre suficientes. Imagine que las cartas en una baraja, por algún método, se han mezclado completamente hasta que usted las coloca boca abajo y elige una aleatoriamente, puede obtener ya sea una u otra carta.

a. ¿Cuál es el espacio muestral de los resultados?

b. ¿Cuál es el evento de que la carta elegida es una carta de cara negra?

c. ¿Cuál es la probabilidad de que la carta elegida es una carta de cara negra?

Solución

a. Los resultados en el espacio muestral S son las 52 cartas de la baraja.

b. Sea E el evento de que se elige una carta de cara negra. Los resultados en E son la sota, la reina y el rey de tréboles y la sota, la reina y el rey de espadas. Simbólicamente,

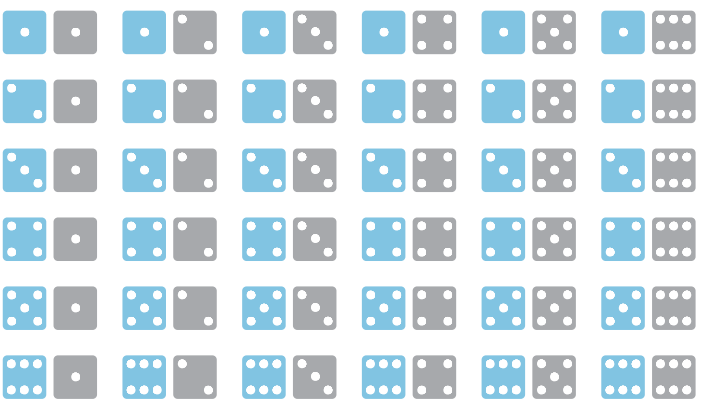
$$E = \{\text{J}\clubsuit, \text{Q}\clubsuit, \text{K}\clubsuit, \text{J}\spadesuit, \text{Q}\spadesuit, \text{K}\spadesuit\}.$$

c. Por el inciso b), $N(E) = 6$ y de acuerdo con la descripción de la situación, los 52 resultados en el espacio muestral son equiprobables. Por tanto, por la fórmula de probabilidad de eventos equiprobables, la probabilidad de que la carta elegida sea una carta de cara negra es

$$P(E) = \frac{N(E)}{N(S)} = \frac{6}{52} \cong 11.5\%.$$ ■

Ejemplo 9.1.2 Lanzamiento de un par de dados

Un dado es uno de un par de dados. Es un cubo con seis lados, que tienen de uno a seis puntos, llamados *pepitas*. Supongamos que un dado azul y un dado gris se tiran juntos y se registra el número de puntos que presentan en la cara de arriba de cada uno. Los posibles resultados se pueden enumerar como se muestra a continuación, donde en cada caso el dado de la izquierda es azul y el de la derecha es gris.



Una notación más compacta identifica, por ejemplo,  con la notación 24,  con 53 y así sucesivamente.

a. Utilice la notación compacta para escribir el espacio muestral S de posibles resultados.

b. Use la notación de conjunto para escribir el evento E que los números que se muestran cara arriba suman 6 y encuentre la probabilidad de este evento.

Solución

a. $S = \{11, 12, 13, 14, 15, 16, 21, 22, 23, 24, 25, 26, 31, 32, 33, 34, 35, 36, 41, 42, 43, 44, 45, 46, 51, 52, 53, 54, 55, 56, 61, 62, 63, 64, 65, 66\}$.

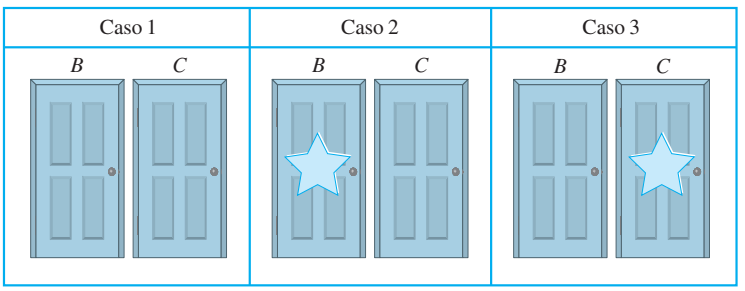
b. $E = \{15, 24, 33, 42, 51\}$.

La probabilidad de que la suma de los números es $6 = P(E) = \dfrac{N(E)}{N(S)} = \dfrac{5}{36}$. ■

El ejemplo siguiente se llama el problema de *Monty Hall* en honor al conductor de un viejo programa de concursos, "Hagamos un trato". Cuando originalmente se publicó en la columna de un periódico y en un programa de radio, generó gran controversia. Mucha gente altamente educada, aún algunos con doctorado, presentaron soluciones incorrectas o argumentaron fuertemente en contra de la solución correcta. Antes de leer la respuesta, piense cuál sería su respuesta a la situación.

Ejemplo 9.1.3 El problema de *Monty Hall*

Hay tres puertas en el escenario de un programa de juegos. Llamadas A, B y C. Si selecciona la puerta derecha gana el premio. Selecciona la puerta A. El conductor del programa, *Monty Hall*, abre una de las otras dos y revela que no hay ningún premio detrás de ésta. Mantiene las restantes dos puertas cerradas, le pregunta si desea cambiar su elección a la otra puerta cerrada o si permanece con su elección original de puerta A. ¿Qué debe hacer si desea maximizar su oportunidad de ganar el premio: permanecer en la puerta A o cambiar, o de cualquier forma la probabilidad de ganar sería la misma?



Solución En el momento justo antes de que el conductor abra una de las puertas cerradas, no hay información acerca de la ubicación del premio. Por tanto hay tres posibilidades equiprobables para lo que está detrás de las puertas: (Caso 1) el premio está detrás de A (es decir, no está detrás de B o C), (Caso 2) el premio está detrás de B; (Caso 3) el premio está detrás de C.

Ya que no hay ningún premio detrás de la puerta el conductor la abre, en el caso 1 el conductor podría abrir cualquier puerta y ganaría quedándose con su elección original: puerta A. En el caso 2 el conductor debe abrir la puerta C y así podría ganar cambiando a la puerta B. En el caso 3 el conductor debe abrir la puerta B y así podría ganar cambiando a la puerta C. Así, en dos de los tres casos equiprobables, ganaría con el cambio a la otra puerta cerrada. Sólo en uno de los tres casos equiprobables ganaría quedándose con su elección original. Por tanto, debe cambiar.

Una nota real: El análisis utilizado para esta solución se aplica sólo si el conductor *siempre* abre una de la puertas cerradas y ofrece al concursante la opción de quedarse con la elección original o cambiar. En el programa original, *Monty Hall* hacía esta oferta sólo ocasionalmente, con frecuencia cuando sabía que el concursante ya había elegido la puerta correcta. ■

Bettmann/CORBIS

Pierre-Simon Laplace (1749-1827)

Muchos de los principios fundamentales de probabilidad se formularon a mediados del siglo XVII en un intercambio de cartas entre Pierre de Fermat y Blaise Pascal en respuesta a las preguntas formuladas por un noble francés interesado en juegos de azar. En 1812, Pierre Simon Laplace publicó el primer tratado matemático general sobre el tema y amplió la gama de aplicaciones a una variedad de problemas prácticos y científicos.

Conteo de los elementos de una lista

Algunos de los problemas de conteo son tan simples como el conteo de los elementos de una lista. Por ejemplo, ¿cuántos enteros existen de 5 al 12? Para responder a esta pregunta, imagine que va a lo largo de la lista de enteros del 5 al 12, contando uno cada vez.

lista:	5	6	7	8	9	10	11	12
	↕	↕	↕	↕	↕	↕	↕	↕
conteo:	1	2	3	4	5	6	7	8

Por lo que la respuesta es 8.

Más generalmente, si m y n son enteros y $m \leq n$, ¿cuántos enteros existen de m a n? Para responder a esta pregunta, observe que $n = m + (n - m)$, donde $n - m \geq 0$ [*ya que* $n \geq m$]. Observe también que el elemento $m + 0$ es el primer elemento de la lista, el elemento $m + 1$ es el segundo elemento, el elemento $m + 2$ es el tercero y así sucesivamente. En general, el elemento $m + i$ es el $(i + 1)$ésimo elemento de la lista.

$$\begin{array}{lccccccc} \text{lista:} & m(=m+0) & m+1 & m+2 & \dots & n\,(=m+(n-m)) \\ & \updownarrow & \updownarrow & \updownarrow & & \updownarrow \\ \text{conteo:} & 1 & 2 & 3 & \dots & (n-m)+1 \end{array}$$

Y así el número de elementos en la lista es $n - m + 1$.

Este resultado general es lo suficientemente importante como para ser replanteado como un teorema, la demostración formal utiliza inducción matemática. (Vea el ejercicio 28 del final de esta sección.) El corazón de la demostración es la observación de que si la lista $m, m + 1, \dots, k$ tiene $k - m + 1$ números, entonces, la lista $m, m + 1, \dots, k, k + 1$ tiene $(k - m + 1) + 1 = (k + 1) - m + 1$ números.

Teorema 9.1.1 El número de elementos en una lista

Si m y n son enteros y $m \leq n$, entonces hay $n - m + 1$ enteros de m a n inclusive.

Ejemplo 9.1.4 Conteo de los elementos de una sublista

a. ¿Cuántos enteros de tres dígitos (enteros del 100 a 999 inclusive) son divisibles entre 5?

b. ¿Cuál es la probabilidad de que un entero aleatorio de tres dígitos sea divisible entre 5?

Solución

a. Imagine escribir enteros de tres dígitos en un renglón, observe los que son múltiplos de 5 y dibuje flechas entre cada uno de los enteros y su correspondiente múltiplo de 5.

$$\begin{array}{ccccccccccccccccccc} 100 & 101 & 102 & 103 & 104 & 105 & 106 & 107 & 108 & 109 & 110 & \cdots & 994 & 995 & 996 & 997 & 998 & 999 \\ \updownarrow & & & & & \updownarrow & & & & & \updownarrow & & & \updownarrow & & & & & \\ 5\cdot 20 & & & & & 5\cdot 21 & & & & & 5\cdot 22 & & & 5\cdot 199 & & & & & \end{array}$$

Del esbozo es claro que hay tantos números de tres dígitos que son múltiplos de 5 como enteros del 20 al 199 inclusive. Por el teorema 9.1.1, hay $199 - 20 + 1$, o 180, de esos enteros. Por tanto hay 180 enteros de tres dígitos que son divisibles entre 5.

b. Por el teorema 9.1.1 el número total de enteros del 100 al 999 es $999 - 100 + 1 = 900$. Por el inciso *a*), 180 de ellos son divisibles entre 5. Por tanto la probabilidad de que un entero aleatorio de tres dígitos sea divisible entre 5 es $180/900 = 1/5$. ■

Ejemplo 9.1.5 Aplicación: conteo de elementos de un arreglo unidimensional

El análisis de muchos algoritmos de computadora requiere de la habilidad en el conteo de los elementos de un arreglo unidimensional. Sea $A[1], A[2], \dots, A[n]$ un arreglo unidimensional, donde n es un entero positivo.

a. Suponga que el arreglo se corta en un valor medio $A[m]$ por lo que se forman dos subarreglos:

$$1)\ A[1], A[2], \dots, A[m] \quad \text{y} \quad 2)\ A[m+1], A[m+2], \dots, A[n].$$

¿Cuántos elementos tiene cada subarreglo?

b. ¿Cuál es la probabilidad de que se elija aleatoriamente un elemento del arreglo que tenga subíndice par

i) si n es par? ii) si n es impar?

Solución

a. El arreglo (1) tiene el mismo número de elementos que la lista de enteros del 1 al m. Así por el teorema 9.1.1, se tienen m, o $m - 1 + 1$, elementos. El arreglo (2) tiene el mismo número de elementos que la lista de enteros del $m + 1$ al n. Así por el teorema 9.1.1, se tienen $n - m$ o $n - (m + 1) + 1$, elementos.

b. i) Si n es par, cada subíndice que comienza con 2 y termina con n se puede relacionar con un entero del 1 a $n/2$.

$$\begin{array}{cccccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & \cdots & n \\ & \updownarrow & & \updownarrow & & \updownarrow & & \updownarrow & & \updownarrow & & \updownarrow \\ & 2\cdot 1 & & 2\cdot 2 & & 2\cdot 3 & & 2\cdot 4 & & 2\cdot 5 & & 2\cdot n/2 \end{array}$$

Así hay $n/2$ arreglos de elementos con subíndices pares. Dado que el arreglo completo tiene n elementos, la probabilidad de que un elemento elegido aleatoriamente tenga un subíndice par es $\dfrac{n/2}{n} = \dfrac{1}{2}$.

ii) Si n es impar, entonces el subíndice par mayor del arreglo es $n - 1$. Por tanto hay tantos subíndices pares entre 1 y n como de 2 a $n - 1$. Entonces el razonamiento de i) se puede usar para concluir que hay $(n - 1)/2$ arreglos de elementos con subíndices pares.

$$\begin{array}{ccccccccccc} 1 & 2 & 3 & 4 & 5 & 6 & \cdots & n-1 & & n \\ & \updownarrow & & \updownarrow & & \updownarrow & & \updownarrow & & \\ & 2\cdot 1 & & 2\cdot 2 & & 2\cdot 3 & \cdots & 2\cdot(n-1)/2 & & \end{array}$$

Ya que todo el arreglo tiene n elementos, la probabilidad de que un elemento aleatorio tenga un subíndice par es $\dfrac{(n-1)/2}{n} = \dfrac{n-1}{2n}$. Observe que conforme n es cada vez más grande, esta probabilidad estará cada vez más cerca de $1/2$.

Observe que las respuestas a i) y ii) pueden combinarse usando la notación de piso. Por el teorema 4.5.2, el número de elementos del arreglo con subíndices pares es $\lfloor n/2 \rfloor$, por lo que la probabilidad de que un elemento aleatorio tenga un subíndice par es $\dfrac{\lfloor n/2 \rfloor}{n}$. ■

Autoexamen

Las respuestas a las preguntas del autoexamen se encuentran al final de cada sección.

1. Un espacio muestral de un proceso aleatorio o experimento es _____.
2. Un evento en un espacio muestral es _____.
3. Para calcular la probabilidad de un evento mediante la fórmula de probabilidad de eventos equiprobables, tome la razón de _____ con _____.
4. Si $m \leq n$, el número de enteros de m a n inclusive es _____.

Conjunto de ejercicios 9.1*

1. Lance 30 veces dos monedas y haga una tabla que muestre las frecuencias relativas de 0, 1 y 2 caras. ¿Cómo se comparan sus valores con los que se muestran en la tabla 9.1.1?

2. En el ejemplo del lanzamiento de dos monedas de 25 centavos, ¿cuál es la probabilidad de que al menos se obtenga una cara? ¿De que la moneda *A* sea una cara? ¿De que las monedas *A* y *B* sean ambas caras o ambas cruces?

En los ejercicios del 3 al 6 utilice el espacio muestral del ejemplo 9.1.1. Escriba cada evento como un conjunto y calcule su probabilidad.

3. El evento de que la carta elegida sea roja y no sea una carta de cara.

4. El evento de que la carta elegida sea negra y sea un número par.

5. El evento que la denominación de la carta seleccionada es de al menos 10 (contando al as como el más alto).

6. El evento que la denominación de la carta elegida es como máximo 4 (contando al as como el más alto).

En los ejercicios del 7 al 10, utilice al espacio muestral del ejemplo 9.1.2. Escriba cada uno de los siguientes eventos como un conjunto y calcule su probabilidad.

7. El evento de que la suma de los números que se muestran sea 8.

8. El evento de que la suma de los números que se muestran sean iguales.

9. El evento de que la suma de los números que se muestran sean a lo más 6.

10. El evento de que la suma de los números que se muestran sea por lo menos 9.

11. Suponga que se lanza tres veces una moneda y se anota el lado que muestra en cada tirada. Suponga también que en cada tirada las caras y cruces son equiprobables. Sea que *HHT* indique que en las dos primeras tiradas se obtienen dos caras y una cruz en la tercera, el resultado *THT* indica el resultado de que es cruz en la primera y en la tercera tirada y cara en la segunda y así sucesivamente.
    a. Liste los ocho elementos del espacio muestral cuyos efectos son todas las sucesiones de cara-cruz posibles obtenidas en las tres tiradas.
    b. Escriba cada uno de los siguientes eventos como un conjunto y encuentre su probabilidad:
        i) el evento en que exactamente una tirada da como resultado una cara.
        ii) El evento en que al menos dos tiradas dan como resultado una cara.
        iii) El evento en el que no se obtiene cara.

12. Suponga que cada hijo que nace es equiprobable que sea un niño o una niña. Considere una familia con tres hijos. Sea que *VVN* indique que los dos primeros hijos son varones y el tercer hijo es una niña, que *NVN* indique que el primero y el tercer hijo son niñas y el segundo es un varón y así sucesivamente.
    a. Enumere los ocho elementos en el espacio muestral cuyos resultados son todos los géneros posibles de los tres hijos.
    b. Escriba cada uno de los eventos en la siguiente columna como un conjunto y encuentre su probabilidad.
        i) el evento que exactamente un hijo es una niña.
        ii) el evento de que al menos dos hijos son niñas.
        iii) el evento que ningún hijo es una niña.

13. Supongamos que en un examen de verdadero/falso no tiene idea en absoluto sobre las respuestas a tres preguntas. Elija respuestas aleatoriamente y por tanto tienen un 50% de probabilidades de que esté correcto en cualquier pregunta. Sea que *CCE* indique que estaba correcto en las primeras dos preguntas y que se equivocó en la tercera, que *ECE* indique que estaba equivocado en la primera y en la tercera pregunta y correcto en la segunda y así sucesivamente.
    a. Enumere los elementos en el espacio muestral cuyos resultados son todas las posibles sucesiones de respuestas incorrectas y correctas.
    b. Escriba cada uno de los siguientes eventos como un conjunto y encuentre su probabilidad:
        i) El evento de que exactamente una respuesta es correcta.
        ii) El evento de que al menos dos respuestas son correctas.
        iii) El evento de que la respuesta no es correcta.

14. Tres personas han sido expuestas a una cierta enfermedad. Una vez expuesta, una persona tiene 50% de probabilidades de enfermarse realmente.
    a. ¿Cuál es la probabilidad de que exactamente una de las personas enferme?
    b. ¿Cuál es la probabilidad de que al menos dos de las personas enfermen?
    c. ¿Cuál es la probabilidad de que ninguna de las tres personas enferme?

15. Cuando se analiza conteo y probabilidad, a menudo consideramos situaciones que pueden parecer frívolas o de valor poco práctico, como lanzar monedas, elegir cartas o tirar dados. La razón es que estos ejemplos relativamente simples sirven como modelos para una amplia variedad de situaciones más complejas del mundo real. A la luz de esta observación, comente la relación entre su respuesta del ejercicio 11 y sus respuestas a los ejercicios del 12 al 14.

16. Dos caras de un dado de seis caras están pintadas de rojo (*R*), dos están pintadas de azul (*B*) y dos están pintadas de amarillo (*Y*). Se tira el dado tres veces y se registran los colores que se muestran en la primera, segunda y tercera tirada.
    a. Sea que *BBR* denote el resultado donde el color que se muestra en la primera y segunda tiradas sea azul y el color que se muestra en la tercera tirada sea rojo. Ya que hay tantas caras de un color como de cualquier otro, los resultados de este experimento son equiprobables. Enumere todos los 27 posibles resultados.
    b. Considere el evento de que todas las tres tiradas producen diferentes colores. Un resultado en un evento es *RBY* y otro *RYB*. Enumere los resultados del evento. ¿Cuál es la probabilidad del evento?

*Para los ejercicios con números o letras azules, en el apéndice B se presentan las soluciones. El símbolo ***H*** indica que sólo se presenta una sugerencia o una solución parcial. El símbolo ✶ indica que un ejercicio es más desafiante de lo habitual.

c. Considere el evento que dos de los colores que se muestran son los mismos. Un resultado de este evento es *RRB* y otro es *RBR*. Enumere todos los resultados en el evento. ¿Cuál es la probabilidad del evento?

17. Considere la situación descrita en ejercicio 16.
   a. Encuentre la probabilidad del evento de que exactamente uno de los colores que se muestran es rojo.
   b. Encuentre la probabilidad del evento que al menos uno de los colores que se muestran es rojo.

18. Una urna contiene dos bolas azules (que se denotan por B_1 y B_2) y una bola blanca (que se denotan por W). Se saca una bola y se registra su color y se regresa a la urna. Entonces, se saca otra bola y se registra su color.
   a. Sea que B_1W denote el resultado de que la primera bola que se saca sea B_1 y la segunda bola que se saca es W. Debido a que la primera bola se regresa al sacar la segunda bola, el resultado del experimento es equiprobable. Enumere los nueve posibles resultados del experimento.
   b. Considere el evento de que la primera bola que saque sea azul. Enumere todos los resultados del evento. ¿Cuál es la probabilidad del evento?
   c. Considere el evento que las dos bolas que se sacan sean de diferentes colores. Enumere todos los resultados en el evento. ¿Cuál es la probabilidad del evento?

19. Una urna contiene dos bolas azules (que se denotan por B_1 y B_2) y tres bolas blancas (que se denotan por W_1, W_2 y W_3). Se saca una bola, se registra su color y se regresa a la urna. Después, se saca otra bola y se registra su color.
   a. Sea que B_1W_2 denote el resultado de que la primera bola que se saque sea B_1 y la segunda bola que se saca es W_2. Ya que la primera bola se sustituye antes de que se saque la segunda bola, los resultados del experimento son equiprobables. Enumere todos los 25 posibles resultados del experimento.
   b. Considere el evento de que la primera bola que se saca es azul. Enumere todos los resultados del evento. ¿Cuál es la probabilidad del evento?
   c. Considere el evento que se sacan sólo bolas blancas. Enumere todos los resultados del evento. ¿Cuál es la probabilidad del evento?

20. Consulte el ejemplo 9.1.3. Suponga que se está presentando en un concurso con un premio detrás de una de cinco puertas cerradas: *A*, *B*, *C*, *D* y *E*. Si selecciona la puerta derecha, gana el premio. Selecciona la puerta *A*. El conductor del juego abre una de las otras puertas y encuentra que no existe ningún premio detrás de ésta. Entonces el conductor le da la opción de permanecer con su elección original de la puerta *A* o cambiar a una de las otras puertas que todavía está cerrada.
   a. Si mantiene su elección original, ¿cuál es la probabilidad de que va a ganar el premio?
   b. Si cambia a otra puerta, ¿cuál es la probabilidad de que va a ganar el premio?

21. a. ¿Cuántos enteros positivos de dos dígitos son múltiplos de 3?
   b. ¿Cuál es la probabilidad de que un entero aleatorio de dos dígitos sea un múltiplo de 3?
   c. ¿Cuál es la probabilidad de que un entero aleatorio de dos dígitos sea un múltiplo de 4?

22. a. ¿Cuántos enteros positivos de tres dígitos son múltiplos de 6?
   b. ¿Cuál es la probabilidad de que un entero aleatorio de tres dígitos es un múltiplo de 6?
   c. ¿Cuál es la probabilidad de que un entero aleatorio de tres dígitos es un múltiplo de 7?

23. Suponga que $A[1]$, $A[2]$, $A[3]$,..., $A[n]$ es un arreglo unidimensional y $n \geq 50$.
   a. ¿Cuántos elementos están en el arreglo?
   b. ¿Cuántos elementos se encuentran en el subarreglo.

$$A[4], A[5], \ldots, A[39]?$$

   c. Si $3 \leq m \leq n$, ¿cuál es la probabilidad de que un elemento del arreglo elegido de forma aleatoria esté en el subarreglo

$$A[3], A[4], \ldots, A[m]?$$

   d. ¿Cuál es la probabilidad de que un elemento elegido en forma aleatoria se encuentre en el subarreglo que se muestra a continuación si $n = 39$?

$$A[\lfloor n/2 \rfloor], A[\lfloor n/2 \rfloor + 1], \ldots, A[n]$$

24. Suponga que $A[1]$, $A[2]$,..., $A[n]$ es un arreglo unidimensional y $n \geq 2$. Considere el subarreglo

$$A[1], A[2], \ldots, A[\lfloor n/2 \rfloor].$$

   a. ¿Cuántos elementos se encuentran en el subarreglo i) si n es par? y ii) si n es impar?
   b. ¿Cuál es la probabilidad de que un elemento del arreglo aleatorio esté en el subarreglo i) ¿si n es par? y ii) ¿si n es impar?

25. Suponga que $A[1]$, $A[2]$,..., $A[n]$ es un arreglo unidimensional y $n \geq 2$. Considere un subarreglo

$$A[\lfloor n/2 \rfloor], A[\lfloor n/2 \rfloor + 1], \ldots, A[n].$$

   a. ¿Cuántos elementos se encuentran en el subarreglo i) si n es par? y ii) si n es impar?
   b. ¿Cuál es la probabilidad de que un elemento del arreglo aleatorio esté en el subarreglo i) si n es par? y ii) si n es impar?

26. ¿Cuál es el 27-avo elemento en el arreglo unidimensional $A[42]$, $A[43]$,..., $A[100]$?

27. ¿Cuál es el elemento 62-avo del arreglo unidimensional $B[29]$, $B[30]$,..., $B[100]$?

28. Si el más grande de 56 enteros consecutivos es 279, ¿cuál es el más pequeño?

29. Si el más grande de 87 enteros consecutivos es 326, ¿cuál es el más pequeño?

30. ¿Cuántos enteros pares hay entre 1 y 1 001?

31. ¿Cuántos enteros que son múltiplos de 3 están entre 1 y 1 001?

32. Un cierto año no bisiesto tiene 365 días y el 1 de enero es un lunes.
   a. ¿Cuántos domingos hay en el año?
   b. ¿Cuántos lunes hay en el año?

✶ 33. Demuestre el teorema 9.1.1. (Sea m cualquier entero y demuestre el teorema con inducción matemática en n.)

Respuestas del autoexamen

1. el conjunto de todos los resultados del proceso aleatorio o experimento 2. un subconjunto del espacio muestral 3. número de resultados en el evento; número total de resultados 4. $n - m + 1$

9.2 Árbol de probabilidad y la regla de multiplicación

No crea nada a menos que haya pensado usted acerca de esto.
—Anna Pell Wheeler, 1883-1966

Una estructura de árbol es una herramienta útil para el seguimiento sistemático de todas las posibilidades en las situaciones en las que los acontecimientos ocurren en orden. El ejemplo siguiente muestra cómo utilizar una estructura para contar el número de resultados diferentes de un torneo.

Ejemplo 9.2.1 Posibilidades para los juegos de un torneo

Los equipos A y B juegan entre sí repetidamente hasta que uno gana dos partidos consecutivos o un total de tres juegos. Una forma en la que se puede jugar este torneo es que A gana el primer juego, B gana el segundo y A gana el tercer y el cuarto partidos. Esto se denota escribiendo A-B-A-A.

a. ¿De cuántas maneras se puede jugar el torneo?

b. Suponiendo que todas las formas de jugar el torneo son equiprobables, ¿cuál es la probabilidad de que se necesiten cinco juegos para determinar el ganador del torneo?

Solución

a. Las formas posibles para jugar el torneo se representan por los caminos distintos de la "raíz" (el comienzo) de la "hoja" (un punto terminal) en el árbol que se muestra hacia los lados en la figura 9.2.1. La etiqueta de cada punto de ramificación indica el ganador del juego. Las anotaciones entre paréntesis indican el ganador del torneo.

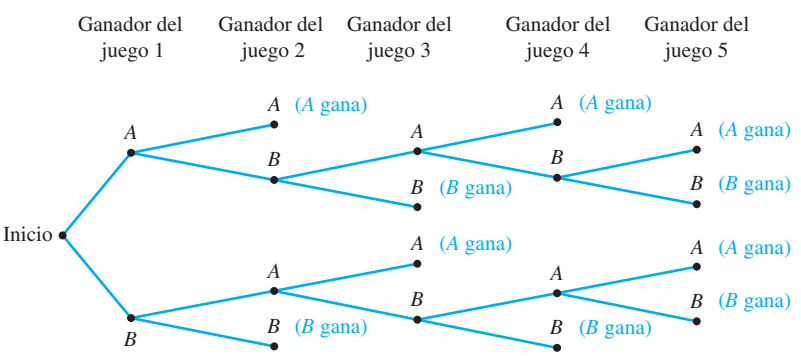


Figura 9.2.1 Los resultados de un torneo

El hecho de que hay diez caminos de la raíz del árbol a sus hojas muestra que hay diez maneras posibles de jugar el torneo. Estos son (bajando desde la parte superior): A-A, A-B-A-A, A-B-A-B-A, A-B-A-B-B, A-B-B, B-A-A, B-A-B-A-A, B-A-B-A-B, B-A-B-B y B-B. En cinco casos A gana y en los otros cinco B gana. El menor número de juegos que debe jugarse para determinar un ganador es de dos y lo más que tendrá que jugar es cinco.

b. Ya que todas las formas posibles de jugar el torneo se enumeraron en el inciso *a*) se supone que son equiprobables y el listado muestra que se necesitan cinco juegos en cuatro casos diferentes (*A*-*B*-*A*-*B*-*A*, *A*-*B*-*A*-*B*-*B*, *B*-*A*-*B*-*A*-*B* y *B*-*A*-*B*-*A*-*A*), la probabilidad de que se necesitan cinco juegos es $4/10 = 2/5 = 40\%$. ■

La regla de la multiplicación

Considere el siguiente ejemplo. Supongamos que la instalación de una computadora tiene cuatro unidades de entrada/salida (*A*, *B*, *C* y *D*) y tres unidades centrales de procesamiento (*X*, *Y* y *Z*). Cualquier unidad de entrada y salida puede estar relacionada con cualquier unidad de procesamiento central. ¿Cuántas maneras existen de relacionar una unidad de entrada y salida con una unidad de procesamiento central?

Para responder a esta pregunta, imaginemos la relación de los dos tipos de unidades como una operación de dos pasos:

Paso 1: Seleccione la unidad de entrada y salida.

Paso 2: Seleccione la unidad de procesamiento central.

Los posibles resultados de esta operación se muestran en el árbol de probabilidad de la figura 9.2.2.

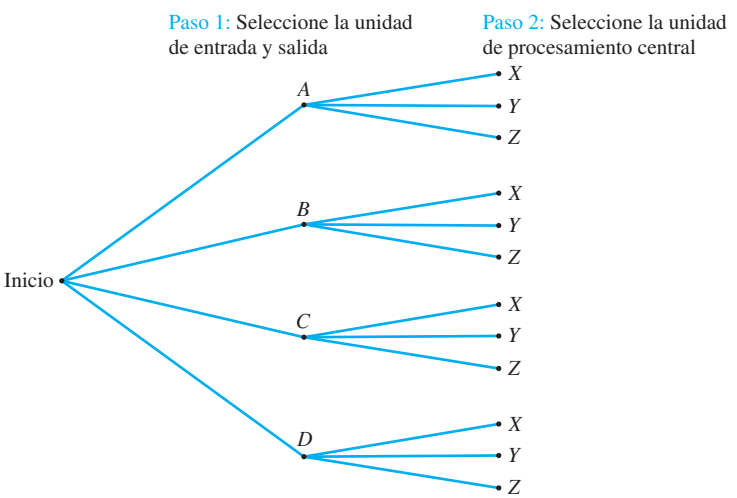


Figura 9.2.2 **Relación de objetos usando un árbol de probabilidad**

La ruta superior de "raíz" a "hoja" indica que la unidad de entrada y salida *A* está relacionada con la unidad de procesamiento central *X*. La rama inferior siguiente indica que la unidad de entrada y salida *A* está relacionada con la unidad central de procesamiento *Y*, y así sucesivamente.

Así, el número total de formas de relacionar los dos tipos de unidades es el mismo que el número de ramas del árbol, que es

$$3 + 3 + 3 + 3 = 4 \cdot 3 = 12.$$

La idea detrás de este ejemplo se puede utilizar para demostrar la siguiente regla. Una demostración formal usa inducción matemática y se deja a los ejercicios.

Teorema 9.2.1 La regla de la multiplicación

Si una operación consiste en k pasos y

el primer paso se puede realizar en n_1 formas,

el segundo paso se puede realizar en n_2 formas *[independientemente de cómo se realizó el primer paso]*,

$\vdots$

el k-ésimo paso se puede realizar en n_k formas *[independientemente de cómo se realizan los pasos anteriores]*,

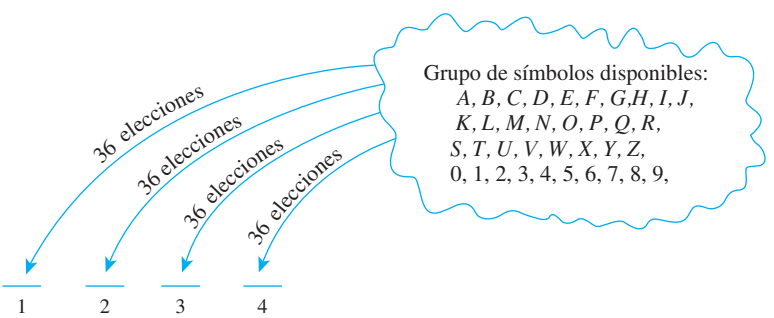
entonces, la operación se puede realizar de $n_1 n_2 \cdots n_k$ formas.

Para aplicar la regla de la multiplicación, piense en los objetos que desea contar como resultado de una operación de varios pasos. Las formas posibles para realizar un paso pueden depender de cómo se realizaron los pasos anteriores, pero el *número* de formas de realizar cada paso debe ser constante, independientemente de las medidas adoptadas en los pasos anteriores.

Ejemplo 9.2.2 Número de números de identificaciones personales (NIPs)

Un típico NIP (número de identificación personal) es una sucesión de cuatro símbolos elegidos de las 26 letras del alfabeto y de los diez dígitos, con repetición permitida. ¿Cuántos NIPs diferentes son posibles?

Solución Los NIPs típicos son CARE, 3387, B32B y así sucesivamente. Se puede considerar formando un NIP como una operación de cuatro pasos para llenar cada uno de los cuatro símbolos en sucesión.



Paso 1: Seleccione el primer símbolo.

Paso 2: Seleccione el segundo símbolo.

Paso 3: Seleccione el tercer símbolo.

Paso 4: Seleccione el cuarto símbolo.

Hay un número fijo de formas de realizar cada paso, es decir 36, independientemente de cómo se realizaron los pasos anteriores. Y así, por la regla de la multiplicación, hay $36 \cdot 36 \cdot 36 \cdot 36 = 36^4 = 1\,679\,616$ NIPs en total. ■

Otra forma de mirar los NIPs del ejemplo 9.2.2 es como una 4-tupla ordenada. Por ejemplo, puede pensar al NIP M2ZM como la 4-tupla ordenada (M, 2, Z, M). Por tanto, el número total de NIPs es igual al número total de 4-tuplas ordenadas cuyos elementos son ya sea letras del alfabeto o dígitos. Uno de los usos más importantes de la regla de la multiplicación es deducir una fórmula general para el número de elementos en cualquier producto cartesiano de un número finito de conjuntos finitos. En el ejemplo 9.2.3, esto se hace para un producto cartesiano de cuatro conjuntos.

Ejemplo 9.2.3 El número de elementos en un producto cartesiano

Suponga que A_1, A_2, A_3 y A_4 son conjuntos con n_1, n_2, n_3 y n_4 elementos, respectivamente. Demuestre que el conjunto $A_1 \times A_2 \times A_3 \times A_4$ tiene $n_1 n_2 n_3 n_4$ elementos.

Solución Cada elemento en $A_1 \times A_2 \times A_3 \times A_4$ es una 4-tupla ordenada de la forma (a_1, a_2, a_3, a_4), donde $a_1 \in A_1$, $a_2 \in A_2$, $a_3 \in A_3$ y $a_4 \in A_4$. Imagine el proceso de construcción de estas tuplas ordenadas como una operación de cuatro-pasos:

Paso 1: Elija el primer elemento de la 4-tupla.

Paso 2: Elija el segundo elemento de la 4-tupla.

Paso 3: Elija el tercer elemento de la 4-tupla.

Paso 4: Elija el cuarto elemento de la 4-tupla.

Hay n_1 formas de realizar el paso 1, n_2 formas de realizar el paso 2, n_3 formas de realizar el paso 3 y n_4 formas de realizar el paso 4. Por tanto, por la regla de la multiplicación, hay $n_1 n_2 n_3 n_4$ formas de realizar toda la operación. Por tanto, hay $n_1 n_2 n_3 n_4$ 4-tuplas distintas en $A_1 \times A_2 \times A_3 \times A_4$. ■

Ejemplo 9.2.4 Número de NIPs sin repetición

En el ejemplo 9.2.2 formamos NIPs utilizando cuatro símbolos, ya sean letras del alfabeto o dígitos y se supone que las letras se podrían repetir. Ahora supongamos que no se permite la repetición.

a. ¿Cuántos NIPs diferentes se pueden formar?

b. Si todos los NIPs son equiprobables, ¿cuál es la probabilidad de que un NIP escogido aleatoriamente no contenga ningún símbolo repetido?

Solución

a. Piense nuevamente en formar un NIP como una operación de cuatro-pasos: Elija el primer símbolo, después el segundo, luego el tercero y, a continuación, el cuarto. Hay 36 maneras de elegir el primer símbolo, 35 maneras de elegir el segundo (ya que no se puede utilizar el primer símbolo de nuevo), 34 maneras de elegir el tercero (ya que no se pueden volver a utilizar los dos primeros símbolos) y 33 maneras de elegir el cuarto (ya que no se pueden volver a utilizar los tres primeros símbolos). Por tanto, se puede aplicar la regla de la multiplicación para concluir que hay $36 \cdot 35 \cdot 34 \cdot 33 = 1\,413\,720$ NIPs diferentes con ningún símbolo repetido.

b. Del inciso *a*) hay 1 413 720 NIPs con ningún símbolo repetido y del ejemplo 9.2.2 hay 1 679 616 NIPs en total. Por tanto la probabilidad de que un NIP elegido aleatoriamente no contenga ningún símbolo repetido es $\frac{1\,413\,720}{1\,679\,616} \cong .8417$. En otras palabras, aproximadamente 84% de los NIPs no tienen ningún símbolo repetido. ■

Cualquier circuito con dos señales de entrada P y Q tiene una tabla de entrada y salida que consiste en cuatro filas correspondientes a las cuatro posibles asignaciones de valores de P y Q: 11, 10, 01 y 00. El ejemplo siguiente muestra que sólo hay 16 formas diferentes en que dicho circuito puede funcionar.

Ejemplo 9.2.5 Número de tablas de entrada/salida para un circuito con dos señales de entrada

Considere el conjunto de todos los circuitos con dos señales de entrada P y Q. Para cada circuito se puede construir una tabla de entrada y salida, pero, como se muestra en la sección 2.4, estas dos tablas de entrada/salida pueden tener los mismos valores. ¿Cuántas distintas tablas de entrada/salida se pueden construir para circuitos con entrada y salida de señales P y Q?

Solución Arregle el orden de los valores de entrada de P y Q. Entonces, dos tablas de entrada y salida son distintas si sus valores de salida difieren en al menos un renglón. Por ejemplo, las tablas de entrada y salida que se muestran a continuación son distintas, porque sus valores de salida difieren en el primer renglón.

P	Q	Salida
1	1	1
1	0	0
0	1	1
0	0	0

P	Q	Salida
1	1	0
1	0	0
0	1	1
0	0	0

Para un orden fijo de valores de entrada, se puede obtener una tabla completa de entrada/salida llenando las entradas de la columna de salida. Se puede considerar esto como una operación de cuatro-pasos:

Paso 1: Llene el valor de salida del primer renglón.

Paso 2: Llene el valor de salida del segundo renglón.

Paso 3: Llene el valor de salida del tercer renglón.

Paso 4: Llene el valor de salida del cuarto renglón.

Cada paso puede realizarse de dos formas: puede poner ya sea un 1 o un 0. Por tanto, por la regla de la multiplicación, hay

$$2 \cdot 2 \cdot 2 \cdot 2 = 16$$

formas de realizar la operación completa. Por lo que hay $2^4 = 16$ tablas distintas de un circuito con dos señales de entrada P y Q de entrada y salida. Esto significa que el circuito puede funcionar en sólo 16 formas distintas. ■

Recuerde, de la sección 5.9, que si S es un conjunto finito de caracteres no vacío, entonces una cadena sobre S es una sucesión finita de elementos de S. El número de caracteres de una cadena se llama la **longitud** de la cadena. La **cadena nula sobre S** es la "cadena" sin caracteres. Normalmente se denota por ε y se dice que tiene longitud 0.

Observe que en los ejemplos 9.2.2 y 9.2.4, el conjunto de todos los NIPs de longitud 4 es igual al conjunto de todas las cadenas de longitud 4 sobre el conjunto

$$S = \{x \mid x \text{ es una letra del alfabeto o } x \text{ es un dígito}\}.$$

También observe que es otra manera de pensar del ejemplo 9.2.5 para darse cuenta de que hay tantas tablas de entrada/salida para un circuito con dos señales de entrada como cadenas de bits de longitud 4 (escritas verticalmente) que se pueden utilizar para llenar los valores de salida. Como otro ejemplo, a continuación se presenta una lista de todas las cadenas de bits de longitud 3:

$$000, \quad 001, \quad 010, \quad 100, \quad 011, \quad 101, \quad 110, \quad 111.$$

Ejemplo 9.2.6 Conteo del número de iteraciones de un bucle anidado

Considere el siguiente bucle anidado:

```
for i := 1 to 4
    for j := 1 to 3
        [Enunciados en el cuerpo del bucle interior.
        Ninguno contiene enunciados
        que ramifiquen fuera del bucle interior.]
    next j
next i
```

¿Cuántas veces se repiten los bucles internos cuando se implementa y se ejecuta el algoritmo?

Solución El bucle externo se itera cuatro veces y durante cada iteración del bucle exterior, hay tres iteraciones del bucle interior. Por tanto por la regla de la multiplicación, el número de iteraciones del bucle interior es $4 \cdot 3 = 12$. Esto se ilustra en la siguiente tabla de seguimiento.

i	1 →			2 →			3 →			4 →		
j	1	2	3	1	2	3	1	2	3	1	2	3

$3 + 3 + 3 + 3 = 12$ ■

Cuando la regla de la multiplicación es difícil o imposible de aplicar

Considere el siguiente problema:

> Tres funcionarios: un presidente, un tesorero y un secretario, deben elegirse entre cuatro personas: Ann, Bob, Cyd y Dan. Suponga que, por diversas razones, Ann no puede ser presidente y Cyd o Dan debe ser secretario. ¿De cuántas maneras se pueden elegir a los funcionarios?

Es natural tratar de resolver este problema mediante la regla de la multiplicación. Una persona puede responder como sigue:

> Hay tres opciones para Presidente (todos excepto Ann), tres opciones para tesorero (todos excepto el elegido como Presidente) y dos opciones de Secretario (Cyd o Dan). Por tanto, por la regla de la multiplicación, hay $3 \cdot 3 \cdot 2 = 18$ opciones en total.

Lamentablemente, este análisis es incorrecto. El número de formas de elegir al secretario varía dependiendo de a quién se ha elegido para presidente y tesorero. Por ejemplo, si Bob es elegido para presidente y Ann para tesorero, entonces hay dos opciones para secretario: Cyd y Dan. Pero si se ha elegido a Bob para presidente y a Cyd para tesorero, entonces hay una opción para secretario: Dan. La manera más clara para ver todas las opciones posibles es construir el árbol de probabilidad, que se muestra en la figura 9.2.3.

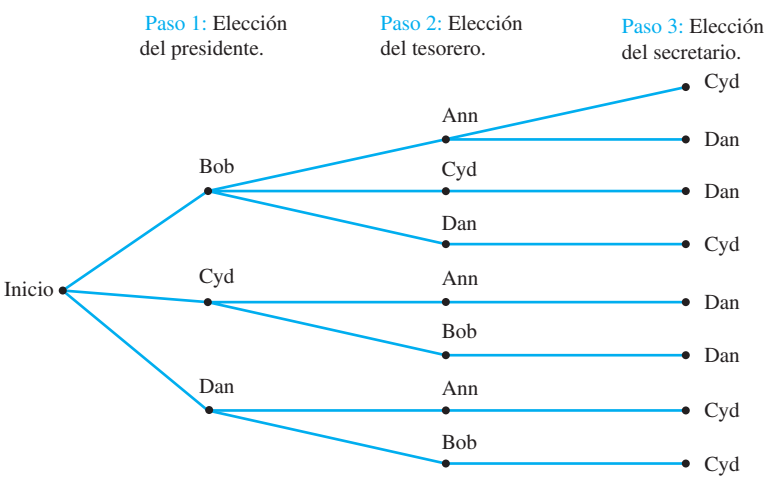


Figura 9.23

Usando el árbol es fácil ver que hay sólo ocho maneras de elegir un presidente, un tesorero, un secretario que satisfagan las condiciones dadas.

Otra forma de resolver este problema es algo sorprendente. Resulta que se pueden reordenar los pasos de forma ligeramente diferente, por lo que el número de formas de realizar cada paso es constante independientemente de la forma en que se realizaron los pasos anteriores.

Ejemplo 9.2.7 Un uso más sutil de la regla de multiplicación

Reordene los pasos para la elección de funcionarios en el ejemplo anterior para que el número total de maneras de elección de funcionarios pueda calcularse utilizando la regla de la multiplicación.

Solución

Paso 1: Elección del secretario.

Paso 2: Elección del presidente.

Paso 3: Elección del tesorero.

Hay dos formas de realizar el paso 1 (se puede elegir a Cyd o Dan), dos formas de realizar el paso 2 (ni Ann ni la persona elegida en el paso 1 se puede elegir pero cualquiera de los otros dos sí se puede elegir) y dos formas para realizar el paso 3 (cualquiera de las dos personas no elegidas como secretario o presidente se puede elegir como tesorero). Por tanto, por la regla de la multiplicación, el número total de maneras de elegir funcionarios es $2 \cdot 2 \cdot 2 = 8$. En la figura 9.2.4, se muestra un árbol de probabilidad que ilustra esta sucesión de opciones. Observe cómo está equilibrado este árbol comparado con el de la figura 9.2.3.

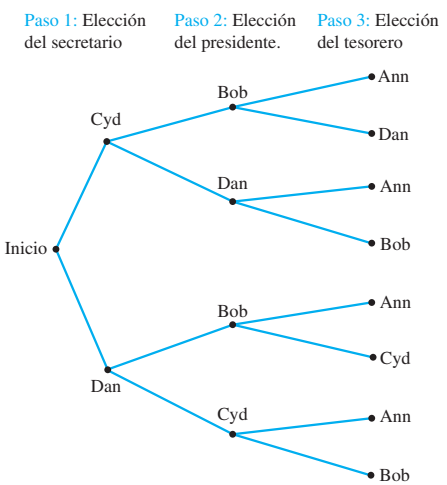


Figura 9.2.4 ■

Permutaciones

Una **permutación** de un conjunto de objetos es un ordenamiento de los objetos en un renglón. Por ejemplo, el conjunto de elementos a, b y c tiene seis permutaciones.

$$abc \quad acb \quad cba \quad bac \quad bca \quad cab$$

En general, dado un conjunto de n objetos, ¿cuántas permutaciones son posibles con los elementos del conjunto? Imagine formar una permutación como una operación de n-pasos:

Paso 1: Elección de un elemento para escribirlo en primer lugar.

Paso 2: Elección de un elemento para escribirlo en segundo lugar.

⋮ ⋮

Paso n: Elección de un elemento para escribirlo en $n$ésimo lugar.

Puede elegir cualquier elemento del conjunto en el paso 1, así hay n maneras de realizar el paso 1. Cualquier elemento salvo el elegido en el paso 1 se puede elegir en el paso 2, por tanto hay $n - 1$ formas de realizar el paso 2. En general, el número de formas de realizar cada paso sucesivo es uno menos que el número de formas de realizar el paso anterior. En el momento en que se elige el enésimo elemento, hay sólo un elemento, hay sólo una forma de realizar el paso n. Por tanto, por la regla de la multiplicación, hay

$$n(n-1)(n-2)\cdots 2\cdot 1 = n!$$

formas de realizar la operación completa. En otras palabras, hay $n!$ permutaciones de un conjunto de n elementos. Este razonamiento se resume en el siguiente teorema. Una demostración formal utiliza inducción matemática y se deja como un ejercicio.

Teorema 9.2.2

Para cualquier entero n con $n \geq 1$, el número de permutaciones de un conjunto con n elementos es $n!$

Ejemplo 9.2.8 Permutaciones de las letras de una palabra

a. ¿De cuántas maneras se pueden ordenar las letras de la palabra *EQUIPO* en un renglón?

b. ¿De cuántas formas se pueden ordenar las letras de la palabra *EQUIPO* si las letras *EQ* deben permanecer juntas (en orden) como una unidad?

c. Si las letras de la palabra *EQUIPO* están arregladas aleatoriamente en un renglón, ¿Cuál es la probabilidad de que las letras *EQ* permanecen juntas (en orden) como una unidad?

Solución

a. Todas las seis letras en la palabra *EQUIPO* son distintas, por lo que el número de formas en que podemos arreglar las letras es igual al número de permutaciones de un conjunto de seis elementos. Esto equivale a $6! = 720$.

b. Si el grupo de letras *EQ* se trata como una unidad, entonces efectivamente hay sólo cinco objetos que se pueden arreglar en un renglón.

EQ	U	I	P	O

Por tanto hay tantas formas de escribir las letras como de permutaciones de un conjunto de cinco elementos, es decir $5! = 120$.

c. Cuando las letras están arregladas aleatoriamente en un renglón, el número total de arreglos es 720 por el inciso *a*) y el número de arreglos con las letras *EQ*, juntas (en orden), como una unidad es 120. Por tanto la probabilidad es

$$\frac{120}{720} = \frac{1}{6} = 16.67\%$$

■

Ejemplo 9.2.9 Permutaciones de objetos alrededor de un círculo

En una reunión de diplomáticos, los seis participantes deben estar sentados alrededor de una mesa circular. Dado que la mesa no tiene extremos para conferir un estatus particular, no importa en dónde se siente el presidente. Pero importa cómo se sienten los diplomáticos respecto a los demás. En otras palabras, dos asientos son considerados iguales si uno es rotación del otro. ¿De cuántas maneras diferentes pueden sentarse los diplomáticos?

Solución Llame a los diplomáticos por las letras A, B, C, D, E y F. Ya que sólo importa la posición relativa, puede comenzar con cualquier diplomático (por ejemplo A), coloque al diplomático en cualquier lugar (por ejemplo en el asiento superior del diagrama que se muestra en la figura 9.2.5) y, después examine todas las disposiciones de los otros diplomáticos alrededor de él. De B a F puede organizarse en los asientos alrededor del diplomático en todos los órdenes posibles. Por tanto hay $5! = 120$ formas de sentar al grupo.

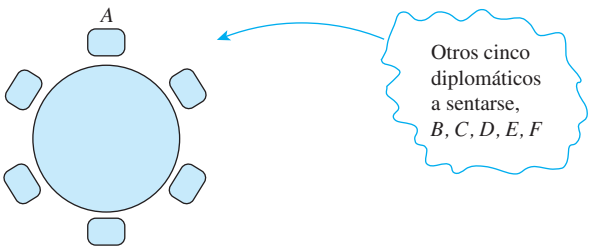


Figura 9.2.5 ■

Permutaciones de elementos seleccionados

Dado el conjunto $\{a, b, c\}$, hay seis formas de seleccionar dos letras del conjunto y escribirlas en orden.

$$ab \quad ac \quad ba \quad bc \quad ca \quad cb$$

Cada uno de estos ordenamientos de dos elementos de $\{a, b, c\}$ se llama una 2-*permutación* de $\{a, b, c\}$.

• Definición

Una ***r*-permutación** de un conjunto de n elementos es una selección ordenada de r elementos tomados del conjunto de n elementos. El número de r-permutaciones de un conjunto de n elementos se denota por $\boldsymbol{P(n, r)}$.

Teorema 9.2.3

Si n y r son enteros y $1 \leq r \leq n$, entonces el número de r-permutaciones de un conjunto de n elementos está dada por la fórmula

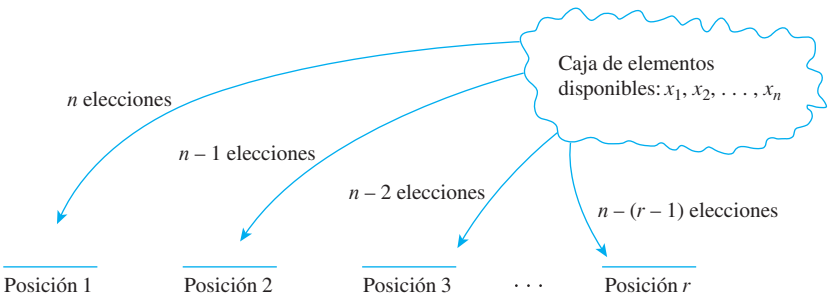
$$P(n, r) = n(n-1)(n-2)\ldots(n-r+1) \qquad \text{primera versión}$$

o, equivalente,

$$P(n, r) = \frac{n!}{(n-r)!} \qquad \text{segunda versión.}$$

Una demostración formal de este teorema usa inducción matemática y se basa en la regla de la multiplicación. La idea de la demostración es la siguiente.

Suponga que se le da un conjunto de n elementos. La formación de una r-permutación puede considerarse como un proceso de r-pasos. Paso 1 se elige el elemento que será primero. Dado que el conjunto tiene n elementos, hay n formas de realizar el paso 1. Paso 2 se elige el elemento que será el segundo. Dado que el elemento seleccionado en el paso 1 ya no está disponible, hay $n - 1$ formas de realizar el paso 2. Paso 3 se elige el elemento que estará en el tercer lugar. Dado que ninguno de los dos elementos elegidos en los dos primeros pasos está disponible, hay $n - 2$ opciones para el paso 3. Este proceso se repite r veces, como se muestra en la siguiente página.



El número de formas de realizar cada paso sucesivo es uno menos que el número de formas de realizar el paso anterior. El paso r es seleccionar el r-ésimo elemento. En el momento justo antes de que se realice el paso r, ya se han seleccionado $r-1$ elementos y por tanto hay

$$n-(r-1)=n-r+1$$

por elegir. Por tanto hay $n-r+1$ formas de realizar el paso r. Se sigue por la regla de la multiplicación que el número de formas para formar una r-permutación es

$$P(n,r)=n(n-1)(n-2)\cdots(n-r+1).$$

Observe que

$$\frac{n!}{(n-r)!}=\frac{n(n-1)(n-2)\cdots(n-r+1)\cancel{(n-r)(n-r-1)\cdots3\cdot2\cdot1}}{\cancel{(n-r)(n-r-1)\cdots3\cdot2\cdot1}}$$
$$=n(n-1)(n-2)\cdots(n-r+1).$$

Por tanto la fórmula puede escribirse como

$$P(n,r)=\frac{n!}{(n-r)!}.$$

La segunda versión de la fórmula es más fácil de recordar. Sin embargo, cuando realmente se utiliza, primero se sustituyen los valores de n y r; después se elimina inmediatamente el valor numérico de $(n-r)!$ del numerador y del denominador. Debido a que los factoriales son rápidamente muy grandes, el uso directo de la segunda versión de la fórmula sin eliminación puede sobrecargar la capacidad de la calculadora para la aritmética exacta, aún cuando n y r sean muy pequeñas. Por ejemplo, si $n=15$ y $r=2$, entonces,

$$\frac{n!}{(n-r)!}=\frac{15!}{13!}=\frac{1\,307\,674\,368\,000}{6\,227\,020\,800}.$$

Pero si elimina $(n-r)!=13!$ obtendrá del denominador y del numerador antes de multiplicar,

$$\frac{n!}{(n-r)!}=\frac{15!}{13!}=\frac{15\cdot14\cdot\cancel{13!}}{\cancel{13!}}=15\cdot14=210.$$

De hecho, muchas calculadoras científicas permiten calcular $P(n, r)$ simplemente introduciendo los valores de n y r; presionando una tecla o haciendo una elección del menú. Puede ver notaciones alternativas para $P(n, r)$ en el manual de su calculadora como son ${}_nP_r$, $P_{n,r}$ y ${}^nP_r$.

Ejemplo 9.2.10 Evaluación de r-permutaciones

a. Evalúe $P(5, 2)$.

b. ¿Cuántas 4-permutaciones hay en un conjunto de siete objetos?

c. ¿Cuántas 5-permutaciones hay en un conjunto de cinco objetos?

Solución

a. $P(5, 2) = \dfrac{5!}{(5-2)!} = \dfrac{5 \cdot 4 \cdot \cancel{3} \cdot \cancel{2} \cdot \cancel{1}}{\cancel{3} \cdot \cancel{2} \cdot \cancel{1}} = 20$

b. El número de 4-permutaciones de un conjunto de siete objetos es

$$P(7, 4) = \frac{7!}{(7-4)!} = \frac{7 \cdot 6 \cdot 5 \cdot 4 \cdot \cancel{3} \cdot \cancel{2} \cdot \cancel{1}}{\cancel{3} \cdot \cancel{2} \cdot \cancel{1}} = 7 \cdot 6 \cdot 5 \cdot 4 = 840.$$

c. El número de 5-permutaciones de un conjunto de cinco objetos es

$$P(5, 5) = \frac{5!}{(5-5)!} = \frac{5!}{0!} = \frac{5!}{1} = 5! = 120.$$

Observe que la definición de 0! como 1 hace que este cálculo salga como debe, ya que el número de 5-permutaciones de un conjunto de cinco objetos es ciertamente igual al número de permutaciones del conjunto. ■

Ejemplo 9.2.11 Permutaciones de letras seleccionadas de una palabra

a. ¿De cuántas diferentes maneras pueden tres de las letras de las palabra *BYTES* elegirse y escribirse en un renglón?

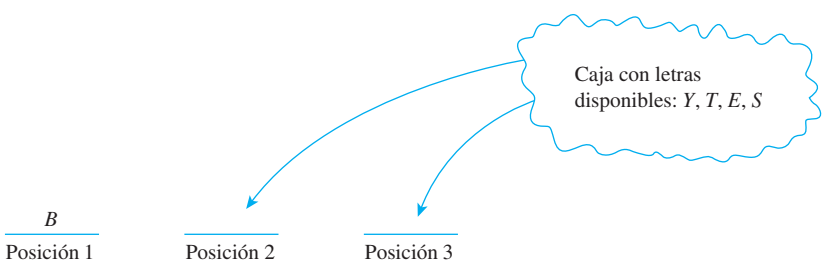
b. ¿De cuántas maneras se puede hacer esto si la primera letra es *B*?

Solución

a. La respuesta es igual al número de 3-permutaciones de un conjunto de cinco elementos. Esto es igual a

$$P(5, 3) = \frac{5!}{(5-3)!} = \frac{5 \cdot 4 \cdot 3 \cdot \cancel{2} \cdot \cancel{1}}{\cancel{2} \cdot \cancel{1}} = 5 \cdot 4 \cdot 3 = 60.$$

b. Ya que la primera letra debe ser *B*, efectivamente sólo hay dos letras a elegir y se colocan en las otras dos posiciones. Y ya que *B* se utiliza en la primera posición, hay cuatro letras disponibles para llenar las dos posiciones que faltan.



Por tanto la respuesta es el número de 2-permutaciones de un conjunto de cuatro elementos, que es

$$P(4, 2) = \frac{4!}{(4-2)!} = \frac{4 \cdot 3 \cdot \cancel{2} \cdot \cancel{1}}{\cancel{2} \cdot \cancel{1}} = 4 \cdot 3 = 12.$$ ■

En muchas aplicaciones de las matemáticas de conteo, es necesario ser hábil en el trabajo algebraico con cantidades de la forma $P(n, r)$. El ejemplo siguiente muestra un tipo de problema que da la práctica para desarrollar dicha habilidad.

Ejemplo 9.2.12 Demostrando una propiedad de $P(n, r)$

Demuestre que para todos los enteros $n \geq 2$,

$$P(n, 2) + P(n, 1) = n^2.$$

Solución Suponga que n es un entero mayor o igual a 2. Por el teorema 9.2.3,

$$P(n, 2) = \frac{n!}{(n-2)!} = \frac{n(n-1)\cancel{(n-2)!}}{\cancel{(n-2)!}} = n(n-1)$$

y

$$P(n, 1) = \frac{n!}{(n-1)!} = \frac{n \cdot \cancel{(n-1)!}}{\cancel{(n-1)!}} = n.$$

Por tanto

$$P(n, 2) + P(n, 1) = n \cdot (n-1) + n = n^2 - n + n = n^2,$$

que es lo que se quería demostrar. ■

Autoexamen

1. La regla de la multiplicación dice que si una operación puede realizarse en k pasos y, para cada i con $1 \leq i \leq k$, el i-ésimo paso se puede realizar en n_i formas (independientemente de cómo se realizaron los pasos anteriores), entonces la operación como un todo se puede realizar en _____.
2. Una permutación de elementos de un conjunto es _____.
3. El número de permutaciones de un conjunto de n elementos es igual a _____.
4. Una r-permutación de un conjunto de n elementos es _____.
5. El número de r-permutaciones de un conjunto de n elementos se denota por _____.
6. Una fórmula para el número de r-permutaciones de un conjunto de n elementos es _____ y otra fórmula es _____.

Conjunto de ejercicios 9.2

En los ejercicios del 1 al 4, use el hecho de que en la serie mundial de béisbol, el primer equipo en ganar cuatro juegos gana la serie.

1. Suponga que el equipo A gana los primeros tres juegos. ¿De cuántas maneras se puede completar la serie? (Dibuje un árbol.)

2. Suponga que el equipo A gana los dos primeros juegos. ¿De cuántas maneras se puede completar la serie? (Dibuje un árbol.)

3. ¿De cuántas maneras se puede jugar una serie mundial si el equipo A gana cuatro juegos consecutivos?

4. ¿De cuántas maneras se puede jugar una serie mundial si ningún equipo gana dos partidos consecutivos?

5. En una competencia entre los jugadores X y Y, el primer jugador gana tres juegos consecutivos o un total de cuatro juegos. ¿De cuántas maneras puede ser la competencia si X gana el primer juego y Y gana el segundo y tercer juegos? (Dibuje un árbol.)

6. Una urna contiene dos bolas negras (etiquetadas por B_1 y B_2) y una bola blanca. Una segunda urna contiene una bola negra y dos bolas blancas (etiquetadas por W_1 y W_2). Suponga que se realiza el siguiente experimento: Aleatoriamente se elige una de las dos urnas. A continuación se elige aleatoriamente una bola de la urna. Después se elige aleatoriamente una segunda bola de la misma urna sin reemplazar la primera bola.
   a. Construya un árbol de probabilidad que muestre todos los posibles efectos de este experimento.
   b. ¿Cuál es el número total de resultados de este experimento?
   c. ¿Cuál es la probabilidad de que se elijan dos bolas negras?
   d. ¿Cuál es la probabilidad de que se elijan dos bolas de color diferente?

7. Una urna contiene una bola azul (etiquetada con B_1) y tres bolas rojas (etiquetadas con R_1, R_2 y R_3). Una segunda urna contiene dos bolas rojas (R_4 y R_5) y dos bolas azules (B_2 y B_3). Se realiza un experimento en el que se elige aleatoriamente una de las dos urnas y después se eligen aleatoriamente dos bolas de ésta, una tras otra sin reemplazo.
   a. Construya el árbol de probabilidad que muestre todos los posibles resultados de este experimento.
   b. ¿Cuál es el número total de resultados de este experimento?
   c. ¿Cuál es la probabilidad de que se elijan dos bolas rojas?

8. A una persona que compra un sistema de computadora personal se le ofrece una opción de tres modelos de la unidad básica, dos modelos de teclado y dos modelos de impresora. ¿Cuántos sistemas distintos puede adquirir?

9. Suponga que hay tres carreteras de la ciudad A a la ciudad B y cinco carreteras de la ciudad B a la ciudad C.
   a. ¿De cuántas formas es posible viajar de la ciudad A a la ciudad C pasando por la ciudad B?
   b. ¿Cuántos caminos diferentes de ida y vuelta existen de la ciudad A a B a C a B y de regreso a A?
   c. ¿Cuántos caminos diferentes existen de la ciudad A a B a C a B y de regreso a A tal que ningún camino se recorra dos veces?

10. Supongamos que hay tres rutas del punto norte del río Boulder, dos rutas del río Boulder a la presa Beaver, dos rutas de la presa Beaver al lago Estrella y cuatro directamente del río Boulder al lago Estrella. (Realice un dibujo.)
    a. ¿Cuántas rutas del Punto norte al Lago Estrella atraviesan la presa Beaver?
    b. ¿Cuántas rutas del punto norte al Lago Estrella bordean la presa Beaver?

11. **a.** Una cadena de bits es una sucesión finita de 0 y 1. ¿Cuántas cadenas de bits tienen longitud 8?
    b. ¿Cuántas cadenas de bits de longitud 8 comienzan con tres 0?
    c. ¿Cuántas cadenas de bits de longitud 8 comienzan y terminan con un 1?

12. Los números hexadecimales se forman usando dieciséis dígitos 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F. Se denotan con el subíndice 16. Por ejemplo, $9A2D_{16}$ y $BC54_{16}$ son números hexadecimales.
    a. ¿Cuántos números hexadecimales comienzan con uno de los dígitos de 3 a B y terminan con uno de los dígitos de 5 a F y tienen una longitud de 5 dígitos?
    b. ¿Cuántos números hexadecimales comienzan con uno de los dígitos de 4 a D y terminan con uno de los dígitos de 2 a E y tienen una longitud de 6 dígitos?

13. Se lanza una moneda cuatro veces. Cada vez se registra el resultado *H* para caras o *T* para cruces. Un resultado *HHTT* significa que se obtuvo cara en los dos primeros lanzamientos y cruces en los dos segundos. Suponga que las caras y cruces son equiprobables en cada lanzamiento.
    a. ¿Cuántos resultados distintos son posibles?
    b. ¿Cuál es la probabilidad de que exactamente ocurran dos caras?
    c. ¿Cuál es la probabilidad de que exactamente ocurra una cara?

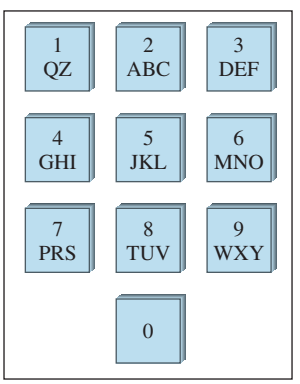
14. Supongamos que en un determinado estado, todas las placas de automóviles tienen cuatro letras seguidas de tres dígitos.
    a. ¿Cuántas placas diferentes son posibles?
    b. ¿Cuántas placas podrían empezar con *A* y terminar con 0?
    c. ¿Cuántas placas podrían empezar con *TGIF*?
    d. ¿Cuántas placas son posibles en las que todas las letras y dígitos son distintos?
    e. ¿Cuántas placas podrían empezar con *AB* y tienen todas las letras y dígitos distintos?

15. Un candado de combinación requiere tres selecciones de números, cada una del 1 al 30.
    a. ¿Cuántas combinaciones son posibles?
    b. Suponga que cada candado está construido de tal manera que ningún número puede utilizarse dos veces. ¿Cuántas combinaciones diferentes son posibles?

16. a. ¿Cuántos enteros hay del 10 a 99?
    b. ¿Cuántos enteros impares hay del 10 a 99?
    c. ¿Cuántos enteros del 10 a 99 tienen dígitos distintos?
    d. ¿Cuántos enteros impares de 10 a 99 tienen dígitos distintos?
    e. ¿Cuál es la probabilidad de que un entero elegido aleatoriamente de dos dígitos tenga dígitos distintos?, ¿tenga dígitos distintos y sea impar?

17. a. ¿Cuántos enteros hay de 1 000 a 9 999?
    b. ¿Cuántos enteros impares hay de 1 000 a 9 999?
    c. ¿Cuántos enteros de 1 000 a 9 999 tienen dígitos distintos?
    d. ¿Cuántos enteros impares de 1 000 a 9 999 tienen dígitos distintos?
    e. ¿Cuál es la probabilidad de que un entero aleatorio de cuatro dígitos tenga dígitos distintos? ¿tenga dígitos distintos y sea impar?

18. El siguiente diagrama muestra el teclado de un cajero automático. Como puede ver, la misma sucesión de teclas representa una variedad de diferentes NIPs. Por ejemplo, 2133, AZDE, BQ3F y todos están escritos exactamente de la misma manera.



    a. ¿Cuántos NIPs diferentes están representados por la misma sucesión de teclas como 2133?
    b. ¿Cuántos NIPs diferentes están representados por la misma sucesión de teclas que 5031?
    c. En un cajero automático, cada NIP corresponde a una sucesión numérica de cuatro dígitos. Por ejemplo, TWJM corresponde a 8956. ¿Cuántas de tales sucesiones numéricas no contienen ningún dígito repetido?

19. Tres funcionarios: un presidente, un tesorero y un secretario, deben elegirse de entre cuatro personas: Ann, Bob, Cyd y Dan. Supongamos que Bob no está calificado para ser tesorero y otros compromisos hacen imposible que Cyd sea su secretaria. ¿De cuántas maneras se puede elegir los funcionarios? ¿Puede utilizarse la regla de la multiplicación para resolver este problema?

20. Modifique el ejemplo 9.2.4 suponiendo que un NIP no debe comenzar con cualquiera de las letras de la A a la M y debe terminar con un dígito. Continúe suponiendo que ningún símbolo puede utilizarse más de una vez y que el número total de NIPs está por determinarse.

a. Encuentre el error en la siguiente "solución".

"Construir un NIP es un proceso de cuatro pasos.

Paso 1: Elija el símbolo del extremo izquierdo.

Paso 2: Elija el segundo símbolo desde la izquierda.

Paso 3: Elija el tercer símbolo de la izquierda.

Paso 4: Elija el símbolo del extremo derecho.

Debido a que ninguna de las trece letras de la A a la M se pueden elegir en el paso 1, hay $36 - 13 = 23$ formas de realizar el paso 1. Hay 35 formas de realizar el paso 2 y 34 formas para realizar el paso 3 porque los símbolos utilizados previamente ya no se pueden utilizar. Puesto que el símbolo elegido en el paso 4 debe ser un dígito no utilizado anteriormente, hay $10 - 3 = 7$ formas de realizar el paso 4. Por tanto hay $23 \cdot 35 \cdot 34 \cdot 7 = 191\,590$ NIPs diferentes que satisfacen las condiciones dadas".

b. Reordene los pasos del 1 al 4 en el inciso *a*) como sigue:

Paso 1: Elija el símbolo del extremo derecho.

Paso 2: Elija el símbolo del extremo izquierdo.

Paso 3: Elija el segundo símbolo desde la izquierda.

Paso 4: Elija el tercer símbolo desde la izquierda.

Utilice la regla de la multiplicación para encontrar el número de NIPs que satisfacen las condiciones dadas.

***H* 21.** Suponga que A es un conjunto con m elementos y B es un conjunto con n elementos.
a. ¿Cuántas relaciones hay de A a B? Explique.
b. ¿Cuántas funciones hay de A a B? Explique.
c. ¿Qué fracción de las relaciones de A a B son funciones?

22. **a.** ¿Cuántas funciones hay de un conjunto con tres elementos a un conjunto con cuatro elementos?
b. ¿Cuántas funciones hay de un conjunto con cinco elementos a un conjunto con dos elementos?
c. ¿Cuántas funciones existen de un conjunto con m elementos a un conjunto con n elementos, donde m y n son enteros positivos?

23. En la sección 2.5 mostramos cómo se pueden representar los enteros por cadenas de 0 y de 1 en una computadora digital. De hecho, a través de varios esquemas de codificación, las cadenas de 0 y 1 se pueden utilizar para representar todo tipo de símbolos. Un código comúnmente utilizado es el Código Extendido de Binario Codificado Decimal (EBCDIC) en el que cada símbolo tiene una representación de 8 bits. ¿Cuántos símbolos distintos se pueden representar con este código?

En cada uno de los ejercicios del 24 al 28, determine cuántas veces iterará el bucle interno cuando el segmento del algoritmo se implemente y ejecute. (Suponga que m, n, p, a, b, c y d son todos enteros positivos.)

24.
for $i := 1$ **to** 30
  for $j := 1$ **to** 15
    [*Enunciados en el cuerpo del bucle interior. Ninguno contiene enunciados que ramifiquen fuera del bucle.*]
  next j
next i

25.
for $j := 1$ **to** m
  for $k := 1$ **to** n
    [*Enunciados en el cuerpo del bucle interior. Ninguno contiene enunciados que ramifiquen fuera del bucle.*]
  next k
next j

26.
for $i := 1$ **to** m
  for $j := 1$ **to** n
    for $k := 1$ **to** p
      [*Enunciados en el cuerpo del bucle interior. Ninguno contiene enunciados que ramifiquen fuera del bucle.*]
    next k
  next j
next i

27.
for $i := 5$ **to** 50
  for $j := 10$ **to** 20
    [*Enunciados en el cuerpo del bucle interior. Ninguno contiene enunciados que ramifiquen fuera del bucle.*]
  next j
next i

28. Suponga que $a \leq b$ y $c \leq d$.
for $i := a$ **to** b
  for $j := c$ **to** d
    [*Enunciados en el cuerpo del bucle interior. Ninguno contiene enunciados que ramifiquen fuera del bucle.*]
  next j
next i

***H* ∗ 29.** Considere los números del 1 a 99 999 en sus representaciones decimales ordinarias. ¿Cuántos contienen exactamente uno de cada uno de los dígitos 2, 3, 4 y 5?

✶ 30. Sea $n = p_1^{k_1} p_2^{k_2} \cdots p_m^{k_m}$ donde $p_1, p_2, \ldots, p_m$ son números primos distintos y $k_1, k_2, \ldots, k_m$ son enteros positivos. ¿De cuántas formas se puede escribir n como un producto de dos enteros positivos que no tienen factores comunes
   a. ¿suponga que importa el orden (es decir, $8 \cdot 15$ y $15 \cdot 8$ se consideran diferentes)?
   b. ¿suponga que no importa el orden (es decir, $8 \cdot 15$ y $15 \cdot 8$ se consideran iguales)?

✶ 31. **a.** ¿Si p es un número primo y a es un entero positivo, cuántos divisores positivos distintos tiene p^a?
   b. Si p y q son números primos distintos y a y b son enteros positivos, ¿cuántos divisores positivos distintos tiene $p^a q^b$?
   c. Si p, q y r son números primos distintos y a, b y c son enteros positivos, cuántos divisores positivos distintos tiene $p^a q^b r^c$?
   d. Si $p_1, p_2, \ldots, p_m$ son números primos distintos y $a_1, a_2, \ldots, a_m$ son enteros positivos, ¿cuántos divisores positivos distintos tiene $p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}$?
   e. ¿Cuál es el entero más pequeño con exactamente 12 divisores?

32. **a.** ¿De cuántas maneras pueden las letras de la palabra *ALGORITMO* arreglarse en un renglón?
   b. ¿De cuántas formas pueden las letras de la palabra *ALGORITMO* arreglarse en un renglón si *A* y *L* deben permanecer juntos (en orden) como una unidad?
   c. ¿De cuántas formas pueden las letras de la palabra *ALGORITMO* arreglarse en un renglón si las letras *GOR* deben permanecer juntas (en orden) como una unidad?

33. Seis personas asisten el teatro juntas y se sientan en una fila con exactamente seis asientos.
   a. ¿De cuántas maneras se pueden sentar juntas en la fila?
   b. Supongamos que uno de los seis es una doctora que debe sentarse en el pasillo, en caso de que sea buscada. ¿De cuántas maneras pueden las personas sentarse juntas en la fila con la doctora en un asiento de pasillo?
   c. Suponga que las seis personas constan de tres parejas y que cada pareja quiere sentarse junto con su esposo a la izquierda. ¿De cuántas maneras pueden los seis sentarse juntos en la fila?

34. Cinco personas se deben sentar alrededor de una mesa circular. Dos asientos se consideran iguales si uno es una rotación del otro. ¿Cuántas maneras diferentes de sentarse son posibles?

35. Escriba todas las 2-permutaciones de $\{W, X, Y, Z\}$.

36. Escriba todas las 3-permutaciones de $\{s, t, u, v\}$.

37. Evalúe las siguientes cantidades.
   a. $P(6, 4)$ b. $P(6, 6)$ c. $P(6, 3)$ d. $P(6, 1)$

38. **a.** ¿Cuántas 3-permutaciones hay de un conjunto de cinco objetos?
   b. ¿Cuántas 2-permutaciones hay de un conjunto de ocho objetos?

39. **a.** ¿De cuántas maneras pueden seleccionarse y escribirse en un renglón tres letras de la palabra *ALGORITMO*?
   b. ¿De cuántas maneras pueden seleccionarse y escribirse en un renglón seis de las letras de la palabra *ALGORITMO*?
   c. ¿De cuántas maneras pueden seleccionarse y escribirse en un renglón seis de las letras de la palabra *ALGORITMO* siendo *A* la primera letra?
   d. ¿De cuántas maneras pueden seleccionarse y escribirse en un renglón seis de las letras de la palabra *ALGORITMO*, si deben las dos primeras letras ser *OR*?

40. Demuestre que todos los enteros $n \geq 2$, $P(n + 1, 3) = n^3 - n$.

41. Demuestre que todos los enteros $n \geq 2$,

$$P(n + 1, 2) - P(n, 2) = 2P(n, 1).$$

42. Demuestre que para todos los enteros $n \geq 3$,

$$P(n + 1, 3) - P(n, 3) = 3P(n, 2).$$

43. Demuestre que para todos los enteros $n \geq 2$, $P(n, n) = P(n, n - 1)$.

44. Demuestre el teorema 9.2.1 por inducción matemática.

***H* 45.** Demuestre el teorema 9.2.2 por inducción matemática.

✶ 46. Demuestre el teorema 9.2.3 por inducción matemática.

47. Una permutación en un conjunto se puede considerar como una función del conjunto a sí mismo. Por ejemplo, una permutación de $\{1, 2, 3, 4\}$ es 2341. Se puede identificar con la función que envía a cada posición numérica al número que ocupará esa posición. Ya que la posición 1 es ocupada por 2, 1 es enviado a 2 o $1 \rightarrow 2$; ya que la posición 2 está ocupada por 3, 2 se envía a 3 o $2 \rightarrow 3$; y así sucesivamente. Toda la permutación puede escribirse con flechas como sigue:

$$\begin{array}{cccc} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 3 & 4 & 1 \end{array}$$

   a. Utilice las flechas para escribir cada una de las seis permutaciones de $\{1, 2, 3\}$.
   b. Utilice las flechas para escribir cada una de las permutaciones de $\{1, 2, 3, 4\}$ que mantenga a 2 y 4 fijos.
   c. ¿Qué permutaciones de $\{1, 2, 3\}$ no conservan elementos fijos?
   d. Utilice flechas para escribir todas las permutaciones de $\{1, 2, 3, 4\}$ que no mantienen elementos fijos.

Respuestas del autoexamen

1. $n_1 n_2 \ldots n_k$ formas 2. un ordenamiento de los elementos del conjunto en un renglón 3. $n!$ 4. un ordenamiento seleccionando r elementos del conjunto 5. $P(n, r)$ 6. $n(n-1)(n-2)\cdots(n-r+1)$; $\frac{n!}{(n-r)!}$

9.3 Conteo de elementos de conjuntos disjuntos: la regla de la suma

La totalidad de la ciencia no es más que un refinamiento del pensamiento cotidiano.
—Albert Einstein, 1879-1955

En la última sección analizamos problemas de conteo que se pueden resolver con árboles de probabilidad. En esta sección trabajamos con problemas de conteo que se pueden resolver contando el número de elementos en la unión de los dos conjuntos, la diferencia de dos conjuntos o la intersección de dos conjuntos.

La regla básica subyacente en el cálculo del número de elementos en una unión o diferencia o intersección es la regla de la suma. Esta regla establece que el número de elementos en una unión de conjuntos finitos mutuamente disjuntos es igual a la suma del número de elementos en cada uno de los conjuntos componentes.

Teorema 9.3.1 La regla de la suma

Suponga un conjunto finito A que es igual a la unión de k subconjuntos distintos mutuamente disjuntos $A_1, A_2, \ldots, A_k$. Entonces,

$$N(A) = N(A_1) + N(A_2) + \cdots + N(A_k).$$

Una demostración formal de este teorema usa inducción matemática y se deja como ejercicio.

Ejemplo 9.3.1 Conteo de contraseñas con tres o menos letras

Una contraseña de acceso a la computadora consta de una a tres letras elegidas de las 26 letras del alfabeto con repeticiones permitidas. ¿Cuántas contraseñas diferentes son posibles?

Solución El conjunto de todas las contraseñas puede particionarse en subconjuntos conformados por los de longitud 1, los de longitud 2 y los de longitud 3, como se muestra en la figura 9.3.1.

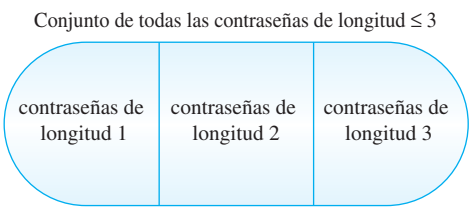


Figura 9.3.1

Por la regla de adición, el número total de contraseñas es igual a la cantidad de contraseñas de longitud 1, más el número de contraseñas de longitud 2, más el número de contraseñas de longitud 3. Ahora el

número de contraseñas de longitud $1 = 26$ ya que hay 26 letras en el alfabeto

número de contraseñas de longitud $2 = 26^2$ ya que formar esa palabra puede considerarse como un proceso de dos-pasos en el que hay 26 formas de realizar cada paso

número de contraseñas de longitud $3 = 26^3$ ya que formar dicha palabra puede considerarse como un proceso de tres-pasos en el que hay 26 formas de realizar cada paso.

Por tanto el número total de contraseñas $= 26 + 26^2 + 26^3 = 18\,278$. ■

Ejemplo 9.3.2 Conteo del número de enteros divisibles por 5

¿Cuántos enteros de tres dígitos (enteros de 100 a 999 inclusive) son divisibles por 5?

Solución Una solución a este problema se analizó en el ejemplo 9.1.4. Otro enfoque utiliza la regla de adición. Enteros que son divisibles por 5 y terminan en 5 o en 0. Así, el conjunto de todos los enteros de tres dígitos que son divisibles por 5 puede dividirse en dos subconjuntos mutuamente disjuntos A_1 y A_2 como se muestra en la figura 9.3.2.

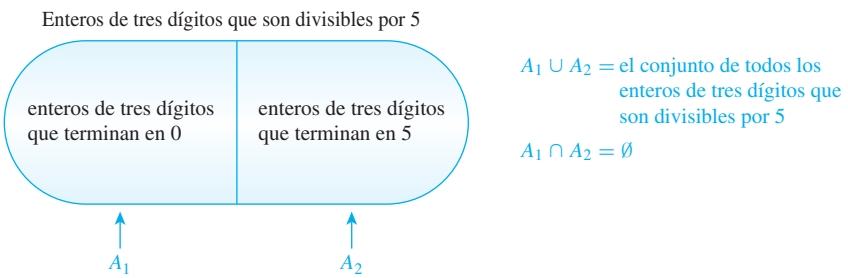


Figura 9.3.2

Ahora hay tantos enteros de tres dígitos que terminan en 0 como opciones posibles para los dígitos de en medio y del extremo izquierdo (ya que el dígito de la derecha debe ser 0). Como se muestra a continuación, hay nueve opciones para el dígito del extremo izquierdo (dígitos del 1 al 9) y diez opciones para el dígito de en medio (dígitos de 0 a 9). Por tanto $N(A_1) = 9 \cdot 10 = 90$.

$$\underset{\substack{\uparrow \\ \text{9 opciones} \\ \text{1, 2, 3, 4, 5, 6, 7, 8, 9}}}{\square} \qquad \underset{\substack{\uparrow \\ \text{10 opciones} \\ \text{0, 1, 2, 3, 4, 5, 6, 7, 8, 9}}}{\square} \qquad \underset{\substack{\uparrow \\ \text{números que} \\ \text{terminan en 0}}}{\square}$$

Un razonamiento similar (con 5 en lugar de 0) también muestra que $N(A_2) = 90$. Por tanto

$$\begin{bmatrix}\text{número de tres} \\ \text{dígitos enteros que} \\ \text{son divisibles por 5}\end{bmatrix} = N(A_1) + N(A_2) = 90 + 90 = 180. \quad \blacksquare$$

La regla de la diferencia

Una consecuencia importante de la regla de adición es el hecho de que si el número de elementos en un conjunto A y el número en un subconjunto B de A son ambos conocidos, entonces el número de elementos que se encuentran en A y no se encuentran en B se puede calcular.

Teorema 9.3.2 La regla de la diferencia

Si A es un conjunto finito y B es un subconjunto de A, entonces

$$N(A - B) = N(A) - N(B).$$

La regla de la diferencia se ilustra en la figura 9.3.3.

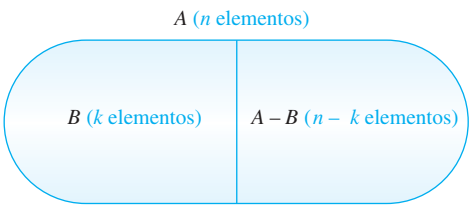


Figura 9.3.3 La regla de la diferencia

La regla de diferencia vale por la siguiente razón: si B es un subconjunto de A, entonces los dos conjuntos B y $A - B$ no tienen elementos en común y $B \cup (A - B) = A$. Por tanto, por la regla de la suma,

$$N(B) + N(A - B) = N(A).$$

Restando $N(B)$ de ambos lados de la ecuación

$$N(A - B) = N(A) - N(B).$$

Ejemplo 9.3.3 Conteo de NIPs con símbolos repetidos

Los NIPs analizados en los ejemplos 9.2.2 y 9.2.4 se han formado de exactamente cuatro símbolos elegidos de las 26 letras del alfabeto y de diez dígitos, con repeticiones permitidas.

a. ¿Cuántos NIPs contienen símbolos repetidos?

b. Si todos NIPs son equiprobables, ¿cuál es la probabilidad que un NIP elegido de forma aleatoria contenga un símbolo repetido?

Solución

a. De acuerdo con el ejemplo 9.2.2, hay $36^4 = 1\,679\,616$ NIPs cuando se permite la repetición y por el ejemplo 9.2.4, hay 1 413 720 NIPs cuando no se permite la repetición. Así, por la regla de la diferencia, hay

$$1\,679\,616 - 1\,413\,720 = 265\,896$$

NIPs que contienen al menos un símbolo repetido.

b. Por el ejemplo 9.2.2 hay 1 679 616 NIPs en total y por el inciso *a*) 265 896 de estos contienen al menos un símbolo repetido. Así, por la fórmula de probabilidad de eventos equiprobables, la probabilidad que un NIP elegido de forma aleatoria contenga un símbolo repetido es $\frac{265\,896}{1\,679\,616} \cong 0.158 = 15.8\%$. ■

Una solución alternativa al ejemplo 9.3.3*b*) se basa en la observación de que si S es el conjunto de todos los NIPs y A es el conjunto de todos los NIPs con ningún símbolo repetido, entonces $S - A$ es el conjunto de todos los NIPs con al menos un símbolo repetido. De lo que se deduce que

$$\begin{aligned}
P(S - A) &= \frac{N(S - A)}{N(S)} && \text{por definición de probabilidad en el caso de eventos equiprobables} \\
&= \frac{N(S) - N(A)}{N(S)} && \text{por la regla de la diferencia} \\
&= \frac{N(S)}{N(S)} - \frac{N(A)}{N(S)} && \text{por las leyes de las fracciones} \\
&= 1 - P(A) && \text{por definición de probabilidad en el caso de eventos equiprobables} \\
&\cong 1 - 0.842 && \text{por el ejemplo 9.2.4} \\
&\cong 0.158 = 15.8\%
\end{aligned}$$

Esta solución ilustra una propiedad más general de probabilidades: que la probabilidad del complemento de un evento se obtiene restando la probabilidad del evento del número 1. En la sección 9.8 deducimos esta fórmula a partir de los axiomas de probabilidad.

Fórmula para la probabilidad del complemento de un evento

Si S es un espacio muestral finito y A es un evento en S, entonces

$$P(A^c) = 1 - P(A).$$

Ejemplo 9.3.4 Número de identificadores *Python* de ocho o menos caracteres

En el lenguaje de programación *Python*, los identificadores deben empezar con uno de los 53 símbolos: ya sea una de las 52 letras del alfabeto romano minúsculas o mayúsculas o un carácter subrayado (_). El carácter inicial puede ser independiente, estar seguido de cualquier número de caracteres adicionales elegidos de un conjunto de 63 símbolos: los 53 símbolos permitidos como un carácter inicial y diez dígitos. Sin embargo, determinadas palabras clave, tales como *y*, *si*, *imprimir*, etc., se hacen a un lado y no se admitirán como identificadores. En una implementación de *Python* hay 31 palabras clave reservadas, ninguna de las cuales tiene más de ocho caracteres. ¿Cuántos identificadores *Python* hay de longitud menor o igual a ocho caracteres?

Solución El conjunto de todos los identificadores *Python* con menos de ocho caracteres puede particionarse en ocho subconjuntos, los identificadores de longitud 1, los identificadores de longitud 2 y así sucesivamente, como se muestra en la figura 9.3.4. Las palabras reservadas tienen diferentes longitudes (todas menores de o iguales a 8), por lo que el conjunto de palabras reservadas muestra la superposición de diversos subconjuntos.

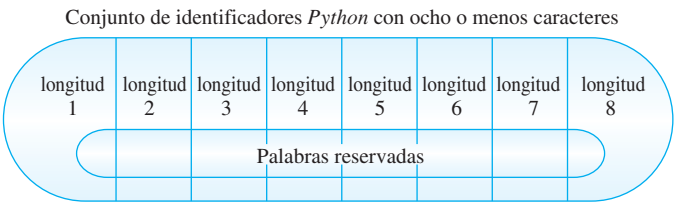


Figura 9.3.4

De acuerdo con las reglas para crear identificadores *Python*, hay

53 identificadores potenciales de longitud 1 — ya que hay 53 opciones para el primer carácter

$53 \cdot 63$ identificadores potenciales de longitud 2 — ya que el primer carácter puede ser cualquiera de los 53 símbolos y el segundo carácter puede ser cualquiera de 63 símbolos

$53 \cdot 63^2$ identificadores potenciales de longitud 3 — ya que el primer carácter puede ser cualquiera de los 53 símbolos y cada uno de los siguientes dos caracteres puede ser cualquiera de 63 símbolos

⋮

$53 \cdot 63^7$ identificadores potenciales de longitud 8 — ya que el primer carácter puede ser cualquiera de los 53 símbolos y cada uno de los siguientes siete caracteres puede ser cualquiera de 63 símbolos.

Así, por la regla de adición, que es el número de posibles identificadores *Python* con menos de ocho caracteres

$$\begin{aligned} 53 + 53 \cdot 63 + 53 \cdot 63^2 + 53 \cdot 63^3 + 53 \cdot 63^4 + 53 \cdot 63^5 + 53 \cdot 63^6 + 53 \cdot 63^7 & \\ = 53 \left(\frac{63^8 - 1}{63 - 1} \right) & \\ = 212\,133\,167\,002\,880. & \end{aligned}$$

Ahora están reservados 31 de estos identificadores potenciales, por la regla de la diferencia, el número real de identificadores *Python* con menos de ocho caracteres es

$$212\,133\,167\,002\,880 - 31 = 212\,133\,167\,002\,849.$$ ■

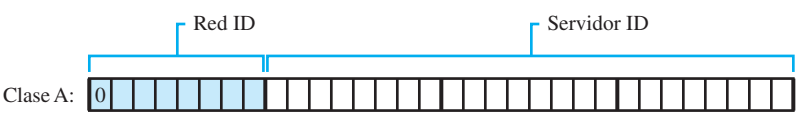
Ejemplo 9.3.5 Direcciones de internet

Para comunicar eficazmente, cada equipo de una red necesita un nombre distintivo denominado una dirección. En internet esta dirección es actualmente un número de 32 bits llamado la dirección de Protocolo de Internet (IP) (aunque direcciones de 128 bits están siendo gradualmente acomodadas por el crecimiento del internet). Por razones técnicas, algunas computadoras tienen más de una dirección, mientras que otros conjuntos de computadoras, que utilizan internet sólo esporádicamente, pueden compartir un conjunto de direcciones que se asignan de forma temporal. Como los números de teléfono, las direcciones IP se dividen en partes: uno, el ID de red, especifica la red local a la que pertenece una computadora dada y el otro, el ID del servidor, especifica la computadora en particular.

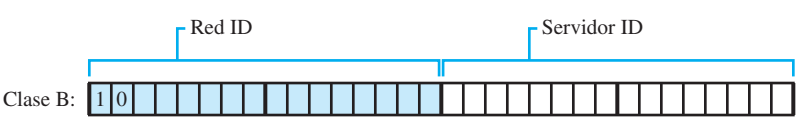
Un ejemplo de una dirección IP es 10001100 11000000 00100000 10001000, donde los 32 bits se han dividido en cuatro grupos de 8 para facilitar la lectura. Para facilitar la lectura aún más, las direcciones IP se escriben normalmente como "puntos decimales", en el que cada grupo de 8 bits se convierte en un número decimal entre 0 y 255. Por ejemplo, la dirección IP anterior se convierte en 140.192.32.136.

Para acomodar los diferentes tamaños de las redes locales conectadas a través del internet, los identificadores de red se dividen en varias clases, las más importantes de las cuales son llamadas *A*, *B* y *C*. En cada clase, un ID del servidor no puede consistir de todos 0 o todos 1.

Se utilizan identificadores de red de clase *A* para grandes redes locales. El bit del extremo izquierdo se hace 0 y los 8 bits de la izquierda dan el identificador de red completo. Los 24 bits restantes se utilizan para cada identificador del servidor. Sin embargo, no se permite 000000000 ni 01111111 como un identificador de red para una dirección IP de clase *A*.



Los identificadores de red de clase *B* se utilizan para redes locales de medianas a grandes. Los dos bits del extremo izquierdo se hacen igual a 10 y los 16 bits de la izquierda dan el identificador de red completo. Los 16 bits restantes se utilizan para cada identificador del servidor.



Los identificadores de red de la clase *C* se utilizan para pequeñas redes locales. Los tres bits del extremo izquierdo se hacen igual a 110 y los 24 bits de la izquierda dan el identificador de red completo. Los 8 bits restantes se utilizan para cada identificador del servidor particular.

a. Compruebe que la forma con punto decimal de 10001100 11000000 00100000 10001000 es 140.192.32.136.

b. ¿Cuántas redes de clase *B* pueden existir?

c. ¿Cuál es la forma de punto decimal de la dirección IP de una computadora en una red de clase *B*?

d. ¿Cuántos identificadores de servidor pueden existir para una red de clase *B*?

Solución

a. $10001100 = 1\cdot 2^7 + 1\cdot 2^3 + 1\cdot 2^2 = 128 + 8 + 4 = 140$
$11000000 = 1\cdot 2^7 + 1\cdot 2^6 = 128 + 64 = 192$
$00100000 = 1\cdot 2^5 = 32$
$10001000 = 1\cdot 2^7 + 1\cdot 2^3 = 128 + 8 = 136$

b. El identificador de red para una red de clase *B* consta de 16 bits y comienza con 10. Ya que hay dos opciones para cada una de las 14 posiciones restantes (0 o 1), el número total de identificadores de red posible es 2^{14}, o 16 384.

c. La parte del identificador de red de una dirección IP de clase *B* proviene de

10000000 00000000 a 10111111 11111111.

Como puntos decimales, estos números van de 128.0 a 191.255 ya que $10000000_2 = 128_{10}$, $00000000_2 = 0_{10}$, $10111111_2 = 191_{10}$ y $11111111_2 = 255_{10}$. Por tanto la forma de punto decimal de la dirección IP de una computadora en una red de clase *B* es $w.x.y.z$, donde $128 \le w \le 191$, $0 \le x \le 255$, $0 \le y \le 255$ y $0 \le z \le 255$. Sin embargo, a y y z no se les permiten a ambas ser 0 o 255 ya que los identificadores de servidor no pueden consistir de todos 0 o todos 1.

d. Para una red de clase *B*, se utilizan 16 bits para identificadores de servidor. Se tienen dos opciones (0 o 1) para cada una de las 16 posiciones da un potencial total de 2^{16} o 65 536, identificadores de servidor. Pero ya que dos de estos no están permitidos (todos 0 o todos 1), el número total de identificadores de servidor es 65 534. ■

La regla de inclusión/exclusión

La regla de la suma dice cuántos elementos se encuentran en una unión de conjuntos si los conjuntos son mutuamente disjuntos. Ahora consideremos la cuestión de cómo determinar el número de elementos en una unión de conjuntos cuando algunos de los conjuntos se superponen. Por simplicidad, comencemos observando una unión de dos conjuntos *A* y *B*, como se muestra en la figura 9.3.5.

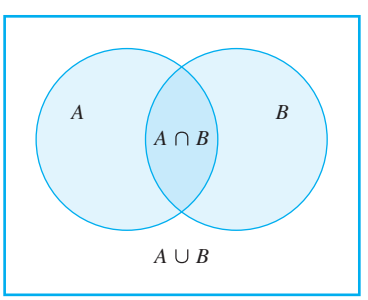


Figura 9.3.5

Primero observe que el número de elementos en $A \cup B$ varía de acuerdo con el número de elementos que los dos conjuntos tienen en común. Si A y B no tienen elementos en común, entonces, $N(A \cup B) = N(A) + N(B)$. Si A y B coinciden, entonces $N(A \cup B) = N(A)$. Por tanto cualquier fórmula general para $N(A \cup B)$ debe contener una referencia al número de elementos que dos conjuntos tienen en común, $N(A \cap B)$, así como a $N(A)$ y $N(B)$.

La forma más simple de deducir una fórmula para $N(A \cup B)$ es razonar de la forma siguiente: El número $N(A)$ cuenta con los elementos que se encuentran en A y no están en B y también los elementos que se encuentran tanto en A como en B. Del mismo modo, el número $N(B)$ cuenta con los elementos que se encuentran en B y no en A y, también, los elementos que están tanto en A como en B. Por tanto cuando se agregan los dos números $N(A)$ y $N(B)$, los elementos que se encuentran en A y en B se cuentan dos veces. Para obtener una cifra exacta de los elementos en $A \cup B$, es necesario restar el número de elementos que se encuentran tanto en A como en B. Porque éstos son los elementos en $A \cap B$,

$$N(A \cup B) = N(A) + N(B) - N(A \cap B).$$

Nota Una demostración alternativa se bosqueja en el ejercicio 46 al final de la sección.

Un análisis similar da una fórmula para el número de elementos en una unión de tres conjuntos, como se muestra en el teorema 9.3.3.

Teorema 9.3.3 La regla de inclusión/exclusión de dos o tres conjuntos

Si A, B y C son conjuntos finitos cualesquiera, entonces

$$N(A \cup B) = N(A) + N(B) - N(A \cap B)$$

y

$$N(A \cup B \cup C) = N(A) + N(B) + N(C) - N(A \cap B) - N(A \cap C) - N(B \cap C) + N(A \cap B \cap C).$$

Puede demostrarse con inducción matemática (vea el ejercicio 48 al final de esta sección) que fórmulas análogas a las del teorema 9.3.3 se mantienen para conjuntos de cualquier número finito de conjuntos.

Ejemplo 9.3.6 Conteo de elementos de una unión general

a. ¿Cuántos enteros del 1 al 1 000 son múltiplos de 3 o múltiplos de 5?

b. ¿Cuántos enteros del 1 al 1 000 ni son múltiplos de 3 ni son múltiplos de 5?

Solución

a. Sea A = el conjunto de todos los enteros del 1 al 1 000 que son múltiplos de 3.
Sea B = el conjunto de todos los enteros del 1 al 1 000 que son múltiplos de 5.

Entonces

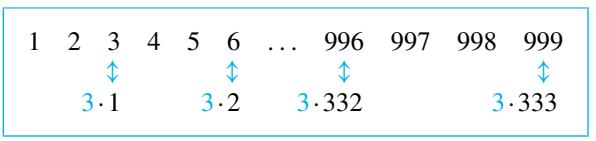
$A \cup B$ = el conjunto de todos los enteros del 1 al 1 000 que son múltiplos de 3 o múltiplos de 5

y

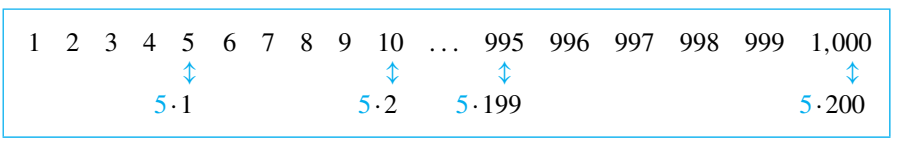
$A \cap B$ = el conjunto de todos los enteros del 1 al 1 000 que son múltiples tanto de 3 como de 5
= el conjunto de todos los enteros del 1 al 1 000 que son múltiplos de 15.

[Ahora calcule $N(A)$, $N(B)$ y $N(A \cap B)$ y utilice la regla de inclusión/exclusión para encontrar $N(A \cup B)$.]

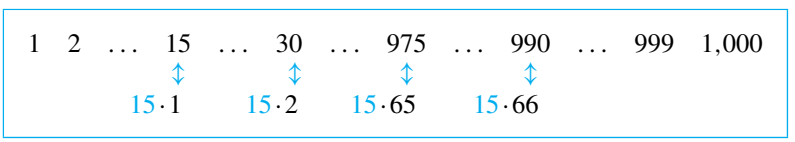
Ya que cada tercer entero del 3 al 999 es un múltiplo de 3, cada uno se puede representar en la forma $3k$, para algún entero k del 1 al 333. Por tanto hay 333 múltiplos de 3 entre 1 y 1 000 y así $N(A) = 333$.



Similarmente, cada múltiplo de 5 del 1 al 1 000 tiene la forma $5k$, para algún entero k entre 1 y 200.



Por tanto hay 200 múltiplos de 5 del 1 al 1 000 y $N(B) = 200$. Por último, cada múltiplo de 15 que va del 1 al 1 000 tiene la forma $15k$, para algún entero k del 1 al 66 (ya que $990 = 66 \cdot 15$).



Por tanto hay 66 múltiplos de 15 del 1 al 1 000 y $N(A \cap B) = 66$. Por la regla de inclusión/exclusión se tiene que

$$\begin{aligned} N(A \cup B) &= N(A) + N(B) - N(A \cap B) \\ &= 333 + 200 - 66 \\ &= 467. \end{aligned}$$

Por tanto, 467 enteros del 1 al 1 000 son múltiplos de 3 o múltiplos de 5.

b. Hay 1 000 enteros del 1 al 1 000 y por el inciso *a*), 467 de estos son múltiplos de 3 o múltiplos de 5. Así, por la regla de la diferencia, hay $1\,000 - 467 = 533$ que ni son múltiplos de 3 ni múltiplos de 5. ■

Observe que la solución del inciso *b*) del ejemplo 9.3.6 escondió un uso de la ley de De Morgan. El número de elementos que no están ni en A ni están en B es $N(A^c \cap B^c)$ y por la ley de De Morgan, $A^c \cap B^c = (A \cup B)^c$. Así que $N((A \cup B)^c)$ se calcula usando la regla de diferencia de conjuntos: $N((A \cup B)^c) = N(U) - N(A \cup B)$, donde el universo U es el conjunto de todos los enteros de 1 al 1 000. Los ejercicios del 37 al 39 al final de esta sección exploran esta técnica aún más.

Ejemplo 9.3.7 Conteo del número de elementos en una intersección

Un profesor en una clase de matemáticas discretas pasa un formato pidiendo a los estudiantes que registren todos los cursos de matemáticas y de informática que han tomado recientemente. Encontrando que de un total de 50 alumnos de la clase,

30 tomaron precálculo;
18 tomaron cálculo;
26 tomaron Java;
9 tomaron tanto precálculo como cálculo;
16 tomaron tanto precálculo como Java;
8 tomaron tanto cálculo como Java;
47 tomaron al menos uno de los tres cursos.

Observe que cuando escribimos "30 estudiantes tomaron precálculo", entendemos que el número total de estudiantes que tomaron precálculo es 30 y nos permite la posibilidad de que algunos de estos estudiantes hubiese tomado uno o dos de los otros cursos. Si queremos decir que 30 estudiantes tomaron *sólo* precálculo (y no cualquiera de los otros cursos), lo diremos explícitamente.

a. ¿Cuántos estudiantes no tomaron ninguno de los tres cursos?

b. ¿Cuántos estudiantes tomaron los tres cursos?

c. ¿Cuántos estudiantes tomaron precálculo y cálculo pero no Java? ¿Cuántos estudiantes tomaron precálculo pero ni cálculo ni Java?

Solución

a. Por la regla de diferencia, el número de estudiantes que no tomó ninguno de los tres cursos es igual al número de la clase menos el número que tomó al menos un curso. Por tanto el número de estudiantes que no tomó ninguno de los tres cursos es

$$50 - 47 = 3.$$

b. Sea

$$P = \text{el conjunto de estudiantes que tomaron precálculo}$$
$$C = \text{el conjunto de estudiantes que tomaron cálculo}$$
$$J = \text{el conjunto de estudiantes que tomaron Java.}$$

Entonces, por la regla de inclusión/exclusión,

$$N(P \cup C \cup J) = N(P) + N(C) + N(J) - N(P \cap C) - N(P \cap J) - N(C \cap J) + N(P \cap C \cap J)$$

Sustituyendo valores conocidos, obtenemos

$$47 = 30 + 26 + 18 - 9 - 16 - 8 + N(P \cap C \cap J).$$

Resolviendo para $N(P \cap C \cap J)$ se obtiene

$$N(P \cap C \cap J) = 6.$$

Por tanto hay seis estudiantes que tomaron los tres cursos. En general, si conoce cualquiera de siete de los ocho términos en la fórmula de inclusión/exclusión de tres conjuntos, se puede resolver para el octavo término.

c. Para responder las preguntas del inciso *c*), observe el diagrama de la figura 9.3.6.

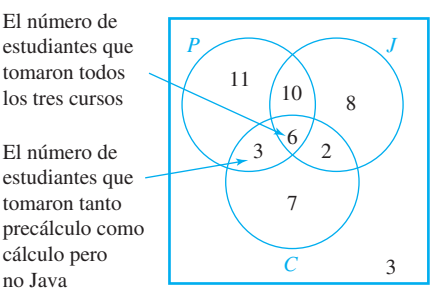


Figura 9.3.6

Ya que $N(P \cap C \cap J) = 6$, se pone el número 6, dentro de la región más interna. Entonces se trabaja hacia afuera para encontrar el número de estudiantes, representados por las otras regiones del diagrama. Por ejemplo, ya que nueve estudiantes tomaron tanto precálculo como cálculo y seis tomaron los tres cursos, $9 - 6 = 3$ estudiantes tomaron precálculo y cálculo pero no Java. Similarmente, ya que 16 estudiantes tomaron precálculo y cálculo y seis tomaron los tres cursos, $16 - 6 = 10$ estudiantes tomaron precálculo y cálculo pero no Java. Ahora el número total de estudiantes que tomaron precálculo es 30. De estos 30, tres también tomaron cálculo pero no Java, diez tomaron Java pero no cálculo y seis tomaron tanto cálculo como Java. Lo que da que 11 estudiantes tomaron precálculo, pero ninguno de los otros dos cursos.

Se puede utilizar un análisis similar para completar los números para las demás regiones del diagrama. ■

Autoexamen

1. La regla de adición dice que si un conjunto finito equivale a la unión de k subconjuntos distintos mutuamente disjuntos $A_1, A_2, \ldots, A_k$, entonces _____.
2. La regla de la diferencia dice que si A es un conjunto finito y B es un subconjunto de A, entonces _____.
3. Si S es un espacio muestral finito y A es un evento en S entonces, la probabilidad de A^c es igual a _____.
4. La regla de inclusión/exclusión de dos conjuntos dice que si A y B son conjuntos finitos cualesquiera, entonces _____.
5. La regla de inclusión/exclusión de tres conjuntos dice que si A, B y C son conjuntos finitos cualesquiera, entonces _____.

Conjunto de ejercicios 9.3

1. a. ¿Cuántas cadenas de bits consisten de uno a cuatro dígitos? (Cadenas de diferentes longitudes se consideran distintas. Y así 10 y 0010 son cadenas distintas.)
   b. ¿Cuántas cadenas de bits consisten de cinco a ocho dígitos?

2. a. ¿Cuántas cadenas de dígitos hexadecimales consisten de uno a tres dígitos? (Recuerde que los números hexadecimales se construyen usando los 16 dígitos 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F.)
   b. ¿Cuántas cadenas de dígitos hexadecimales consisten de dos a cinco dígitos?

3. a. ¿Cuántos enteros entre 1 y 999 no tienen dígitos repetidos?
   b. ¿Cuántos enteros entre 1 y 999 tienen al menos un dígito repetido?
   c. ¿Cuál es la probabilidad de que un entero elegido aleatoriamente entre 1 y 999 tenga al menos un dígito repetido?

4. ¿Cuántos arreglos en una fila de no más de tres letras se pueden formar con las letras de la palabra *NETWORK* (sin repeticiones permitidas)?

5. a. ¿Cuántos enteros de cinco dígitos (enteros de 10 000 a 99 999) son divisibles entre 5?
   b. ¿Cuál es la probabilidad de que un número de cinco dígitos elegido aleatoriamente sea divisible entre 5?

6. En un estado dado, las placas consisten de cero a tres letras seguidas de cero a cuatro dígitos, sin embargo, con la provisión de que no está permitida una placa en blanco.
   a. ¿Cuántas placas diferentes se pueden producir en el estado?
   b. Suponga que no se permitieron 85 combinaciones de letras debido a su potencial de ofender. ¿Cuántas placas diferentes puede producir el estado?

7. En otro estado, todas las placas consisten de cuatro a seis símbolos elegidos de las 26 letras del alfabeto junto con los diez dígitos del 0 al 9.
   a. ¿Cuántas placas son posibles si se permite la repetición de símbolos?
   b. ¿Cuántas placas no contienen ningún símbolo repetido?
   H c. ¿El número de matrículas tienen al menos un símbolo repetido?
   d. ¿Cuál es la probabilidad de que una placa elegida aleatoriamente tenga un símbolo repetido?

8. En una cierta empresa, las contraseñas deben tener de 3 a 5 símbolos largos y compuestos de las 26 letras del alfabeto, los diez dígitos del 0 al 9 y los 14 símbolos!, @, #, $, %, ^, &, *, (,), −, +, { y }.
   a. ¿Cuántas contraseñas son posibles si se permite la repetición de símbolos?
   b. ¿Cuántas contraseñas no contienen símbolos repetidos?

c. ¿Cuántas contraseñas tienen al menos un símbolo repetido?
d. ¿Cuál es la probabilidad de que una contraseña elegida aleatoriamente tenga n símbolos repetidos?

9. **a.** Considere el siguiente segmento de algoritmo:

```
for i := 1 to 4
    for j := 1 to i
    [Enunciados en el cuerpo del bucle interior.
    Ninguno contiene enunciados
    con ramificaciones fuera del bucle.]
    next j
next i
```

¿Cuántas veces se iterarán los bucles internos cuando el algoritmo se implemente y ejecute?

b. Sea n un entero positivo y considere el siguiente segmento de algoritmo:

```
for i := 1 to n
    for j := 1 to i
    [Enunciados en el cuerpo del bucle interior.
    Ninguno contiene enunciados
    con ramificaciones fuera del bucle.]
    next j
next i
```

¿Cuántas veces iterarán los bucles internos cuando el algoritmo se implemente y ejecute?

✶ 10. Una calculadora tiene una pantalla de ocho dígitos y un punto decimal que se encuentra en el extremo derecho de la pantalla, en el extremo izquierdo o entre cualquier par de dígitos. La calculadora también puede mostrar un signo en el extremo izquierdo del número. ¿Cuántos números distintos puede mostrar la calculadora? (Observe que algunos números son iguales, como 1.9, 1.90 y 01.900 y por tanto, no deben contarse dos veces.)

11. a. ¿De cuántas maneras pueden las letras de la palabra *QUICK* ordenarse en una fila?
b. ¿De cuántas formas pueden las letras de la palabra *QUICK* ordenarse en una fila si la Q y la U deben permanecer al lado juntas en el orden QU?
c. ¿De cuántas formas pueden las letras de la palabra *QUICK* ordenarse en una fila si las letras QU deben permanecer juntas pero pueden estar en el orden QU o en el orden UQ?

12. a. ¿De cuántas maneras pueden las letras de la palabra *THEORY* ordenarse en una fila?
b. ¿De cuántas maneras pueden las letras de la palabra *THEORY* ordenarse en una fila si T y H deben permanecer juntas ya sea como *TH* o como *HT*?

13. Un grupo de ocho personas asisten al cine juntos.
a. Dos de los ocho insisten en sentarse uno al lado del otro. ¿De cuántas maneras pueden los ocho sentarse juntos en una fila?
b. Dos de las personas no se caen bien y no desean sentarse juntas. ¿Ahora de cuántas maneras pueden sentarse los ocho juntos en una fila?

14. Un compilador primitivo reconocía nombres de variable de acuerdo con las reglas siguientes: Los nombres de variables numéricas deben comenzar con una letra y después de una letra podría seguir otra letra o un dígito o nada en absoluto. Los nombres de variables de cadena deben comenzar con el símbolo $ seguido de una letra, que podría ser seguida por otra letra, un dígito o nada en absoluto. ¿Cuántos nombres de variables distintos fueron reconocidos por este compilador?

***H* 15.** Los identificadores en un determinado lenguaje de base de datos deben comenzar con una letra y después la letra puede ser seguida por otros caracteres, que pueden ser letras, dígitos o caracteres de subrayado (_). Sin embargo, 82 palabras clave (todos con 15 caracteres o menos) se reservan y no se pueden utilizar como identificadores. ¿Cuántos identificadores con 30 o menos caracteres son posibles? (Escriba la respuesta usando la notación de suma y evalúe con una fórmula de la sección 5.2).

16. a. ¿Si cualquiera de siete dígitos podría utilizarse para formar un número de teléfono, el número telefónico de siete dígitos no tendría dígitos repetidos?
b. ¿Cuántos números de teléfono de siete dígitos tendrían al menos un dígito repetido?
c. ¿Cuál es la probabilidad de que un número de teléfono de siete dígitos aleatorio tendría al menos un dígito repetido?

17. a. ¿Cuántas cadenas de cuatro dígitos hexadecimales no tienen dígitos repetidos?
b. ¿Cuántas cadenas de cuatro dígitos hexadecimales tienen al menos un dígito repetido?
c. ¿Cuál es la probabilidad de que una cadena elegida aleatoriamente de cuatro dígitos hexadecimales tenga al menos un dígito repetido?

18. Tal como la regla de la diferencia da lugar a una fórmula para la probabilidad del complemento de un evento, por lo que las reglas de inclusión/exclusión de adición dan lugar a las fórmulas para la probabilidad de la unión de eventos mutuamente disjuntos y para una unión general de eventos (no necesariamente mutuamente excluyentes).
a. Demuestre que para eventos mutuamente disjuntos A y B,

$$P(A \cup B) = P(A) + P(B).$$

b. Demuestre que para cualesquiera eventos A y B.

$$P(A \cup B) = P(A) + P(B) - P(A \cap B).$$

***H* 19.** Un candado de combinación requiere tres selecciones de números, cada una del 1 al 39. Suponga que el candado está construido de tal forma que ningún número se puede utilizar dos veces en una fila pero el mismo número puede aparecer en primer y en tercer lugar. Por ejemplo, 20 13 20 sería aceptable pero 20 20 13 no. ¿Cuántas diferentes combinaciones son posibles?

✶ 20. **a.** ¿Cuántos enteros del 1 a 100 000 contienen exactamente el dígito 6 una vez?
b. ¿Cuántos enteros entre 1 y 100 000 contienen al menos una vez el dígito 6?
c. Si un entero es elegido aleatoriamente del 1 al 100 000, ¿cuál es la probabilidad de que contenga dos o más veces el dígito 6?

H ✶ **21.** Seis nuevos empleados, de los cuales dos están casados entre sí, se les deben asignar seis escritorios que se alinean en una fila. Si se realiza aleatoriamente la asignación de empleados a los escritorios, ¿cuál es la probabilidad de que el matrimonio tendrán escritorios no adyacentes? (*Sugerencia:* Primero encuentre la probabilidad de que la pareja tenga escritorios adyacentes y después, reste este número de 1.)

✶ 22. Considere cadenas de longitud n sobre el conjunto $\{a, b, c, d\}$.
a. ¿Cuántas de esas cadenas contendrán al menos un par de caracteres adyacentes que son iguales?
b. Si una cadena de longitud diez sobre $\{a, b, c, d\}$ se elige aleatoriamente, ¿cuál es la probabilidad de que contiene al menos un par de caracteres adyacentes que son iguales?

23. **a.** ¿Cuántos enteros del 1 al 1 000 son múltiplos de 4 o múltiplos de 7?
b. Suponga que se elige aleatoriamente un entero entre 1 y 1 000. Utilice el resultado del inciso *a*) para encontrar la probabilidad de que el entero es un múltiplo de 4 o un múltiplo de 7.
c. ¿Cuántos enteros del 1 al 1 000 ni son múltiplos de 4 ni múltiplos de 7?

24. a. ¿Cuántos enteros del 1 al 1 000 son múltiplos de 2 o múltiplos de 9?
b. Suponga que se elige aleatoriamente un entero entre 1 y 1 000. Utilice el resultado del inciso *a*) para encontrar la probabilidad de que el entero es un múltiplo de 2 o un múltiplo de 9.
c. ¿Cuántos enteros del 1 al 1 000 ni son múltiplos de 2 ni múltiplos de 9?

25. *Conteo de cadenas*:
a. Realice una lista de todas las cadenas de bits de longitud cero, uno, dos, tres y cuatro que no contengan el patrón de bits 111.
b. Para cada entero $n \geq 0$, sea d_n = número de cadenas de bits de longitud n que no contienen el patrón de bits 111. Encuentre d_0, d_1, d_2, d_3 y d_4.
c. Encuentre una relación de recurrencia para $d_0, d_1, d_2, \ldots$.
d. Utilice los resultados de los incisos *b*) y *c*) para encontrar el número de cadenas de bits de longitud cinco que no contengan el patrón 111.

26. *Conteo de cadenas*: Considere el conjunto de todas las cadenas de a, b y c.
a. Haga una lista de todas estas cadenas de longitud cero, uno, dos y tres que no contengan el patrón aa.
b. Para cada entero $n \geq 0$, sea s_n = número de cadenas de a, b y c, de longitud n que no contienen el patrón aa. Encuentre s_0, s_1, s_2 y s_3.
H **c.** Encuentre una relación de recurrencia para $s_0, s_1, s_2, \ldots$.
d. Utilice los resultados de los incisos *b*) y *c*) para encontrar el número de cadenas de a, b y c de longitud cuatro que no contengan el patrón aa.
H **e.** Utilice la técnica descrita en la sección 5.8 para encontrar una fórmula explícita para $s_0, s_1, s_2, \ldots$.

27. Para cada entero $n \geq 0$, sea a_k el número de cadenas de bits de longitud n que no contienen el patrón 101.
a. Demuestre que $a_k = a_{k-1} + a_{k-3} + a_{k-4} + \ldots + a_0 + 2$, para todos los enteros $k \geq 3$.
b. Utilice el resultado del inciso *b* para mostrar que si $k \geq 3$ entonces, $a_k = 2a_{k-1} - a_{k-2} + a_{k-3}$.

✶ 28. Para cada entero $n \geq 2$ sea a_n el número de permutaciones de $\{1, 2, 3, \ldots, n\}$ en las que ningún número está a más de un lugar movido de su posición "natural". Así, $a_1 = 1$ ya que una permutación de $\{1\}$, es decir 1, no se mueve 1 de su posición natural. También $a_2 = 2$ ya que ninguna de las dos permutaciones de $\{1, 2\}$, es decir 12 y 21, mueve el número más de un lugar de su posición natural.
a. Determine a_3.
b. Encuentre una relación de recurrencia para $a_1, a_2, a_3, \ldots$

29. Consulte el ejemplo 9.3.5.
a. Escriba la siguiente dirección IP en forma de punto decimal:

11001010 00111000 01101011 11101110.

b. ¿Cuántas redes de clase A pueden existir?
c. ¿Cuál es la forma de punto decimal de la dirección IP de una computadora en una red de clase A?
d. ¿Cuántos identificadores de servidor pueden existir para una red de clase A?
e. ¿Cuántas redes de clase C pueden existir?
f. ¿Cuál es la forma de punto decimal de la dirección IP de una computadora en una red de clase C?
g. ¿Cuántos identificadores de servidor pueden existir para una red de clase C?
h. ¿Cómo puede decir, observando el primero de los cuatro números en la forma de punto decimal de una dirección IP, de qué clase es la red? Explique.
i. Una dirección IP es 140.192.32.136. ¿De qué clase de red proviene?
j. Una dirección IP es 202.56.107.238. ¿De qué clase de red proviene?

✶ 30. Una fila en un salón de clase tiene n asientos. Sea s_n el número de formas de conjuntos no vacíos de estudiantes que se pueden sentar en la fila tal que ningún estudiante se siente directamente junto a cualquier otro estudiante. (Por ejemplo, una fila de tres asientos podría tener un solo estudiante en cualquiera de los asientos o un par de estudiantes en los dos asientos exteriores. Así $s_3 = 4$.) Encuentre una relación de recurrencia para $s_1, s_2, s_3, \ldots$.

31. Suponga que los cumpleaños son equiprobables en cualquiera de los 12 meses del año.
a. Dado un grupo de cuatro personas A, B, C y D, ¿cuál es el número total de formas en las que los meses de nacimiento se pueden asociar con A, B, C y D? (Por ejemplo, A y B podrían haber nacido en mayo, C en septiembre y D en febrero. Como otro ejemplo, A podría haber nacido en enero, B en junio, C en marzo y D en octubre.)

b ¿De cuántas formas los meses del nacimiento podrían asociarse con A, B, C y D por lo que no hay dos personas que compartan el mismo mes de nacimiento?

c. ¿De cuántas formas podrían los meses de nacimiento asociarse con A, B, C y D para que al menos dos personas compartan el mismo mes de nacimiento?

d. ¿Cuál es la probabilidad de que al menos dos personas de A, B, C y D compartan el mismo mes de nacimiento?

e. ¿Qué tan grande debe ser n para que en cualquier grupo de n personas, la probabilidad de que dos o más compartan el mismo mes de nacimiento es al menos de 50%?

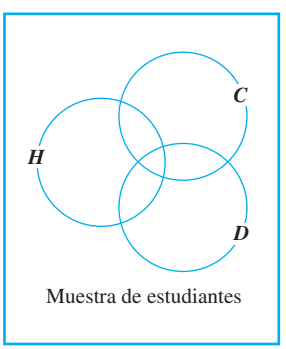
***H* 32.** ¿Suponiendo que todos los años tienen 365 días y todos los cumpleaños ocurren con igual probabilidad, ¿qué tan grande debe ser n para que en cualquier grupo elegido de forma aleatoria de n personas, la probabilidad de que dos o más tengan el mismo cumpleaños sea al menos 1/2? (Esto se llama el **problema del cumpleaños**. Muchas personas encuentran respuestas sorprendentes.)

33. Un colegio realizó una encuesta para explorar los logros e intereses académicos de los estudiantes. Pidió a los estudiantes colocar controles al lado de los números de todos los enunciados que fueron verdaderos para ellos. El enunciado #1 fue "Yo estaba en el cuadro de honor inscrito en el último curso", el enunciado #2 fue "Pertenezco a un club académico, tales como el club de matemáticas o el club de español" y el enunciado #3 fue "Soy especialista en al menos dos temas". De una muestra de 100 estudiantes, 28 indicaron el #1, 26 el #2 y 14 el #3, 8 indicaron tanto el #1 como el #2, 4 indicaron tanto al #1 como al #3, 3 indicaron tanto al #2 como al #3 y 2 indicaron los tres enunciados.

a. ¿Cuántos estudiantes indicaron al menos uno de los enunciados?

b. ¿Cuántos estudiantes no indicaron ninguno de los enunciados?

c. Sea H el conjunto de estudiantes que indican el #1, C el conjunto de estudiantes que indican el #2 y D el conjunto de estudiantes que indican el #3. Llene los números de todas las ocho regiones del diagrama siguiente.



d. ¿Cuántos estudiantes indicaron el #1 y el #2 pero no el #3?

e. ¿Cuántos estudiantes indicaron el #2 y el #3 pero no el #1?

f. ¿Cuántos estudiantes indicaron el #2 pero ninguno de los otros dos?

34. Se realizó un estudio realizado para determinar la eficacia de tres medicamentos diferentes: A, B y C, para aliviar el dolor de cabeza. Durante el periodo cubierto por el estudio, 50 individuos tuvieron la oportunidad de usar todos los tres medicamentos. Se obtuvieron los siguientes resultados:

21 reportaron mejoría usando el medicamento A.

21 reportaron mejoría usando el medicamento B.

31 reportaron mejoría usando el medicamento C.

9 reportaron mejoría usando ambos medicamentos A y B.

14 reportaron mejoría usando ambos medicamentos A y C.

15 reportaron mejoría usando ambos medicamentos B y C.

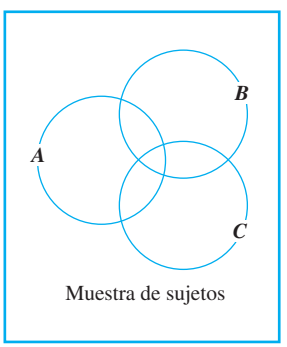
41 reportaron mejoría usando al menos uno de los medicamentos.

Observe que algunos de los 21 sujetos que reportaron mejoría con el medicamento A pueden también reportar mejoría con los medicamentos B o C. Un fenómeno similar puede ser cierto para los otros datos.

a. ¿Cuánta gente mejora sin los medicamentos?

b. ¿Cuántas personas mejoran usando los tres medicamentos?

c. Sea A el conjunto de todos los sujetos que obtuvieron mejoría con los medicamentos A, B el conjunto de todos los sujetos que mejoraron con los medicamentos B y C el conjunto de todos los sujetos que mejoraron con el medicamento C. Llene los números para todas las ocho regiones del diagrama siguiente.



d. ¿Cuántos sujetos mejoran sólo con el medicamento A?

35. Un interesante uso de la regla de inclusión/exclusión es comprobar la consistencia de los números de una encuesta. Por ejemplo, supongamos que un encuestador de opinión pública indica que de una muestra nacional de 1 200 adultos, 675 está casados, 682 tienen de 20 a 30 años de edad, 684 son mujeres, 195 están casadas y tienen de 20 a 30 años de edad, 467 son mujeres casadas, 318 son mujeres de 20 a 30 años de edad y 165 son mujeres casadas de 20 a 30 años de edad. ¿Son las cifras del encuestador consistentes? ¿Podría haber ocurrido como resultado de una muestra real de encuesta?

36. Llene en las razones de cada paso siguiente. Si A y B son conjuntos en un universo finito U, entonces

$$N(A \cap B) = N(U) - N((A \cap B)^c) \quad \underline{\text{(a)}}$$
$$= N(U) - N(A^c \cup B^c) \quad \underline{\text{(b)}}$$
$$= N(U) - (N(A^c) + N(B^c) - N(A^c \cap B^c)) \quad \underline{\text{(c)}}.$$

Para cada uno de los ejercicios del 37 al 39, el número de elementos en un conjunto dado se puede encontrar calculando el número en algún gran universo que no está en el conjunto y restarlo del total. En cada caso, como se indica en el ejercicio 34, se pueden utilizar las leyes de De Morgan y la regla de inclusión/exclusión para calcular el número que no está en el conjunto.

37. ¿Cuántos enteros positivos menores a 1 000 no tienen factores comunes con 1 000?

✶ 38. ¿Cuántas permutaciones de *abcde* existen en las que el primer carácter es *a*, *b* o *c* y el último carácter es *c*, *d* o *e*?

✶ 39. ¿Cuántos enteros entre 1 y 999 999 contienen cada uno de los dígitos 1, 2 y 3? (*Sugerencia:* Para cada $i = 1, 2$ y 3, sea A_i el conjunto de todos los enteros entre 1 y 999 999 que no contienen el dígito i.)

Para los ejercicios 40 y 41, utilice la definición de la función phi ϕ de la página 396.

***H* 40.** Utilice el principio de inclusión/exclusión para demostrar lo siguiente: Si $n = pq$, donde p y q son números primos distintos, entonces $\varphi(n) = (p - 1)(q - 1)$.

41. Utilice el principio de inclusión/exclusión para demostrar lo siguiente: Si $n = pqr$, donde p, q y r son números primos distintos, entonces $\varphi(n) = (p - 1)(q - 1)(r - 1)$.

42. Un jugador decide realizar juegos sucesivos de blackjack hasta que pierda tres veces consecutivas. (Así el jugador podría jugar cinco juegos perdiendo el primero, ganando al segundo y perdiendo el tercero y final o ganar los dos primeros dos y perdiendo el tercero y final. Estas posibilidades se pueden simbolizar como *LWLLL* y *WWLLL*). Sea g_n el número de formas, que el jugador puede realizar n juegos.
   a. Determine g_3, g_4 y g_5.
   b. Encuentre g_6.
   ***H* c.** Encuentre una relación de recurrencia para g_3, g_4, g_5,….

✶ 43. Un *desorden* del conjunto $\{1, 2,\ldots, n\}$ es una permutación que mueve cada elemento del conjunto de su posición "natural". Por tanto 21 es un desorden de $\{1, 2\}$ y 231 y 312 son desórdenes de $\{1, 2, 3\}$. Para cada entero positivo n, sea d_n el número de desórdenes del conjunto $\{1, 2,\ldots,n\}$.
   a. Determine d_1, d_2 y d_3.
   b. Encuentre d_4.
   ***H* c.** Encuentre una relación de recurrencia para d_1, d_2, d_3,….

44. Observe que un producto $x_1x_2x_3$, se puede poner entre paréntesis de dos maneras diferentes: $(x_1x_2)x_3$ y $x_1(x_2x_3)$. Del mismo modo, hay varias maneras de poner entre paréntesis $x_1x_2x_3x_4$. Esas dos formas son $(x_1x_2)(x_3x_4)$ y $x_1((x_2x_3)x_4)$. Sea P_n el número de poner entre paréntesis al producto $x_1x_2\ldots x_4$. Demuestre que si $P_1 = 1$, entonces

$$P_n = \sum_{k=1}^{n-1} P_k P_{n-k} \quad \text{para todos los enteros } n \geq 2.$$

(Resulta que la sucesión de P_1, P_2, P_3,... es la misma que la sucesión de números de Catalan: $P_n = C_{n-1}$ para todos los enteros $n \geq 1$. Vea el ejemplo 5.6.4.)

45. Use inducción matemática para demostrar el teorema 9.3.1.

46. Demuestre la regla de inclusión/exclusión de dos conjuntos A y B demostrando que $A \cup B$ puede particionarse en $A \cap B$, $A - (A \cap B)$ y $B - (A \cap B)$ y después utilizar las reglas de la suma y de la diferencia.

47. Demuestre la regla de la inclusión/exclusión para tres conjuntos.

***H* ✶ 48.** Use inducción matemática para demostrar la regla general de inclusión/exclusión:

Si $A_1, A_2,\ldots, A_n$ son conjuntos finitos, entonces

$$\begin{aligned} N(A_1 \cup A_2 \cup \cdots \cup A_n) &= \sum_{1 \leq i \leq n} N(A_i) - \sum_{1 \leq i < j \leq n} N(A_i \cap A_j) \\ &\quad + \sum_{1 \leq i < j < k \leq n} N(A_i \cap A_j \cap A_k) \\ &\quad - \cdots + (-1)^{n+1} N(A_1 \cap A_2 \cap \cdots \cap A_n). \end{aligned}$$

(La notación $\sum_{1 \leq i < j \leq n} N(A_i \cap A_j)$ significa que las cantidades de la forma $N(A_i \cap A_j)$ deben sumarse juntas para todos los enteros, i y j con $1 \leq i < j \leq n$.)

✶ 49. Un disco circular se divide en n distintos sectores, cada forma parece un pedazo de pastel y se encuentran todos en el punto central del disco. Cada sector está pintado de rojo, verde, amarillo o azul de tal manera que no hay dos sectores adyacentes pintados del mismo color. Sea S_n el número de formas para pintar el disco.

   ***H* a.** Encuentre una relación de recurrencia para S_k de S_{k-1} y S_{k-2} para cada entero $k \geq 4$.

   b. Encuentre una fórmula explicita para S_n para $n \geq 2$.

Respuestas del autoexamen

1. el número de elementos en A es igual a $N(A_1) + N(A_2) + \ldots + N(A_n)$ 2. el número de elementos en $A - B$ es la diferencia entre el número de elementos en A y el número de elementos en B, es decir, $N(A - B) = N(A) - N(B)$. 3. $1 - P(A)$ 4. $N(A \cup B) = N(A) + N(B) - N(A \cap B)$ 5. $N(A \cup B \cup C) = N(A) + N(B) + N(C) - N(A \cap B) - N(A \cap C) - N(B \cap C) + N(A \cap B \cap C)$

9.4 El principio de las casillas

La intuición sagaz, la hipótesis fértil, el valiente salto a una conclusión tentativa, son la moneda más valiosa del pensador en el trabajo —Jerome S. Bruner, 1960

El principio de las casillas establece que si n palomas vuelan hacia m casillas y $n > m$, entonces, al menos una casilla debe contener dos o más de las palomas. Este principio se ilustra en la figura 9.4.1 para $n = 5$ y $m = 4$. La figura *a*) muestra las palomas posadas junto a sus casillas y la figura *b*) muestra la correspondencia entre palomas y casillas. El principio de las casillas a veces se llama el *Principio de cajas de Dirichlet* porque fue enunciado formalmente primero por J. P. G. L. Dirichlet (1805-1859).

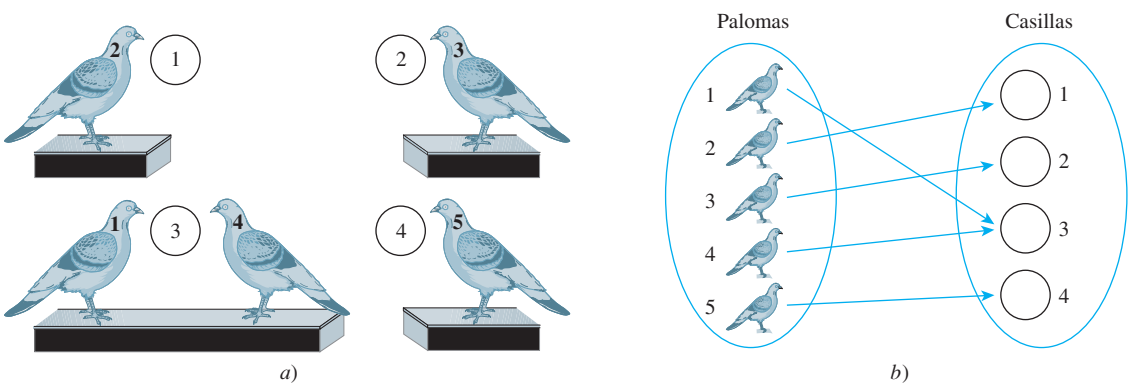


Figura 9.4.1

La figura *b*) sugiere la siguiente forma matemática para enunciar el principio.

Principio de las casillas

Una función de un conjunto finito a un conjunto finito más pequeño no puede ser uno a uno: debe haber al menos dos elementos en el dominio que tengan la misma imagen en el codominio.

Por tanto un diagrama de flecha para una función de un conjunto finito a un conjunto finito más pequeño debe tener al menos dos flechas del dominio que apuntan al mismo elemento del codominio. En la figura 9.4.1*b*), ambas flechas de las palomas 1 y 4 apuntan a la casilla 3.

Ya que realmente el principio de las casillas es fácil de aceptar de forma intuitiva, inmediatamente nos movemos a las aplicaciones, dejando la demostración formal para el final de la sección. Las aplicaciones del principio de las casillas van de lo totalmente obvio a lo muy sutil. En los ejercicios se presenta una muestra representativa y a continuación se presentan ejemplos.

Ejemplo 9.4.1 Aplicación del principio de las casillas

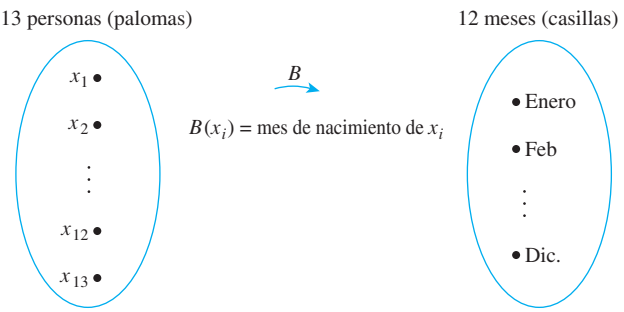
a. ¿En un grupo de seis personas, debe haber al menos dos que nacieron en el mismo mes? ¿En un grupo de trece personas, debe haber al menos dos que nacieron en el mismo mes? ¿Por qué?

b. Entre los residentes de la ciudad de Nueva York, ¿debe haber al menos dos personas con el mismo número de cabellos en sus cabezas? ¿Por qué?

Solución

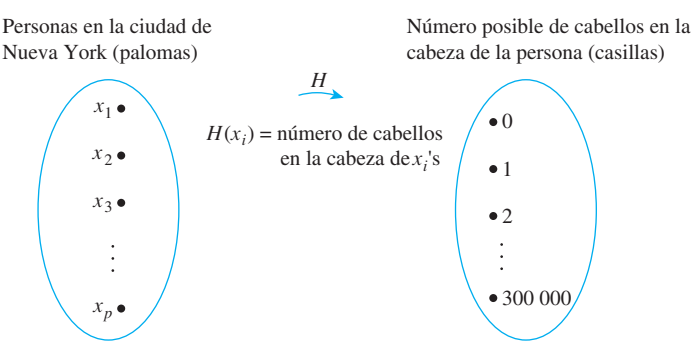
a. Un grupo de seis personas no debe contener dos personas que nacieron el mismo mes. Por ejemplo, seis personas podrían tener cumpleaños en cada uno de los seis meses de enero a junio.

Sin embargo, un grupo de trece personas, debe contener al menos dos que nacieron en el mismo mes, ya que sólo hay doce meses en un año y $13 > 12$. Para obtener la esencia de este razonamiento, piense en las trece personas como las palomas y en los doce meses del año como las casillas. Denote a las trece personas por los símbolos x_1, x_2,…, x_{13} y defina una función B del conjunto de personas al conjunto de doce meses como se muestra en el siguiente diagrama de flecha.



El principio de las casillas dice que no importa la asignación especial de meses a personas, debe haber al menos dos flechas que apunten al mismo mes. Por lo que, al menos dos personas deben haber nacido en el mismo mes.

b. La respuesta es sí. En este ejemplo, las palomas son las personas de la ciudad de Nueva York y las casillas son todos los números posibles de cabellos en cualquier cabeza de una persona. Llame a la población de la ciudad de Nueva York P. Se sabe que P es al menos de 5 000 000. También se sabe que el número máximo de cabellos en la cabeza de una persona no es más de 300 000. Defina una función H del conjunto de personas en la ciudad de Nueva York $\{x_1, x_2,\ldots, x_p\}$ al conjunto $\{0, 1, 2, 3,\ldots, 300\,000\}$, como se muestra a continuación.



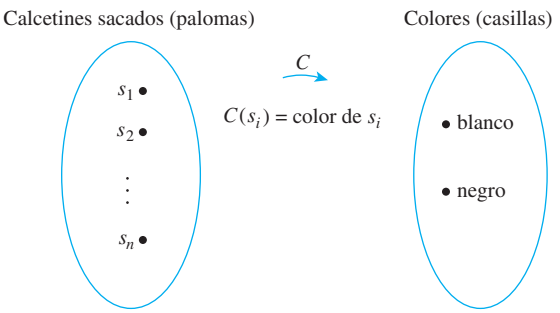
Ya que el número de personas en la ciudad de Nueva York es mayor que el número de posibles cabellos en sus cabezas, la función H no es uno a uno; al menos dos flechas apuntan al mismo número. Pero eso significa que al menos dos personas tienen el mismo número de cabellos en sus cabezas. ■

Ejemplo 9.4.2 Determinación del número de elecciones para asegurar un resultado

Un cajón contiene diez calcetines blancos y diez negros. Extrae un calcetín al azar. ¿Cuál es el número *mínimo* de calcetines que debe sacar para asegurarse de obtener un par que coincide? Explique la respuesta usando el principio de las casillas.

Solución Si selecciona sólo dos calcetines, pueden tener colores diferentes. Pero cuando se elige un tercer calcetín, debe tener el mismo color que uno de los calcetines que ya se ha elegido. Por tanto la respuesta es tres.

Esta respuesta se podría redactar más formalmente como sigue: Los calcetines que se sacan se denotan por s_1, s_2, s_3,…, s_n y considere la función C que envía cada calcetín a su color, como se muestra a continuación.



Si $n = 2$, C podría haber una correspondencia uno a uno (si los dos calcetines sacados fueran de diferentes colores). Pero si $n > 2$, entonces el número de elementos en el dominio de C es mayor que el número de elementos en el codominio de C. Por tanto por el principio de las casillas, C no es uno a uno: $C(s_i) = C(s_j)$ para algunas $s_i \neq s_j$. Esto significa que si se sacaron al menos tres calcetines, entonces al menos dos de ellos tienen el mismo color. ■

Ejemplo 9.4.3 Selección de un par de enteros con una suma dada

Sea $A = \{1, 2, 3, 4, 5, 6, 7, 8\}$.

a. Si se seleccionan cinco enteros de A, ¿debe haber al menos un par de enteros que sumen 9?

b. Si se seleccionan cuatro enteros de A, ¿debe haber al menos un par de enteros que sumen 9?

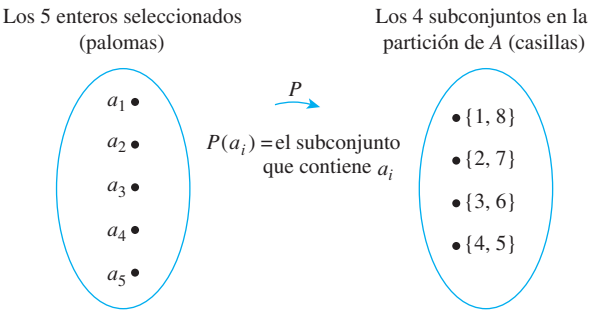
Solución

a. Sí. Se particiona el conjunto A en los siguientes cuatro subconjuntos disjuntos:

$$\{1, 8\}, \quad \{2, 7\}, \quad \{3, 6\} \quad \text{y} \quad \{4, 5\}$$

Observe que cada uno de los enteros en A se presenta en exactamente uno de los cuatro subconjuntos y que la suma de los enteros en cada subconjunto es 9. Así, si se seleccionan cinco enteros de A, entonces por el principio de las casillas, dos deben provenir del mismo subconjunto. Se deduce que la suma de estos dos enteros es 9.

Para ver exactamente cómo se aplica el principio de las casillas, sean las palomas los cinco enteros seleccionados (los llamaremos a_1, a_2, a_3, a_4 y a_5) y sean las casillas los subconjuntos de la partición. La función P de las palomas a las casillas se define haciendo a $P(a_i)$ el subconjunto que contiene a a_i.



La función P está bien definida ya que para cada entero a_i en el dominio, a_i pertenece a uno de los subconjuntos (ya que la unión de los subconjuntos es A) y a_i no pertenece a más de un subconjunto (ya que los subconjuntos son disjuntos).

Ya que hay más palomas que casillas, al menos dos palomas deben ir a la misma casilla. Así dos enteros distintos se envían al mismo conjunto. Pero eso implica que esos dos enteros son los dos elementos distintos del conjunto, por lo que su suma es 9. Más formalmente, por el principio de las casillas, ya que P no es uno a uno, hay enteros a_i y a_j tal que

$$P(a_i) = P(a_j) \quad \text{y} \quad a_i \neq a_j.$$

Pero entonces, por definición de P, a_i y a_j pertenecen al mismo subconjunto. Ya que los elementos en cada subconjunto suman 9, $a_i + a_j = 9$.

b. La respuesta es no. Se trata de un caso donde no se aplica el principio de las casillas; el número de palomas no es mayor que el número de casillas. Por ejemplo, si selecciona los números 1, 2, 3 y 4, entonces ya que la mayor suma de dos de estos números es 7, no hay dos de ellas que sumen 9. ■

Aplicación a expansiones decimales de fracciones

Una consecuencia importante del principio de las casillas es el hecho de que

la expansión decimal de cualquier número racional ya sea termina o se repite.

Un decimal termina como

$$3.625,$$

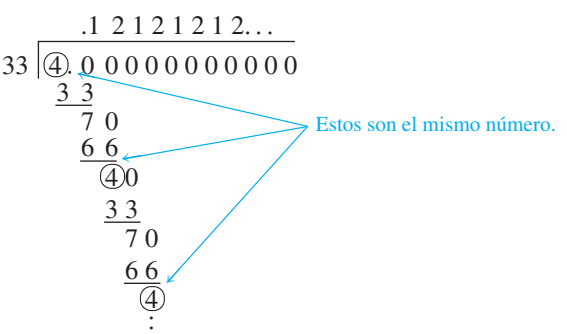
y un decimal con repetición es como

$$2.38\overline{246},$$

donde la barra sobre los dígitos 246 significa que estas cifras siempre se repiten.

Nota Estrictamente hablando una terminación decimal como 3.625 se pueden considerar como un decimal que repite ceros agregados al final: $3.625 = 3.625\overline{0}$. Esto también se puede escribir como $3.624\overline{9}$.

Recuerde que un número racional es uno que puede escribirse como una razón de enteros, en otras palabras, como una fracción. Recuerde también que la expansión decimal de una fracción se obtiene dividiendo su numerador entre su denominador mediante la división larga. Por ejemplo, la expansión decimal de 4/33 se obtiene como sigue:

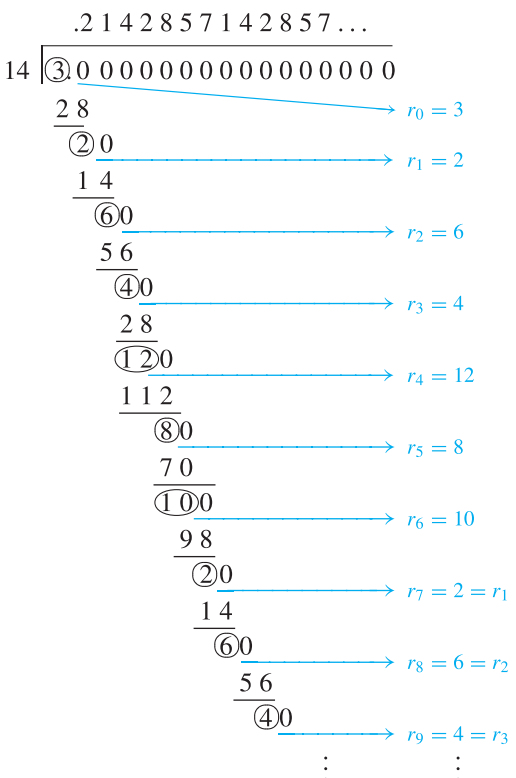


Ya que el número 4 vuelve a aparecer como un residuo en el proceso de división larga, la sucesión de residuos y cocientes que dan los dígitos de la expansión decimal siempre se repite; por tanto los dígitos de la expansión decimal siempre se repiten.

En general, cuando un entero se divide entre otro, es el principio de las casillas (junto con el teorema del cociente-residuo) lo que garantiza tal repetición de residuos y por tanto siempre se deben presentar dígitos decimales. Esto se explica en el siguiente ejemplo. El análisis en el ejemplo utiliza una evidente generalización del principio de las casillas, saber que una función de un conjunto infinito a un conjunto finito no puede ser inyectiva.

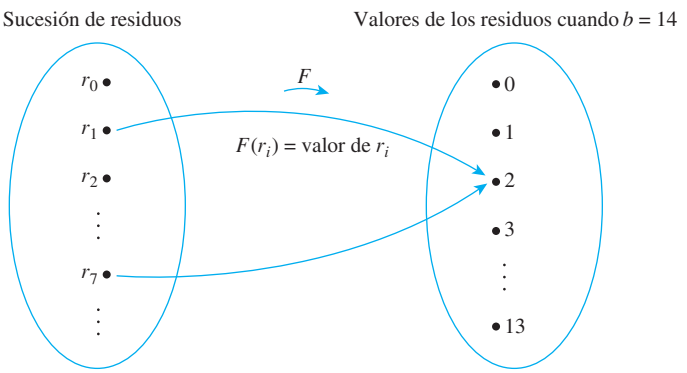
Ejemplo 9.4.4 La expansión decimal de una fracción

Considere una fracción a/b, donde por simplicidad se supone que tanto a como b son positivos. La expansión decimal de a/b se obtiene dividiendo a entre b, como se muestra aquí para $a = 3$ y $b = 14$.



Sea $r_0 = a$ y sean $r_1, r_2, r_3, \ldots$ los sucesivos residuos obtenidos en la división larga de a entre b. Por el teorema del cociente-residuo, cada residuo entre 0 y $b - 1$. (En este ejemplo, a es 3 y b es 14, por lo que los residuos van de 0 a 13.) Si algunos residuos son $r_i = 0$, entonces la división termina y a/b tiene una expansión decimal que termina, si no $r_i = 0$, entonces, el proceso de división y por tanto la sucesión de residuos continúa por siempre. Por el principio de las casillas, puesto que hay más residuos que valores que los residuos puedan

tomar, algún valor del residuo se debe repetir: $r_j = r_k$, para algunos índices j y k con $j < k$. Esto se muestra a continuación para $a = 3$ y $b = 14$.

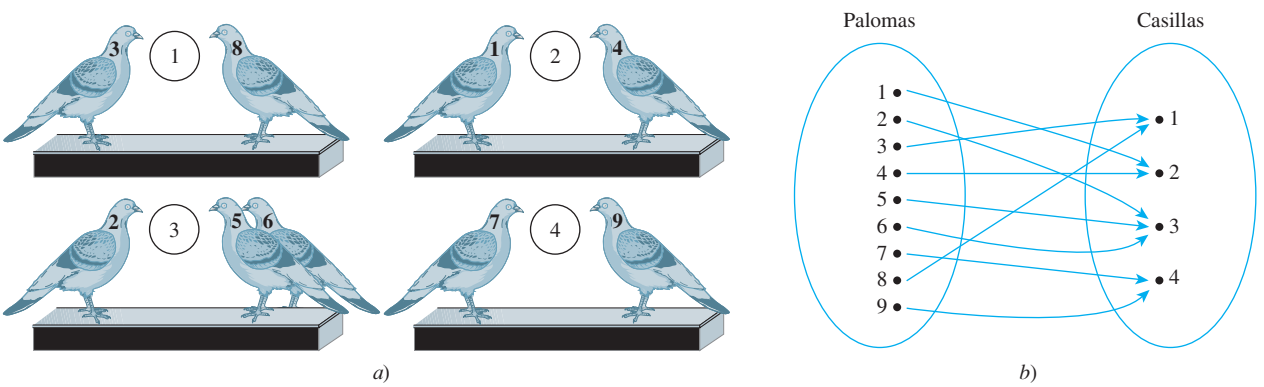


Se tiene que los dígitos decimales obtenidos de las divisiones entre r_j y r_{k-1} se repiten por siempre. En el caso de $3/14$, la repetición comienza con $r_7 = 2 = r_1$ y la expansión decimal repite los cocientes obtenidos de las divisiones de r_1 a r_6 por siempre: $3/14 = 0.2\overline{142857}$. ■

Observe, que la expansión decimal de cualquier número racional, termina o se repite, si un número tiene una expansión decimal que no termina ni se repite, entonces no puede ser racional. Así, por ejemplo, el siguiente número no puede ser racional: 0.010110111011110111111… (donde cada cadena de 1 es uno más de la cadena anterior.)

Principio generalizado de las casillas

Una generalización del principio de las casillas establece que si n palomas vuelan a m casillas y, para algún k entero positivo, $k < n/m$, entonces al menos una casilla contiene $k + 1$ o más palomas. Esto se ilustra en la figura 9.4.2 para $m = 4$, $n = 9$ y $k = 2$. Ya que $2 < 9/4 = 2.25$, al menos una casilla contiene tres $(2 + 1)$ o más palomas. (En este ejemplo, la casilla 3 contiene tres palomas.)



a) *b)*

Figura 9.4.2

Principio de las casillas generalizado

Para cualquier función f de un conjunto finito X con n elementos a un conjunto finito Y con m elementos y para cualquier entero positivo k, si $k < n/m$, entonces hay algún $y \in Y$ tal que y es la imagen de al menos $k + 1$ elementos distintos de X.

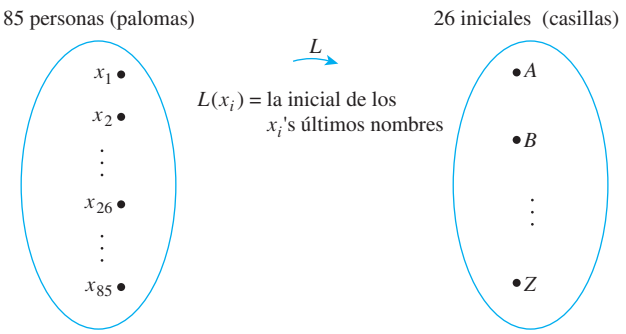
Ejemplo 9.4.5 Aplicación del principio de casillas generalizado

Demuestre cómo el principio de las casillas generalizado implica que en un grupo de 85 personas, al menos 4 debe tener la misma última inicial.

Solución En este ejemplo las palomas son las 85 personas y las casillas son las 26 últimas iniciales posibles de sus nombres. Observe que

$$3 < 85/26 \cong 3.27.$$

Considere la función L de las personas a las iniciales definida por el siguiente diagrama de flecha.



Ya que $3 < 85/26$, el principio de las casillas generalizado dice que algunas iniciales deben ser la imagen de al menos cuatro $(3 + 1)$ personas. Así, al menos cuatro personas tienen la misma última inicial. ■

Considere la siguiente forma contrapositiva del principio de las casillas generalizado.

Principio de las casillas generalizado (forma contrapositiva)

Para cualquier función f de un conjunto finito X con n elementos a un conjunto finito Y con m elementos y para cualquier entero positivo k, si cada $y \in Y, f^{-1}(y)$ tiene a lo más k elementos, entonces X tiene a lo más km elementos; en otras palabras, $n \leq km$.

Puede que le resulte natural utilizar la forma contrapositiva del principio de las casillas generalizado en ciertas situaciones. Por ejemplo, el resultado del ejemplo 9.4.5 se puede explicar de la forma siguiente:

> Suponga que ninguna de las 4 personas que salen de las 85 tenía la misma última inicial. Entonces a lo más 3 compartirían una inicial particular. Por el principio de las casillas generalizado (forma contrapositiva), esto implicaría que el número total de personas es a lo más $3 \cdot 26 = 78$. Pero esto contradice el hecho de que hay 85 personas en total. Por tanto al menos 4 personas comparten una última inicial.

Ejemplo 9.4.6 Utilizando la forma contrapositiva del principio de las casillas generalizado

Hay 42 estudiantes que comparten 12 computadoras. Cada alumno utiliza exactamente 1 computadora y ninguna computadora se utiliza por más de 6 estudiantes. Demuestre que al menos 5 computadoras son utilizadas por 3 o más estudiantes.

Solución

a. ***Utilización de un argumento por contradicción:*** Supongamos que no. Supongamos que se utilizan 4 o menos computadoras por 3 o más estudiantes. *[Se deducirá una contradicción.]* Entonces se utilizan 8 o más computadoras por 2 o menos de los estudiantes. Dividiendo al conjunto de computadoras en dos subconjuntos: C_1 y C_2. En C_1 se colocan 8 de las computadoras que se utilizan por 2 o menos de los estudiantes; en C_2 se colocan las computadoras que son utilizadas por 3 o más estudiantes más cualquiera de las computadoras restantes (haciendo un total de 4 computadoras en C_2). (Vea la figura 9.4.3.)

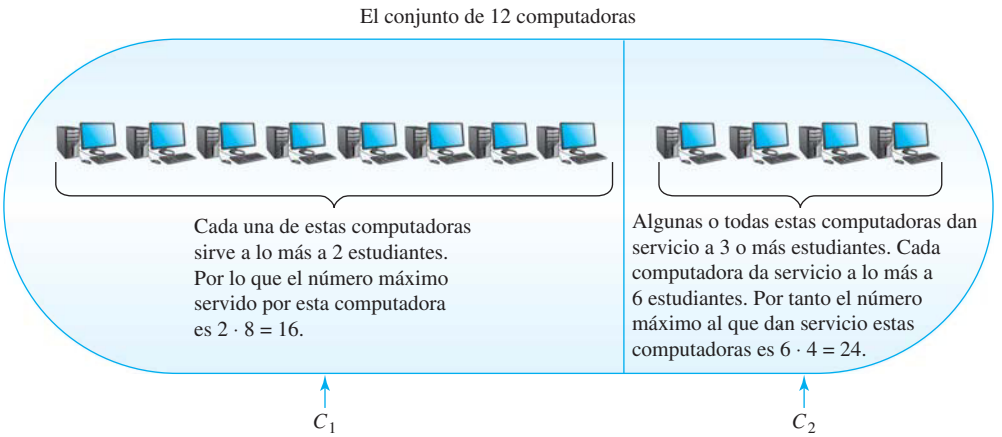


Figura 9.4.3

Ya que a lo más 6 estudiantes se les da servicio con cualquier computadora, por la forma contrapositiva del principio de las casillas generalizado, las computadoras en el conjunto C_2 dan servicio a lo más a $6 \cdot 4 = 24$ estudiantes. Dado que a lo más 2 estudiantes se les da servicio con cualquier computadora de C_1, por el principio de las casillas generalizado (forma contrapositiva), las computadoras en el conjunto C_1 dan servicio a lo más a $2 \cdot 8 = 16$ estudiantes. Por tanto el número de alumnos al que se le da servicio con las computadoras es $24 + 16 = 40$. Pero esto contradice el hecho de que cada uno de los 42 estudiantes se le da servicio con un computadora. Por tanto, la suposición es falsa: al menos 5 computadoras son utilizadas por 3 o más estudiantes.

b. ***Utilización de un argumento directo:*** Sea k el número de computadoras utilizadas por 3 o más estudiantes. *[Debemos demostrar que $k \geq 5$.]* Ya que cada computadora se utiliza a lo más por 6 estudiantes, estas computadoras se utilizan a lo más por $6k$ estudiantes (por la forma contrapositiva del principio de las casillas generalizado). Cada una de las $12 - k$ computadoras restantes se utiliza a lo más por 2 estudiantes. Por tanto, en conjunto, las computadoras son utilizadas a lo más por $2(12 - k) = 24 - 2k$ estudiantes (otra vez, por la forma contrapositiva del principio de las casillas generalizado). Por tanto el número máximo de alumnos al que le dan servicio las computadoras es $6k + (24 - 2k) = 4k + 24$. Ya que a 42 estudiantes se le da servicio con las computadoras, $4k + 24 \geq 42$. Despejando a k se obtiene que $k \geq 4.5$ y ya que k es un entero, esto implica que $k \geq 5$ *[como se quería demostrar]*. ■

Demostración del principio de las casillas

La verdad del principio de las casillas depende esencialmente de que los conjuntos implicados sean finitos. Recuerde de la sección 1.4 que un conjunto se llama **finito** si y sólo si, es el conjunto vacío o hay una correspondencia uno a uno de $\{1, 2, \ldots, n\}$ a éste, donde n es un entero positivo. En el primer caso, se dice que el **número de elementos** en el conjunto es 0 y en el segundo caso se dice que es n. Un conjunto que no es finito se llama **infinito**.

Por tanto cualquier conjunto finito es vacío o se puede escribir en la forma $\{x_1, x_2, \ldots, x_n\}$ donde n es un entero positivo.

Teorema 9.4.1 El principio de las casillas

Para cualquier función f de un conjunto finito X con n elementos a un conjunto finito Y con m elementos, si $n > m$, entonces f no es inyectiva.

Demostración:

Supongamos que f es cualquier función de un conjunto finito X con n elementos a un conjunto finito Y con m elementos donde $n > m$. Se denotan los elementos de Y por $y_1, y_2, \ldots, y_m$. Recuerde que para cada y_i en Y, el conjunto de imágenes inversas $f^{-1}(y_i) = \{x \in X \mid f(x) = y_i\}$. Ahora considere la colección de todo el conjunto de imágenes inversas para todos los elementos de Y:

$$f^{-1}(y_1), f^{-1}(y_2), \ldots, f^{-1}(y_m).$$

Por definición de función, cada elemento de X se envía por f a algún elemento de Y. Por tanto, cada elemento de X está en uno de los conjuntos de imágenes inversas y así la unión de todos estos conjuntos es igual a X. Pero también, por definición de función, ningún elemento de X se envía por f a más de un elemento de Y. Así, cada elemento de X está sólo en uno de los conjuntos de imágenes inversas y así los conjuntos de imágenes inversas son mutuamente disjuntos. Por tanto, por la regla de adición,

$$N(X) = N(f^{-1}(y_1)) + N(f^{-1}(y_2)) + \cdots + N(f^{-1}(y_m)). \qquad 9.4.1$$

Ahora suponga que f es inyectiva *[que es lo opuesto de lo que queremos demostrar]*. Cada conjunto $f^{-1}(y_i)$ tiene a lo más un elemento y así

$$N(f^{-1})y_1)) + N(f^{-1})y_2)) + \cdots + N(f^{-1})y_m)) \leq \underbrace{1 + 1 + \cdots + 1}_{m \text{ términos}} = m \qquad 9.4.2$$

Juntando las ecuaciones (9.4.1) y (9.4.2) se obtiene

$$n = N(X) \leq m = N(Y).$$

Esto contradice el hecho de que $n > m$ y así suponiendo que f sea inyectiva debe ser falso. Por tanto f no es inyectiva *[como se quería demostrar]*.

Un teorema importante que se deduce del principio de las casillas establece que una función de un conjunto finito a otro conjunto finito del mismo tamaño es uno a uno si y sólo si, es sobreyectiva. Como se mostró en la sección 7.4, este resultado no es válido para conjuntos infinitos.

Teorema 9.4.2 Inyectiva y sobreyectiva para conjuntos finitos

Sean X y Y conjuntos finitos con el mismo número de elementos y suponga que f es una función de X a Y. Entonces f es inyectiva, si y sólo si, es sobreyectiva.

Demostración:

Suponga que f es una función de X a Y, donde X y Y son conjuntos finitos con m elementos. Sea $X = \{x_1, x_2, \ldots, x_m\}$ y $Y = \{y_1, y_2, \ldots, y_m\}$.

Si f es inyectiva, entonces es sobreyectiva: Suponga que f es inyectiva. Entonces $f(x_1), f(x_2), \ldots, f(x_m)$ son todos distintos. Considere el conjunto S de todos los elementos de Y que no son la imagen de cualquier elemento de X.

Entonces los conjuntos

$$\{f(x_1)\}, \{f(x_2)\}, \ldots, \{f(x_m)\} \quad \text{y} \quad S$$

son mutuamente disjuntos. Por la regla de adición,

$$\begin{aligned} N(Y) &= N(\{f(x_1)\}) + N(\{f(x_2)\}) + \cdots + N(\{f(x_m)\}) + N(S) \\ &= \underbrace{1 + 1 + \cdots + 1}_{m \text{ términos}} + N(S) \qquad \text{ya que cada } \{f(x_i)\} \text{ es un conjunto con un elemento} \\ &= m + N(S). \end{aligned}$$

Así

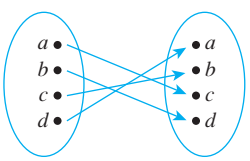
$$\begin{aligned} m &= m + N(S) \qquad \text{ya que } N(Y) = m, \\ \Rightarrow N(S) &= 0 \qquad \text{restando } m \text{ de ambos lados.} \end{aligned}$$

Por tanto S es vacío y así no hay ningún elemento de Y que no es la imagen de algún elemento de X. En consecuencia, es sobreyectiva.

Si f es sobreyectiva entonces f es inyectiva: Suponga que f es sobreyectiva. Entonces $f^{-1}(y_i) \neq \emptyset$ y así $Nf^{-1}(y_i)) \geq 1$ para todo $i = 1, 2, \ldots, m$. Como en la demostración del principio de las casillas (teorema 9.4.1), X es la unión de los conjuntos mutuamente disjuntos $f^{-1}(y_1), f^{-1}(y_2), \ldots, f^{-1}(y_m)$. Por el principio de la adición,

$$N(X) = \underbrace{N(f^{-1}(y_1)) + N(f^{-1}(y_2)) + \cdots + N(f^{-1}(y_m))}_{m \text{ términos, cada uno} \geq 1} \geq m. \qquad 9.4.3$$

Ahora si cualquiera de los conjuntos $f^{-1}(y_i)$ tiene más de un elemento, entonces la suma en la ecuación (9.4.3) es mayor que m. Pero sabemos que éste no es el caso porque $N(X) = m$. Por tanto cada conjunto $f^{-1}(y_i)$ tiene exactamente un elemento y así f es inyectiva *[como se quería demostrar]*.



Observe que el teorema 9.4.2 se aplica en particular al caso $X = Y$. Así una función inyectiva de un conjunto finito a sí mismo es sobreyectiva y una función sobreyectiva de un conjunto finito a sí mismo es inyectiva. Estas funciones son permutaciones de los conjuntos en que están definidas. Por ejemplo, la función definida por el diagrama de la izquierda es otra representación de la permutación *cdba* obtenida enumerando en orden las imágenes de a, b, c y d.

Autoexamen

1. El principio de las casillas establece que _____.
2. El principio de las casillas generalizado establece que _____.
3. Si X y Y son conjuntos finitos y f es una función de X a Y entonces f es inyectiva si y sólo si, _____.

Conjunto de ejercicios 9.4

1. a. Si se seleccionan 4 cartas de una baraja estándar de 52 cartas, ¿debe haber al menos 2 del mismo palo? ¿Por qué?
   b. Si se seleccionan 5 cartas de una baraja estándar de 52 cartas, ¿debe haber al menos 2 del mismo palo? ¿Por qué?

2. a. Si se seleccionan 13 cartas de una baraja estándar de 52 cartas, ¿debe haber al menos 2 de la misma denominación? ¿Por qué?
   b. Si se seleccionan 20 cartas de una baraja estándar de 52 cartas, ¿debe haber al menos 2 de la misma denominación? ¿Por qué?

3. Una pequeña ciudad tiene sólo 500 habitantes. ¿Debe haber dos residentes que tengan el mismo cumpleaños? ¿Por qué?

4. En un grupo de 700 personas, ¿debe haber 2 que tengan la misma primer y última iniciales? ¿Por qué?

5. a. Dado cualquier conjunto de cuatro enteros, ¿debe haber dos que tengan el mismo residuo cuando se dividen por 3? ¿Por qué?
b. Dado cualquier conjunto de tres enteros, ¿debe haber dos que tengan el mismo residuo cuando se dividen por 3? ¿Por qué?

6. a. Dado cualquier conjunto de siete enteros, ¿debe haber dos que tengan el mismo residuo cuando se dividen por 6? ¿Por qué?
b. Dado cualquier conjunto de siete enteros, ¿debe haber dos que tengan el mismo residuo cuando se dividen por 8? ¿Por qué?

***H* 7.** Sea $S = \{3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$. Suponga que se eligen seis enteros de S. ¿Debe haber dos enteros cuya suma es 15? ¿Por qué?

8. Sea $T = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$. Suponga que se eligen cinco enteros de T. ¿Debe haber dos enteros cuya suma es 10? ¿Por qué?

9. a. Si se eligen siete enteros entre 1 y 12 incluso, ¿debe por lo menos uno de ellos ser impar? ¿Por qué?
b. Si se eligen diez enteros entre 1 y 20 incluso, ¿al menos uno de ellos debe ser par? ¿Por qué?

10. Si se eligen $n + 1$ enteros en el conjunto

$$\{1, 2, 3, \ldots 2n\},$$

donde n es un entero positivo, ¿al menos uno de ellos debe ser impar? ¿Por qué?

11. Si se eligen $n + 1$ enteros del conjunto

$$\{1, 2, 3, \ldots 2n\},$$

donde n es un entero positivo, ¿al menos uno de ellos debe ser par? ¿Por qué?

12. ¿Cuántas cartas tiene que elegir de una baraja estándar de 52 cartas para asegurarse que al menos 1 carta sea roja? ¿Por qué?

13. Suponga que se avientan juntos seis pares de botas similares en un montón. ¿Cuántas botas individuales debe elegir para asegurarse de obtener un par? ¿Por qué?

14. ¿Cuántos enteros entre 0 y 60 se deben elegir en orden para asegurarse de obtener por lo menos uno que sea impar? ¿Al menos uno que sea par?

15. Si n es un entero positivo, ¿cuántos enteros entre 0 y $2n$ debe elegir en orden para asegurarse de obtener por lo menos uno que es impar? ¿Al menos uno que es par?

16. ¿Cuántos enteros entre 1 y 100 se deben elegir para asegurarse de obtener uno que sea divisible por 5?

17. ¿Cuántos enteros se deben elegir para asegurarse de que al menos dos de ellos tienen el mismo residuo cuando se divide por 7?

18. ¿Cuántos enteros se deben elegir para asegurarse de que al menos dos de ellos tienen el mismo residuo cuando se divide por 15?

19. ¿Cuántos enteros de 100 a 999 se deben elegir para asegurarse de que al menos dos de ellos tengan un dígito en común? (Por ejemplo, 256 y 530 tienen el dígito común 5.)

20. a. Si se realizan divisiones repetidas entre 20 483 ¿cuántos residuos distintos pueden obtenerse?
b. Cuando se escribe 5/20 483 como un decimal, ¿cuál es la longitud máxima de la sección que se repite en la expansión decimal?

21. Cuando se escribe 683/1 493 como un decimal, ¿cuál es la longitud máxima de la sección que se repite en la expansión decimal?

22. ¿Es 0.101001000100001000001... racional o irracional (donde cada cadena de 0 es uno más que el anterior)?

23. ¿Es 56.556655566655556666... racional o irracional (donde las cadenas de 5 y 6 serán más largas en cada repetición)?

24. Demuestre que dentro de cualquier conjunto de trece enteros elegidos del 2 al 40, hay al menos dos enteros con un divisor común superior a 1.

25. En un grupo de 30 personas, ¿deben al menos 3 haber nacido en el mismo mes? ¿Por qué?

26. En un grupo de 30 personas, ¿deben al menos 4 haber nacido en el mismo mes? ¿Por qué?

27. En un grupo de 2 000 personas, ¿deben al menos 5 tener el mismo cumpleaños? ¿Por qué?

28. Un programador escribe 500 líneas de código de computadora en 17 días. ¿Debe haber al menos 1 día en el que el programador escribió 30 o más líneas de código? ¿Por qué?

29. Una cierta clase de colegio tiene 40 estudiantes. Se sabe que todos los alumnos de la clase son de 17 a 34 años de edad. Desea hacer una apuesta de qué clase contiene al menos x estudiantes de la misma edad. ¿Qué tan grande puede ser x y aún estar seguro de ganar su apuesta?

30. Una colección de monedas de 5¢ contiene doce monedas de 5¢ de 1967, siete monedas de 5¢ centavos de 1968 y once monedas de 5¢ de 1971. Si recoge algunas monedas de 5¢ centavos sin mirar las fechas, ¿cuántas debe tomar para asegurarse de obtener por lo menos cinco monedas de 5¢ del mismo año?

***H* 31.** Un grupo de 15 ejecutivos deben compartir a 5 asistentes. A cada ejecutivo se le asigna exactamente 1 auxiliar y no se asigna algún asistente a más de 4 ejecutivos. Demuestre que al menos 3 asistentes se asignan a 3 o más ejecutivos.

***H* ⋆ 32.** Sea A un conjunto de seis enteros positivos cada uno de los cuales es menor de 13. Demuestre que debe haber dos subconjuntos distintos de A cuyos elementos cuando se suman dan la misma suma. (Por ejemplo, si $A = \{5, 12, 10, 1, 3, 4\}$, entonces los elementos de los subconjuntos $S_1 = \{1, 4, 10\}$ y $S_2 = \{5, 10\}$ ambos suman 15.)

***H* 33.** Sea A un conjunto de seis enteros positivos cada uno de cuales es menor a 15. Demuestre que deben haber dos distintos sub-

conjuntos de A cuyos elementos cuando se suman den la misma suma. (Gracias a Jonathan Goldstine por este problema.)

34. Sea S un conjunto de diez enteros de 1 a 50. Demuestre que el conjunto contiene al menos dos diferentes subconjuntos (pero no necesariamente disjuntos) de cuatro enteros que suman el mismo número. (Por ejemplo, si diez números son {3, 8, 9, 18, 24, 34, 35, 41, 44, 50}, pueden tomarse los subconjuntos {8, 24, 34, 35} y {9, 18, 24, 50}. Los números en ambos suman hasta 101.)

H ✶ **35.** Dado un conjunto de 52 enteros distintos, demuestre que deben haber 2 cuya suma o diferencia sea divisible por 100.

H ✶ **36.** Demuestre que si se eligen 101 enteros del 1 al 200 inclusive, debe haber 2 con la propiedad de que uno es divisible por otro.

✶ 37. a. Suponga que $a_1, a_2, \ldots, a_n$ es una sucesión de n enteros ninguno de los cuales es divisible por n. Demuestre que al menos una de las diferencias $a_i - a_j$ (para $i \neq j$) debe ser divisible por n.

H **b.** Demuestre que cada sucesión finita $x_1, x_2, \ldots, x_n$ de enteros tiene una subsucesión consecutiva $x_{i+1}, x_{i+2}, \ldots, x_j$ cuya suma es divisible por n. (Por ejemplo, la sucesión 3, 4, 17, 7, 16 tiene la subsucesión consecutiva 17, 7,16 cuya suma es divisible por 5). (De: James E. Schultz y William F. Burger, "Un enfoque a la solución de problemas utilizando equivalencia de clases módulo n" *College Mathematics Journal (15)*, No. 5, 1984, 401-405.)

H ✶ **38.** Observe que la sucesión 12, 15, 8, 13, 7, 18, 19, 11, 14, 10 tiene tres subsucesiones crecientes de longitud cuatro: 12, 15, 18, 19; 12, 13, 18, 19 y 8, 13, 18, 19. También tiene una subsucesión decreciente de longitud cuatro: 15, 13, 11, 10. Demuestre que en cualquier sucesión de $n^2 + 1$ distintos números reales, debe haber una sucesión de longitud $n + 1$ que es estrictamente creciente o estrictamente decreciente.

✶ 39. ¿Cuál es el mayor número de elementos que puede tener un conjunto de enteros entre 1 y 100 para que no haya un elemento en el conjunto que sea divisible por otro? (*Sugerencia:* Imagine escribir todos los números por 1 y 100 en el forma $2^k \cdot m$, donde $k \geq 0$ y m es impar).

40. Supongamos que X y Y son conjuntos finitos, X tiene más elementos que Y y $F: X \to Y$ es una función. Por el principio de las casillas, existen elementos a y b en X tal que $a \neq b$ y $F(a) = F(b)$. Escriba un algoritmo de computadora para encontrar tal par de elementos a y b.

Respuestas del autoexamen

1. si vuelan n palomas a m casillas y $n > m$, entonces al menos dos palomas en la misma casilla *O:* una función de un conjunto finito a un conjunto finito más pequeño no puede ser inyectiva. 2. si n palomas vuelan en m casillas y, para algún entero positivo k, $k < n/m$ entonces al menos una casilla contiene $k + 1$ o más palomas *O:* para cualquier función f de un conjunto finito X con n elementos a un conjunto finito Y con m elementos y para cualquier entero positivo k, si $k < n/m$, hay alguna $y \in Y$ tal que y es la imagen de al menos $k + 1$ elementos distintos de Y 3. f es sobreyectiva

9.5 Conteo de subconjuntos de un conjunto: combinaciones

"Pero 'gloria' no significa 'un argumento que deje bien aplastado'", objetó Alicia. "Cuando yo uso una palabra" insistió Humpty Dumpty con un tono de voz más bien desdeñoso "quiere decir lo que yo quiero que diga— ni más ni menos". —Lewis Carroll, *A través del espejo*, 1872

Considere la siguiente pregunta:

> Suponga que se eligen cinco miembros de un grupo de doce para trabajar como un equipo en un proyecto especial. ¿Cuántos equipos distintos de cinco personas se pueden seleccionar?

En el ejemplo 9.5.4 se responde a esa pregunta. ¿Es un caso especial de la siguiente pregunta más general:

> Dado un conjunto S con n elementos, ¿cuántos subconjuntos de tamaño r se pueden elegir de S?

El número de subconjuntos de tamaño r que se pueden elegir de S es igual al número de subconjuntos de tamaño r que tiene S. Cada subconjunto individual de tamaño r se llama una *r-combinación* del conjunto.

• Definición

Sean n y r enteros no negativos con $r \leq n$. Una ***r*-combinación** de un conjunto de n elementos es un subconjunto de r de los n elementos. Como se indica en la sección 5.1, el símbolo

$$\binom{n}{r},$$

que se lee "de n elija r", denota el número de subconjuntos de tamaño r (r-combinaciones) que se puede elegir de un conjunto de n elementos.

Recuerde, de la sección 5.1, que las calculadoras generalmente usan símbolos como $C(n, r)$, ${}_nC_r$, $C_{n,r}$, o ${}^nC_r$ en lugar de $\binom{n}{r}$.

Ejemplo 9.5.1 3-combinaciones

Sea $S = \{\text{Ann, Bob, Cyd, Dan}\}$. Cada comité formado por tres de las cuatro personas en S es una 3-combinación de S.

a. Enumere todas esas 3-combinaciones de S. b. ¿A qué es igual $\binom{4}{3}$?

Solución

a. Cada 3-combinación de S es un subconjunto de S de tamaño 3. Pero cada subconjunto de tamaño 3 puede obtenerse sacando uno de los elementos de S. Las 3-combinaciones son

$\{\text{Bob, Cyd, Dan}\}$ sale Ann
$\{\text{Ann, Cyd, Dan}\}$ sale Bob
$\{\text{Ann, Bob, Dan}\}$ sale Cyd
$\{\text{Ann, Bob, Cyd}\}$ sale Dan.

b. Ya que $\binom{4}{3}$ es el número de 3-combinaciones de un conjunto con cuatro elementos, por el inciso *a*), $\binom{4}{3} = 4$. ■

Hay dos métodos diferentes que se pueden utilizar para seleccionar r objetos de un conjunto de n elementos. En una **selección ordenada**, no es sólo qué elementos se eligen sino también importa el orden en que se eligen. Dos selecciones ordenadas se dice que son iguales si los elementos elegidos son iguales y también si los elementos se eligen en el mismo orden. Una selección ordenada de r elementos de un conjunto de n elementos es una r-permutación del conjunto.

Por otra parte, en una **selección no ordenada**, sólo la identidad de los elementos seleccionados es lo que importa. Dos selecciones no ordenadas se dicen que son iguales si se componen de los mismos elementos, independientemente del orden en que se eligen los elementos. Una selección no ordenada de r elementos de un conjunto de n elementos es igual que un subconjunto de tamaño r o una r-combinación del conjunto.

Ejemplo 9.5.2 Selecciones no ordenadas

¿Cómo pueden hacerse selecciones no ordenadas de dos elementos del conjunto {0, 1, 2, 3}?

Solución Una selección no ordenada de dos elementos de {0, 1, 2, 3} es igual que una 2-combinación, o un subconjunto de tamaño 2, tomado del conjunto. Estos se pueden enumerar sistemáticamente:

$\{0, 1\}, \{0, 2\}, \{0, 3\}$ subconjuntos que contienen 0
$\{1, 2\}, \{1, 3\}$ subconjuntos que contienen 1 pero ya no se enumeran
$\{2, 3\}$ subconjuntos que contienen 2 pero ya no se enumeran.

Dado que este listado agota todas las posibilidades, hay seis subconjuntos en total. Por tanto $\binom{4}{2} = 6$, que es el número de selecciones no ordenadas de dos elementos de un conjunto de cuatro. ■

Cuando los valores de n y r son pequeños, es razonable calcular los valores de $\binom{n}{r}$ mediante el método de **enumeración completa** (listando todas las posibilidades) ilustrada en los ejemplos 9.5.1 y 9.5.2. Pero cuando n y r son grandes, no es factible calcular estos números listando y contando todas las posibilidades.

Los valores generales de $\binom{n}{r}$ se pueden encontrar con un método simple pero indirecto. Se deduce una ecuación que contiene a $\binom{n}{r}$ como un factor. Luego se resuelve esta ecuación para obtener una fórmula para $\binom{n}{r}$. El método se ilustra en el ejemplo 9.5.3.

Ejemplo 9.5.3 Relación entre permutaciones y combinaciones

Escriba todas las 2-permutaciones del conjunto $\{0, 1, 2, 3\}$. Encuentre una ecuación que relacione el número de 2-permutaciones, $P(4, 2)$ y el número de 2-combinaciones, $\binom{4}{2}$ y resuelva esta ecuación para $\binom{4}{2}$.

Solución De acuerdo con el teorema 9.2.3, el número de 2-permutaciones del conjunto $\{0, 1, 2, 3\}$ es $P(4, 2)$, que es igual a

$$\frac{4!}{(4-2)!} = \frac{4 \cdot 3 \cdot \cancel{2} \cdot \cancel{1}}{\cancel{2} \cdot \cancel{1}} = 12.$$

Ahora el acto de construir una 2-permutación de $\{0, 1, 2, 3\}$ puede considerarse como un proceso de dos-pasos:

Paso 1: Elija un subconjunto de dos elementos de $\{0, 1, 2, 3\}$.

Paso 2: Elija un ordenamiento para el subconjunto de dos elementos.

Este proceso se puede ilustrar con el árbol de probabilidad que se muestra en la figura 9.5.1.

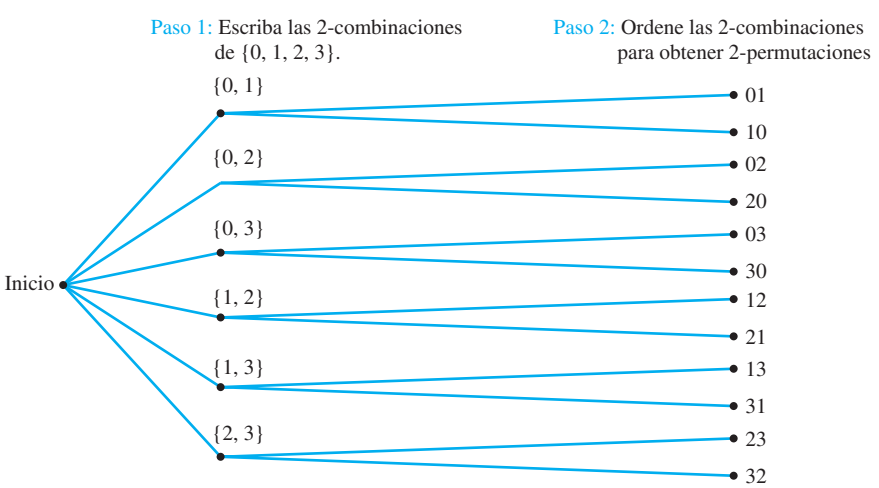


Figura 9.5.1 Relación entre permutaciones y combinaciones

El número de formas de realizar el paso 1 es $\binom{4}{2}$, es igual al número de subconjuntos de tamaño 2 que se puede elegir de $\{0, 1, 2, 3\}$. El número de formas de realizar el paso 2 es 2!, el número de formas para ordenar los elementos en un subconjunto de tamaño 2. Ya que el número de formas de realizar todo el proceso es el número de 2-permutaciones del conjunto $\{0, 1, 2, 3\}$, que es igual a $P(4, 2)$, por lo que se deduce de la regla de la multiplicación que

$$P(4, 2) = \binom{4}{2} \cdot 2!.$$ Esta es una ecuación que relaciona a $P(4, 2)$ y $\binom{4}{2}$.

Resolviendo la ecuación para $\binom{4}{2}$ se obtiene

$$\binom{4}{2} = \frac{P(4, 2)}{2!}$$

Recuerde que $P(4, 2) = \frac{4!}{(4-2)!}$. Por tanto, sustituyendo se obtiene

$$\binom{4}{2} = \frac{\frac{4!}{(4-2)!}}{2!} = \frac{4!}{2!(4-2)!} = 6.$$

El razonamiento utilizado en el ejemplo 9.5.3 se aplica también en el caso general. Para formar una r-permutación de un conjunto de n elementos, primero se elige un subconjunto de r elementos de n (hay $\binom{n}{r}$ formas de realizar este paso) y después se elige un ordenamiento para los r elementos (hay $r!$ formas de realizar este paso). Por tanto el número de r-permutaciones es

$$P(n, r) = \binom{n}{r} \cdot r!.$$

Ahora resuelva para $\binom{n}{r}$ para obtener la fórmula

$$\binom{n}{r} = \frac{P(n, r)}{r!}.$$

Ya que $P(n, r) = \frac{n!}{(n-r)!}$, sustituyendo se obtiene

$$\binom{n}{r} = \frac{\frac{n!}{(n-r)!}}{r!} = \frac{n!}{r!(n-r)!}.$$

El resultado de este análisis se resume y amplia en el teorema 9.5.1.

Teorema 9.5.1

El número de subconjuntos de tamaño r (o r-combinaciones) que se pueden elegir entre un conjunto de n elementos, $\binom{n}{r}$, está dado por la fórmula

$$\binom{n}{r} = \frac{P(n, r)}{r!}$$ primera versión

o, de forma equivalente,

$$\binom{n}{r} = \frac{n!}{r!(n-r)!}$$ segunda versión

donde n y r son enteros no negativos con $r \leq n$.

Observe que el análisis que se presenta antes del teorema demuestra el teorema en todos los casos donde n y r son positivos. Si r es cero y n es cualquier entero no negativo,

entonces $\binom{n}{0}$ es el número de subconjuntos de tamaño cero de un conjunto con n elementos. Pero se sabe de la sección 6.2 que sólo hay un conjunto que no tiene elementos. En consecuencia, $\binom{n}{0} = 1$. También

$$\frac{n!}{0!(n-0)!} = \frac{n!}{1 \cdot n!} = 1$$

ya que por definición $0! = 1$. (Recuerde que dijimos que la definición ¡resultaría conveniente!) Por tanto, la fórmula

$$\binom{n}{0} = \frac{n!}{0!(n-0)!}$$

vale para todos los enteros $n \geq 0$ y así el teorema es cierto para todos los enteros no negativos n y r con $r \leq n$.

Ejemplo 9.5.4 Cálculo del número de equipos

Considere nuevamente el problema de la elección de cinco miembros de un grupo de doce para trabajar como un equipo en un proyecto especial. ¿Cuántos equipos de cinco personas distintos se pueden elegir?

Solución El número de distintos equipos de cinco personas es el mismo que el número de subconjuntos de tamaño 5 (o 5-combinaciones) que se pueden seleccionar del conjunto de los doce. Este número es $\binom{12}{5}$. Por el teorema 9.5.1,

$$\binom{12}{5} = \frac{12!}{5!(12-5)!} = \frac{12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 \cdot 7!}{(5 \cdot 4 \cdot 3 \cdot 2 \cdot 1) \cdot 7!} = 11 \cdot 9 \cdot 8 = 792.$$

Así hay 792 equipos distintos de cinco personas. ■

La fórmula para el número de r-combinaciones de un conjunto se puede aplicar a una amplia variedad de situaciones. Algunas de estas se ilustran en los siguientes ejemplos.

Ejemplo 9.5.5 Equipos que contienen ambos o ninguno

Suponga que dos miembros del grupo de los doce insisten en trabajar en pareja: cualquier equipo debe contener a los dos o a ninguno. ¿Cuántos equipos de cinco personas se pueden formar?

Solución Llame a los dos miembros del grupo que insisten en trabajar como un par A y B. Entonces cualquier equipo formado debe contener tanto a A como a B o ni A ni B. El conjunto de todos los equipos posibles puede dividirse en dos subconjuntos como se muestra en la figura 9.5.2 de la página siguiente.

Ya que un equipo que contiene tanto a A, como B, contiene exactamente otras tres de las restantes diez personas del grupo, hay tantos de esos equipos como subconjuntos de tres personas se pueden elegir de las diez restantes. Por el teorema 9.5.1, este número es

$$\binom{10}{3} = \frac{10!}{3! \cdot 7!} = \frac{10 \cdot \overset{3}{9} \cdot \overset{4}{8} \cdot 7!}{3 \cdot 2 \cdot 1 \cdot 7!} = 120.$$

Ya que un equipo que no contiene a A ni a B contiene exactamente cinco personas de las diez restantes, hay tantos de esos equipos como subconjuntos de cinco personas que se pueden elegir de las diez restantes. Por el teorema 9.5.1, este número es

$$\binom{10}{5} = \frac{10!}{5! \cdot 5!} = \frac{\overset{2}{10} \cdot 9 \cdot \overset{2}{8} \cdot 7 \cdot 6 \cdot 5!}{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \cdot 5!} = 252.$$

Ya que el conjunto de equipos que contienen tanto a A como a B está separado del conjunto de equipos que no contienen ni A ni a B, por la regla de la adición,

$$\begin{bmatrix}\text{número de equipos que}\\ \text{contienen tanto a } A \text{ como a } B\\ \text{o ni } A \text{ ni a } B\end{bmatrix} = \begin{bmatrix}\text{número de equipos}\\ \text{que contienen a}\\ A \text{ como a } B\end{bmatrix} + \begin{bmatrix}\text{número de equipos}\\ \text{que no contienen}\\ \text{ni a } A \text{ ni a } B\end{bmatrix}$$
$$= 120 + 252 = 372.$$

Este razonamiento se resume en la figura 9.5.2.

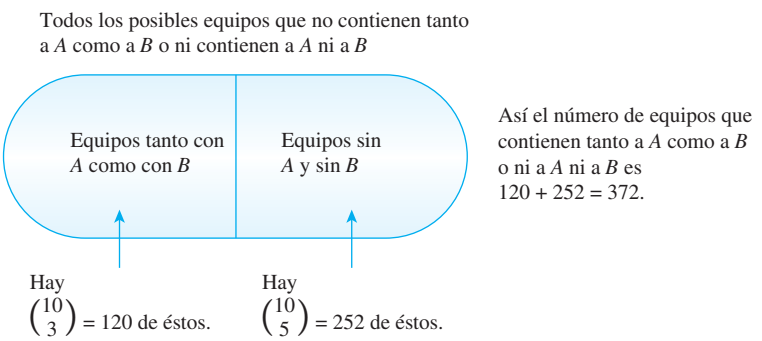


Figura 9.5.2

Ejemplo 9.5.6 Equipos que no contienen a ambos

Supongamos que dos miembros del grupo no se llevan bien y se niegan a trabajar juntos en un equipo. ¿Cuántos equipos de cinco personas se pueden formar?

Solución Llamamos a las personas que se niegan a trabajar juntas C y D. Hay dos maneras de responder a la pregunta dada: Una utiliza la regla de la adición y la otra utiliza la regla de la diferencia.

Para utilizar la regla de la adición, se particiona el conjunto de todos los equipos que no contienen tanto a C como a D en los tres subconjuntos que se muestran en la figura 9.5.3 de la página siguiente.

Ya que cualquier equipo que contiene C pero no D contiene exactamente otras cuatro personas de las diez restantes en el grupo, por el teorema 9.5.1 el número de esos equipos es

$$\binom{10}{4} = \frac{10!}{4!(10-4)!} = \frac{10\cdot 9\cdot 8\cdot 7\cdot 6!}{4\cdot 3\cdot 2\cdot 1\cdot 6!} = 210.$$

Similarmente, hay $\binom{10}{4} = 210$ equipos que contienen a D pero no a C. Por último, por el mismo razonamiento como en el ejemplo 9.5.5, hay 252 equipos que no contienen a C ni a D. Así, por la regla de adición,

$$\begin{bmatrix}\text{número de equipos que no}\\ \text{contienen ni a } C \text{ ni a } D\end{bmatrix} = 210 + 210 + 252 = 672.$$

Este razonamiento se resume en la figura 9.5.3.

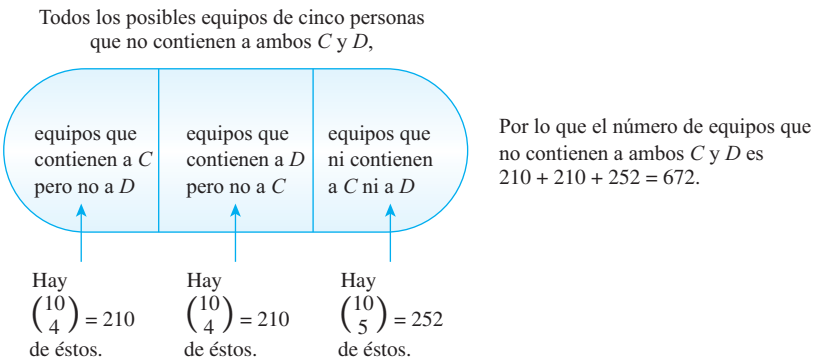


Figura 9.5.3

La solución alternativa por la regla de la diferencia se basa en la siguiente observación: El conjunto de todos los equipos de cinco personas que no contienen a ambos C y D es igual a la diferencia entre el conjunto de todos los equipos de cinco personas y el conjunto de todos los equipos que contienen ambos C y D. Por el ejemplo 9.5.4 el número total de cinco personas es $\binom{12}{5} = 792$. Así, por la regla de la diferencia,

$$\begin{bmatrix}\text{número de equipos que no}\\ \text{contienen a ambos } C \text{ y } D\end{bmatrix} = \begin{bmatrix}\text{número total de}\\ \text{equipos de cinco}\end{bmatrix} - \begin{bmatrix}\text{número de equipos que}\\ \text{contienen ambos a } C \text{ y } D\end{bmatrix}$$
$$= \binom{12}{5} - \binom{10}{3} = 792 - 120 = 672.$$

Este razonamiento se resume en la figura 9.5.4. ■

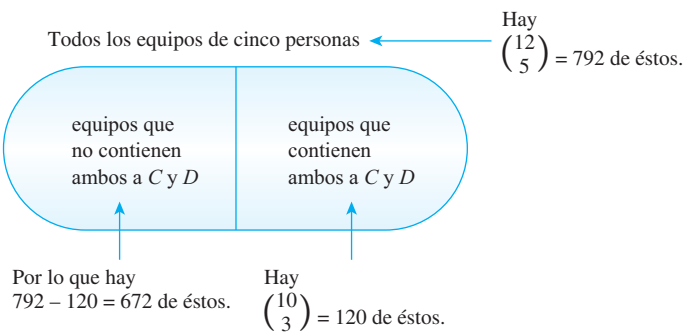


Figura 9.5.4

Antes de comenzar el ejemplo siguiente, haremos una observación acerca de las frases *al menos* y *a lo más* en este orden:

> La frase **al menos *n*** significa "n o más".
> La frase **a lo más *n*** significa "n o menos".

Por ejemplo, si un conjunto consta de tres elementos y elige al menos dos, seleccionará dos o tres; Si elige a lo más dos, selecciona ninguno, o uno o dos.

Ejemplo 9.5.7 Equipos con miembros de dos tipos

Supongamos que el grupo de doce consta de cinco hombres y siete mujeres.

a. ¿Cuántos equipos de cinco personas se pueden elegir que consten de tres hombres y dos mujeres?

b. ¿Cuántos equipos de cinco personas contienen al menos un hombre?

c. ¿Cuántos equipos de cinco personas contienen a lo más un hombre?

Solución

a. Para responder a esta pregunta, piense en formar un equipo como un proceso de dos pasos:

Paso 1: Seleccione a los hombres.

Paso 2: Elija a las mujeres.

Hay $\binom{5}{3}$ formas de elegir tres hombres de los cinco y $\binom{7}{2}$ maneras de elegir a las dos mujeres de las siete. Por tanto, por la regla de la multiplicación,

$$\begin{bmatrix}\text{número de equipos de cinco que}\\ \text{contienen tres hombres y dos mujeres}\end{bmatrix} = \binom{5}{3}\binom{7}{2} = \frac{5!}{3!2!}\cdot\frac{7!}{2!5!}$$
$$= \frac{7\cdot 6\cdot 5\cdot 4\cdot 3\cdot 2\cdot 1}{3\cdot 2\cdot 1\cdot 2\cdot 1\cdot 2\cdot 1}$$
$$= 210.$$

b. También se puede responder a esta pregunta por la regla de adición o por la regla de la diferencia. La solución por la regla de la diferencia es más breve y se presenta primero.

Observe que el conjunto de equipos de cinco personas que contiene al menos un hombre es igual a la diferencia entre el conjunto de todos los equipos de cinco personas y el conjunto de equipos de cinco personas que no contienen a ningún hombre. Vea la figura 9.5.5 que se muestra a continuación.

Ahora un equipo con ningún hombre consta de cinco mujeres escogidas de las siete mujeres en el grupo, por lo que hay $\binom{7}{5}$ de tales equipos. También, por el ejemplo 9.5.4, el número total de equipos de cinco personas es $\binom{12}{5} = 792$. Por tanto, por la regla de diferencia,

$$\begin{bmatrix}\text{número de equipos}\\ \text{con al menos un}\\ \text{hombre}\end{bmatrix} = \begin{bmatrix}\text{número total}\\ \text{de equipos}\\ \text{de cinco}\end{bmatrix} - \begin{bmatrix}\text{número de equipos de}\\ \text{cinco que no contienen}\\ \text{ningún hombre}\end{bmatrix}$$
$$= \binom{12}{5} - \binom{7}{5} = 792 - \frac{7!}{5!\cdot 2!}$$
$$= 792 - \frac{7\cdot \overset{3}{6}\cdot 5!}{5!\cdot 2\cdot 1} = 792 - 21 = 771.$$

El razonamiento se resume en la figura 9.5.5

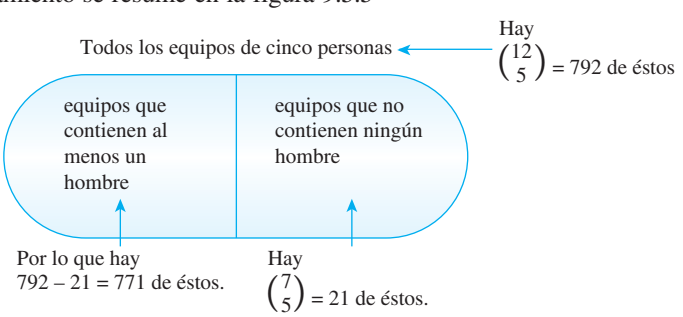


Figura 9.5.5

Alternativamente, usando la regla de la adición, observe que el conjunto de equipos que contienen al menos un hombre se puede particionar como se muestra en la figura 9.5.6. El número de equipos en cada subconjunto de la partición se calcula mediante el método que se ilustra en el inciso *a*). Hay

$\binom{5}{1}\binom{7}{4}$ equipos con un hombre y cuatro mujeres

$\binom{5}{2}\binom{7}{3}$ equipos con dos hombres y tres mujeres

$\binom{5}{3}\binom{7}{2}$ equipos con tres hombres y dos mujeres

$\binom{5}{4}\binom{7}{1}$ equipos con cuatro hombres y una mujer

$\binom{5}{5}\binom{7}{0}$ equipos con cinco hombres y ninguna mujer.

Por tanto, por la regla de la adición,

$$\begin{bmatrix}\text{número de equipos con}\\ \text{al menos un hombre}\end{bmatrix}$$

$$= \binom{5}{1}\binom{7}{4} + \binom{5}{2}\binom{7}{3} + \binom{5}{3}\binom{7}{2} + \binom{5}{4}\binom{7}{1} + \binom{5}{5}\binom{7}{0}$$

$$= \frac{5!}{1!4!}\cdot\frac{7!}{4!3!} + \frac{5!}{2!3!}\cdot\frac{7!}{3!4!} + \frac{5!}{3!2!}\cdot\frac{7!}{2!5!} + \frac{5!}{4!1!}\cdot\frac{7!}{1!6!} + \frac{5!}{5!0!}\cdot\frac{7!}{0!7!}$$

$$= \frac{5\cdot\cancel{4!}\cdot 7\cdot\cancel{6}\cdot 5\cdot\cancel{4!}}{\cancel{4!}\cdot\cancel{3}\cdot\cancel{2}\cdot 4!} + \frac{5\cdot\overset{2}{\cancel{4}}\cdot\cancel{3!}\cdot 7\cdot\cancel{6}\cdot 5\cdot\cancel{4!}}{\cancel{3!}\cdot\cancel{2}\cdot\cancel{4!}\cdot\cancel{3}\cdot\cancel{2}} + \frac{5\cdot\overset{2}{\cancel{4}}\cdot\cancel{3!}\cdot 7\cdot\overset{3}{\cancel{6}}\cdot\cancel{5!}}{\cancel{2}\cdot\cancel{3!}\cdot\cancel{5!}\cdot\cancel{2}}$$

$$+ \frac{5\cdot\cancel{4!}\cdot 7\cdot\cancel{6!}}{\cancel{4!}\cdot\cancel{6!}} + \frac{\cancel{5!}\cdot\cancel{7!}}{\cancel{5!}\cdot\cancel{7!}}$$

$$= 175 + 350 + 210 + 35 + 1 = 771.$$

Este razonamiento se resume en la figura 9.5.6.

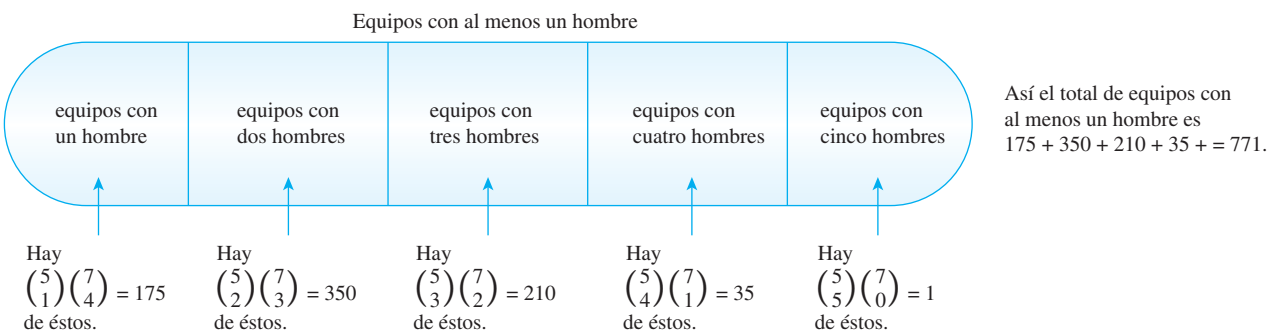


Figura 9.5.6

c. Como se muestra en la figura 9.5.7 en la página siguiente, el conjunto de equipos que contienen a lo más un hombre puede particionarse en el conjunto de los que no contienen a ningún hombre y el conjunto de los que contienen exactamente un hombre. Por tanto, por la regla de la adición,

$$\begin{bmatrix}\text{número de}\\ \text{equipos con a lo}\\ \text{más un hombre}\end{bmatrix} = \begin{bmatrix}\text{número de}\\ \text{equipos sin}\\ \text{ningún hombre}\end{bmatrix} + \begin{bmatrix}\text{número de}\\ \text{equipos con}\\ \text{un hombre}\end{bmatrix}$$
$$= \binom{5}{0}\binom{7}{5} + \binom{5}{1}\binom{7}{4} = 21 + 175 = 196.$$

Este razonamiento se resume en la figura 9.5.7

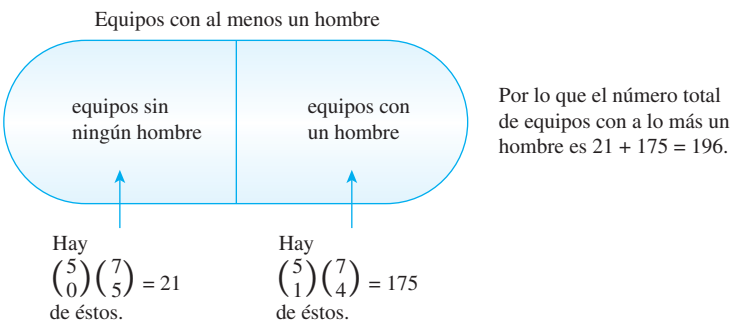


Figura 9.5.7 ■

Ejemplo 9.5.8 Problemas de mano de póquer

El juego de póquer se juega con una baraja ordinaria de cartas (vea el ejemplo 9.1.1). A varias manos de póquer de cinco cartas se le dan nombres especiales y ciertas manos de póquer le ganan a otras manos de póquer. A continuación se enumeran las manos de póquer con nombres de mayor a menor.

Escalera real: 10, J, Q, K, A del mismo palo

Escalera de color: cinco denominaciones adyacentes del mismo palo, pero no una escalera real: El as puede ser alta o baja, así A, 2, 3, 4, 5 del mismo palo es una escalera.

Póquer (cuatro de un tipo)*:* cuatro cartas de una denominación; la quinta carta puede ser cualquier otra de la baraja

Full: tres cartas de una denominación, dos cartas de otra denominación

Color: cinco cartas del mismo palo, pero no una escalera o una escalera real

Escalera: cinco cartas de denominaciones adyacentes, pero no todas del mismo palo: los ases pueden ser altos o bajos

Tercia: tres cartas de la misma denominación y otras dos tarjetas de diferentes denominaciones

Doble par: dos cartas de una primera denominación, dos cartas de una segunda denominación y una quinta carta de un tercera denominación

Par: dos cartas de una denominación y las otras tres cartas de diferentes denominaciones

No pares: todas las cartas de diferentes denominaciones, pero no una escalera o una escalera real o de color.

a. ¿Cuántas manos de póquer de cinco cartas contienen dos pares?

b. Si se saca aleatoriamente una mano de cinco cartas de una baraja ordinaria de cartas, ¿cuál es la probabilidad de que la mano contenga dos pares?

Solución

a. Considere la formación de una mano con dos pares como un proceso de cuatro pasos:

Paso 1: Elija las dos denominaciones de los pares.

Paso 2: Elija las dos cartas de la denominación más pequeña.

Paso 3: Elija las dos cartas de la denominación más grande.

Paso 4: Elija una carta de las restantes.

El número de formas de realizar el paso 1 es $\binom{13}{2}$ ya que hay 13 denominaciones en total. El número de formas de realizar los pasos 2 y 3 es $\binom{4}{2}$ ya que hay cuatro cartas de cada denominación, una en cada palo. El número de formas de realizar el paso 4 es $\binom{44}{1}$ ya que la quinta carta se elige de las once denominaciones no incluidas en el par y hay cuatro cartas de cada denominación. Así,

$$\begin{bmatrix}\text{número total de manos}\\ \text{con dos pares}\end{bmatrix} = \binom{13}{2}\binom{4}{2}\binom{4}{2}\binom{44}{1}$$

$$= \frac{13!}{2!(13-2)!}\cdot\frac{4!}{2!(4-2)!}\cdot\frac{4!}{2!(4-2)!}\cdot\frac{44!}{1!(44-1)!}$$

$$= \frac{13\cdot 12\cdot 11!}{(2\cdot 1)\cdot 11!}\cdot\frac{4\cdot 3\cdot 2!}{(2\cdot 1)\cdot 2!}\cdot\frac{4\cdot 3\cdot 2!}{(2\cdot 1)\cdot 2!}\cdot\frac{44\cdot 43!}{1\cdot 43!}$$

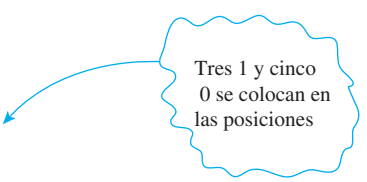
$$= 78\cdot 6\cdot 6\cdot 44 \;=\; 123\,552.$$

b. El número total de manos de cinco cartas de una baraja ordinaria es $\binom{52}{5} = 2\,598\,960$. Así, si todas las manos son equiprobables, la probabilidad de obtener una mano con dos pares es $\frac{123\,552}{2\,598\,960} \cong 4.75\%$. ■

Ejemplo 9.5.9 Número de cadenas de bits con un número fijo de 1

¿Cuántas cadenas de ocho bits tienen exactamente tres 1?

Solución Para resolver este problema, imagine ocho posiciones vacías en la que se colocará el 0 y el 1 de la cadena de bits. En el paso 1, se eligen las posiciones para los tres 1 y en el paso 2, se coloca el 0.



1 2 3 4 5 6 7 8

Una vez que se ha elegido un subconjunto de tres posiciones de los ocho que contienen 1, entonces las cinco restantes posiciones debe contener 0 (ya que la cadena es exactamente de tres 1). Se deduce que el número de formas de construir una cadena de ocho bits con exactamente tres 1 es igual que el número de subconjuntos de tres posiciones que se pueden elegir de los ocho lugares en el que desea colocar el 1. Por el teorema de 9.5.1, esto es igual a

$$\binom{8}{3} = \frac{8!}{3!\cdot 5!} = \frac{8\cdot 7\cdot 6\cdot 5!}{3\cdot 2\cdot 5!} = 56.$$

■

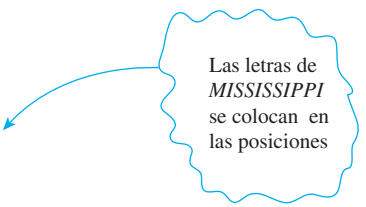
Ejemplo 9.5.10 Permutaciones de un conjunto con elementos repetidos

Considere varias formas de ordenar las letras en la palabra *MISSISSIPPI:*

IIMSSPISSIP, *ISSSPMIIPIS*, *PIMISSSSIIP*, etcétera.

¿Cuántos ordenamientos distinguibles existen?

Solución Este ejemplo generaliza el ejemplo 9.5.9. Imagine que coloca las 11 letras de *MISSISSIPPI* una tras otra en 11 lugares.



Porque copias de la misma letra no pueden distinguirse entre sí, una vez que se conocen las posiciones para una determinada letra, todas las copias de la letra pueden entrar en las posiciones en cualquier orden. Se deduce que construir un orden de las letras puede considerarse como un proceso de cuatro-pasos:

Paso 1: Elija un subconjunto de cuatro posiciones para las *S*.

Paso 2: Elija un subconjunto de cuatro posiciones para las *I*.

Paso 3: Elija un subconjunto de dos posiciones para las *P*.

Paso 4: Elija un subconjunto de una posición para la *M*.

Ya que hay 11 posiciones en total, hay $\binom{11}{4}$ subconjuntos de cuatro posiciones para la *S*. Una vez que las cuatro *S* están en su lugar, hay siete posiciones que permanecen vacías, por lo que hay $\binom{7}{4}$ subconjuntos de cuatro posiciones para las *I*. Después de que las *I* están en su lugar, hay tres posiciones vacías, por lo que hay $\binom{3}{2}$ subconjuntos de dos posiciones para las *P*. Lo que deja una posición para la *M*. Pero $1 = \binom{1}{1}$. Por tanto por la regla de multiplicación,

$$\begin{bmatrix}\text{número de maneras de}\\ \text{colocar todas las letras}\end{bmatrix} = \binom{11}{4}\binom{7}{4}\binom{3}{2}\binom{1}{1}$$

$$= \frac{11!}{4!7!}\cdot\frac{7!}{4!3!}\cdot\frac{3!}{2!1!}\cdot\frac{1!}{1!0!}$$

$$= \frac{11!}{4!\cdot 4!\cdot 2!\cdot 1!} = 34{,}650.$$

■

En el ejercicio 18 del final de la sección, se le pide demostrar que cambiar el orden en que se colocan las letras en las posiciones no cambia la respuesta a este ejemplo.

El mismo razonamiento utilizado en este ejemplo puede utilizarse para obtener el siguiente teorema general.

Teorema 9.5.2 Permutaciones con conjuntos de objetos no distinguibles

Suponga que una colección consiste de n objetos n de los cuales

$$\begin{aligned} &n_1 \text{ son de tipo 1 y son no distinguibles entre sí} \\ &n_2 \text{ son de tipo 2 y son no distinguibles entre sí} \\ &\vdots \\ &n_k \text{ son de tipo } k \text{ y son no distinguibles entre sí} \end{aligned}$$

y suponga que $n_1 + n_2 + \cdots + n_k = n$. Entonces el número de permutaciones de los n objetos es

$$\binom{n}{n_1}\binom{n-n_1}{n_2}\binom{n-n_1-n_2}{n_3}\cdots\binom{n-n_1-n_2-\cdots-n_{k-1}}{n_k} = \frac{n!}{n_1!\,n_2!\,n_3!\cdots n_k!}.$$

Algunos consejos acerca del conteo

Los estudiantes que están aprendiendo técnicas de conteo con frecuencia preguntan, ¿cómo sé qué multiplicar y qué sumar? ¿Cuándo se utiliza la regla de multiplicación y cuándo se utiliza la regla de adición? Por desgracia, estas preguntas no tienen respuestas fáciles. Necesita imaginar, tan claramente como sea posible, los objetos que está contando. Incluso puede comenzar a hacer una lista real de los elementos que intenta contar para hacerse una idea de cómo obtenerlo en forma sistemática. Después debe construir un modelo que le permitirá seguir contando los objetos uno por uno si tiene tiempo suficiente. Si se puede imagine los elementos que está contando con un proceso de varios pasos (en el que cada paso se realiza en un número fijo de maneras independientemente de cómo se realizaron los pasos anteriores), después puede utilizar la regla de multiplicación. El número total de elementos será el producto del número de formas para realizar cada paso. Si, sin embargo, puede imaginar que el conjunto de elementos que está contando se divide en subconjuntos separados, puede utilizar la regla de adición. El número total de elementos del conjunto será la suma del número de elementos en cada subconjunto.

Uno de los errores más comunes de los estudiantes es contar ciertas posibilidades más de una vez.

Ejemplo 9.5.11 Doble conteo

Considere de nuevo el problema del ejemplo 9.5.7*b*). Un grupo consiste de cinco hombres y siete mujeres. ¿Cuántos equipos de cinco contienen al menos un hombre?

¡Precaución! Procure evitar contar los elementos dos veces cuando utiliza la regla de la multiplicación.

Solución incorrecta
Imagine construir el equipo como un proceso de dos-pasos:

Paso 1: Elija un subconjunto de uno de los cinco hombres.

Paso 2: Elija un subconjunto de los otros cuatro de las once personas restantes.

Por tanto, por la multiplicación de regla, hay $\binom{5}{1}\cdot\binom{11}{4} = 1\,650$ equipos de cinco personas que contienen al menos un hombre.

Análisis de la solución incorrecta El problema con la solución anterior es que algunos equipos se cuentan más de una vez. Supongamos que los hombres son Anwar, Ben, Carlos,

Dwayne y Ed y las mujeres son Fumiko, Gail, Hui-Fan, Inez, Jill, Kim y Laura. Según el método descrito anteriormente, un posible resultado del proceso de dos pasos es el siguiente:

Resultado del paso 1: Anwar

Resultado del paso 2: Ben, Gail, Inez y Jill.

En este caso el equipo sería {Anwar, Ben, Gail, Inez, Jill}. Pero otro resultado posible es

Resultado del paso 1: Ben

Resultado del paso 2: Anwar, Gail, Inez y Jill,

que también da el equipo {Anwar, Ben, Gail, Inez, Jill}. Así este equipo está dado por dos diferentes ramas del árbol de probabilidad y así se cuenta dos veces. ■

La mejor manera de evitar errores como el que acabo de describir es visualizar el árbol de probabilidad que corresponde a cualquier uso de la regla de la multiplicación y la partición del conjunto que corresponde a un uso de la regla de adición. Compruebe como funciona su división trabajando por pasos aplicando a algunos datos reales; como se hizo en el análisis anterior e intente recolectar datos que sean tan típicos o genéricos como sea posible.

A menudo ayuda a preguntarse a sí mismo: 1) ¿Estoy contando todo? y 2) ¿Estoy contando dos veces? Cuando se utiliza la regla de multiplicación, estas preguntas se convierten en: 1) ¿Cada resultado se presenta como una rama del árbol? y 2) ¿Algún resultado se presenta en más de una rama del árbol? Cuando se utiliza la regla de adición, las preguntas se convierten en: 1) ¿Cada resultado se presenta en algún subconjunto del diagrama? y 2) ¿Cualesquiera dos subconjuntos del diagrama comparten elementos comunes?

El número de particiones de un conjunto en r subconjuntos

En una sucesión normal (o *simplemente indexada*), n enteros están asociados con los números a_n. En una sucesión *doblemente indexada*, los pares ordenados de enteros (m, n) están asociados con los números $a_{m,n}$. Por ejemplo, se pueden considerar a las combinaciones como los términos de una sucesión doblemente indexado definida por $C_{n,r} = \binom{n}{r}$ para todos los enteros n y r con $0 \leq r \leq n$.

Nota Los números de Stirling de primera clase se utilizan para contar r-permutaciones con varias propiedades.

Un ejemplo importante de una sucesión doblemente indexada es la sucesión de los *números de Stirling de segunda clase*. Estos números, se llaman así en honor del matemático escocés James Stirling (1692-1770), surgen en una sorprendentemente gran variedad de problemas de conteo. Están definidos de forma recursiva y pueden interpretarse en términos de particiones de un conjunto.

Observe que si un conjunto de tres elementos $\{x_1, x_2, x_3\}$ se particiona en dos subconjuntos, entonces uno de los subconjuntos tiene un elemento y el otro tiene dos elementos. Por tanto, hay tres maneras en que se puede particionar al conjunto:

$\{x_1, x_2\}\{x_3\}$ poniendo a x_3 mismo
$\{x_1, x_3\}\{x_2\}$ poniendo a x_2 mismo
$\{x_2, x_3\}\{x_1\}$ poniendo a x_1 mismo

En general, sea

$S_{n,r} =$ número de formas en que un conjunto de tamaño n se puede particionar en r subconjuntos

Entonces, por la ecuación anterior, $S_{3,2} = 3$. Los números $S_{n,r}$ se llaman **números de Stirling de segunda clase**.

Ejemplo 9.5.12 Valores de los números de Stirling

Determine $S_{4,1}$, $S_{4,2}$, $S_{4,3}$ y $S_{4,4}$.

Solución Dado un conjunto con cuatro elementos, se denotan por $\{x_1, x_2, x_3, x_4\}$. El número de Stirling $S_{4,1} = 1$ debido a un conjunto de cuatro elementos se puede particionar en un subconjunto de una sola forma:

$$\{x_1,\ x_2,\ x_3,\ x_4\}.$$

Similarmente, $S_{4,4} = 1$ ya que hay sólo una manera de particionar un conjunto de cuatro elementos en cuatro subconjuntos:

$$\{x_1\}\{x_2\}\{x_3\}\{x_4\}.$$

El número $S_{4,2} = 7$. La razón es que cualquier partición de $\{x_1, x_2, x_3, x_4\}$ en dos subconjuntos debe consistir en cualquiera de los dos subconjuntos de tamaño dos o de un subconjunto tener tamaño tres y un subconjunto de tamaño uno. Las particiones para las cuales ambos conjuntos tienen tamaño dos deben emparejar con x_1 con x_2, con x_3 o con x_4, lo que da lugar a estas tres particiones:

$$\begin{aligned}
\{x_1, x_2\}\{x_3, x_4\} &\quad x_2 \text{ asociado con } x_1\\
\{x_1, x_3\}\{x_2, x_4\} &\quad x_3 \text{ asociado con } x_1\\
\{x_1, x_4\}\{x_2, x_3\} &\quad x_4 \text{ asociado con } x_1
\end{aligned}$$

Las particiones para un subconjunto tienen tamaño uno y el otro tiene tamaño tres pueden tener cualquiera de los cuatro elementos en el subconjunto de tamaño uno, lo que conduce a estas cuatro particiones:

$$\begin{aligned}
\{x_1\}\{x_2, x_3, x_4\} &\quad x_1 \text{ por sí mismo}\\
\{x_2\}\{x_1, x_3, x_4\} &\quad x_2 \text{ por sí mismo}\\
\{x_3\}\{x_1, x_2, x_4\} &\quad x_3 \text{ por sí mismo}\\
\{x_4\}\{x_1, x_2, x_3\} &\quad x_4 \text{ por sí mismo}
\end{aligned}$$

Por lo que se deduce que el número total de maneras que el conjunto $\{x_1, x_2, x_3, x_4\}$ se puede particionar en dos subconjuntos es $3 + 4 = 7$.

Por último, $S_{4,3} = 6$ porque cualquier partición de un conjunto de cuatro elementos en tres subconjuntos debe tener dos elementos en un subconjunto y los otros dos elementos en subconjuntos por ellos mismos. Hay $\binom{4}{2} = 6$ maneras de elegir los dos elementos que se ponen juntos, lo que resulta en las siguientes seis posibles particiones:

$$\begin{aligned}
&\{x_1, x_2\}\{x_3\}\{x_4\} \quad \{x_2, x_3\}\{x_1\}\{x_4\}\\
&\{x_1, x_3\}\{x_2\}\{x_4\} \quad \{x_2, x_4\}\{x_1\}\{x_3\}\\
&\{x_1, x_4\}\{x_2\}\{x_3\} \quad \{x_3, x_4\}\{x_1\}\{x_2\}
\end{aligned}$$

■

Ejemplo 9.5.13 Determinación de una relación de recurrencia de $S_{n,r}$

Determine una relación de recurrencia $S_{n,r}$ para valores de la sucesión con índices bajo n y r y que dan las condiciones para la recursión.

Solución Para resolver este problema de forma recursiva, supongamos que ha encontrado un procedimiento para contar el número de formas de dividir un conjunto de $n - 1$ elementos en $r - 1$ subconjuntos y el número de formas para particionar un conjunto de $n - 1$ elementos en r subconjuntos. Las particiones de un conjunto de n elementos $\{x_1, x_2, \ldots, x_n\}$ en r subconjuntos se puede dividir, como se muestra en la figura 9.5.8 en la siguiente página, en los que contienen al conjunto $\{x_n\}$ y los que no.

Para obtener el resultado que se muestra en la figura 9.5.8 primero se cuenta el número de particiones de $\{x_1, x_2, \ldots, x_n\}$ en r subconjuntos, donde uno de los subconjuntos es $\{x_n\}$. Para hacer esto, imagine cualquiera de las $S_{n-1,r-1}$ particiones de $\{x_1, x_2, \ldots, x_{n-1}\}$ en

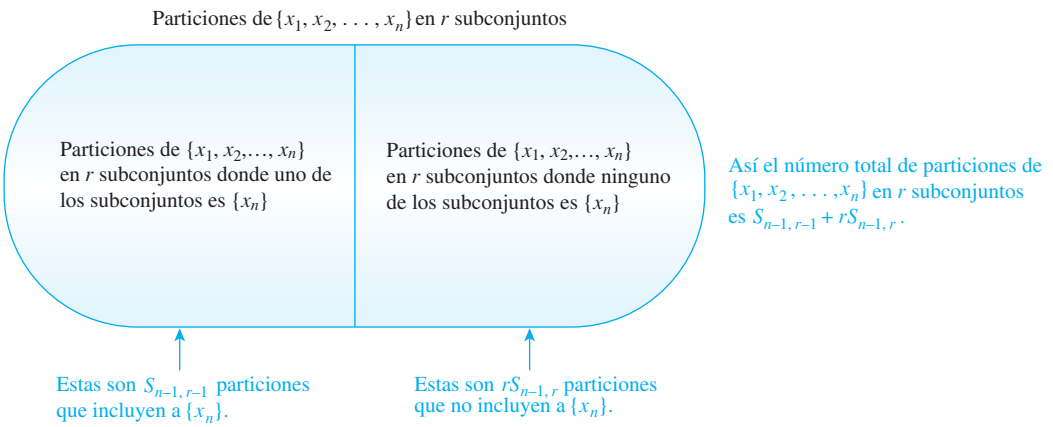


Figura 9.5.8

$r-1$ subconjuntos y sumar el subconjunto $\{x_n\}$ a la partición. Por ejemplo, si $n=4$ y $r=3$, que podría adoptar una de las tres particiones de $\{x_1, x_2, x_3\}$ en dos subconjuntos, a saber:

$$\{x_1,\ x_2\}\{x_3\}, \quad \{x_1,\ x_3\}\{x_2\}, \quad \text{o} \quad \{x_2,\ x_3\}\{x_1\},$$

y sumando $\{x_4\}$. El resultado sería una de las particiones

$$\{x_1,\ x_2\}\{x_3\}\{x_4\}, \quad \{x_1,\ x_3\}\{x_3\}\{x_4\}, \quad \text{o} \quad \{x_2,\ x_3\}\{x_1\}\{x_4\}.$$

Claramente, cualquier partición de $\{x_1, x_2, \ldots, x_n\}$ en r subconjuntos con $\{x_n\}$ como uno de los subconjuntos puede obtenerse de esta manera. Por tanto $S_{n-1,r-1}$ es el número de particiones de $\{x_1, x_2, \ldots, x_n\}$ en r subconjuntos, de los cuales uno es $\{x_n\}$.

A continuación, cuente el número de particiones de $\{x_1, x_2, \ldots, x_n\}$ en r subconjuntos donde $\{x_n\}$ *no* es uno de los subconjuntos de la partición. Imagine que alguna de las $S_{n-1,r}$ particiones de $\{x_1, x_2, \ldots, x_{n-1}\}$ en r subconjuntos. Ahora imagine elegir uno de los r subconjuntos de la partición y sumar en el elemento x_n. El resultado es una partición de $\{x_1, x_2, \ldots, x_n\}$ en r subconjuntos de ninguno de los cuales es el subconjunto con un elemento $\{x_n\}$. Ya que el elemento x_n podría sumarse cualquiera de los r subconjuntos de la partición, se deduce de la regla de multiplicación que existen $rS_{n-1,r}$ particiones de este tipo. Por ejemplo, si $n=4$ y $r=3$, podría tomar la (única) partición de $(x_1, x_2, x_3\}$ en tres subconjuntos, es decir $\{x_1\}\{x_2\}\{x_3\}$ y sumar x_4 a uno de estos conjuntos. El resultado sería una de las particiones

$$\underset{\uparrow}{\{x_1, x_4\}}\{x_2\}\{x_3\}, \quad \{x_1\}\underset{\uparrow}{\{x_2, x_4\}}\{x_3\}, \quad \text{o} \quad \{x_1\}\{x_2\}\underset{\uparrow}{\{x_3, x_4\}}.$$

x_4 se suma a $\{x_1\}$ x_4 se suma a $\{x_2\}$ x_4 se suma a $\{x_3\}$

Claramente, cualquier partición de $\{x_1, x_2, \ldots, x_n\}$ en r subconjuntos, ninguno de los cuales es $\{x_n\}$, puede obtenerse en la forma descrita anteriormente, para cuando se remueve x_n de cualquier subconjunto que lo contiene en una partición, el resultado es una partición de $\{x_1, x_2, \ldots, x_{n-1}\}$ en r subconjuntos. Por tanto $rS_{n-1,r}$ es el número de particiones de $\{x_1, x_2, \ldots, x_n\}$ que no contienen a $\{x_n\}$.

Ya que cualquier partición de $\{x_1, x_2, \ldots, x_n\}$ contiene $\{x_n\}$ o no,

$$\begin{bmatrix}\text{el número de particiones}\\ \text{de } \{x_1,\ x_2, \ldots, x_n\}\\ \text{en } r \text{ subconjuntos}\end{bmatrix} = \begin{bmatrix}\text{el número de particiones de}\\ \{x_1,\ x_2, \ldots, x_n\} \text{ en } r \text{ subconjuntos}\\ \text{de los cuales } \{x_n\} \text{ es uno}\end{bmatrix} + \begin{bmatrix}\text{el número de particiones de}\\ \{x_1,\ x_2, \ldots, x_n\} \text{ en } r \text{ subconjuntos}\\ \text{ninguno de los cuales es } \{x_n\}\end{bmatrix}$$

Así

$$S_{n,r} = S_{n-1,r-1} + r\,S_{n-1,r}$$

para todos los enteros n y r con $1 < r < n$.

Las condiciones iniciales para la relación de recurrencia son

$$S_{n,1} = 1 \quad \text{y} \quad S_{n,n} = 1 \text{ para todos los enteros } n \geq 1$$

ya que sólo hay una forma de particionar $\{x_1, x_2, \ldots, x_n\}$ en un subconjunto, a saber:

$$\{x_1, x_2, \ldots, x_n\}.$$

y sólo una forma de particionar $\{x_1, x_2, \ldots, x_n\}$ en n subconjuntos, a saber:

$$\{x_1\}, \{x_2\}, \ldots, \{x_n\}.$$

■

Autoexamen

1. El número de subconjuntos de tamaño r que se puede formar a partir de un conjunto con n elementos se denota por _____, que se lee como "_____".
2. El número de r-combinaciones de un conjunto de n elementos es _____.
3. Dos selecciones no ordenadas se dicen que son iguales si los elementos elegidos son los mismos, independientemente del _____.
4. Una fórmula que relaciona a $\binom{n}{r}$ y $P(n, r)$ es _____.
5. La frase "al menos n" significa _____ y la frase "a lo más n" significa _____.
6. Supongamos que una colección consiste de n objetos de los cuales, para cada i con $1 \leq i \leq k$, n_i son del tipo i y son no distinguibles entre sí. Suponga también que $n = n_1 + n_2 + \cdots + n_k$. Entonces el número de permutaciones distintas de n objetos es _____.
7. El número de Stirling de segunda clase, $S_{n,r}$, se puede interpretar como _____.
8. Ya que cualquier partición de un conjunto $X = \{x_1, x_2, \ldots, x_n\}$ contiene ya sea a $\{x_n\}$ o no, el número de particiones de X en r subconjuntos es igual a _____ más _____.

Conjunto de ejercicios 9.5.

1. a. Enumere todas las 2-combinaciones del conjunto $\{x_1, x_2, x_3\}$. Deduzca el valor de $\binom{3}{2}$.

b. Enumere todas las selecciones no ordenadas de cuatro elementos del conjunto $\{a, b, c, d, e\}$. Deduzca el valor de $\binom{5}{4}$.

2. a. Enumere todas las 3-combinaciones para el conjunto $\{x_1, x_2, x_3, x_4, x_5\}$. Deduzca el valor de $\binom{5}{3}$.

b. Enumere todas las selecciones no ordenadas de dos elementos del conjunto $\{x_1, x_2, x_3, x_4, x_5, x_6\}$. Deduzca el valor de $\binom{6}{2}$.

3. Escriba una ecuación que relacione a $P(7, 2)$ con $\binom{7}{2}$.

4. Escriba una ecuación que relacione a $P(8, 3)$ con $\binom{8}{3}$.

5. Utilice el teorema 9.5.1 para calcular cada una de las siguientes expresiones.

a. $\binom{6}{0}$ **b.** $\binom{6}{1}$ c. $\binom{6}{2}$

d. $\binom{6}{3}$ e. $\binom{6}{4}$ f. $\binom{6}{5}$ g. $\binom{6}{6}$

6. Un consejo estudiantil consta de 15 estudiantes.

a. ¿De cuántas maneras puede seleccionar a un comité de seis de los miembros del consejo?

b. Dos miembros del consejo tienen la misma especialidad y no pueden servir juntos en un comité. ¿Cuántas formas hay de seleccionar un comité de seis miembros del consejo?

c. Dos miembros del consejo siempre insisten en servir juntos en un comité. Si no se sirven juntos, no sirven en absoluto. ¿De cuántas maneras se puede seleccionar un comité de seis miembros del consejo?

d. Suponga que el consejo contiene ocho hombres y siete mujeres.

i) ¿Cuántos comités de seis personas contienen tres hombres y tres mujeres?

ii) ¿Cuantos comités de seis personas contienen al menos una mujer?

e. Suponga que el consejo está formado por tres estudiantes de primer año, cuatro estudiantes, tres profesores jóvenes y cinco con experiencia. ¿Cuántos comités de ocho contienen dos representantes de cada clase?

7. Un equipo de programación tiene 13 miembros.

a. ¿De cuántas maneras se puede elegir un grupo de siete para trabajar en un proyecto?

b. Supongamos que siete miembros del equipo son mujeres y seis hombres.

i) ¿Cuántos grupos de siete se pueden elegir que contengan cuatro mujeres y tres hombres?

ii) ¿Cuántos grupos de siete se pueden elegir que contengan al menos un hombre?

iii) ¿Cuántos grupos de siete se pueden elegir que contengan como máximo tres mujeres?

c. Suponga que dos miembros del equipo se niegan a colaborar en proyectos. ¿Cuántos grupos de siete se pueden elegir para trabajar en un proyecto?
d. Suponga que dos miembros del equipo insisten ambos en trabajar juntos o no en proyectos. ¿Cuántos grupos de siete se pueden elegir para trabajar en un proyecto?

H **8.** Un instructor aplica un examen con catorce preguntas. Los alumnos pueden elegir cualesquiera de diez para responder.
a. ¿Cuántas opciones diferentes de diez preguntas existen?
b. Suponga que seis preguntas requieren demostración y ocho no.
i) ¿Cuántos grupos de diez preguntas contienen cuatro que requieren demostración y seis que no?
ii) ¿Cuántos grupos de diez preguntas contienen al menos una que requiere demostración?
iii) ¿Cuántos grupos de diez preguntas contienen como máximo tres que requieren demostración?
c. Suponga que las instrucciones del examen especifican que a lo más una de las preguntas 1 y 2 podrá incluirse entre las diez. ¿Cuántas opciones diferentes de diez preguntas existen?
d. Suponga que las instrucciones de examen especifican que ambas preguntas 1 y 2 deben incluirse entre las diez o que no se incluya ninguna de ellas. ¿Cuántas opciones diferentes de diez preguntas existen?

9. Un club está considerando modificar sus estatutos. En una votación de tanteo inicial sobre el tema, 24 de los 40 miembros del club favoreció el cambio y 16 no. Se eligió un comité de seis de los miembros de los 40 miembros del club para dedicarse a seguir estudiando la posibilidad.
a. ¿Cuántos comités de seis pueden formarse a partir de los miembros del club?
b. ¿Cuántos comités pueden formarse que contengan al menos tres miembros del club que, en el estudio preliminar, favorecieron el cambio en los estatutos?

10. Se están probando dos nuevos medicamentos usando un grupo de 60 ratones de laboratorio, cada uno con una etiqueta con un número de identificación. El medicamento A se les da a 22 ratones, el medicamento B se les da a otros 22 ratones y los 16 ratones restantes se utilizan como controles. ¿De cuántas maneras se puede hacer la asignación de tratamientos a los ratones? (Una sola asignación consiste en especificar el tratamiento para cada ratón; si el medicamento A, medicamento B o ningún medicamento).

✶ 11. Consulte el ejemplo 9.5.8. Para cada mano de póquer que se menciona a continuación, 1) encuentre el número de manos de póquer de cinco cartas con esa jugada; 2) encuentre la probabilidad de que un conjunto aleatorio de cinco cartas tenga esa tirada.
a. escalera real b. escalera de color **c.** cuatro de una clase
d. full e. color **f.** escalera
g. tercia de una clase h. un par.
i. ni una denominación repetida ni cinco del mismo palo ni cinco denominaciones adyacentes

12. ¿Cuántas parejas de dos enteros distintos se eligen en el conjunto {1, 2, 3,…, 101} tienen una suma que es par?

13. Se lanza diez veces una moneda. En cada caso el resultado se registra como *H* (para cara) o *T* (para cruz). (Un posible resultado de las diez tiradas se denota por *T H H T T T H T T H*).
a. ¿Cuál es el número total de posibles resultados del experimento de lanzamiento de la moneda?
b. ¿En cuántos de los posibles resultados se obtienen exactamente cinco caras?
c. ¿En cuántos de los posibles resultados se obtienen al menos ocho caras?
d. ¿En cuántos de los posibles resultados se obtiene al menos una cara?
e. ¿En cuántos de los posibles resultados se obtiene a lo más una cara?

14. a. ¿Cuántas cadenas de 16 bits contienen exactamente siete 1?
b. ¿Cuántas cadenas de 16 bits contienen al menos trece 1?
c. ¿Cuántas cadenas de 16 bits contienen al menos un 1?
d. ¿Cuántas cadenas de 16 bits contienen al más un 1?

15. a. ¿Cuántos enteros pares están en el conjunto

$$\{1, 2, 3,\ldots, 100\}?$$

b. ¿Cuántos enteros impares se encuentran en el conjunto

$$\{1, 2, 3,\ldots, 100\}?$$

c. ¿De cuántas maneras se pueden seleccionar dos enteros en el conjunto {1, 2, 3,…, 100} para que su suma sea par?
d. ¿De cuántas maneras se pueden seleccionar dos enteros en el conjunto {1, 2, 3,…, 100} para que su suma sea impar?

16. Supongamos que tres juntas de computadora en una corrida de producción de cuarenta están defectuosas. Se selecciona una muestra de cinco para controlar defectos.
a. ¿Cuántas muestras diferentes se pueden elegir?
b. ¿Cuántas muestras contendrá al menos una junta defectuosa?
c. ¿Cuál es la probabilidad de que en una muestra de cinco elegida aleatoriamente contenga al menos una junta defectuosa?

17. Diez puntos *A*, *B*, *C*, *D*, *E*, *F*, *G*, *H*, *I*, *J* están arreglados en un plano de tal manera que no hay tres que se encuentren sobre la misma línea recta.
a. ¿Cuántas líneas rectas se determinan por los diez puntos?
b. ¿Cuántas de estas líneas rectas no pasan por el punto *A*?
c. ¿Cuántos triángulos tienen tres de los diez puntos como vértices?
d. ¿Cuántos de estos triángulos no tienen a *A* como vértice?

18. Suponga que se colocan las letras en el ejemplo 9.5.10 en posiciones en el siguiente orden: primero la *M*, después la *I*, luego la *D* y después la *P*. Demuestre que obtendrá la misma respuesta para el número de ordenamientos distinguibles.

19. a. ¿De cuántas maneras distinguibles se pueden ordenar las letras de la palabra *HULLABALOO* cuando se arreglan en orden?

b. ¿Cuántos ordenamientos distinguibles de las letras de *HULLABALOO* comienzan con *U* y terminan con *L*?
c. ¿Cuántos ordenamientos distinguibles de las letras de *HULLABALOO* contienen las dos letras *HU* al lado del otro en orden?

20. a. ¿En cuántas maneras distinguibles se pueden arreglar las letras de la palabra *MILLIMICRON*?
b. ¿Cuántos ordenamientos distinguibles de las letras de *MILLIMICRON* comienzan con *M* y terminan con *N*?
c. ¿Cuántos ordenamientos distinguibles de las letras de *MILLIMICRON* contienen las letras *CR* juntas en orden y también las letras *ON* juntas en orden?

21. En el código Morse, los símbolos se representan por sucesiones de longitud variable de puntos y guiones. (Por ejemplo, $A = \cdot -$, $1 = \cdot - - - -$, $? = \cdot \cdot - - \cdot \cdot$.) ¿Cuántos símbolos diferentes se pueden representar por sucesiones de siete o menos puntos y guiones?

22. Cada símbolo en el código de Braille está representado por un arreglo rectangular de seis puntos, cada uno de los cuales podrá elevarse o aplanarse contra un fondo plano. Por ejemplo, cuando la palabra Braille se deletrea, luce así:

Dado que al menos uno de los seis puntos se debe elevar, cuántos símbolos se pueden representar en el código Braille?

23. En un tablero de 8×8, una torre se puede mover a cualquier número de cuadros horizontal o verticalmente. ¿Cuántos caminos diferentes puede seguir una torre desde el cuadrado de la parte inferior izquierda del tablero al cuadrado de la parte superior derecha del tablero si todos se mueven hacia la derecha o hacia arriba?

24. El número 42 tiene la factorización $2 \cdot 3 \cdot 7$. Así se puede escribir 42 de cuatro maneras como un producto de dos factores enteros (sin considerar el orden de los factores): $1 \cdot 42$, $2 \cdot 21$, $14 \cdot 3$ y $6 \cdot 7$. Responda las preguntas de la a a la d que se presentan a continuación sin considerar el orden de los factores.
a. Enumere las distintas maneras en que se puede escribir el número 210 como producto de dos factores de enteros positivos.
b. Si $n = p_1p_2p_3p_4$, donde las p_i son números primos distintos, ¿de cuántas maneras puede escribirse n como un producto de dos factores de enteros positivos?
c. Si $n = p_1p_2p_3p_4p_5$, donde las p_i son números primos distintos, ¿de cuántas maneras puede escribirse n como un producto de dos factores de enteros positivos?
d. Si $n = p_1p_2 \ldots p_k$, donde las p_i son números primos distintos, ¿de cuántas maneras puede escribirse n como producto de dos factores de enteros positivos?

25. **a.** ¿Cuántas funciones inyectivas existen de un conjunto con tres elementos a un conjunto con cuatro elementos?
b. ¿Cuántas funciones inyectivas existen de un conjunto con tres elementos a un conjunto con dos elementos?
c. ¿Cuántas funciones inyectivas existen de un conjunto con tres elementos a un conjunto con tres elementos?
d. ¿Cuántas funciones inyectivas existen de un conjunto con tres elementos a un conjunto con cinco elementos?
***H* e.** ¿Cuántas funciones inyectivas existen de un conjunto con m elementos a un conjunto con n elementos, donde $m \leq n$?

26. **a.** ¿Cuántas funciones sobreyectivas existen de un conjunto con tres elementos a un conjunto con dos elementos?
b. ¿Cuántas funciones sobreyectivas existen de un conjunto con tres elementos a un conjunto con cinco elementos?
***H* c.** ¿Cuántas funciones sobreyectivas existen de un conjunto con tres elementos a un conjunto con tres elementos?
d. ¿Cuántas funciones sobreyectivas existen de un conjunto con cuatro elementos a un conjunto con dos elementos?
e. ¿Cuántas funciones sobreyectivas existen de un conjunto con cuatro elementos a un conjunto con tres elementos?
***H* ∗ f.** Sea $c_{m,n}$ el número de funciones sobreyectivas de un conjunto de m elementos a un conjunto de n elementos, donde $m \geq n \geq 1$. Encuentre una fórmula que relacione a $c_{m,n}$ con $c_{m-1,n}$ y $c_{m-1,n-1}$.

27. Sea A un conjunto con ocho elementos.
a. ¿Cuántas relaciones hay en A?
b. ¿Cuántas relaciones de A son reflexivas?
c. ¿Cuántas relaciones de A son simétricas?
d. ¿Cuántas relaciones de A son tanto simétricas como reflexivas?

***H* ∗ 28.** Un consejo estudiantil consta de tres estudiantes de primer año, cuatro estudiantes, cuatro profesores jóvenes y cinco con experiencia. ¿Cuántos comités de ocho miembros del consejo contienen al menos un miembro de cada clase?

∗ 29. Una alternativa para deducir el teorema 9.5.1 utiliza la siguiente *regla de división*: Sean n y k enteros para los que k divide a n. Si un conjunto compuesto de n elementos se divide en subconjuntos que contienen k elementos, entonces el número de esos subconjuntos es n/k. Explique cómo el teorema 9.5.1 se puede deducir usando la regla de la división.

30. Encuentre el error en el siguiente razonamiento: "Considere la formación de una mano de póquer con doble par como un proceso de cinco-pasos.

Paso 1: Elija la denominación de un par.
Paso 2: Elija las dos cartas de esa denominación.
Paso 3: Elija la denominación del otro par.
Paso 4: Elija las dos cartas de esa segunda denominación.
Paso 5: Elija la quinta carta de las denominaciones restantes.

Hay $\binom{13}{1}$ formas de realizar el paso 1, $\binom{4}{2}$ maneras de realizar el paso 2, $\binom{12}{1}$ formas de realizar el paso 3, $\binom{4}{2}$ formas de realizar el paso 4 y $\binom{44}{1}$ formas de realizar el paso 5. Por tanto, el número total de manos de póquer de cinco cartas con dos pares es $13 \cdot 6 \cdot 12 \cdot 6 \cdot 44 = 247\,104$".

∗ 31. Sea P_n el número de particiones de un conjunto con n elementos. Demuestre que

$$P_n = \binom{n-1}{0} P_{n-1} + \binom{n-1}{1} P_{n-2} + \cdots + \binom{n-1}{n-1} P_0$$

para todos los enteros $n \geq 1$.

Consulte la sucesión de los números de Stirling de segunda clase para resolver los ejercicios del 32 al 38.

32. Encuentre $S_{3,4}$ al exhibir todas las particiones de $\{x_1, x_2, x_3, x_4, x_5\}$ en cuatro subconjuntos.

33. Utilice los valores calculados en el ejemplo 9.5.12 y la relación de recurrencia y condiciones iniciales encontradas en el ejemplo 9.5.13 para calcular $S_{5,2}$.

34. Utilice los valores calculados en el ejemplo 9.5.12 y la relación de recurrencia y condiciones iniciales encontradas en el ejemplo 9.5.13 para calcular $S_{5,3}$.

35. Utilice los resultados de ejercicios 32 al 34 para encontrar el número total de particiones diferentes de un conjunto con cinco elementos.

36. Utilice inducción matemática y la relación de recurrencia del ejemplo 9.5.13 para demostrar que todos los enteros $n \geq 2$, $S_{n,2} = 2^{n-1} - 1$.

37. Utilice la inducción matemática y la relación de recurrencia del ejemplo 9.5.13 para demostrar que para todos los enteros $n \geq 2$, $\sum_{k=2}^{k}(3^{4-k}S_{k,2}) - S_{n+1,3}$.

***H* 38.** Si X es un conjunto con n elementos y Y es un conjunto con m elementos, exprese el número de funciones sobreyectivas de X y Y utilizando los números de Stirling de segunda clase. Justifique su respuesta.

Respuestas del autoexamen

1. $\binom{n}{r}$; de n se elige r 2. $\binom{n}{r}$ (*O:* de n se elige r) 3. El orden en el que se elijan 4. $\binom{n}{r} = \frac{P(n,r)}{r!}$ 5. n o más; n o menos 6. $\binom{n}{n_1}\binom{n-n_1}{n_2}\binom{n-n_1-n_2}{n_3}\cdots\binom{n-n_1-n_2-\cdots-n_{k-1}}{n_k}$ $\left(O : \frac{n!}{n_1!n_2!n_3!\cdots n_k!}\right)$ 7. el número de formas en que un conjunto de tamaño n se puede particionar en r subconjuntos 8. el número de particiones de X en r subconjuntos de los cuales $\{x_n\}$ es uno; el número de particiones de X en r subconjuntos, ninguno de los cuales es $\{x_n\}$.

9.6 r-combinaciones con repetición permitida

El valor de las matemáticas en cualquier ciencia se encuentra más en el análisis disciplinado y en el pensamiento abstracto que en las teorías y técnicas particulares. —Alan Tucker, 1982

En la sección 9.5 demostramos que hay $\binom{n}{r}$ r-combinaciones o subconjuntos de tamaño r, de un conjunto de n elementos. En otras palabras, hay $\binom{n}{r}$ formas de elegir r elementos distintos sin considerar el orden de un conjunto de n elementos. Por ejemplo, hay $\binom{4}{3} = 4$ formas de elegir tres elementos de un conjunto de cuatro: $\{1, 2, 3\}$, $(1, 2, 4\}$, $\{1, 3, 4\}$, $\{2, 3, 4\}$.

En esta sección nos preguntamos: ¿cuántas formas hay para elegir r elementos sin considerar el orden de un conjunto de n elementos *si se permite repetición*? Una buena manera de imaginar esto es visualizar los n elementos como categorías de objetos de las que se pueden realizar selecciones múltiples. Por ejemplo, si se etiquetan las categorías 1, 2, 3 y 4 y se eligen tres elementos, es posible que elija dos elementos del tipo 3 y uno del tipo 1 o todos los tres del tipo 2 o uno de los tipos 1, 2 y 4. Denotamos tales opciones [3, 3, 1], [2, 2, 2] y [1, 2, 4], respectivamente. Observe que no importa el orden, [3, 3, 1] = [3, 1, 3] = [1, 3, 3], por ejemplo.

• Definición

Una ***r*-combinación con repetición permitida** o **multiconjunto de tamaño *r***, elegida de un conjunto X de n elementos es una selección no ordenada de elementos tomados de X con repetición permitida. Si $X = \{x_1, x_2, \ldots, x_n\}$ escribimos una r-combinación con repetición permitida o multiconjunto de tamaño r, como $[\boldsymbol{x_{i_1}, x_{i_2}, \ldots, x_{i_r}}]$ donde cada x_{i_j} está en X y algunos de los x_{i_j} pueden ser iguales entre sí.

Ejemplo 9.6.1 Repetición permitida con *r*-combinaciones

Escriba una lista completa para encontrar el número de 3-combinaciones con repetición permitida, o multiconjuntos de tamaño 3, que se puede seleccionar de $\{1, 2, 3, 4\}$. Observe que ya que no importa el orden en que se eligen los elementos, los elementos de cada selección pueden escribirse en orden creciente y al escribir los elementos en orden creciente se asegurará que no se pasan por alto combinaciones.

Solución

[1, 1, 1] ; [1, 1, 2]; [1, 1, 3]; [1, 1, 4]	todas las combinaciones con 1, 1
[1, 2, 2] ; [1, 2, 3]; [1, 2, 4];	todas las combinaciones posibles con 1, 2
[1, 3, 3] ; [1, 3, 4]; [1, 4, 4];	todas las combinaciones posibles con 1, 3 o 1, 4
[2, 2, 2] ; [2, 2, 3]; [2, 2, 4];	todas las combinaciones posibles con 2, 2
[2, 3, 3] ; [2, 3, 4]; [2, 4, 4];	todas las combinaciones posibles con 2, 3 o 2, 4
[3, 3, 3] ; [3, 3, 4]; [3, 4, 4];	todas las combinaciones posibles con 3, 3 o 3, 4
[4, 4, 4]	la única combinación adicional con 4, 4

Por tanto hay veinte 3-combinaciones con repetición permitida. ■

¿Cómo se podría haber predicho el número veinte de otra manera que haciendo una lista completa? Considere los números 1, 2, 3 y 4 como categorías e imagine elegir un total de tres números de las categorías con selecciones múltiples de cualquier categoría permitida. Los resultados de varias de esas selecciones están representados por la tabla que se muestra a continuación.

Categoría 1	Categoría 2	Categoría 3	Categoría 4	Resultado de la selección
|	× |		| ××	1 de la categoría 2 2 de la categoría 4
× |		× |	× |	1 de cada una de las categorías 1, 3 y 4
× × × |		|	|	3 de la categoría 1

Como se puede ver, cada selección de tres números de cuatro categorías se puede representar por una cadena de barras verticales y cruces. Se utilizan tres barras verticales para separar las cuatro categorías y se utilizan tres cruces para indicar cuántos elementos de cada categoría se han elegido. Cada cadena distinta de tres barras verticales y tres cruces representa una selección distinta. Por ejemplo, la cadena

$$\times \times | \; | \times |$$

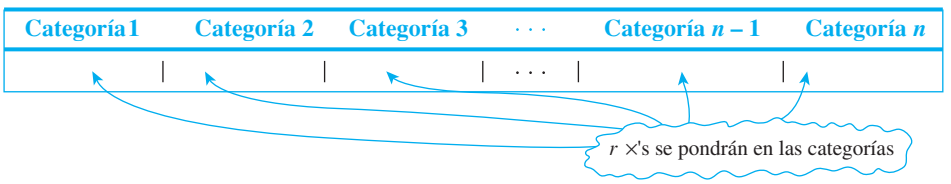
representa la selección: dos de la categoría 1, ninguno de la categoría 2, uno de la categoría 3 y ninguno de la categoría 4. Así el número de selecciones distintas de los tres elementos que pueden formar el conjunto $\{1, 2, 3, 4\}$ con repetición permitida es igual al número de cadenas distintas de seis símbolos que consta de tres | y de tres $\times$. Pero esto es igual al número de formas de seleccionar tres posiciones de seis porque una vez que se han elegido tres posiciones para la $\times$, los | se colocan en las restantes tres posiciones. Por tanto, la respuesta es

$$\binom{6}{3} = \frac{6!}{3!(6-3)!} = \frac{6 \cdot 5 \cdot 4 \cdot 3!}{3 \cdot 2 \cdot 1 \cdot 3!} = 20,$$

como se obtuvo anteriormente con un cuidadoso listado.

El análisis de este ejemplo se extiende hasta el caso general. Para contar el número de *r*-combinaciones con repetición permitida o multiconjuntos de tamaño *r*, que se pueden

seleccionar de un conjunto de n elementos, piense en los elementos del conjunto como categorías. A continuación, cada combinación r con repetición permitida puede representarse como una cadena de $n - 1$ barras verticales (para las n categorías separadas) y r cruza (para representar a los elementos r a elegirse). El número de x en cada categoría representa el número de veces que se repite el elemento representado en esa categoría.



El número de cadenas de $n - 1$ barras verticales y r cruces es el número de formas para elegir r posiciones, en los que colocar las r cruces, de un total de $r + (n - 1)$ posiciones, dejando las restantes posiciones para las barras verticales. Pero por el teorema 9.5.1, este número es $\binom{r+n-1}{r}$.

Este análisis demuestra el teorema siguiente.

Teorema 9.6.1

El número de r-combinaciones con repetición permitida (multiconjuntos de tamaño r) que se pueden seleccionar de un conjunto de n elementos es

$$\binom{r+n-1}{r}.$$

Este es igual al número de formas en que se pueden seleccionar r objetos de n categorías de objetos con repetición permitida.

Ejemplo 9.6.2 Selección de 15 latas de refrescos de cinco diferentes tipos

Una persona que da una fiesta quiere poner 15 latas de refrescos surtidos para sus invitados. Él compra en una tienda que vende cinco tipos diferentes de refrescos.

a. ¿Cuántas selecciones diferentes de latas de 15 refrescos puede hacer?

b. Si la cerveza de raíz es uno de los tipos de bebidas, ¿cuántas diferentes selecciones incluyen por lo menos seis latas de cerveza de raíz?

c. Si la tienda tiene sólo cinco latas de cerveza, pero al menos 15 latas de otros tipos de refrescos, ¿cuántas selecciones diferentes existen?

Solución

a. Piense en los cinco tipos diferentes de refrescos como las n categorías y en las 15 latas de refrescos a ser elegidas como los objetos r (así $n = 5$ y $r = 15$). Cada selección de latas de refrescos se representa por una cadena de $5 - 1 = 4$ barras verticales (para separar las categorías de refrescos) y 15 cruces (para representar las latas seleccionadas). Por ejemplo, la cadena

$$\times\times\times|\times\times\times\times\times\times\times|\quad|\times\times\times|\times\times$$

representa una selección de tres latas de refrescos del tipo 1, siete del tipo 2, ninguno del tipo 3, tres del tipo 4 y dos del tipo 5. El número total de selecciones de 15 latas de

refrescos de los cinco tipos es el número de cadenas de 19 símbolos, $5 - 1 = 4$ de $|$ y 15 de $\times$:

$$\binom{15+5-1}{15} = \binom{19}{15} = \frac{19 \cdot \overset{6}{\cancel{18}} \cdot 17 \cdot \overset{2}{\cancel{16}} \cdot \cancel{15!}}{\cancel{15!} \cdot \cancel{4} \cdot \cancel{3} \cdot \cancel{2} \cdot 1} = 3{,}876.$$

b. Si se incluyen por lo menos seis latas de cerveza de raíz, podemos imaginar elegir seis de esas latas primero y después elegir 9 latas más. La elección de las nueve latas adicionales se puede representar como una cadena de 9 $\times$ y 4 $|$. Por ejemplo, si la cerveza de raíz es del tipo 1, entonces, la cadena $\times \times \times |\ \ |\times|\times\times\times\times|$ representa una selección de tres latas de cerveza de raíz (además de las seis elegidas inicialmente), ninguno del tipo 2, dos del tipo 3, cuatro del tipo 4 y ninguno del tipo 5. Así, el número total de selecciones de 15 latas de refrescos de los cinco tipos, incluyendo al menos seis latas de cerveza de raíz, es el número de cadenas de 13 símbolos, 4 $(= 5 - 1)$ de $|$ y 9 de $\times$:

$$\binom{9+4}{9} = \binom{13}{9} = \frac{13 \cdot \cancel{12} \cdot 11 \cdot \overset{5}{\cancel{10}} \cdot \cancel{9!}}{\cancel{9!} \cdot \cancel{4} \cdot \cancel{3} \cdot \cancel{2} \cdot 1} = 715.$$

c. Si el almacén tiene sólo cinco latas de cerveza de raíz, el número de selecciones diferentes de 15 latas de refrescos de los cinco tipos es igual al número de selecciones diferentes que contienen cinco o menos latas de cerveza. Sea T el conjunto de selecciones para los que el tipo de latas de cerveza de raíz no está restringido, $R_{\leq 5}$ el conjunto de selecciones que contienen cinco o menos latas de cerveza de raíz y $R_{\geq 6}$ el conjunto de selecciones con seis o más latas de cerveza de raíz. Entonces

$$T = R_{\leq 5} \cup R_{\geq 6} \quad \text{y} \quad R_{\leq 5} \cap R_{\geq 6} = \emptyset.$$

Por el inciso *a*) $N(T) = 3\,876$ y por el inciso *b*) $N(R_{\geq 6}) = 715$. Así, por la regla de diferencia,

$$N(R_{\leq 5}) = N(T) - N(R_{\geq 6}) = 3\,876 - 715 = 3\,161.$$

Por lo que el número de selecciones diferentes de refrescos es 3 161. ■

Ejemplo 9.6.3 Conteo de ternas (i, j, k) con $1 \leq i \leq j \leq k \leq n$

Si n es un entero positivo, ¿cuántas ternas de enteros del 1 al n se pueden formar en las que los elementos de la terna están escritos en orden creciente, pero no son necesariamente distinto? En otras palabras, ¿cuántas ternas de enteros (i, j, k) existen con $1 \leq i \leq j \leq k \leq n$?

Solución Cualquier terna de enteros (i, j, k) con $1 \leq i \leq j \leq k \leq n$ se puede representar como una cadena de $n - 1$ barras verticales y tres cruces, con las posiciones de las cruces indicando que tres enteros del 1 al n se incluyen en la terna. La siguiente tabla muestra esto para $n = 5$.

Categoría 1	2	3	4	5	Resultado de la selección
|	|	$\times\times$	|	$\times$	(3, 3, 5)
$\times$ |	$\times$ |		| $\times$	|	(1, 2, 4)

Por tanto el número de estas ternas es igual al número de cadenas de $(n-1)$ | y 3 ×, que es

$$\binom{3+(n-1)}{3} = \binom{n+2}{3} = \frac{(n+2)!}{3!(n+2-3)!}$$
$$= \frac{(n+2)(n+1)n(n-1)!}{3!(n-1)!} = \frac{n(n+1)(n+2)}{6}. \quad \blacksquare$$

Observe que en los ejemplos 9.6.2 y 9.6.3 el razonamiento detrás del teorema 9.6.1 se utiliza en lugar del enunciado del teorema mismo. Alternativamente, en cada ejemplo que podríamos invocar el teorema 9.6.1 directamente al reconocer que los elementos a contar son r-combinaciones con repetición permitida o son el mismo número de dichas combinaciones. Por ejemplo, en el ejemplo 9.6.3 podríamos observar que hay exactamente tantas ternas de enteros (i, j, k) con $1 \le i \le j \le k \le n$ como hay 3-combinaciones de enteros del 1 al n con repetición porque los elementos de cualquier 3-combinación se pueden escribir en orden en sólo una forma creciente.

Ejemplo 9.6.4 Conteo de iteraciones de un bucle

¿Cuántas veces se repetirá el bucle interno cuando el segmento del algoritmo siguiente se implementa y ejecuta? (Suponga que n es un entero.)

```
for k := 1 to n
    for j := 1 to k
        for i := 1 to j
            [Enunciados en el cuerpo del bucle interior,
            ninguno contiene enunciados que ramifiquen
            fuera del bucle]
        next i
    next j
next k
```

Solución Se construye una tabla de seguimiento para las valores de k, j e i para que se ejecuten los enunciados en el cuerpo del bucle más interno. (Vea la tabla siguiente.) Ya que i va del 1 al 7, siempre es el caso de que $i \le j$. Del mismo modo, j va de 1 a k, siempre es el caso de que $j \le k$. Para centrarse en los detalles de la construcción de la tabla, veamos lo que ocurre cuando $k = 3$. En este caso, j toma cada valor 1, 2 y 3. Cuando $j = 1$, sólo puede tomar el valor 1 (porque $i \le j$). Cuando $j = 2$, i toma cada valor 1 y 2 (una vez más porque $i \le j$). Cuando $j = 3$ toma cada valor 1, 2 y 3 (una vez más porque $i \le j$).

k	1	2	→	→	3	→	→	→	→	→	⋯	n	→	→	→	→	→	→
j	1	1	2	→	1	2	→	3	→	→	⋯	1	2	→	⋯	n	→	→
i	1	1	1	2	1	1	2	1	2	3	⋯	1	1	2	⋯	1	⋯	n

Observe que existe una iteración del bucle interno para cada columna de la tabla y hay una columna de la tabla para cada terna de enteros (i, j, k) con $1 \le i \le j \le k \le n$. Pero el ejemplo 9.6.3 mostró que el número de esas ternas es $[n(n+1)(n+2)]/6$. Así hay $[n(n+1)(n+2)]/6$ iteraciones del bucle más interno. $\blacksquare$

La solución en el ejemplo 9.6.4 es la más elegante y generalizable. (Vea los ejercicios 8 y 9.) Una solución alternativa usando sumas se bosqueja en el ejercicio 21.

Ejemplo 9.6.5 El número de soluciones enteras de una ecuación

¿Cuántas soluciones existen para la ecuación $x_1 + x_2 + x_3 + x_4 = 10$ si x_1, x_2, x_3 y x_4 son enteros no negativos?

Solución Piense en el número 10 como dividido en diez unidades individuales y las variables, x_1, x_2, x_3 y x_4 como cuatro categorías en las que se colocan estas unidades. El número de unidades en cada categoría x_i indica los valores de x_i en una solución de la ecuación. Cada solución, puede representarse por una cadena de tres barras verticales (para separar las cuatro categorías) y diez cruces (para representar las diez unidades individuales). Por ejemplo, en la siguiente tabla, las dos cruces bajo x_1, cinco cruces bajo x_2 y tres cruces bajo x_4 representan la solución $x_1 = 2$, $x_2 = 5$, $x_3 = 0$ y $x_4 = 3$.

Categorías				Solución de la ecuación $x_1 + x_2 + x_3 + x_4 = 10$
x_1	x_2	x_3	x_4	
× × |	× × × × × |	|	× × ×	$x_1 = 2$, $x_2 = 5$, $x_3 = 0$, y $x_4 = 3$
× × × × |	× × × × × × |	|		$x_1 = 4$, $x_2 = 6$, $x_3 = 0$, y $x_4 = 0$

Por tanto, hay tantas soluciones a la ecuación como hay cadenas de diez cruces y tres barras verticales, es decir

$$\binom{10+3}{10} = \binom{13}{10} = \frac{13!}{10!(13-10)!} = \frac{13 \cdot 12 \cdot 11 \cdot \cancel{10!}}{\cancel{10!} \cdot 3 \cdot 2 \cdot 1} = 286.$$

■

El ejemplo 9.6.6 ilustra una variación del ejemplo 9.6.5.

Ejemplo 9.6.6 Restricciones adicionales en el número de soluciones

¿Cuántas soluciones enteras existen para la ecuación $x_1 + x_2 + x_3 + x_4 = 10$ si cada $x_i \geq 1$?

Solución En este caso imagine empezar a poner una cruz en cada una de las cuatro categorías. Después distribuya las restantes seis cruces entre las categorías. Esta distribución se puede representar por una cadena de tres barras verticales y seis cruces. Por ejemplo, la cadena

$$\times \times \times \mid \quad \mid \times \times \mid \times$$

indica que hay tres cruces más en la categoría x_1 además de la cruz que ya está (así $x_1 = 4$), no más cruces en la categoría x_2 además de la que ya está (así $x_2 = 1$), dos cruces más en la categoría x_3 además de la que ya está (así $x_3 = 3$) y una cruz más en la categoría x_4 además de la que ya está (así $x_4 = 2$). De lo que se deduce que el número de soluciones a la ecuación que cumplen la condición dada es igual que el número de cadenas de tres barras verticales y seis cruces, es decir

$$\binom{6+3}{6} = \binom{9}{6} = \frac{9!}{6!(9-6)!} = \frac{9 \cdot 8 \cdot 7 \cdot 6!}{6! \cdot 3 \cdot 2 \cdot 1} = 84.$$

Una solución alternativa para este ejemplo se basa en la observación de que ya que cada $x_i \geq 1$, podemos introducir nuevas variables $y_i = x_i - 1$ para cada $i = 1, 2, 3, 4$. Entonces cada $y_i \geq 0$ y $y_1 + y_2 + y_3 + y_4 = 6$. Por tanto el número de soluciones de $y_1 + y_2 + y_3 + y_4 = 6$ en enteros no negativos es igual que el número de soluciones de $x_1 + x_2 + x_3 + x_4 = 10$ en enteros positivos. ■

¿Qué fórmula usar?

Las secciones 9.2, 9.3, 9.5 y 9.6 han examinado cuatro formas diferentes de elegir k elementos de n. El orden en que se toman las decisiones puede o no puede importar y la repetición puede o no puede permitirse. La siguiente tabla resume qué fórmula se utiliza y en qué caso.

	Importa el orden	**No importa el orden**
Repetición permitida	n^k	$\binom{k+n-1}{k}$
Repetición no permitida	$P(n, k)$	$\binom{n}{k}$

Autoexamen

1. Dado un conjunto $X = \{x_1, x_2,\ldots,x_n\}$, una r-combinación con repetición permitida o un multiconjunto de tamaño r, elegido de X es _____, que se denota por _____.
2. Si $X = \{x_1, x_2,\ldots,x_n\}$, el número de r-combinaciones con repetición permitida (o multiconjuntos de tamaño r) elegido de X es _____.
3. Cuando se eligen k elementos de un conjunto de n elementos, el orden puede o no puede importar y la repetición puede o no puede permitirse.
   - El número de formas de elegir k elementos cuando se permite repetición y el orden importante es _____.
   - El número de formas de elegir k elementos cuando no se permite repetición y el orden importante es _____.
   - El número de formas de elegir k elementos cuando no se permite repetición y no importa el orden es _____.
   - El número de formas de elegir k elementos cuando se permite repetición y no importa el orden es _____.

Conjunto de ejercicios 9.6

1. a. De acuerdo con el teorema 9.6.1, ¿cuántas 5-combinaciones con repetición permitida se pueden elegir de un conjunto de tres elementos?
   b. Enumere todas las 5-combinaciones que se pueden elegir con repetición permitida de {1, 2, 3}.

2. **a.** De acuerdo con el teorema 9.6.1, ¿cuántos multiconjuntos de tamaño cuatro se pueden elegir de un conjunto de tres elementos?
   b. Enumere todos los multiconjuntos de tamaño cuatro que se pueden seleccionar del conjunto $\{x, y, z\}$.

3. Una panadería produce seis diferentes tipos de panes, una de los cuales es el choux. Supongamos que hay al menos 20 panes de cada tipo.
   a. ¿Cuántas diferentes selecciones de veinte panes existen?
   b. ¿Cuántas diferentes selecciones de veinte panes existen si al menos tres deben ser choux?
   c. ¿Cuántas diferentes selecciones de veinte panes contienen como máximo dos choux?

4. Una tienda de cámaras compra ocho diferentes tipos de baterías, uno de los cuales es de tipo A7b. Suponga que hay por lo menos 30 baterías de cada tipo.
   a. ¿De cuántas maneras puede un inventario total de 30 baterías distribuirse entre los ocho tipos diferentes?
   b. ¿De cuántas maneras puede un inventario total de 30 baterías distribuirse entre los ocho tipos diferentes si el inventario debe incluir por lo menos cuatro baterías A7b?
   c. ¿De cuántas maneras puede un inventario total de 30 baterías distribuirse entre los ocho tipos de diferentes si el inventario incluye como máximo tres baterías A7b?

5. ¿Si n es un entero positivo, ¿cuántas 4-tuplas de enteros del 1 al n se pueden formar en las que los elementos de la 4-tupla están escritos en orden creciente, pero no son necesariamente distintos? En otras palabras, ¿cuántas 4-tuplas de números enteros (i, j, k, m) existen con $1 \le i \le j \le k \le m \le n$?

6. Si n es un entero positivo, ¿cuántas 5-tuplas de enteros del 1 al n pueden formarse en el que se escriben los elementos de la 5-tupla en orden decreciente pero no son distintos necesariamente?, es decir, ¿cuántas 5-tuplas de enteros (h, i, j, k, m) existen con $n \le h \ge i \ge j \ge k \ge m \ge 1$?

7. Otra manera de contar el número de soluciones enteras no negativas de una ecuación de la forma $x_1 + x_2 + \cdots + x_n = m$ es reducir el problema de encontrar el número de n-tuplas $(y_1, y_2, \ldots, y_n)$ con $0 \le y_1 \le y_2 \le \cdots \le y_n \le m$. La reducción resulta al hacer $y_i = x_1 + x_2 + \cdots + x_i$ para cada $i = 1, 2, \ldots, n$. Use este método para obtener una fórmula general para el número de soluciones enteras no negativas a $x_1 + x_2 + \cdots + x_n = m$.

En los ejercicios 8 y 9, ¿cuántas veces se repetirá el bucle interno cuando se implementa y ejecuta el segmento de algoritmo? Suponga que n, m, k y j son enteros positivos.

8.
for $m := 1$ **to** n
  for $k := 1$ **to** m
    for $j := 1$ **to** k
      for $i := 1$ **to** j
        [*Enunciados en el interior del cuerpo del bucle, ninguno contiene ramificaciones que salgan del bucle*]
      next i
    next j
  next k
next m

9.
for $k := 1$ **to** n
  for $j := k$ **to** n
    for $i := j$ **to** n
      [*Enunciados en el interior del cuerpo del bucle, ninguno contiene ramificaciones que salgan del bucle*]
    next i
  next j
next k

En los ejercicios del 10 al 14, encuentre todas las soluciones simples que hay a la ecuación dada que satisfagan la condición dada.

10. $x_1 + x_2 + x_3 = 20$, cada x_i es un entero no negativo.

11. $x_1 + x_2 + x_3 = 20$, cada x_i es un entero positivo.

12. $y_1 + y_2 + y_3 + y_4 = 30$, cada y_i es un entero no negativo.

13. $y_1 + y_2 + y_3 + y_4 = 30$, cada y_i es un entero que es al menos 2.

14. $a + b + c + d + e = 500$, cada uno de a, b, c, d y e es un entero que es al menos 10.

✶ 15. ¿Cuántos números enteros entre 1 y 99 999 satisfacen que la suma de sus dígitos es igual a 10?

16. Considere la situación del ejemplo 9.6.2.
a. Suponga que la tienda tiene sólo seis latas de limonada, pero al menos hay 15 latas de cada una de los otros cuatro tipos de refresco. ¿En cuántas diferentes maneras se pueden seleccionar cinco latas de refresco?
b. Suponga que la tienda tiene sólo cinco latas de cerveza de raíz y sólo seis latas de limonada, pero al menos 15 latas de cada uno de los otros tres tipos de bebidas. ¿De cuántas diferentes maneras se pueden seleccionar cinco latas de refresco?

***H* 17.** a. Una tienda vende 8 tipos de globos con al menos 30 de cada tipo. ¿Cuántas combinaciones se pueden elegir con 30 globos?
b. Si la tienda tiene sólo 12 globos rojos pero al menos 30 de cada uno de otros tipos de globos, ¿cuántas combinaciones se pueden elegir de globos?
c. Si la tienda tiene sólo 8 globos azules pero al menos 30 de cada uno de otro tipo de globo, ¿cuántas combinaciones de globos se pueden elegir?
d. Si la tienda tiene sólo 12 globos rojos y sólo 8 azules pero al menos 30 de cada uno de otro tipo de globo, ¿cuántas combinaciones de globos se pueden elegir?

18. Un gran montón de monedas consiste en monedas de 5¢, de 10¢ y de 25¢.
a. ¿Cuántas diferentes colecciones de 30 monedas se pueden elegir si hay al menos 30 de cada tipo de moneda?
b. Si el montón contiene sólo 15 monedas de 25¢ pero al menos 30 de otro tipo, ¿cuántas colecciones de 30 monedas hay?
c. Si el montón contiene sólo 20 de 20¢ pero al menos 30 de cada uno de otro tipo de moneda, ¿cuántas colecciones de 30 monedas se pueden elegir?
d. Si el montón contiene sólo 15 monedas de 25¢ y sólo 20 de 20¢ pero al menos 30 de cada uno de otro tipo de moneda, ¿cuántas colecciones de 30 monedas se pueden elegir?

***H* 19.** Supongamos que la panadería del ejercicio 3 tiene sólo diez choux pero tiene al menos veinte de cada uno de los otros tipos de panes.
a. ¿Cuántas selecciones diferentes de veinte panes existen?
b. Supongamos que además tiene sólo diez choux, la panadería sólo tiene ocho rebanados de napoleón. ¿Cuántas diferentes selecciones de veinte panes existen?

20. Supongamos que la tienda de cámaras del ejercicio 4 puede obtener como máximo diez baterías A7b pero puede obtener al menos 30 de cada uno de los otros tipos.
a. ¿De cuántas maneras se puede distribuir un inventario total de 30 baterías entre los ocho tipos diferentes?
b. Supongamos que además de ser capaz de obtener sólo diez baterías A7b, la tienda sólo puede obtener seis del tipo D303. ¿De cuántas maneras se puede distribuir un inventario total de 30 baterías entre los ocho tipos diferentes?

21. Observe que el número de columnas en la tabla de seguimiento del ejemplo 9.6.4 se puede expresar como la suma de

$$1 + (1 + 2) + (1 + 2 + 3) + \cdots + (1 + 2 + \cdots + n).$$

Explique por qué esto es así y demuestre cómo se simplifica esta suma a la misma expresión de la solución del ejemplo 9.6.4. *Sugerencia:* Utilice la fórmula del ejercicio de la sección 5.2.

Respuestas del autoexamen

1. una selección no ordenada de elementos tomados de X con repetición permitida; $[x_{i_1}, x_{i_2}, \ldots, x_{i_r}]$ donde cada x_{i_j} está en X y algunas de las x_{i_j} pueden ser iguales a cada uno de los otros 2. $\binom{r+n-1}{r}$ 3. n^k; $n(n-1)(n-2)\cdots(n-k+1)$ $(Or: P(n,k))$; $\binom{n}{k}$; $\binom{k+n-1}{k}$

9.7 Fórmula de Pascal y el teorema del binomio

Conozco muy bien, también, en asuntos matemáticos, entiendo ecuaciones simples y cuadráticas. Acerca del teorema del binomio estoy formando un equipo con una gran cantidad de noticias, con muchos datos alegres acerca del cuadrado de la hipotenusa.
—William S. Gilbert, *Los piratas de Penzance*, 1880

En esta sección se deducen varias fórmulas para valores de $\binom{n}{r}$. Lo más importante es la fórmula de Pascal, que es la base del triángulo de Pascal y es un componente crucial de una de las demostraciones del teorema del binomio. Ofrecemos dos demostraciones distintas tanto para la fórmula de Pascal como para el teorema del binomio. Una de ellas se llama "algebraica" porque se basa en gran medida en el manejo algebraico y la otra se llama "por combinaciones", porque se basa en el tipo argumentos de conteo que hemos analizado en este capítulo.

Ejemplo 9.7.1 Valores de $\binom{n}{n}, \binom{n}{n-1}, \binom{n}{n-2}$

Piense en el teorema 9.5.1 como un modelo general: independientemente de qué número no negativo se coloca en los cuadros, si el número en el cuadro inferior es menor que el número en el cuadro superior, entonces

$$\binom{\square}{\diamondsuit} = \frac{\square!}{\diamondsuit!(\square - \diamondsuit)!}.$$

Use el teorema 9.5.1 para demostrar que para todos los enteros $n \geq 0$,

$$\binom{n}{n} = 1 \tag{9.7.1}$$

$$\binom{n}{n-1} = n, \quad \text{si } n \geq 1 \tag{9.7.2}$$

$$\binom{n}{n-2} = \frac{n(n-1)}{2}, \quad \text{si } n \geq 2. \tag{9.7.3}$$

Solución

$$\binom{n}{n} = \frac{n!}{n!(n-n)!} = \frac{1}{0!} = 1 \quad \text{ya que } 0! = 1 \text{ por definición}$$

$$\binom{n}{n-1} = \frac{n!}{(n-1)!(n-(n-1))!}$$

$$= \frac{n \cdot (n-1)!}{(n-1)!(n-n+1)!} = \frac{n}{1} = n$$

$$\binom{n}{n-2} = \frac{n!}{(n-2)!(n-(n-2))!}$$

$$= \frac{n \cdot (n-1(\cdot(n-2)!}{(n-2)!2!} = \frac{n(n-1)}{2}$$

■

Observe que el resultado deducido algebraicamente anteriormente, de que $\binom{n}{n}$ es igual a 1, está de acuerdo con el hecho de que un conjunto con n elementos tiene sólo un subconjunto de tamaño n, a saber el mismo. Del mismo modo, el ejercicio 1 al final de la sección pide que se demuestre algebraicamente que $\binom{n}{0} = 1$, que concuerda con el hecho de que un conjunto con n elementos tiene un subconjunto, el conjunto vacío, de tamaño 0. En el ejercicio 2 también deberá mostrar algebraicamente que $\binom{n}{1} = n$. Este resultado coincide con el hecho de que hay n subconjuntos de tamaño 1 que se pueden seleccionar de un conjunto con n elementos, a saber los subconjuntos compuestos sólo por cada elemento.

Ejemplo 9.7.2 $\binom{n}{r} = \binom{n}{n-r}$

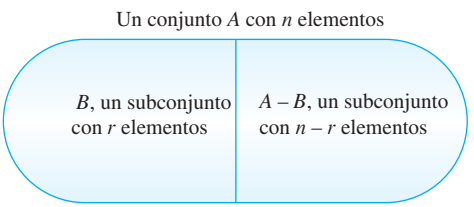
En el ejercicio 5 del final de la sección se le pedirá que compruebe algebraicamente que

$$\binom{n}{r} = \binom{n}{n-r}$$

para todos los enteros no negativos n y r con $r \leq n$.

Una forma alternativa de deducir esta fórmula es interpretarla diciendo que un conjunto A con n elementos tiene exactamente tantos subconjuntos de tamaño r como subconjuntos de tamaño $n - r$. Deduzca la fórmula usando este razonamiento.

Solución Observe que cualquier subconjunto de tamaño r se puede especificar ya sea diciendo que r elementos se encuentran en el subconjunto o diciendo que $n - r$ elementos se encuentran fuera del subconjunto.



Supongamos que A tiene subconjuntos k de tamaño r: $B_1, B_2, \ldots, B_k$. Entonces, cada B_i se puede emparejar con un conjunto de tamaño $n - r$, es decir con su complemento $A - B_i$ como se muestra a continuación.

$$\begin{array}{ccc} B_1 & \longleftrightarrow & A - B_1 \\ B_2 & \longleftrightarrow & A - B_2 \\ \vdots & & \vdots \\ B_k & \longleftrightarrow & A - B_k \end{array}$$

Todos los subconjuntos de tamaño r se enumeran en la columna de la izquierda y todos los subconjuntos de tamaño $n - r$ se enumeran en la columna de la derecha. El número de subconjuntos de tamaño r es igual al número de subconjuntos de tamaño $n - r$ y así $\binom{n}{r} = \binom{n}{n-r}$. ■

El tipo de razonamiento utilizado en este ejemplo se llama *combinaciones*, porque se obtiene contando cosas que se combinan de diferentes maneras. Un número de teoremas tiene demostraciones por combinaciones y demostraciones que son puramente algebraicas.

Fórmula de Pascal

Hulton-Deutch Collection/CORBIS

Blaise Pascal (1623-1662)

La fórmula de Pascal, nombrada así en honor del matemático y filósofo francés del siglo XVII, Blaise Pascal, es una de las más famosas y útiles en combinaciones (que es el término formal para el estudio del conteo y enumeración de problemas). Relaciona el valor de $\binom{n+1}{r}$ con los valores de $\binom{n}{r-1}$ y $\binom{n}{r}$. Específicamente, dice que

$$\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}$$

siempre que n y r son números enteros positivos con $r \leq n$. Esta fórmula es más fácil para calcular grandes combinaciones en función de menores: Si se conocen todos los valores de $\binom{n}{r}$ se conocen, entonces los valores de $\binom{n+1}{r}$ pueden calcularse para toda r tal que $0 < r \leq n$.

En la tabla 9.7.1 se muestra el triángulo de Pascal, es una versión geométrica de la fórmula de Pascal. A veces simplemente se llama el triángulo aritmético ya que fue utilizado siglos antes de Pascal por los matemáticos chinos y persas. Pero Pascal lo descubrió independientemente y desde 1654, cuando publicó un tratado que exploraba muchas de sus características, generalmente se ha conocido como el triángulo de Pascal.

Tabla 9.7.1 **Triángulo de Pascal para** $\left(\text{Valores de } \binom{n}{r}\right)$

n \ r	0	1	2	3	4	5	$\cdots$	$r-1$		r	$\cdots$
0	1										
1	1	1									
2	1	2	1								
3	1	3	3	1							
4	1	4	6	+ 4	1						
5	1	5	10	= 10	5	1					
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$		$\vdots$	$\vdots$
n	$\binom{n}{0}$	$\binom{n}{1}$	$\binom{n}{2}$	$\binom{n}{3}$	$\binom{n}{4}$	$\binom{n}{5}$	$\cdots$	$\binom{n}{r-1}$	+	$\binom{n}{r}$	$\cdots$
$n+1$	$\binom{n+1}{0}$	$\binom{n+1}{1}$	$\binom{n+1}{2}$	$\binom{n+1}{3}$	$\binom{n+1}{4}$	$\binom{n+1}{5}$	$\cdots$		=	$\binom{n+1}{r}$	$\cdots$
.											
.											
.											

Cada entrada en el triángulo es un valor de $\binom{n}{r}$. La fórmula de Pascal se traduce en el hecho de que la entrada en el renglón $n+1$, columna r es igual a la suma de la entrada en el renglón n, columna $r-1$ más la entrada en el renglón n, columna r. Es decir, la entrada en una determinada posición interior es igual a la suma de las dos entradas directamente arriba y arriba a la izquierda. Las entradas de los extremos izquierdo y derecho en cada renglón son 1 ya que $\binom{n}{n} = 1$ por el ejemplo 9.7.1 y $\binom{n}{0} = 1$ por el ejercicio 1 al final de esta sección.

Ejemplo 9.7.3 Cálculo de $\binom{n}{r}$ usando el triángulo de Pascal

Utilice el triángulo de Pascal para calcular los valores de

$$\binom{6}{2} \quad \text{y} \quad \binom{6}{3}.$$

Solución Por construcción, el valor en el renglón n, columna r del triángulo de Pascal es el valor de $\binom{n}{r}$, para cada par de números enteros positivos n y r con $r \leq n$. Por la fórmula de Pascal $\binom{n+1}{r}$ se puede calcular sumando $\binom{n}{r-1}$ y $\binom{n}{r}$, que se encuentra directamente arriba y arriba a la izquierda de $\binom{n+1}{r}$. Por tanto,

$$\binom{6}{2} = \binom{5}{1} + \binom{5}{2} = 5 + 10 = 15 \quad \text{y}$$

$$\binom{6}{3} = \binom{5}{2} + \binom{5}{3} = 10 + 10 = 20.$$

■

La fórmula de Pascal se puede obtener por dos argumentos completamente diferentes. Uno es algebraico; utiliza la fórmula para el número de combinaciones de r obtenidos en el teorema 9.5.1. El otro es usando combinaciones; utiliza la definición del número de r-combinaciones como el número de subconjuntos de tamaño r de un conjunto con un cierto número de elementos. Presentamos ambas demostraciones, ya que ambos enfoques tienen aplicaciones en muchas otras situaciones.

Teorema 9.7.1 Fórmula de Pascal

Sean n y r enteros positivos enteros y suponga que $r \leq n$. Entonces

$$\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r}.$$

Demostración (versión algebraica)

Sean n y r enteros positivos con $r \leq n$. Por el teorema 9.5.1,

$$\begin{aligned}\binom{n}{r-1} + \binom{n}{r} &= \frac{n!}{(r-1)!(n-(r-1))!} + \frac{n!}{r!(n-r)!} \\ &= \frac{n!}{(r-1)!(n-r+1)!} + \frac{n!}{r!(n-r)!}.\end{aligned}$$

Para sumar estas fracciones, se necesita un denominador común, así al multiplicar el numerador y el denominador de la fracción de la izquierda por r y multiplicar el numerador y el denominador de la fracción de la derecha por $(n-r+1)$. Entonces

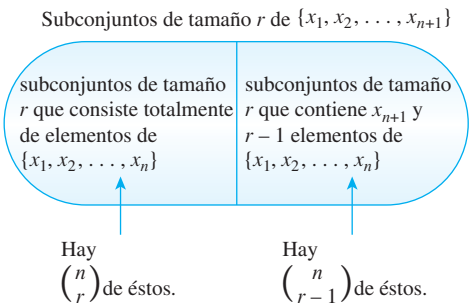
$$\begin{aligned}\binom{n}{r-1} + \binom{n}{r} &= \frac{n!}{(r-1)!(n-r+1)!}\cdot\frac{r}{r} + \frac{n!}{r!(n-r)!}\cdot\frac{(n-r+1)}{(n-r+1)} \\ &= \frac{n!\cdot r}{(n-r+1)!r(r-1)!} + \frac{n\cdot n! - n!\cdot r + n!}{(n-r+1)(n-r)!r!} \\ &= \frac{\cancel{n!\cdot r} + n!\cdot n - \cancel{n!\cdot r} + n!}{(n-r+1)!r!} = \frac{n!(n+1)}{(n+1-r)!r!} \\ &= \frac{(n+1)!}{((n+1)-r)!r!} = \binom{n+1}{r}.\end{aligned}$$

Demostración (versión usando combinaciones):

Sean n y r enteros positivos con $r \leq n$. Suponga que S es un conjunto con $n+1$ elementos. El número de subconjuntos de S de tamaño r puede calcularse pensando que S consiste de dos piezas: uno con n elementos $\{x_1, x_2, \ldots, x_n\}$ y el otro con un elemento $\{x_{n+1}\}$.

Cualquier subconjunto de S con r elementos contiene ya sea a x_{n+1} o no. Si contiene x_{n+1}, entonces contiene $r-1$ elementos del conjunto $\{x_1, x_2, \ldots, x_n\}$. Si no contiene a x_{n+1}, entonces contiene r elementos del conjunto $\{x_1, x_2, \ldots, x_n\}$.

continúa en la página 596



Por la regla de la adición,

$$\begin{bmatrix}\text{número de subconjuntos}\\ \text{de } \{x_1, x_2, \ldots, x_n, x_{n+1}\}\\ \text{de tamaño } r\end{bmatrix} = \begin{bmatrix}\text{número de subconjuntos}\\ \text{de } \{x_1, x_2, \ldots, x_n\}\\ \text{de tamaño } r-1\end{bmatrix} + \begin{bmatrix}\text{número de subconjuntos}\\ \text{de } \{x_1, x_2, \ldots, x_n\}\\ \text{de tamaño } r\end{bmatrix}.$$

Por el teorema 9.5.1, el conjunto $\{x_1, x_2, \ldots, x_n, x_{n+1}\}$ tiene $\binom{n+1}{r}$, subconjuntos de tamaño r, el conjunto $\{x_1, x_2, \ldots, x_n\}$ tiene $\binom{n}{r-1}$ subconjuntos de tamaño $r-1$ y el conjunto $\{x_1, x_2, \ldots, x_n\}$ tiene $\binom{n}{r}$ subconjuntos de tamaño r. Así

$$\binom{n+1}{r} = \binom{n}{r-1} + \binom{n}{r},$$

como se quería demostrar.

Ejemplo 9.7.4 Deducción de nuevas fórmulas a partir de la fórmula de Pascal

Utilice la fórmula de Pascal para deducir una fórmula para $\binom{n+2}{r}$ en función de los valores de $\binom{n}{r}$, $\binom{n}{r-1}$ y $\binom{n}{r-2}$. Suponga que n y r son enteros no negativos y $2 \le r \le n$.

Solución Por la fórmula de Pascal,

$$\binom{n+2}{r} = \binom{n+1}{r-1} + \binom{n+1}{r}.$$

Ahora aplicando la fórmula de Pascal a $\binom{n+1}{r-1}$ y $\binom{n+1}{r}$ y sustituyendo en la ecuación anterior se obtiene

$$\binom{n+2}{r} = \left[\binom{n}{r-2} + \binom{n}{r-1}\right] + \left[\binom{n}{r-1} + \binom{n}{r}\right].$$

La combinación de los dos términos de en medio da

$$\binom{n+2}{r} = \binom{n}{r-2} + 2\binom{n}{r-1} + \binom{n}{r}$$

para todos los enteros no negativos n y r tal que $2 \le r \le n$. ■

El teorema binomial

En álgebra una suma de dos términos, tal como $a + b$, se llama un **binomio**. El *teorema binomial* da una expresión para las potencias de binomio $(a + b)^n$, para cada entero positivo n y todos los números reales a y b.

Considere lo que ocurre al calcular las primeras pocas potencias de $a + b$. De acuerdo con la ley distributiva de álgebra, tomamos la suma de los productos de todas las combinaciones de términos individuales:

$$\begin{aligned}(a+b)^2 &= (a+b)(a+b) = aa + ab + ba + bb,\\ (a+b)^3 &= (a+b)(a+b)(a+b)\\ &= aaa + aab + aba + abb + baa + bab + bba + bbb,\\ (a+b)^4 &= \underbrace{(a+b)(a+b)(a+b)(a+b)}_{\substack{\text{primer}\\ \text{factor}}\ \ \substack{\text{segundo}\\ \text{factor}}\ \ \substack{\text{tercer}\\ \text{factor}}\ \ \substack{\text{cuarto}\\ \text{factor}}}\\ &= aaaa + aaab + aaba + aabb + abaa + abab + abba + abbb\\ &\quad + baaa + baab + baba + babb + bbaa + bbab + bbba + bbbb.\end{aligned}$$

Ahora nos dedicamos al desarrollo de $(a + b)^4$. (Es concreto y sin embargo, tiene todas las características del caso general.) Se obtiene una expresión típica de este desarrollo multiplicando uno de los dos términos del primer factor por uno de los dos términos del segundo factor por uno de los dos términos del tercer factor por uno de los dos términos del cuarto factor. Por ejemplo, el término *abab* se obtiene multiplicando la *a* y la *b* marcados con las flechas hacia abajo.

$$\begin{matrix}\downarrow & & \downarrow & \downarrow & & \downarrow\\ (a+b)(a+b)(a+b)(a+b)\end{matrix}$$

Ya que hay dos posibles valores: —*a* o *b*— para cada término seleccionado de uno de los cuatro factores, hay $2^4 = 16$ términos en el desarrollo de $(a + b)^4$.

Ahora algunos términos en el desarrollo son "términos semejantes" y se puede combinar. Considere por ejemplo, todos los ordenamientos posibles de tres *a* y una *b*. Por las técnicas de la sección 9.5, hay $\binom{4}{1} = 4$ de ellos. Y cada uno de los cuatro ocurre como un término en el desarrollo de $(a + b)^4$:

$$aaab \quad aaba \quad abaa \quad baaa.$$

Por las leyes asociativa y conmutativa de álgebra, cada término es igual a a^3b, por lo que todos los cuatro son "términos semejantes". Por tanto, cuando se combinan los términos semejantes, el coeficiente de a^3b es igual a $\binom{4}{1}$.

Similarmente, el desarrollo de $(a + b)^4$ contiene $\binom{4}{2} = 6$ diferentes ordenamientos de dos *a* y dos *b*,

$$aabb \quad abab \quad abba \quad baab \quad baba \quad bbaa.$$

todos los cuales son iguales a a^2b^2, por lo que el coeficiente de a^2b^2 es igual a $\binom{4}{2}$. Por un análisis similar, el coeficiente de ab^3 es igual $\binom{4}{3}$. También, puesto que hay sólo una forma de ordenar cuatro *a*, el coeficiente de a^4 es 1 (lo que equivale a $\binom{4}{0}$ y ya hay sólo una forma de ordenar cuatro *b*, el coeficiente de b^4 es 1 (que es igual a $\binom{4}{4}$). Por tanto, cuando se combinan todos los términos semejantes,

$$\begin{aligned}(a+b)^4 &= \binom{4}{0}a^4 + \binom{4}{1}a^3b + \binom{4}{2}a^2b^2 + \binom{4}{3}ab^3 + \binom{4}{4}b^4\\ &= a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4.\end{aligned}$$

El teorema binomial generaliza esta fórmula para un entero arbitrario *n* no negativo.

Teorema 9.7.2 Teorema binomial

Dados cualesquiera números reales a y b y cualquier entero no negativo n,

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^k$$
$$= a^n + \binom{n}{1} a^{n-1}b^1 + \binom{n}{2} a^{n-2}b^2 + \cdots + \binom{n}{n-1} a^1 b^{n-1} + b^n.$$

Observe que la segunda expresión es igual a la primera porque $\binom{n}{0} = 1$ y $\binom{n}{n} = 1$, para todos los enteros n no negativos, siempre que $b^0 = 1$ y $a^{n-n} = 1$.

Es instructivo ver dos demostraciones del teorema binomial: una demostración algebraica y una demostración usando combinaciones. Ambos requieren una definición precisa de la potencia entera.

• Definición

Para cualquier número real a y cualquier entero no negativo n, las **potencias enteras no negativas de *a*** se definen como sigue:

$$a^n = \begin{cases} 1 & \text{si } n = 0 \\ a \cdot a^{n-1} & \text{si } n > 0 \end{cases}$$

Nota Esta es la definición de 0^0 dada por Donald E. Knuth en *The Art of Computer Programing, Volume 1: Fundamental Algorithms*, tercera edición (Reading, Mass: Addison-Wesley, 1997), p. 57.

En algunos contextos matemáticos, 0^0 se deja sin definir. Definirlo igual a 1, como se hace aquí, hace posible escribir fórmulas generales tales como $\sum_{i=0}^{n} x^i = \frac{1}{1-x}$ sin tener que excluir los valores de las variables que resultan de la expresión 0^0.

La versión algebraica del teorema binomial utiliza inducción matemática y llama a la fórmula de Pascal en un momento crucial.

Demostración del teorema binomial (versión algebraica):

Suponga que a y b son números reales. Utilizamos inducción matemática y hacemos que la propiedad $P(n)$ sea la ecuación

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^k. \qquad \leftarrow P(n)$$

Demuestre que P(0) es verdadera: Cuando $n = 0$, el teorema binomial indica que:

$$(a+b)^0 = \sum_{k=0}^{0} \binom{0}{k} a^{0-k}b^k. \qquad \leftarrow P(0)$$

Pero el lado izquierdo es $(a+b)^0 = 1$ *[por definición de poder]* y el lado derecho es

$$\sum_{k=0}^{0} \binom{0}{k} a^{0-k}b^k = \binom{0}{0} a^{0-0}b^0$$
$$= \frac{0!}{0! \cdot (0-0)!} \cdot 1 \cdot 1 = \frac{1}{1 \cdot 1} = 1$$

también *[ya que* $0! = 1$, $a^0 = 1$ *y* $b^0 = 1$*]*. Por tanto $P(0)$ es verdadera.

Demuestre que para todos los enteros $m \geq 0$, si $P(m)$ es verdadera, entonces $P(m+1)$ es verdadera: Sea un entero $m \geq 0$ dado y suponiendo que $P(m)$ es verdadera. Es decir, supongamos

$$(a+b)^m = \sum_{k=0}^{m} \binom{m}{k} a^{m-k} b^k. \qquad P(m) \text{ hipótesis inductiva.}$$

Tenemos que demostrar que $P(m+1)$ es verdadera:

$$(a+b)^{m+1} = \sum_{k=0}^{m+1} \binom{m+1}{k} a^{(m+1)-k} b^k. \qquad P(m+1)$$

Ahora, por la definición $(m+1)$-ésima potencia,

$$(a+b)^{m+1} = (a+b) \cdot (a+b)^m,$$

por sustitución de la hipótesis inductiva,

$$\begin{aligned}(a+b)^{m+1} &= (a+b) \cdot \sum_{k=0}^{m} \binom{m}{k} a^{m-k} b^k \\ &= a \cdot \sum_{k=0}^{m} \binom{m}{k} a^{m-k} b^k + b \cdot \sum_{k=0}^{m} \binom{m}{k} a^{m-k} b^k \\ &= \sum_{k=0}^{m} \binom{m}{k} a^{m+1-k} b^k + \sum_{k=0}^{m} \binom{m}{k} a^{m-k} b^{k+1}\end{aligned}$$

por la ley distributiva generalizada y los hechos de que $a \cdot a^{m-k} = a^{1+m-k} = a^{m+1-k}$ y $b \cdot b^k = b^{1+k} = b^{k+1}$.

Transformamos la segunda suma de la derecha al realizar el cambio de variable $j = k+1$. Cuando $k = 0$, entonces $j = 1$. Cuando $k = m$, entonces $j = m+1$. Y puesto que $k = j-1$, el término general es

$$\binom{m}{k} a^{m-k} b^{k+1} = \binom{m}{j-1} a^{m-(j-1)} b^j = \binom{m}{j-1} a^{m+1-j} b^j.$$

Por tanto la segunda suma en el lado derecho arriba es

$$\sum_{j=1}^{m+1} \binom{m}{j-1} a^{m+1-j} b^j.$$

Pero la j en esta suma es una variable muda; se puede reemplazar por la letra k, siempre que el reemplazo se realiza en todo lugar donde se encuentra la j:

$$\sum_{j=1}^{m+1} \binom{m}{j-1} a^{m+1-j} b^j = \sum_{k=1}^{m+1} \binom{m}{k-1} a^{m+1-k} b^k.$$

Sustituyendo hacia atrás, se obtiene

$$(a+b)^{m+1} = \sum_{k=0}^{m} \binom{m}{k} a^{m+1-k} b^k + \sum_{k=1}^{m+1} \binom{m}{k-1} a^{m+1-k} b^k.$$

[La razón para las manipulaciones anteriores de formar las potencias de a y b de acuerdo con lo que podemos agregar a las sumas juntas término por término, excepto para el primer y el último términos que deben escribirse por separado.]

continúa en la página 600

Así

$$(a+b)^{m+1} = \binom{m}{0} a^{m+1-0}b^0 + \sum_{k=1}^{m}\left[\binom{m}{k} + \binom{m}{k-1}\right] a^{m+1-k}b^k + \binom{m}{(m+1)-1} a^{m+1-(m+1)}b^{m+1}$$

$$= a^{m+1} + \sum_{k=1}^{m}\left[\binom{m}{k} + \binom{m}{k-1}\right] a^{m+1-k}b^k + b^{m+1}$$

ya que $a^0 = b^0 = 1$ y $\binom{m}{0} = \binom{m}{m} = 1$.

Pero

$$\left[\binom{m}{k} + \binom{m}{k-1}\right] = \binom{m+1}{k}$$ Por la fórmula de Pascal.

Por tanto

$$(a \Downarrow b)^{m\Downarrow 1} = a^{m+1} + \sum_{k=1}^{m}\binom{m+1}{k} a^{(m+1)-k}b^k + b^{m+1}$$

$$= \sum_{k=0}^{m+1}\binom{m+1}{k} a^{(m+1)-k}b^k$$ ya que $\binom{m+1}{0} = \binom{m+1}{m+1} = 1$

que es lo que necesitábamos demostrar.

Es instructivo escribir el producto $(a+b)\cdot(a+b)^m$ sin utilizar la notación de suma pero utilizando la hipótesis inductiva acerca de $(a+b)^{\mathrm{m}}$:

$$(a+b)^{m+1} = (a+b)\cdot\left[a^m + \binom{m}{1}a^{m-1}b + \cdots + \binom{m}{k-1}a^{m-(k-1)}b^{k-1} + \binom{m}{k}a^{m-k}b^k + \cdots + \binom{m}{m-1}ab^{m-1} + b^m\right].$$

Observe que el primer y último coeficientes son obviamente 1 y que el término que contiene $a^{m+1-k}b^k$ se obtiene multiplicando $a^{m-k}b^k$ por a y $a^{m+(\mathrm{k}-1)}b^{k-1}$ por b, [*ya que* $m+1-k = m-(k-1)$]. Por tanto el coeficiente de $a^{m+1-\,k}b^k$ es igual a la suma de $\binom{m}{k}$ y $\binom{m}{k-1}$. Este es el punto crucial de la demostración algebraica.

Si n y r son enteros no negativos y $r \le n$, entonces $\binom{n}{r}$ se llama un **coeficiente binomial** porque es uno de los coeficientes en el desarrollo de la expresión binomial $(a+b)^n$.

La demostración por combinaciones del teorema binomial es la siguiente.

Demostración del teorema binomial (versión por combinaciones):

[El argumento por combinaciones utilizado aquí para demostrar el teorema binomial funciona sólo para $n \ge 1$. Si se nos diera sólo esta demostración por combinaciones, se tendría que demostrar por separado el caso para $n = 0$. Ya hemos dado una demostración algebraica completa que incluye el caso $n = 0$, no lo demostraremos una vez más aquí.]

Sean a y b números reales y n un entero que es al menos 1. La expresión $(a+b)^n$ puede ampliarse en productos de n letras, donde cada letra es ya sea a o b.

Para cada $k = 0, 1, 2, \ldots, n$, el producto

$$a^{n-k}b^k = \underbrace{a \cdot a \cdot a \cdots a}_{n-k \text{ factores}} \cdot \underbrace{b \cdot b \cdot b \cdots b}_{k \text{ factores}}$$

se presenta como un término en la suma el mismo número de veces como ordenamientos hay de $(n - k)$ a y k b. Pero este número es $\binom{n}{k}$, el número de formas de elegir k posiciones en el que desea colocar las b *[Las otras $n - k$ posiciones serán llenas por a.]* Por tanto, cuando se combinan los términos, el coeficiente de $a^{n-k}b^k$ en la suma es $\binom{n}{k}$. Por tanto

$$(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k}b^k.$$

Esto es lo que se iba a demostrar.

Ejemplo 9.7.5 Sustituyendo en el teorema binomial

Desarrolle las siguientes expresiones utilizando el teorema binomial:

a. $(a + b)^5$ b. $(x - 4y)^4$

Solución

a. $$\begin{aligned}(a + b)^5 &= \sum_{k=0}^{5} \binom{5}{k} a^{5-k}b^k \\ &= a^5 + \binom{5}{1} a^{5-1}b^1 + \binom{5}{2} a^{5-2}b^2 + \binom{5}{3} a^{5-3}b^3 + \binom{5}{4} a^{5-4}b^4 + b^5 \\ &= a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5\end{aligned}$$

b. Observe que $(x - 4y)^4 = (x + (4y))^4$. Así sea $a = x$ y $b = (-4y)$ y sustituya en el teorema binomial.

$$\begin{aligned}(x - 4y)^4 &= \sum_{k=0}^{4} \binom{4}{k} x^{4-k}(-4y)^k \\ &= x^4 + \binom{4}{1} x^{4-1}(-4y)^1 + \binom{4}{2} x^{4-2}(-4y)^2 + \binom{4}{3} x^{4-3}(-4y)^3 + (-4y)^4 \\ &= x^4 + 4x^3(-4y) + 6x^2(16y^2) + 4x^1(-64y^3) + (256y^4) \\ &= x^4 - 16x^3y + 96x^2y^2 - 256xy^3 + 256y^4\end{aligned}$$

■

Ejemplo 9.7.6 Deducción de otra identidad por combinaciones del teorema binomial

Use el teorema binomial para demostrar que

$$2^n = \sum_{k=0}^{n} \binom{n}{k} = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n}$$

para todo entero $n \geq 0$.

Solución Ya que $2 = 1 + 1$, $2^n = (1 + 1)^n$. Aplique el teorema binomial a esta expresión haciendo $a = 1$ y $b = 1$. Entonces

$$2^n = \sum_{k=0}^{n} \binom{n}{k} \cdot 1^{n-k} \cdot 1^k = \sum_{k=0}^{n} \binom{n}{k} \cdot 1 \cdot 1$$

ya que $1^{n-k} = 1$ y $1^k = 1$. Por tanto

$$2^n = \sum_{k=0}^{n} \binom{n}{k} = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n}.$$

■

Ejemplo 9.7.7 Uso de un argumento por combinaciones para deducir la identidad

De acuerdo con el teorema 6.3.1, un conjunto con n elementos tiene 2^n subconjuntos. Aplique este hecho para dar un argumento por combinaciones para justificar la identidad

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \binom{n}{3} + \cdots + \binom{n}{n} = 2^n.$$

Solución Suponga que S es un conjunto con n elementos. Entonces cada subconjunto de S tiene algún número de elementos k, donde k está entre 0 y n. Se deduce que el número total de subconjuntos de S, $N(\mathscr{P}(S))$, se puede expresar como la suma siguiente:

$$\begin{bmatrix}\text{número de}\\ \text{subconjuntos}\\ \text{de } S\end{bmatrix} = \begin{bmatrix}\text{número de}\\ \text{subconjuntos}\\ \text{de tamaño 0}\end{bmatrix} + \begin{bmatrix}\text{número de}\\ \text{subconjuntos}\\ \text{de tamaño 1,}\end{bmatrix} + \cdots + \begin{bmatrix}\text{número de}\\ \text{subconjuntos}\\ \text{de tamaño } n\end{bmatrix}.$$

Ahora el número de subconjuntos de tamaño k de un conjunto es $\binom{n}{k}$. Por tanto el

$$\text{número de subconjuntos de } S = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n}$$

Pero por el teorema del binomio 6.3.1, S tiene 2^n subconjuntos. Por tanto

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \binom{n}{3} + \cdots + \binom{n}{n} = 2^n.$$

■

Ejemplo 9.7.8 Uso del teorema del binomio para simplificar una suma

Exprese la siguiente suma en **forma cerrada** (sin utilizar un símbolo de suma y usando puntos suspensivos …):

$$\sum_{k=0}^{n} \binom{n}{k} 9^k$$

Solución Cuando el número 1 se eleva a cualquier potencia, el resultado sigue siendo 1. Por tanto

$$\begin{aligned}\sum_{k=0}^{n} \binom{n}{k} 9^k &= \sum_{k=0}^{n} \binom{n}{k} 1^{n-k} 9^k \\ &= (1+9)^n \quad \text{por el teorema binomial con } a = 1 \text{ y } b = 9 \\ &= 10^n.\end{aligned}$$

■

Autoexamen

1. Si n y r son enteros no negativos con $r \leq n$, entonces la relación entre $\binom{n}{r}$ y $\binom{n}{n-r}$ es _____.
2. La fórmula de Pascal dice que si n y r son enteros positivos con $r \leq n$, entonces _____.
3. El punto crucial de la demostración algebraica de la fórmula de Pascal es sumar dos fracciones que necesita expresarlas con un _____.
4. El punto crucial de la demostración por combinaciones de la fórmula de Pascal es que el conjunto de subconjuntos de tamaño r de un conjunto $\{x_1, x_2, \ldots, x_{n+1}\}$ se puede particionar en el conjunto de subconjuntos de tamaño r que contienen _____ y los que _____.
5. El teorema binomial dice que cualesquiera números reales a y b y cualquier entero no negativo n, _____.
6. El punto crucial de la demostración algebraica del teorema binomial es que, después de hacer un cambio de variable para

que dos sumas tengan los mismos límites superior e inferior y los exponentes de a y b son iguales, utilice el hecho de que $\binom{m}{k} + \binom{m}{k-1} =$ _____.

7. El punto crucial de la demostración por combinaciones del teorema del binomio es que el número de formas de arreglar k b y $(n-k)$ a en orden es _____.

Conjunto de ejercicios 9.7

En los ejercicios del 1 al 4 utilice el teorema 9.5.1 para calcular los valores de las cantidades indicadas. (Suponga que n es un entero.)

1. $\binom{n}{0}$, para $n \geq 0$

2. $\binom{n}{1}$, para $n \geq 1$

3. $\binom{n}{2}$, para $n \geq 2$

4. $\binom{n}{3}$, para $n \geq 3$

5. Utilice el teorema 9.5.1 para demostrar algebraicamente que $\binom{n}{r} = \binom{n}{n-r}$, para los enteros n y r con $0 \leq r \leq n$. (Esto se puede hacer con cálculo directo; no es necesario utilizar inducción matemática.)

Justifique las ecuaciones en los ejercicios del 6 al 9 ya sea deduciendo a partir de las fórmulas del ejemplo 9.7.1 o por cálculo directo del teorema 9.5.1. Suponga que m, n, k y r son enteros.

6. $\binom{m+k}{m+k-1} = m+k$, para $m+k \geq 1$

7. $\binom{n+3}{n+1} = \dfrac{(n+3)(n+2)}{2}$, para $n \geq -1$

8. $\binom{k-r}{k-r} = 1$, para $k-r \geq 0$

9. $\binom{2n}{n}$ para $n \geq 0$

10. a. Utilice el triángulo de Pascal indicado en la tabla 9.7.1 para calcular los valores de $\binom{6}{2}$, $\binom{6}{3}$, $\binom{6}{4}$ y $\binom{6}{5}$.

b. Utilice el resultado del inciso *a*) y la fórmula de Pascal para calcular $\binom{7}{3}$, $\binom{7}{4}$ y $\binom{7}{5}$.

c. Complete el renglón del triángulo de Pascal que corresponde a $n = 7$.

11. El renglón del triángulo de Pascal que corresponde a $n = 8$ es el siguiente:

1 8 28 56 70 56 28 8 1.

¿Cuál es el renglón que corresponde a $n = 9$?

12. Use la fórmula de Pascal repetidamente para deducir una fórmula para $\binom{n+3}{r}$ en términos de valores de $\binom{n}{k}$ con $k \leq r$. (Suponga que n y r son enteros con $n \geq r \geq 3$.)

13. Utilice la fórmula de Pascal para demostrar por inducción matemática que si n es un número entero y $n \geq 1$, entonces,

$$\sum_{i=2}^{n+1} \binom{i}{2} = \binom{2}{2} + \binom{3}{2} + \cdots + \binom{n+1}{2} = \binom{n+2}{3}.$$

***H* 14.** Demuestre que si n es un entero y $n \geq 1$, entonces

$$1 \cdot 2 + 2 \cdot 3 + \cdots + n(n+1) = 2\binom{n+2}{3}.$$

15. Demuestre la siguiente generalización del ejercicio 13: Sea r un entero no negativo fijo. Para todos los enteros n con $n \geq r$,

$$\sum_{i=r}^{n} \binom{i}{r} = \binom{n+1}{r+1}.$$

16. Piense en un conjunto con $m+n$ elementos como compuesto de dos partes, una con m elementos y la otra con n elementos. Dé un argumento usando combinaciones para demostrar que

$$\binom{m+n}{r} = \binom{m}{0}\binom{n}{r} + \binom{m}{1}\binom{n}{r-1} + \cdots + \binom{m}{r}\binom{n}{0},$$

donde m y n son enteros y r es un entero que es menor o igual tanto a m como n.

Esta identidad da lugar a muchas útiles identidades adicionales que implican las cantidades, $\binom{n}{k}$. Ya que Alexander Vandermonde publicó un importante artículo al respecto en 1772, generalmente llamado la *convolución de Vandermonde*. Sin embargo, era conocida al menos en el siglo XIV en China por Chu Shih-chieh.

***H* 17.** Demuestre que para todos los enteros $n \geq 0$,

$$\binom{n}{0}^2 + \binom{n}{1}^2 + \cdots + \binom{n}{n}^2 = \binom{2n}{n}.$$

18. Sea m cualquier número entero no negativo. Use inducción matemática y la fórmula de Pascal para demostrar que para todos los enteros $n \geq 0$,

$$\binom{m}{0} + \binom{m+1}{1} + \cdots + \binom{m+n}{n} = \binom{m+n+1}{n}.$$

Utilice el teorema binomial para desarrollar las expresiones en los ejercicios del 19 al 27.

19. $(1+x)^7$ **20.** $(p+q)^6$ **21.** $(1-x)^6$

22. $(u-v)^5$ **23.** $(p-2q)^4$ **24.** $(u^2-3v)^4$

25. $\left(x+\dfrac{1}{x}\right)^5$ **26.** $\left(\dfrac{3}{a}-\dfrac{a}{3}\right)^5$ **27.** $\left(x^2+\dfrac{1}{x}\right)^5$

28. En el ejemplo 9.7.5 se demostró que

$$(a+b)^5 = a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5.$$

Evalúe $(a+b)^6$ sustituyendo la expresión anterior en la ecuación

$$(a+b)^6 = (a+b)(a+b)^5$$

después multiplique y reúna términos semejantes.

En los ejercicios del 29 al 34, encuentre el coeficiente del término dado cuando la expresión se desarrolla con el teorema binomial.

29. x^6y^3 en $(x+y)^9$

30. x^7 en $(2x+3)^{10}$

31. a^5b^7 en $(a-2b)^{12}$

32. $u^{16}v^4$ en $(u^2-v^2)^{10}$

33. $p^{16}q^7$ en $(3p^2-2q)^{15}$

34. x^9y^{10} en $(2x-3y^2)^{14}$

35. Como en la demostración del teorema binomial, transforme la suma

$$\sum_{k=0}^{n}\binom{m}{k}a^{m-k}b^{k+1}$$

haciendo el cambio de variable $j=k+1$.

Use el teorema binomial para demostrar cada enunciado en los ejercicios del 36 al 41.

36. Para todos enteros $n \geq 1$,

$$\binom{n}{0}-\binom{n}{1}+\binom{n}{2}-\cdots+(-1)^n\binom{n}{n}=0.$$

(*Sugerencia:* Use el hecho de que $1+(-1)=0$.)

***H* 37.** Para todos los enteros $n \geq 0$,

$$3^n=\binom{n}{0}+2\binom{n}{1}+2^2\binom{n}{2}+\cdots+2^n\binom{n}{n}.$$

38. Para todos los enteros $m \geq 0$, $\displaystyle\sum_{i=0}^{m}(-1)^i\binom{m}{i}2^{m-i}=1$.

39. Para todos los enteros $n \geq 0$, $\displaystyle\sum_{i=0}^{n}(-1)^i\binom{n}{i}3^{n-i}=2^n$.

40. Para todos los enteros $n \geq 0$ y para todos los números reales no negativos x, $1+nx \leq (1+x)^n$.

***H* 41.** Para todos los enteros $n \geq 1$,

$$\binom{n}{0}-\frac{1}{2}\binom{n}{1}+\frac{1}{2^2}\binom{n}{2}-\frac{1}{2^3}\binom{n}{3}+\cdots+(-1)^{n-1}\frac{1}{2^{n-1}}\binom{n}{n-1}=\begin{cases}0 & \text{si } n \text{ es par}\\ \dfrac{1}{2^{n-1}} & \text{si } n \text{ es impar}\end{cases}.$$

42. Utilice inducción matemática para demostrar que para todos los enteros $n \geq 1$, si S es un conjunto con n elementos, entonces S tiene el mismo número de subconjuntos que un número par de elementos que con un número impar de elementos. Use este hecho para dar un argumento por combinaciones para justificar la identidad del ejercicio 36.

Exprese cada una de las sumas en los ejercicios del 43 al 54 en forma cerrada (sin utilizar un símbolo de suma y sin utilizar puntos suspensivos …).

43. $\displaystyle\sum_{k=0}^{n}\binom{n}{k}5^k$

44. $\displaystyle\sum_{i=0}^{m}\binom{m}{i}4^i$

45. $\displaystyle\sum_{i=0}^{n}\binom{n}{i}x^i$

46. $\displaystyle\sum_{k=0}^{m}\binom{m}{k}2^{m-k}x^k$

47. $\displaystyle\sum_{j=0}^{2n}(-1)^j\binom{2n}{j}x^j$

48. $\displaystyle\sum_{r=0}^{n}\binom{n}{r}x^{2r}$

49. $\displaystyle\sum_{i=0}^{m}\binom{m}{i}p^{m-i}q^{2i}$

50. $\displaystyle\sum_{k=0}^{n}\binom{n}{k}\frac{1}{2^k}$

51. $\displaystyle\sum_{i=0}^{m}(-1)^i\binom{m}{i}\frac{1}{2^i}$

52. $\displaystyle\sum_{k=0}^{n}\binom{n}{k}3^{2n-2k}2^{2k}$

53. $\displaystyle\sum_{i=0}^{n}(-1)^i\binom{n}{i}5^{n-i}2^i$

54. $\displaystyle\sum_{k=0}^{n}(-1)^k\binom{n}{k}3^{2n-2k}2^{2k}$

✶ 55. (Para estudiantes que hayan cursado cálculo)

a. Explique cómo se deduce la ecuación siguiente del teorema binomial:

$$(1+x)^n=\sum_{k=0}^{n}\binom{n}{k}x^k.$$

b. Escriba la fórmula que se obtiene al tomar la derivada de ambos lados de la ecuación del inciso *a*) con respecto a x.

c. Utilice el resultado del inciso *b*) para deducir las fórmulas siguientes.

i) $\displaystyle 2^{n-1}=\frac{1}{n}\left[\binom{n}{1}+2\binom{n}{2}+3\binom{n}{3}+\cdots+n\binom{n}{n}\right]$

ii) $\displaystyle\sum_{k=1}^{n}k\binom{n}{k}(-1)^k=0$

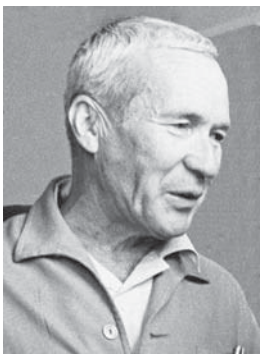
d. Exprese $\displaystyle\sum_{k=1}^{n}k\binom{n}{k}3^k$ en forma cerrada (sin utilizar un signo de suma o puntos suspensivos).

Respuestas del autoexamen

1. $\binom{n}{r}=\binom{n}{n-r}$ 2. $\binom{n+1}{r}=\binom{n}{r-1}+\binom{n}{r}$ 3. común denominador 4. x_{n+1}; no contiene x_{n+1}
5. $(a+b)^n=\displaystyle\sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k$ 6. $\binom{m+1}{k}$ 7. $\binom{n}{k}$

9.8 Axiomas de probabilidad y valor esperado

La teoría de la probabilidad es al final nada pero el sentido común se reduce a un cálculo.
—Pierre-Simon Laplace (1749-1827)



Yevgeny Khaldei/CORBIS

Andrei Nikolaevich Kolmogorov (1903-1987)

Hasta este momento, se han calculado probabilidades sólo para situaciones, tales como el lanzamiento justo de una moneda o tirar un par de dados equilibrados, donde todos los resultados en el espacio muestral son equiprobables. Pero las monedas no siempre son justas y los dados no están siempre balanceados. ¿Cómo es posible calcular las probabilidades para estas situaciones más generales?

Los axiomas siguientes fueron formulados por A. N. Kolmogorov en 1933 para proporcionar una base teórica para una teoría de probabilidad de largo alcance. En esta sección, establecemos los axiomas, para deducir algunas consecuencias e introducir el concepto de valor esperado.

Recuerde que un espacio muestral es un conjunto de todos los resultados de un proceso aleatorio o experimento y que un evento es un subconjunto de un espacio muestral.

Axiomas de probabilidad

Sea S un espacio muestral, una **función de probabilidad** P del conjunto de todos los eventos en S al conjunto de números reales que satisface los tres axiomas siguientes: Para todos los eventos A y B en S,

1. $0 \leq P(A) \leq 1$
2. $P(\emptyset) = 0$ y $P(S) = 1$
3. Si A y B son disjuntos (es decir, si $A \cap B = \emptyset$), entonces la probabilidad de la unión de A y B es
$$P(A \cup B) = P(A) + P(B).$$

Ejemplo 9.8.1 Aplicación de los axiomas de probabilidad

Suponga que A y B son eventos en un espacio muestral S. Si A y B son disjuntos, ¿podrían ser $P(A) = 0.6$ y $P(B) = 0.8$?

Solución No. El número de axioma de probabilidad 3 implicaría que $P(A \cup B) = P(A) + P(B) = 0.6 + 0.8 = 1.4$ y ya que $1.4 > 1$, este resultado violaría el axioma de probabilidad 1. ■

Ejemplo 9.8.2 La probabilidad del complemento de un evento

Suponga que A es un evento en un espacio muestral S. Deduzca que $P(A^c) = 1 - P(A)$.

Solución Por el teorema 6.2.2(5), con S jugando el papel del conjunto universal U,
$$A \cap A^c = \emptyset \quad \text{y} \quad A \cup A^c = S.$$
Así S es la unión disjunta de A y A^c y así
$$P(A \cup A^c) = P(A) + P(A^c) = P(S) = 1.$$
Restando $P(A)$ de ambos lados se obtiene el resultado $P(A^c) = 1 - P(A)$. ■

Probabilidad del complemento de un evento

Si A es cualquier evento en un espacio muestral S, entonces
$$P(A^c) = 1 - P(A). \qquad 9.8.1$$

Es importante comprobar que los axiomas de probabilidad de Kolmogorov son coherentes con los resultados obtenidos usando la fórmula de probabilidad de eventos equiprobables. Para ver que éste es el caso, sea S un espacio muestral finito con resultados a_1, a_2, a_3, …, a_n. Está claro que todos los conjuntos singleton $\{a_1\}$, $\{a_2\}$, $\{a_3\}$,…, $\{a_n\}$ son mutuamente disjuntos y su unión es S. Ya que $P(S) = 1$, el axioma de probabilidad 3 se puede aplicar varias veces (vea el ejercicio 13 al final de esta sección) para obtener

$$P(\{a_1\} \cup \{a_2\} \cup \{a_3\} \cup \cdots \cup \{a_n\}) = \sum_{k=1}^{n} P(\{a_k\}) = 1.$$

Si, además, todos los resultados son equiprobables, hay un número positivo real c tal que

$$P(\{a_1\}) = P(\{a_2\}) = P(\{a_3\}) = \cdots = P(\{a_n\}) = c.$$

Por tanto

$$1 = \sum_{k=1}^{n} c = \underbrace{c + c + \cdots + c}_{n \text{ términos}} = nc,$$

y así

$$c = \frac{1}{n}.$$

Por lo que si A es cualquier evento con resultados $a_{i_1}, a_{i_2}, a_{i_3}, \ldots, a_{i_m}$, entonces

$$P(A) = \sum_{k=1}^{m} P(\{a_{i_k}\}) = \sum_{k=1}^{m} \frac{1}{n} = \frac{m}{n} = \frac{N(A)}{N(S)},$$

que es el resultado dado por la fórmula de probabilidad de eventos equiprobables.

Ejemplo 9.8.3 La probabilidad de una unión general de dos eventos

Siga los pasos descritos en los incisos *a*) y *b*) que se indican a continuación para demostrar la fórmula siguiente:

Probabilidad de una unión general de dos eventos

Si S es cualquier espacio muestral y A y B son los eventos en S, entonces

$$P(A \cup B) = P(A) + P(B) - P(A \cap B). \qquad 9.8.2$$

En ambos pasos, suponga que A y B son los eventos en un espacio muestral S.

a. Demuestre que $A \cup B$ es una unión disjunta de los siguientes conjuntos: $A - (A \cap B)$, $B - (A \cap B)$ y $A \cap B$.

b. En el ejercicio 12 del final de la sección, deberá demostrar que para cualesquiera eventos U y V en un espacio muestral S, si $U \subseteq V$ entonces $P(V - U) = P(V) - P(U)$. Utilice este resultado y el resultado del inciso *a*) para terminar la demostración de la fórmula.

Solución

a. Consulte la figura 9.8.1 de la siguiente página para leer la siguiente explicación. Elementos en el conjunto $A - (A \cap B)$ se encuentran en la región sombreada azul, los elementos en $B - (A \cap B)$ están en la región sombreada gris y elementos en $A \cap B$ están en la región blanca.

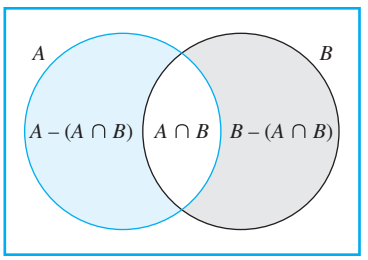


Figura 9.8.1

Parte 1: Demuestre que $A \cup B \subseteq (A - (A \cap B)) \cup (B - (A \cap B)) \cup (A \cap B)$***:*** Dado cualquier elemento x en $A \cup B$, x satisface exactamente una de las tres condiciones siguientes:

$$1)\ x \in A \text{ y } x \in B$$

$$2)\ x \in A \text{ y } x \notin B$$

$$3)\ x \in B \text{ y } x \notin A$$

1. En el primer caso, $x \in A \cap B$ y así $x \in (A - (A \cap B)) \cup (B - (A \cap B)) \cup (A \cap B)$ por definición de unión.
2. En el segundo caso, $x \notin A \cap B$ (ya que $x \notin B$) y así $x \in A - (A \cap B)$. Por tanto $x \in (A - (A \cap B)) \cup (B - (A \cap B)) \cup (A \cap B)$ por definición de unión.
3. En el tercer caso, $x \notin A \cap B$ (ya que $x \notin A$) y por tanto $x \in B - (A \cap B)$. Así una vez más, $x \in (A - (A \cap B)) \cup (B - (A \cap B)) \cup (A \cap B)$ por definición de unión.

Por tanto, en los tres casos, $x \in (A - (A \cap B)) \cup (B - (A \cap B)) \cup (A \cap B)$, con lo que termina la demostración de la parte 1.

Además, dado que las tres condiciones son mutuamente excluyentes, los tres conjuntos $A - (A \cap B)$ y $B - (A \cap B)$ y $A \cap B$ son mutuamente disjuntos.

Parte 2: Demuestre que $(A - (A \cap B)) \cup (B - (A \cap B)) \cup (A \cap B) \subseteq A \cup B$***:*** Suponga que x es cualquier elemento en $(A - (A \cap B)) \cup (B - (A \cap B)) \cup (A \cap B)$. Por definición de unión, $x \in A - (A \cap B)$ o $x \in B - (A \cap B)$ o $x \in A \cup B$.

1. En el caso de que $x \in A - (A \cap B)$, entonces $x \in A$ y $x \notin A \cup B$ por definición de diferencia de conjuntos. En particular, $x \in A$ y así $x \in A \cup B$.
2. En el caso $x \in B - (A \cap B)$, entonces $x \in B$ y $x \notin A \cap B$ por definición de diferencia de conjuntos. En particular, $x \in B$ y así $x \in A \cup B$.
3. En el caso $x \in A \cap B$, entonces en particular, $x \in A$ y así $x \in A \cup B$.

Por tanto, en los tres casos, $x \in A \cup B$, que completa la demostración de la parte 2.

b. $P(A \cup B) = P((A - (A \cap B)) \cup (B - (A \cap B)) \cup (A \cap B))$ por la parte *a*)

$= P(A - (A \cap B)) + P(B - (A \cap B)) + P(A \cap B)$

por el ejercicio 13 del final de la sección y el hecho de que $A - (A \cap B)$, $B - (A \cap B)$ y $A \cap B$ son mutuamente disjuntos

$= P(A) - P(A \cap B) + P(B) - P(A \cap B) + P(A \cap B)$

por el ejercicio 12 del final de la sección ya que $A \cap B \subseteq A$ y $A \cap B \subseteq B$

$= P(A) + P(B) - P(A \cap B)$ por álgebra. ■

Ejemplo 9.8.4 Cálculo de la probabilidad de una unión general de dos eventos

Suponga que aleatoriamente se elige una carta de una baraja ordinaria de 52 cartas (vea la sección 9.1). ¿Cuál es la probabilidad de que la carta sea con una cara (sota, rey o reina) o una de color rojo (corazones o diamantes)?

Solución Sea A el evento de que la elegida sea una carta de cara y sea B el caso de que la carta elegida sea una de color rojo. El evento de que la carta es una carta de cara o es una de color rojo es $A \cup B$. Ahora $N(A) = 4 \cdot 3 = 12$ (ya que cada uno de los cuatro palos tiene tres cartas) y así $P(A) = 12/52$. También $N(B) = 26$ (porque la mitad de las cartas son de color rojo) y así $P(B) = 26/52$. Por último, $N(A \cap B) = 6$ (porque hay tres cartas de cara de corazones y otras tres de diamantes) y así $P(A \cap B) = 6/52$. Por lo que se deduce de la fórmula para la probabilidad de una unión de dos eventos que

$$P(A \cup B) = P(A) + P(B) - P(A \cap B) = \frac{12}{52} + \frac{26}{52} - \frac{6}{52} = \frac{32}{52} \cong 61.5\%.$$

Por tanto la probabilidad de que la carta elegida es una carta de cara o es una de color rojo es aproximadamente 61.5%. ■

Valor esperado

Las personas que compran billetes de lotería regularmente con frecuencia justifican la práctica diciendo que, a pesar de que saben que en promedio perderán dinero, tienen la esperanza de una ganancia significativa, tras lo cual creen que dejarán de jugar. Lamentablemente, cuando las personas han perdido dinero en una cadena de perder billetes de lotería ganan algo de lo mucho que han perdido, por lo general deciden probar suerte en lugar de dejar de jugar.

La forma técnica de decir que en promedio una persona pierde dinero en la lotería es decir que el valor esperado de jugar a la lotería es negativo.

• Definición

Suponga que los posibles resultados de un experimento o proceso aleatorio, son los números $a_1, a_2, a_3, \ldots, a_n$, que se producen con probabilidades $p_1, p_2, p_3, \ldots, p_n$. El **valor esperado** del proceso es

$$\sum_{k=1}^{n} a_k p_k = a_1 p_1 + a_2 p_2 + a_3 p_3 + \cdots + a_n p_n.$$

Ejemplo 9.8.5 Valor esperado de de una lotería

Suponga que 500 000 personas pagan 5 dólares cada uno para jugar una partida de lotería con los siguientes premios: un premio de $1 000 000, 10 segundos premios de $1 000 cada uno, 1 000 terceros premios de $500 cada uno y 10 000 cuartos premios de $10 cada uno. ¿Cuál es el valor esperado de un billete?

Solución Cada uno de los 500 000 billetes de lotería tiene la misma oportunidad que cualquier otro de tener el número ganador de la lotería y así $p_k = \frac{1}{500000}$ para toda $k = 1, 2, 3, \ldots, 500\,000$. Sea $a_1, a_2, a_3, \ldots, a_{500000}$ la ganancia neta de un billete individual, donde $a_1 = 999\,995$ (la ganancia neta para el billete del gran premio, que es de un millón de dólares menos el costo de $5 del billete ganador), $a_2 = a_3 = \cdots = a_{11} = 995$ (la ganancia neta para cada uno de los 10 billetes del segundo premio), $a_{12} = a_{13} \cdots = a_{1011} = 495$ (la ganancia neta para cada uno de los 1 000 boletos del tercer premio) y $a_{1012} = a_{1013} = \cdots = a_{11011} = 5$ (la ganancia neta para cada uno de los 10 000 boletos del cuarto premio). Ya que los restantes 488 989 boletos exactamente pierden sólo $5, $a_{11012} = a_{11013} = \cdots = a_{500000} = -5$.

Por tanto, el valor esperado de un boleto es

$$\begin{aligned}\sum_{k=1}^{500000} a_k p_k &= \sum_{k=1}^{500000} \left(a_k \cdot \frac{1}{500\,000}\right) && \text{ya que cada } p_k = 1/500\,000\\ &= \frac{1}{500\,000} \sum_{k=1}^{500000} a_k && \text{por el teorema 5.1.1(2)}\\ &= \frac{1}{500\,000}\,(999\,995 + 10 \cdot 995 + 1\,000 \cdot 495 + 10\,000 \cdot 5 + (-5) \,.\, 488\,989)\\ &= \frac{1}{500\,000}\,(999\,995 + 9\,950 + 495\,000 + 50\,000 - 2\,444\,945)\\ &= -1.78.\end{aligned}$$

En otras palabras, una persona que continua jugando esta lotería por mucho tiempo probablemente ganará dinero en ocasiones pero en promedio perderá \$1.78 por billete. ■

Ejemplo 9.8.6 Ruina de un jugador

Un jugador apuesta repetidamente \$1 que cuando se avienta una moneda saldrá una cara. Cada vez que la moneda es cara, el jugador gana \$1; cada vez que sale cruz, pierde \$1. El jugador dejará de jugar ya sea cuando él esté arruinado (pierde todo su dinero) o cuando tenga $\$M$ (donde M es un número positivo que ha decidido de antemano). Sea P_n la probabilidad que el jugador esté arruinado si empieza a jugar con $\$n$. Entonces si la moneda es justa (tiene la misma posibilidad de salir cara o cruz),

$$P_{k-1} = \frac{1}{2}P_k + \frac{1}{2}P_{k-2} \quad \text{para cada entero } k \text{ con } \ 2 \le k \le M.$$

(Esto se deduce del hecho de que si el jugador tiene $\$(k-1)$, entonces tiene la misma oportunidad de ganar \$1 o perder \$1 y si gana \$1, entonces su oportunidad de arruinarse es P_k, mientras que si pierde \$1, entonces su oportunidad de arruinarse es P_{k-2}.) También $P_0 = 1$ (porque si tiene \$0, él está seguro de arruinarse) y $P_M = 0$ (porque una vez que tiene $\$M$, se sale y ya no hay ninguna posibilidad de arruinarse). Encuentre una fórmula explícita para P_n. ¿Cómo debe el jugador elegir m para minimizar su oportunidad de arruinarse?

Solución Multiplicando ambos lados de $P_{k-1} = \frac{1}{2}P_k + \frac{1}{2}P_{k-2}$ por 2 y restando P_{k-2} de ambos lados se obtiene

$$P_k = 2P_{k-1} - P_{k-2}.$$

Esta es una relación de recurrencia homogénea de segundo orden con coeficientes constantes. Ya que $P_k - 2P_{k-1} + P_{k-2} = 0$ su ecuación característica es

$$t^2 - 2t + 1 = 0,$$

que tiene la única raíz $r = 1$. Así, por el teorema de una sola-raíz de la sección 5.8,

$$P_n = Cr^n + Dnr^n = C + D_n$$

(ya que $r = 1$), donde C y D se determinan por dos valores de la sucesión. Pero $P_0 = 1$ y $P_M = 0$. Por tanto

$$1 = P_0 = C + D \cdot 0 = C,$$
$$0 = P_M = C + DM = 1 + DM.$$

De lo que se deduce que $C = 1$ y $D = -\frac{1}{M}$ y así

$$P_n = 1 - \frac{1}{M}n = \frac{M-n}{M} \quad \text{para cada entero } n \text{ con } 0 \le n < M.$$

Por ejemplo, un jugador que empieza con \$20 y se decide salir si su total alcanza los \$100 o si se arruina tiene la siguiente oportunidad de arruinarse:

$$P_{20} = \frac{100 - 20}{100} = \frac{80}{100} = 80\%.$$

Observe que entre mayor sea M con respecto a n, más cercano está P_n de 1. En otras palabras, cuanto mayor sea la cantidad de dinero que el jugador establece a sí mismo como destino, lo más probable es que se arruine. Por el contrario, entre más modesto sea su objetivo, más probable es llegar a él. ■

Autoexamen

1. Si A es un evento en un espacio muestral S, $P(A)$ puede tomar valores entre _____ y _____. Además, $P(S) =$ _____ y $P(\emptyset) =$ _____.
2. Si A y B son eventos disjuntos en un espacio muestral S, $P(A \cup B) =$ _____.
3. Si A es un evento en un espacio muestral S, $P(A^c) =$ _____.
4. Si A y B son los eventos cualesquiera en un espacio muestral S, $P(A \cup B) =$ _____.
5. Si los posibles resultados de un proceso aleatorio o experimento son números reales $a_1, a_2, \ldots, a_n$, que ocurren con probabilidades $p_1, p_2, \ldots, p_n$, entonces el valor esperado del proceso es _____.

Conjunto de ejercicios 9.8

1. En cualquier espacio muestral S, ¿qué es P($\emptyset$)?

2. Suponga que A, B y C son eventos mutuamente excluyentes en un espacio muestral S, $A \cup B \cup C =$ S y A y B tienen probabilidades 0.3 y 0.5, respectivamente.
a. ¿Qué es $P(A \cup$ B)? b. ¿Qué es $P(C)$?

3. Supongamos que A y B son eventos mutuamente excluyentes en un espacio muestral S, C es otro evento en S, $A \cup B \cup C = S$ y A y B tienen probabilidades 0.4 y 0.2, respectivamente.
a. ¿Qué es $P(A \cup B)$?
b. ¿Es posible que $P(C) = 0.2$? Explique.

4. Suponga que A y B son eventos en un espacio muestral S con probabilidades 0.8 y 0.7, respectivamente. Suponga también que $P(A \cap B) = 0.6$. ¿Qué es $P(A \cup B)$?

5. Suponga que A y B son eventos en un espacio muestral S y suponga que $P(A) = 0.6$, $P(B^c) = 0.4$, $P(A \cap B) = 0.2$. ¿Qué es $P(A \cup B)$?

6. Suponga que U y V son eventos en un espacio muestral S y suponga que $P(U^c) = 0.3$, $P(V) = 0.6$ y $P(U^c \cup V^c) = 0.4$. ¿Qué es $P(U \cup V)$?

7. Suponga que un espacio muestral S consiste de tres resultados: 0, 1 y 2. Sea $A = \{0\}$, $B = \{1\}$ y $C = \{2\}$ y suponga que $P(A) = 0.4$ y $P(B) = 0.3$. Encuentre cada una de las siguientes probabilidades:
a. $P(A \cup B)$ b. $P(C)$ c. $P(A \cup C)$
d. $P(A^c)$ e. $P(A^c \cap B^c)$ f. $P(A^c \cup B^c)$

8. Rehaga el ejercicio 7 suponiendo que $P(A) = 0.5$ y $P(B) = 0.4$.

9. Sean A y B eventos en un espacio muestral S y sea $C = S - (A \cup B)$. Suponga que $P(A) = 0.4$, $P(B) = 0.5$ y $P(A \cap B) = 0.2$. Encuentre cada una de las siguientes probabilidades:
a. $P(A \cup B)$ b. $P(C)$ c. $P(A^c)$
d. $P(A^c \cap B^c)$ e. $P(A^c \cup B^c)$ f. $P(B^c \cap C)$

10. Rehaga el ejercicio 9 suponiendo que $P(A) = 0.7$, $P(B) = 0.3$ y $P(A \cap B) = 0.1$.

H 11. Demuestre que si S es cualquier espacio muestral y U y V son eventos en S con $U \subseteq V$, entonces $P(U) \leq P(V)$.

H 12. Demuestre que si S es cualquier espacio muestral y U y V son eventos en S, entonces $P(V - U) = P(V) - P(U \cap V)$.

H 13. Utilice los axiomas de inducción matemática de probabilidad y demuestre que para todos los enteros $n \geq 2$, si $A_1, A_2, A_3, \ldots, A_n$ son eventos cualesquiera mutuamente disjuntos en un espacio muestral S, entonces

$$P(A_1 \cup A_2 \cup A_3 \cup \cdots \cup A_n) = \sum_{k=1}^{n} P(A_k).$$

14. Un juego de lotería ofrece 2 millones de dólares para el ganador del gran premio, 20 dólares a cada uno de los 10 000 ganadores del segundo premio y 4 dólares a cada uno de los 50 000 ganadores del tercer premio. El costo de la lotería es de 2 dólares por boleto. Supongamos que se venden 1.5 millones de boletos. ¿Cuál es la ganancia o pérdida esperada de un billete?

15. Una empresa envía a millones de personas un formulario de entrada de un sorteo acompañado de un formulario de pedido para las suscripciones de la revista. El primero, segundo y tercer premios son \$10 000 000, \$1 000 000 y \$50 000 dólares, respectivamente. Para calificar para un premio, una persona no necesita ordenar alguna revista pero tiene que gastar 60 centavos para regresar por correo la forma de entrada. ¿Si califican 30 millones de personas enviando de regreso sus formularios de entrada, ¿Cuál es la pérdida o ganancia que las personas esperan?

16. Una urna contiene cuatro bolas numeradas 2, 2, 5 y 6. Si una persona selecciona aleatoriamente un conjunto de dos bolas, ¿cuál es el valor esperado de la suma de los números de las bolas?

17. Una urna contiene cinco bolas numeradas 1, 2, 2, 8 y 8. Si una persona selecciona aleatoriamente un conjunto de dos bolas, ¿cuál es el valor esperado de la suma de los números de las bolas?

18. Una urna contiene cinco bolas numeradas 1, 2, 2, 8 y 8. Si una persona selecciona aleatoriamente un conjunto de tres bolas, ¿cuál es el valor esperado de la suma de los números de las bolas?

19. Cuando se tira un par de dados balanceados y se calcula la suma de los números que muestran la cara hacia arriba, el resultado puede ser cualquier número entre 2 y 12, incluso. ¿Cuál es el valor esperado de la suma?

***H* 20.** Suponga que una persona le invita a jugar un juego con usted. En este juego, cuando saca una carta de una baraja estándar de 52 cartas, si la carta es de cara gana \$3 y si la carta es cualquier otra cosa pierde \$1. Si está de acuerdo jugar, ¿cuál es la ganancia o pérdida esperada?

21. Una persona paga \$1 para realizar el juego siguiente: la persona lanza una moneda justa cuatro veces. Si no se salen caras, la persona paga \$2 más, si sale una cara, la persona paga \$1 más, si salen dos caras, la persona sólo pierde el dólar inicial, si salen tres caras, la persona gana \$3 y si salen cuatro caras, la persona gana \$4. ¿Cuál es la ganancia o pérdida que la persona espera?

***H* 22.** Se lanza una moneda justa hasta que salen cuatro caras o cuatro cruces. ¿Cuál es el número esperado de lanzamientos?

***H* 23.** Un jugador apuesta repetidamente que tirará un dado y caerá un 6. Cada vez que cae 6, el jugador gana \$1; cada vez que sucede lo contrario, el jugador pierde \$1. Deja de jugar cuando se arruina o cuando gana \$300. Si P_n es la probabilidad de que el jugador se arruine cuando empieza a jugar con \$$n$, entonces $P_{k-1} = \frac{1}{6}P_k + \frac{5}{6}P_{k-2}$ para todo entero k con $2 \leq k \leq 300$. También $P_0 = 1$ y $P_{300} = 0$. Encuentre una fórmula explícita para P_n y utilícela para calcular P_{20}. (En el ejercicio 33 de la sección 9.9 se le pide que deduzca la relación de recurrencia.)

Respuestas del autoexamen

1. 0; 1; 1; 0 2. $P(A) + P(B)$ 3. $1 - P(A)$ 4. $P(A) + P(B) - P(A \cap B)$ 5. $a_1p_1 + a_2p_2 + \cdots + a_np_n$

9.9 Probabilidad condicional, fórmula de Bayes y eventos independientes

Es notable que una ciencia que comenzó con la consideración de juegos de azar fuera el más importante objeto de conocimiento humano…. La mayoría de las cuestiones más importantes de la vida realmente son sólo problemas de probabilidad.
—Pierre-Simon Laplace 1749-1827

En esta sección presentamos el concepto de probabilidad condicional y se analiza el teorema de Bayes y la clase de interesantes resultados a los que conduce. Después se define el concepto de eventos independientes y se presentan algunas aplicaciones.

Probabilidad condicional

Imagine una pareja con dos hijos, cada uno de los cuales es equiprobable que sea un niño o una niña. Ahora suponga que se le da la información de que un hijo es un niño. ¿Cuál es la probabilidad de que el otro hijo sea un niño?

La figura 9.9.1 muestra las cuatro combinaciones equiprobables de género para los niños. Se puede imaginar que la primera letra se refiere al hijo más grande y la segunda

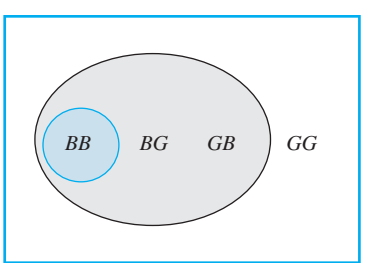


Figura 9.9.1

letra al más pequeño. Así, la combinación *BG* indica que el hijo mayor es niño y la más pequeña es niña.

Las combinaciones donde uno de los hijos es niño están sombreadas de gris y la combinación donde el otro hijo también es un niño está sombreada de azul-gris. Dado que usted sabe que uno de los hijos es un niño, podría ser el caso de que hubiera sólo tres combinaciones en la región gris, por lo que se puede considerar al conjunto de los resultados como un nuevo espacio muestral con tres elementos, que son equiprobables. En el nuevo espacio muestral, hay una combinación donde el otro hijo es un niño (en la región sombreada azul-gris). Por lo que es razonable decir que la probabilidad de que el otro hijo es un niño, dado que al menos uno es un niño, es $1/3 = 33\frac{1}{3}\%$. Observe que el espacio muestral original contenía también cuatro resultados.

$$\frac{P(\text{al menos un hijo es un niño y el otro hijo también es un niño})}{P(\text{al menos un hijo es un niño})} = \frac{\frac{1}{4}}{\frac{3}{4}} = \frac{1}{3}$$

también. Una generalización de esta observación constituye la base para la siguiente definición.

• Definición

Sean A y B eventos en un espacio muestral S. Si $P(A) \neq 0$, entonces la **probabilidad condicional de B dado A**, que se denota por $P(B \mid A)$, es

$$P(B \mid A) = \frac{P(A \cap B)}{P(A)}. \qquad 9.9.1$$

Ejemplo 9.9.1 Cálculo de una probabilidad condicional

Se tiran un par de dados justos, uno azul y el otro gris. ¿Cuál es la probabilidad de que la suma de los números que se presentan es 8, dado que los números son pares?

Solución El espacio muestral es el conjunto de todos los resultados de 36 obtenido cuando se tiran los dos dados y se observan los números que presentan cada uno. Como en la sección 9.1, se denota por *ab* el resultado de que el número que presenta el dado azul es que *a* y el dado gris es *b*. Sea A el evento de que ambos números son pares y B el evento de que la suma de los números es 8. Entonces $A = \{22, 24, 26, 42, 44, 46, 62, 64, 66\}$, $B = \{26, 35, 44, 53, 62\}$ y $A \cap B = \{26, 44, 62\}$. Ya que los dados son justos (todos los resultados son equiprobables), $P(A) = 9/36$, $P(B) = 5/36$ y $P(A \cap B) = 3/36$. Por definición de probabilidad condicional,

$$P(B \mid A) = \frac{P(A \cap B)}{P(A)} = \frac{\frac{3}{36}}{\frac{9}{36}} = \frac{3}{9} = \frac{1}{3}. \quad \blacksquare$$

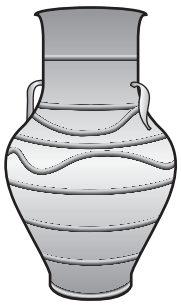
Observe que cuando ambos lados de la fórmula de probabilidad condicional (fórmula 9.9.1) se multiplican por $P(A)$, se obtiene una fórmula para $P(A \cap B)$:

$$P(A \cap B) = P(B \mid A) \cdot P(A). \qquad 9.9.2$$

Dividiendo ambos lados de la fórmula (9.9.2) por $P(B \mid A)$ se obtiene una fórmula para $P(A)$:

$$P(A) = \frac{P(A \cap B)}{P(B \mid A)}. \qquad 9.9.3$$

Ejemplo 9.9.2 Representación de probabilidades condicionales con un diagrama de árbol



Una urna contiene 5 bolas azules y 7 bolas grises. Digamos que se eligen aleatoriamente 2, una tras otra, sin reemplazo.

a. Determine las siguientes probabilidades e ilústrelas con un diagrama de árbol: la probabilidad de que dos bolas sean de color azul, la probabilidad de que la primera bola sea azul y la segunda no sea azul, la probabilidad de que la primera bola no sea azul y la segunda bola sea azul y la probabilidad de que ninguna bola sea azul.

b. ¿Cuál es la probabilidad de que la segunda bola sea azul?

c. ¿Cuál es la probabilidad de que al menos una de las bolas sea azul?

d. Si el experimento de elegir dos bolas de la urna se repite muchas veces más, ¿cuál sería el valor esperado del número de bolas azules?

Solución Sea que S denote el espacio muestral de todas las opciones posibles de dos bolas de la urna, sea B_1 el evento que la primera bola es azul y sea B_2 el evento de que la segunda bola sea azul. Entonces B_1^c es el evento que la primera bola no es azul y B_2^c es el evento que la segunda bola no sea azul.

a. Ya que hay 12 bolas de las cuales 5 son azules y 7 son grises, la probabilidad de que la primera bola sea azul es

$$P(B_1) = \frac{5}{12}$$

y la probabilidad de que la primera bola no sea azul es

$$P(B_1^c) = \frac{7}{12}.$$

Si la primera bola es azul, entonces la urna contendría 4 bolas azules y 7 bolas grises y por tanto

$$P(B_2 \mid B_1) = \frac{1}{11} \quad \text{y} \quad P(B_2^c \mid B_1) = \frac{7}{11}.$$

donde $P(B_2 \mid B_1)$ es la probabilidad de que la segunda bola sea azul, ya que la primera bola es azul y $P(B_2^c \mid B_1)$ es la probabilidad de que la segunda bola no sea azul, ya que la primera bola es azul. De la fórmula (9.9.2) se deduce que

$$P(B_1 \cap B_2) = P(B_2 \mid B_1) \cdot P(B_1) = \frac{4}{11} \cdot \frac{5}{12} = \frac{20}{132}$$

y

$$P(B_1 \cap B_2^c) = P(B_2^c \mid B_1) \cdot P(B_1) = \frac{7}{11} \cdot \frac{5}{12} = \frac{35}{132}.$$

Del mismo modo, si la primera bola no es azul, entonces la urna contendría 5 bolas azules y 6 bolas grises y así

$$P(B_2 \mid B_1^c) = \frac{5}{11} \quad \text{y} \quad P(B_2^c \mid B_1^c) = \frac{6}{11},$$

donde $P(B_2 \mid B_1^c)$ es la probabilidad de que la segunda bola sea azul, dado que la primera bola no es azul y $P(B_2^c \mid B_1^c)$ es la probabilidad de que la segunda bola no sea azul, dado que la primera bola no es azul. De la fórmula (9.9.2) se tiene que

$$P(B_1^c \cap B_2) = P(B_2 \mid B_1^c) \cdot P(B_1^c) = \frac{5}{11} \cdot \frac{7}{12} = \frac{35}{132}$$

y

$$P(B_1^c \cap B_2^c) = P(B_2^c \mid B_1^c) \cdot P(B_1^c) = \frac{6}{11} \cdot \frac{7}{12} = \frac{42}{132}.$$

El diagrama de árbol en la figura 9.9.2 es una forma conveniente para ayudar a calcular estos resultados.

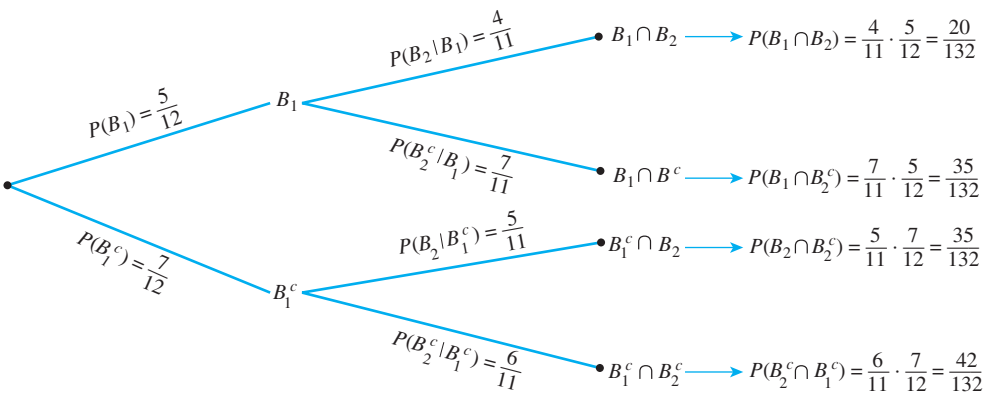


Figura 9.9.2

b. El evento que la segunda bola sea azul puede producirse de dos maneras mutuamente excluyentes: la primera bola es azul y la segunda también es azul, o la primera bola es gris y la segunda es azul. En otras palabras, B_2 es la unión disjunta de $B_2 \cap B_1$ y $B_2 \cap B_1^c$. Por tanto

$$\begin{aligned} P(B_2) &= P\left((B_2 \cap B_1) \cup \left(B_2 \cap B_1^c\right)\right) \\ &= P(B_2 \cap B_1) + P\left(B_2 \cap B_1^c\right) && \text{por el axioma de probabilidad 3} \\ &= \frac{20}{132} + \frac{35}{132} && \text{por el inciso } a) \\ &= \frac{55}{132} = \frac{5}{12}. \end{aligned}$$

Por tanto la probabilidad de que la segunda bola sea azul es 5/12, la misma probabilidad de que la primera bola sea azul.

c. Por la fórmula 9.8.2, para la unión de dos eventos cualesquiera,

$$\begin{aligned} P(B_1 \cup B_2) &= P(B_1) + P(B_2) - P(B_1 \cap B_2) \\ &= \frac{5}{12} + \frac{5}{12} - \frac{20}{132} && \text{por los incisos } a) \text{ y } b). \\ &= \frac{90}{132} = \frac{15}{22}. \end{aligned}$$

Por tanto la probabilidad es 15/22 o aproximadamente 68.2%, de que al menos una de las bolas sea azul.

d. El evento que ninguna bola sea azul es el complemento del evento, de que al menos una de las bolas es azul, así

$$\begin{aligned} P(0 \text{ bolas azules}) &= 1 - P(\text{al menos una de las bolas es azul}) && \text{por la fórmula 9.8.1} \\ &= 1 - \frac{15}{22} && \text{por el inciso } c) \\ &= \frac{7}{22}. \end{aligned}$$

El evento de que una bola sea azul puede producirse de dos maneras mutuamente excluyentes: Ya sea que la segunda bola es azul y la primera no lo es o la primera bola es azul y la segunda no lo es. En el inciso *a*) se demostró que la probabilidad de la primera forma es $\frac{35}{132}$ y la probabilidad de la segunda forma también es $\frac{35}{132}$. Así, por el axioma de probabilidad 3,

$$P(\text{1 bola azul}) = \frac{35}{132} + \frac{35}{132} = \frac{70}{132}.$$

Por último, del inciso *a*),

$$P(\text{2 bolas azules}) = \frac{20}{132}.$$

Por tanto,

$$\begin{aligned}\left[\begin{array}{l}\text{el valor esperado del}\\ \text{número de bolas azules}\end{array}\right] &= 0 \cdot P(\text{0 bolas azules}) + 1 \cdot P(\text{1 bola azul})\\ &\quad + 2 \cdot P(\text{2 bolas azules})\\ &= 0 \cdot \frac{7}{22} + 1 \cdot \frac{70}{132} + 2 \cdot \frac{20}{132}\\ &= \frac{110}{132} \cong 0.8.\end{aligned}$$

Teorema de Bayes

Suponga que una urna contiene 3 bolas azules y 4 bolas grises y una segunda urna contiene 5 bolas azules y 3 bolas grises. Se selecciona una pelota, elija aleatoriamente una de las urnas y, después elija aleatoriamente una bola de esa urna. Si la bola elegida es azul, ¿cuál es la probabilidad de que provenga de la primera urna?

Este problema se puede resolver interpretando cuidadosamente toda la información que se conoce y poniéndola en la forma correcta. Sea A el evento de que la bola elegida sea azul, B_1 el evento de que la bola provenga de la primera urna y B_2 el evento que la bola provenga de la segunda urna. Dado que 3 de las 7 bolas en la urna uno son azules y 5 de las 8 bolas en la urna dos son azules,

$$P(A \mid B_1) = \frac{3}{7} \quad \text{y} \quad P(A \mid B_2) = \frac{5}{8}.$$

Y ya que las urnas son equiprobables de ser elegidas,

$$P(B_1) = P(B_2) = \frac{1}{2}.$$

Además, por la fórmula (9.9.2),

$$\begin{aligned}P(A \cap B_1) &= P(A \mid B_1) \cdot P(B_1) = \frac{3}{7} \cdot \frac{1}{2} = \frac{3}{14}, \quad \text{y}\\ P(A \cap B_2) &= P(A \mid B_2) \cdot P(B_2) = \frac{5}{8} \cdot \frac{1}{2} = \frac{5}{16}.\end{aligned}$$

Pero A es la unión disjunta de $(A \cap B_1)$ y $(A \cap B_2)$, así por el axioma de probabilidad 3,

$$P(A) = P((A \cap B_1) \cup (A \cap B_2)) = P(A \cap B_1) + P(A \cap B_2) = \frac{3}{14} + \frac{5}{16} = \frac{59}{112}.$$

Cortesía de Stephen Stigler

Thomas Bayes (1702-1761)

Por último, por la definición de probabilidad condicional

$$P(B_1 \mid A) = \frac{P(B_1 \cap A)}{P(A)} = \frac{\frac{3}{14}}{\frac{59}{112}} = \frac{336}{826} \cong 40.7\%.$$

Por tanto, si la bola elegida es azul, la probabilidad es 40.7% de que provenga de la primera urna.

Los pasos que se utilizan para deducir la respuesta en el ejemplo anterior se pueden generalizar para demostrar el teorema de Bayes. (Consulte los ejercicios 9.9 y 9.10 del final de esta sección.) Thomas Bayes fue un ministro presbiteriano inglés que dedicó gran parte de sus energías a las matemáticas. El teorema que lleva su nombre fue publicado póstumamente en 1763. El retrato de la izquierda es el único que le atribuyen a él, pero su autenticidad ha entrado recientemente en duda.

Teorema 9.9.1 Teorema de Bayes

Suponga que un espacio muestral es una unión de eventos mutuamente disjuntos B_1, B_2, B_3,..., B_n, suponga que A es un evento en S y suponga que A y todos los B_1 tienen probabilidades distintas de cero. Si k es un entero con $1 \leq k \leq n$, entonces

$$P(B_k \mid A) = \frac{P(A \mid B_k)P(B_k)}{P(A \mid B_1)P(B_1) + P(A \mid B_2)P(B_2) + \cdots + P(A \mid B_n)P(B_n)}$$

Ejemplo 9.9.3 Aplicación del teorema de Bayes

La mayoría de las pruebas médicas ocasionalmente producen resultados incorrectos, llamados falsos positivos y falsos negativos. Cuando se diseña una prueba para determinar si un paciente tiene una determinada enfermedad, un resultado **falso positivo** indica que un paciente tiene la enfermedad cuando el paciente no lo tiene. Un resultado **falso negativo** indica que un paciente no tiene la enfermedad cuando el paciente sí la tiene.

Cuando se realizan exámenes de salud a gran escala para enfermedades con relativamente baja incidencia, quienes desarrollan los procedimientos de detección deben equilibrar varias consideraciones: el costo por persona de los gastos de detección, seguidos de los costos de pruebas adicionales de falsos positivos y la posibilidad de que las personas que tienen la enfermedad desarrollan una confianza injustificada de su estado de salud.

Considere que una prueba médica de pantallas para una enfermedad encuentra 5 personas en 1 000. Suponga que la tasa de falsos positivos es de 3% y la tasa de falsos negativos es de 1%. Entonces 99% de las veces que una persona tiene la condición dé prueba positiva y 97% de las veces que una persona tiene la condición dé prueba negativa. (Vea el ejercicio 4 del final de esta sección.)

a. ¿Cuál es la probabilidad de que una persona elegida aleatoriamente dé prueba positiva para la enfermedad si realmente tiene la enfermedad?

b. ¿Cuál es la probabilidad de que una persona elegida al azar dé prueba negativa para la enfermedad si no tiene la enfermedad?

Solución Considere una persona elegida al azar de entre los seleccionados. Sea A el evento de que la persona dé prueba positiva para la enfermedad, B_1 el evento de que la persona realmente tenga la enfermedad y B_2 el evento de que la persona no tenga la enfermedad. Entonces

$$P(A \mid B_1) = 0.99, \quad P(A^c \mid B_1) = 0.01^{\text{c}} \quad P(A^c \mid B_2) = 0.97 \quad \text{y} \quad P(A \mid B_2) = 0.03.$$

También, ya que 5 personas en 1 000 tienen la enfermedad,

$$P(B_1) = 0.005 \quad \text{y} \quad P(B_2) = 0.995.$$

a. Por el teorema de Bayes,

$$\begin{aligned} P(B_1 \mid A) &= \frac{P(A \mid B_1)P(B_1)}{P(A \mid B_1)P(B_1) + P(A \mid B_2)P(B_2)} \\ &= \frac{(0.99)(0.005)}{(0.99)(0.005) + (0.03)(0.995)} \\ &\cong 0.1422 \cong 14.2\%. \end{aligned}$$

Por tanto la probabilidad de que una persona con un resultado positivo tenga realmente la enfermedad es aproximadamente de 14.2%.

b. Por el teorema de Bayes,

$$\begin{aligned} P(B_2 \mid A^c) &= \frac{P(A^c \mid B_2)P(B_2)}{P(A^c \mid B_1)P(B_1) + P(A^c \mid B_2)P(B_2)} \\ &= \frac{(0.97)(0.995)}{(0.01)(0.005) + (0.97)(0.995)} \\ &\cong 0.999948 \cong 99.995\%. \end{aligned}$$

Por tanto la probabilidad de que una persona con un resultado negativo no tenga la enfermedad es aproximadamente de 99.995%.

Se puede sorprender por estos números, pero son bastante comunes en situaciones donde la prueba de detección es mucho menos costosa que una prueba más precisa de la misma enfermedad, pero produce resultados positivos para casi todas las personas con la enfermedad. Utilizar la prueba de detección limita el gasto innecesario de utilizar una prueba más costosa a un porcentaje relativamente pequeño de la población que se selecciona, mientras que sólo rara vez se indica que una persona tiene la enfermedad cuando está libre de ella. ■

Eventos independientes

Suponga que se lanza una moneda dos veces. Parece intuitivamente claro que los resultados de la primera tirada no dependen de ninguna manera del resultado de la segunda tirada y a la inversa. En otras palabras, si, por ejemplo, A es el evento en que se obtiene una cara en la primera tirada y B es el evento en que se obtiene una cara en la segunda tirada, entonces si la moneda se lanza aleatoriamente dos veces, los eventos A y B deben ser *independientes* en el sentido de que $P(A \mid B) = P(A)$ y $P(B \mid A) = P(B)$. Esta idea intuitiva de independencia se apoya en el siguiente análisis. Si la moneda es justa, entonces los cuatro resultados HH, HT, TH y TT son equiprobables y

$$A = \{HH, HT\}, \quad B = \{TH, HH\}, \quad A \cap B = \{HH\}.$$

Por tanto

$$P(A) = P(B) = \frac{2}{4} = \frac{1}{2}.$$

Pero también

$$P(A \mid B) = \frac{P(A \cap B)}{P(B)} = \frac{\frac{1}{4}}{\frac{1}{2}} = \frac{1}{2} \quad \text{y} \quad P(B \mid A) = \frac{P(A \cap B)}{P(A)} = \frac{\frac{1}{4}}{\frac{1}{2}} = \frac{1}{2}$$

y así $P(A \mid B) = P(A)$ y $P(B \mid A) = P(B)$.

Para obtener la forma final de la definición de independencia, observe

si $P(B) \neq 0$ y $P(A \mid B) = P(A)$, entonces $P(A \cap B) = P(A \mid B) \cdot P(B) = P(A) \cdot P(B)$.

Por el mismo argumento,

$$\text{si } P(A) \neq 0 \text{ y } P(B \mid A) = P(B), \text{ entonces } P(A \cap B) = P(A) \cdot P(B).$$

Por el contrario (vea el ejercicio 18 del final de esta sección),

$$\text{si } P(A \cap B) = P(A) \cdot P(B) \text{ y } P(A) \neq 0, \text{ entonces } P(B \mid A) = P(B)$$

y

$$\text{si } P(A \cap B) = P(A) \cdot P(B) \text{ y } P(B) \neq 0, \text{ entonces } P(A \mid B) = P(A).$$

Nota Sería natural creer que eventos mutuamente disjuntos serían independientes, pero de hecho casi lo contrario es verdadero: Eventos mutuamente disjuntos con probabilidades distintas de cero son dependientes.

Así, para mayor comodidad y para eliminar el requisito de que las probabilidades deben ser distintas de cero, utilizamos la siguiente fórmula de producto para definir eventos independientes.

• Definición

Si A y B son eventos en un espacio muestral S, entonces A y B son independientes si y sólo si,

$$P(A \cap B) = P(A) \cdot P(B).$$

Ejemplo 9.9.4 Eventos disjuntos e independientes

Sean A y B eventos en un espacio muestral S y suponga que $A \cap B = \emptyset$, $P(A) \neq 0$ y $P(B) \neq 0$. Demuestre que $P(A \cap B) \neq P(A) \cdot P(B)$.

Solución Ya que $A \cap \mathrm{B} = \emptyset$, $P(A \cap B) = 0$ por el axioma de probabilidad 2. Pero $P(A) \cdot P(B) \neq 0$ ya que ni $P(A)$ ni $P(B)$ son iguales a cero. Por tanto $P(A \cap B) \neq P(A) \cdot P(B)$ ■

El ejemplo siguiente y su consecuencia inmediata, demuestran cómo la independencia de los dos eventos se extiende a sus complementos.

Ejemplo 9.9.5 La probabilidad de $A \cap B^c$ cuando A y B son eventos independientes

Suponga que A y B son eventos independientes en un espacio muestral S. Demuestre que A y B^c también son independientes.

Solución La solución de los ejercicios 8 y 25 de la sección 6.2 muestra que para todos los conjuntos A y B,

$$1)\ (A \cap B) \cup (A \cap B^c) = A$$

y

$$2)\ (A \cap B) \cap (A \cap B^c) = \emptyset$$

Se tiene que el axioma de probabilidad 3 se puede aplicar a la ecuación (1) para obtener

$$P((A \cap B) \cup (A \cap B^c)) = P(A \cap B) + P(A \cap B^c) = P(A).$$

Resolviendo para $P(A \cap B^c)$ se obtiene que

$$\begin{aligned} P(A \cap B^c) &= P(A) - P(A \cap B) \\ &= P(A) - P(A) \cdot P(B) && \text{ya que } A \text{ y } B \text{ son independientes} \\ &= P(A)(1 - P(B)) && \text{factorizando } P(A) \\ &= P(A) \cdot P(B^c) && \text{por la fórmula 9.8.1} \end{aligned}$$

Por tanto A y B^c son eventos independientes. ■

Se sigue inmediatamente del ejemplo 9.9.5 que si A y B son independientes, A^c y B también son independientes y así son A^c y B^c. (Vea el ejercicio 22 del final de esta sección.) Estos resultados se aplican en el ejemplo 9.9.6.

Ejemplo 9.9.6 Cálculo de probabilidades de las intersecciones de dos eventos independientes

Se carga una moneda para que la probabilidad de cara sea 0.6. Supongamos que se lanza la moneda dos veces. Aunque la probabilidad de cara es mayor que la probabilidad de cruz, no hay ninguna razón para creer que si la moneda cae cara o cruz en una tirada afectará si cae cara o cruz en otra tirada. Por tanto es razonable suponer que los resultados de las tiradas sean independientes.

a. ¿Cuál es la probabilidad de obtener dos caras?

b. ¿Cuál es la probabilidad de obtener una cara?

c. ¿Cuál es la probabilidad de no obtener caras?

d. ¿Cuál es la probabilidad de obtener al menos una cara?

Solución El espacio muestral S consta de los cuatro resultados $\{HH, HT, TH, TT\}$, que no son equiprobables. Sea E el evento en que se obtiene una cara en la primera tirada y sea F el evento en que se obtiene una cara en la segunda tirada. Entonces $P(E) = P(F) = 0.6$ y cabe suponer que E y F son independientes.

a. La probabilidad de obtener dos caras es $P(E \cap F)$. Ya que E y F son independientes,

$$P(\text{dos caras}) = P(E \cap F) = P(E) \cdot P(F) = (0.6)(0.6) = 0.36 = 36\%.$$

b. Se puede obtener una cara en dos formas mutuamente excluyentes: cara en la primera tirada y cruz en la segunda, o cruz en la primera tirada y cara en la segunda. Por tanto, el evento de obtener exactamente una cara es $(E \cap F^c) \cup (E^c \cap F)$. También $(E \cap F^c) \cap (E^c \cap F) = \emptyset$ y, además, por la fórmula de la probabilidad del complemento de un evento, $P(E^c) = P(F^c) = 1 - 0.6 = 0.4$. Por tanto

$$\begin{aligned} P(\text{una cara}) &= P((E \cap F^c) \cup (E^c \cap F)) \\ &= P(E) \cdot P(F^c) + P(E^c) \cdot P(F) \qquad \text{por el ejemplo 9.9.5 y por el ejercicio 22} \\ &= (0.6)(0.4) + (0.4)(0.6) \\ &= 0.48 = 48\%. \end{aligned}$$

c. La probabilidad de no obtener caras es $P(E^c \cap F^c)$. Por el ejercicio 22,

$$P(\text{no caras}) = P(E^c \cap F^c) = P(E^c) \cdot P(F^c) = (0.4)(0.4) = 0.16 = 16\%.$$

d. Hay dos formas de solucionar este problema. Una es observar que, ya que el evento de obtener una cara y el evento de obtener dos caras son mutuamente disjuntos,

$$\begin{aligned} P(\text{al menos una cara}) &= P(\text{una cara}) + P(\text{dos caras}) \\ &= 0.48 + 0.36 \qquad \text{por los incisos } a) \text{ y } b) \\ &= 0.84 = 84\%. \end{aligned}$$

La segunda forma consiste en utilizar el hecho de que el evento de obtener al menos una cara es el complemento del evento de no obtener caras. Así

$$\begin{aligned} P(\text{al menos una cara}) &= 1 - P(\text{no caras}) \\ &= 1 - 0.16 \qquad \text{por el inciso } c) \\ &= 0.84 = 84\%. \end{aligned}$$

■

Ejemplo 9.9.7 Valor esperado del lanzamiento de una moneda cargada dos veces

Suponga que se carga una moneda para que la probabilidad de las caras sea 0.6 y suponga que se lanza la moneda dos veces. Si este experimento se repite muchas veces, ¿cuál es el valor esperado del número de caras?

Solución Piense en los resultados del lanzamiento de la moneda como sólo 0, 1 o 2 caras. En el ejemplo 9.9.6 se demostró que las probabilidades de estos resultados son 0.16, 0.48 y 0.36, respectivamente. Por tanto, por definición de valor esperado, el

$$\text{número esperado de caras} = 0\cdot(0.16) + 1\cdot(0.48) + 2\cdot(0.36) = 1.2.$$ ■

¿Qué pasa si una moneda está cargada más de dos veces? Supongamos que se lanza diez veces o cientos de veces. ¿Cuáles son las probabilidades de varios números de caras? Para responder a esta pregunta, es necesario ampliar el concepto de independencia a más de dos eventos. Por ejemplo, decimos que tres eventos A, B y C son *pares independientes* si y sólo si,

$$P(A \cap B) = P(A)\cdot P(B),\ P(A \cap C) = P(A)\cdot P(C) \text{ y } P(B \cap C) = P(B)\cdot P(C).$$

El siguiente ejemplo muestra que los eventos pueden ser *pares independientes*, pero no satisfacen la condición $P(A \cap B \cap C) = P(A)\cdot P(B)\cdot P(C)$. Por el contrario, se puede satisfacer la condición $P(A \cap B \cap C) = P(A)\cdot P(B)\cdot P(C)$ sin ser pares independientes (vea el ejercicio 26 del final de esta sección).

Ejemplo 9.9.8 Exploración de la independencia de tres eventos

Supongamos que se lanza dos veces una moneda justa. Sea A el evento en que se obtiene una cara en la primera tirada, B el evento en que se obtiene una cara en la segunda tirada y C el evento en que se obtienen dos caras o dos cruces. Demuestre que A, B y C son independientes a pares, pero que no satisfacen la condición de $P(A \cap B \cap C) = P(A)\cdot P(B)\cdot P(C)$.

Solución Ya que hay cuatro resultados equiprobables: HH, HT, TH y TT está claro que $P(A) = P(B) = P(C) = \frac{1}{2}$. También puede ver que $A \cap B = \{HH\}$, $A \cap C = \{HH\}$, $B \cap C = \{HH\}$ y $A \cap B \cap C = \{HH\}$. Por tanto $P(A \cap B) = P(A \cap C) = P(B \cap C) = \frac{1}{4}$ y así $P(A \cap B) = P(A)\cdot P(B)$, $P(A \cap C) = P(A)\cdot P(C)$ y $P(B \cap C) = P(A)\cdot P(C)$. Así A, B y C son pares independientes. Pero

$$P(A \cap B \cap C) = P(\{HH\}) = \frac{1}{4} \neq \left(\frac{1}{2}\right)^3 = P(A)\cdot P(B)\cdot P(C).$$ ■

Debido a las situaciones del ejemplo 9.9.8, se deben incluir cuatro condiciones en la definición de la independencia de tres eventos.

• Definición

Sean A, B y C eventos en un espacio muestral S. A, B y C son **independientes a pares** si y sólo si se satisfacen las condiciones de la 1 a la 3 que se muestran a continuación. Son **mutuamente independientes** si y sólo si, cumplen todas las cuatro condiciones que se muestran a continuación.

1. $P(A \cap B) = P(A)\cdot P(B)$
2. $P(A \cap C) = P(A)\cdot P(C)$
3. $P(B \cap C) = P(B)\cdot P(C)$
4. $P(A \cap B \cap C) = P(A)\cdot P(B)\cdot P(C)$

La definición de independencia mutua para cualquier colección de n eventos con $n \geq 2$ generaliza las dos definiciones dadas previamente.

• Definición

Los eventos, A_1, A_2, A_3,..., A_n en un espacio muestral S son **mutuamente independientes** si y sólo si, la probabilidad de la intersección de cualquier subconjunto de los eventos es el producto de las probabilidades de los eventos en el subconjunto.

Ejemplo 9.9.9 Lanzamiento diez veces de una moneda cargada

Una moneda se carga diez veces para que la probabilidad de las caras sea 0.6 (y por tanto la probabilidad de las cruces es 0.4). Supongamos que la moneda se tira diez veces. Como en el ejemplo 9.9.6, es razonable suponer que los resultados de las tiradas son mutuamente independientes.

a. ¿Cuál es la probabilidad de obtener ocho caras?

b. ¿Cuál es la probabilidad de obtener por lo menos ocho caras?

Solución

a. Para cada $i = 1, 2,..., 10$, sea H_i el evento en que se obtiene una cara en la i-ésima tirada y sea T_i el evento que se obtiene una cruz en la i-ésima tirada. Supongamos que los ocho caras se producen en las ocho primeras tiradas y que las restantes dos tiradas son cruces. Este es el evento $H_1 \cap H_2 \cap H_3 \cap H_4 \cap H_5 \cap H_6 \cap H_7 \cap H_8 \cap T_9 \cap T_{10}$. Por simplicidad, se denotan como $H\ H\ H\ H\ H\ H\ H\ H\ T\ T$. Por definición de eventos mutuamente independientes,

$$P(HHHHHHHHTT) = (0.6)^8(0.4)^2.$$

Debido a la ley conmutativa de la multiplicación, si los ocho caras ocurren en cualquiera de las otras diez tiradas, se obtiene el mismo número. Por ejemplo, si denotamos el evento $H_1 \cap H_2 \cap H_3 \cap H_4 \cap H_5 \cap H_6 \cap H_7 \cap H_8 \cap T_9 \cap H_{10}$ por $H\ H\ T\ H\ H\ H\ H\ H\ T\ H$, entonces

$$P(HHTHHHHHTH) = (0.6)^2(0.4)(0.6)^5(0.4)(0.6) = (0.6)^8(0.4)^2.$$

Ahora hay tantas maneras de obtener ocho caras en diez tiradas como subconjuntos de ocho elementos (los números de tiradas en las que se obtienen caras) que se pueden elegir entre un conjunto de diez elementos. Este número es $\binom{10}{8}$. Se deduce que, debido a que todas las diferentes formas de obtener ocho caras son mutuamente excluyentes,

$$P(\text{ocho caras}) = \binom{10}{8}(0.6)^8(0.4)^2.$$

b. Por un razonamiento similar al del inciso *a*),

$$P(\text{nueve caras}) = \begin{bmatrix}\text{el número de diferentes formas}\\ \text{que se pueden obtener nueve}\\ \text{caras en diez tiradas}\end{bmatrix} \cdot (0.6)^9(0.4)^1 = \binom{10}{9}(0.6)^9(0.4),$$

y

$$P(\text{diez caras}) = \begin{bmatrix}\text{el número de diferentes formas}\\ \text{que se pueden obtener diez}\\ \text{caras en diez tiradas}\end{bmatrix} \cdot (0.6)^{10}(0.4)^0 = \binom{10}{10}(0.6)^{10}.$$

Ya que obtener ocho, obtener nueve y obtener diez caras son eventos mutuamente disjuntos,

$$\begin{aligned} P(\text{al menos ocho caras}) &= P(\text{ocho caras}) + P(\text{nueve caras}) + P(\text{diez caras}) \\ &= \binom{10}{8}(0.6)^8(0.4)^2 + \binom{10}{9}(0.6)^9(0.4) + \binom{10}{10}(0.6)^{10} \\ &\cong 0(167 = 16.7\%. \end{aligned}$$

Nota Las probabilidades binomiales se presentan en situaciones con repeticiones múltiples mutuamente independientes de un proceso aleatorio, cada uno de los cuales tiene los mismos dos posibles resultados con las mismas probabilidades en cada repetición.

Observe la presencia de los coeficientes binomiales $\binom{n}{k}$ en las soluciones de los problemas como el del ejemplo 9.9.9. Por esta razón, las probabilidades de la forma

$$\binom{n}{k} p^{n-k}(1-p)^k,$$

donde $0 \leq p \leq 1$, se denominan **probabilidades binomiales**.

Autoexamen

1. Si A y B son eventos cualesquiera en un espacio muestral S y $P(A) \neq 0$, entonces la probabilidad condicional de B dado que A es $P(B \mid A) =$ _____.
2. El teorema de Bayes dice que si un espacio muestral S es una unión de eventos mutuamente disjuntos $B_1, B_2, \ldots, B_n$ con probabilidades distintas de cero, si A es un evento en S con $P(A) \neq 0$ y si k es un entero con $1 \leq k \leq n$, entonces _____.
3. Los eventos A y B en un espacio muestral S son independientes si y sólo si _____.
4. Los eventos A, B y C en un espacio muestral S son mutuamente independientes si y sólo si, _____, _____, _____ y _____.

Conjunto de ejercicios 9.9

1. Suponga que $P(A \mid B) = 1/2$ y $P(A \cap B) = 1/6$. ¿Qué es $P(B)$?

2. Suponga que $P(X \mid Y) = 1/3$ y $P(Y) = 1/4$. ¿Qué es $P(X \cap Y)$?

H 3. El instructor de una clase de matemática discreta dio dos demostraciones. Veinticinco por ciento de los estudiantes recibió una A en la primera demostración y 15% de los estudiantes recibió A en ambas demostraciones. ¿Qué porcentaje de los estudiantes que recibieron A en la primera demostración también recibieron A en la segunda demostración?

4. **a.** Demuestre que si A y B son los eventos en un espacio muestral S, con $P(B) \neq 0$, entonces $P(A^c \mid B) = 1 - P(A \mid B)$.
   b. Explique cómo este resultado justifica lo siguiente: 1) Si la probabilidad de un falso positivo en una prueba de una condición es 4%, entonces hay 96% de probabilidades que una persona que no tiene la condición tendrá un resultado negativo. 2) Si la probabilidad de un falso negativo en una prueba de una condición es 1%, entonces hay una probabilidad de 99% de que una persona tendrá la condición positiva para la enfermedad.

H 5. Suponga que A y B son eventos en un espacio muestral S y $P(A)$, $P(B)$ y $P(A \mid B)$ son conocidos. Deduzca una fórmula para $P(A \mid B^c)$.

6. Una urna contiene 25 bolas rojas y 15 bolas azules. Se eligen aleatoriamente dos bolas, una tras otra, sin reemplazo.
   a. Utilice un diagrama de árbol para ayudar a calcular las probabilidades siguientes: la probabilidad de que ambas bolas sean rojas, la probabilidad que la primera bola sea roja y la segunda no, la probabilidad de que la primera bola no sea roja y la segunda sea roja, la probabilidad de que ninguna bola sea roja.
   b. ¿Cuál es la probabilidad de que la segunda bola sea roja?
   c. ¿Cuál es la probabilidad de que al menos una de las bolas sea roja?

7. Rehaga el ejercicio 6 suponiendo que la urna contiene 30 bolas rojas y 40 bolas azules.

8. Un grupo de 10 semifinalistas para un trabajo consta de 7 hombres y 3 mujeres. Ya que todos se consideran igualmente calificados, los nombres de dos de los semifinalistas son sacados, uno tras otro, al azar, para convertirse en finalistas para el trabajo.
   a. ¿Cuál es la probabilidad de que ambas finalistas sean mujeres?
   b. ¿Cuál es la probabilidad de que ambos finalistas sean hombres?
   H c. ¿Cuál es la probabilidad de que un finalista sea una mujer y el otro sea un hombre?

H 9. Demuestre el teorema de Bayes para $n = 2$. Es decir, demuestre que si un espacio muestral S es una unión de eventos mutuamente disjuntos B_1 y B_2, si A es un evento en S con $P(A) \neq 0$ y si $k = 1$ o $k = 2$, entonces

$$P(B_k \mid A) = \frac{P(A \mid B_k)P(B_k)}{P(A \mid B_1)P(B_1) + P(A \mid B_2)P(B_2)}.$$

10. Demuestre la versión completa del teorema de Bayes.

11. Una urna contiene 12 bolas azules y 7 bolas blancas y una segunda urna contiene 8 bolas azules y 19 bolas blancas. Se selecciona una urna aleatoriamente y se elige una bola de la urna.
   a. ¿Cuál es la probabilidad de que la bola elegida sea azul?
   b. Si la bola elegida es azul, ¿cuál es la probabilidad de que proviene de la primera urna?

12. Rehaga el ejercicio 11 suponiendo que la primera urna contiene 4 bolas azules y 16 bolas blancas y la segunda urna contiene 10 bolas azules y 9 bolas blancas.

***H* 13.** Una urna contiene 10 bolas rojas y 25 bolas verdes y una segunda urna contiene 22 bolas rojas y 15 bolas verdes. Se elige una pelota como sigue: primero se selecciona una urna lanzando una moneda cargada con probabilidad 0.4 de caer cara y probabilidad 0.6 de caer cruz. Si la moneda cae cara, se elige la primera urna; de lo contrario, se selecciona la segunda urna. Después se elige una bola aleatoriamente de la urna elegida.
   a. ¿Cuál es la probabilidad de que la bola elegida sea verde?
   b. Si la bola elegida es verde, ¿cuál es la probabilidad de que se eligió de la primera urna?

14. Una prueba de detección de drogas se utiliza en una gran población de personas de los cuales 4% consume drogas. Supongamos que la tasa de falsos positivos es de 3% y que la tasa de falsos negativos es de 2%. Así, una persona que usa drogas da prueba positiva 98% de las veces y una persona que no usa drogas da prueba negativa 98.7% de las veces.
   a. ¿Cuál es la probabilidad de que una persona elegida aleatoriamente dé prueba positiva de drogas si utiliza drogas?
   b. ¿Cuál es la probabilidad de que una persona elegida al azar dé prueba negativa de drogas si no usa drogas?

15. Dos fábricas diferentes producen una cierta parte de automóvil. La probabilidad de que un componente de la primera fábrica sea defectuoso es de 2% y la probabilidad de que un componente de la segunda fábrica sea defectuoso es de 5%. En un suministro de 180 partes, 100 se obtuvieron de la primera fábrica y 80 de la segunda fábrica.
   a. ¿Cuál es la probabilidad de que una parte elegida al azar de los 180 sea de la primera fábrica?
   b. ¿Cuál es la probabilidad de que una parte elegida aleatoriamente de los 180 proviene de la segunda fábrica?
   c. ¿Cuál es la probabilidad de que una parte elegida aleatoriamente de los 180 es defectuosa?
   d. Si la parte elegida es defectuosa, ¿cuál es la probabilidad de que provenía de la primera fábrica?

***H* 16.** Tres diferentes proveedores: X, Y y Z, ofrecen productos para una tienda de comestibles. Doce por ciento de los productos de X es de grado superior, 8% de los productos de Y es de grado superior y 15% de los productos de Z es de grado superior. La tienda obtiene 20% de su producción de X, 45% de Y y 35% de Z.
   a. Si se compra una pieza de la producción, ¿cuál es la probabilidad de que sea de grado superior?
   b. Si una pieza de la producción en el almacén es de grado superior, ¿cuál es la probabilidad de que sea de X?

17. Demuestre que si A y B son eventos en un espacio muestral S con la propiedad de que $P(A \mid B) = P(A)$ y $P(A) \neq 0$ entonces, $P(B \mid A) = P(B)$.

18. Demuestre que si $P(A \cap B) = P(A) \cdot P(B)$, $P(A) \neq 0$ y $P(B) \neq 0$, entonces $P(A \mid B) = P(A)$ y $P(B \mid A) = P(B)$.

19. Se lanzan un par de dados, uno azul y el otro gris. Sea A el evento que muestra el número hacia arriba en el dado azul es 2 y sea B el evento de que el número hacia arriba sobre el dado gris es 4 o 5. Demuestre que $P(A \mid B) = P(A)$ y $P(B \mid A) = P(B)$.

20. Suponga que se lanza una moneda tres veces. Sea A el evento en que se obtiene una cara en la primera tirada y sea B el evento en que se obtiene un número par de caras. Demuestre que $P(A \mid B) = P(A)$ y $P(B \mid A) = P(B)$.

21. Si A y B son eventos en un espacio muestral S y $A \cap B = \emptyset$, ¿que debe cumplirse para que A y B sean independientes? Explique.

22. Demuestre que si A y B son eventos independientes en un espacio muestral S, entonces A^c y B también son independientes y también lo son A^c y B^c.

23. Un estudiante que presenta un examen de opción múltiple no sabe las respuestas a dos preguntas. Todas tienen cinco opciones para la respuesta. Para una de las dos preguntas, el alumno puede eliminar dos opciones de respuesta como incorrecta pero no tiene ni idea sobre las otras opciones de respuesta. Para la otra pregunta, el estudiante no tiene ninguna pista sobre la respuesta correcta. Suponga que si el alumno elige la respuesta correcta en una de las preguntas no afecta a si el estudiante elige la respuesta correcta en la otra pregunta.
   a. ¿Cuál es la probabilidad de que el alumno responderá ambas preguntas correctamente?
   b. ¿Cuál es la probabilidad de que el estudiante responderá correctamente a una de las preguntas?
   c. ¿Cuál es la probabilidad de que el alumno no responderá alguna pregunta correctamente?

24. Una empresa utiliza dos correctores X y Y para comprobar un manuscrito dado. X comete 12% en errores tipográficos y Y 15%. Suponga que los correctores trabajan de forma independiente.
   a. ¿Cuál es la probabilidad de que ambos correctores cometan un error tipográfico aleatorio?
   b. Si el manuscrito contiene 1 000 errores tipográficos, ¿qué número se espera de errores?

25. Una moneda se carga para que la probabilidad de las caras sea 0.7 y la probabilidad de las cruces sea 0.3. Supongamos que se lanza la moneda dos veces y que los resultados de las tiradas son independientes.
   a. ¿Cuál es la probabilidad de obtener exactamente dos caras?
   b. ¿Cuál es la probabilidad de obtener exactamente una cara?
   c. ¿Cuál es la probabilidad de no obtener caras?
   d. ¿Cuál es la probabilidad de obtener al menos una cara?

✶ 26. Describa un espacio muestral y los eventos A, B y C, donde $P(A \cap B \cap C) = P(A) \cdot P(B) \cdot P(C)$ pero A, B y C no son independientes a pares.

H 27. El ejemplo utilizado para introducir la probabilidad condicional describe una familia con dos hijos, cada uno de los cuales era equiprobable de ser un niño o una niña. El ejemplo muestra que si se sabe que un hijo es un niño, la probabilidad de que el otro hijo sea un niño es $1/3$. Ahora imagine el mismo tipo de familia: dos hijos cada uno de los cuales es equiprobable de ser un niño o una niña. Suponga que se encuentra con uno de los hijos y ve que es un niño. ¿Cuál es la probabilidad de que el otro hijo sea un niño? Explique. (Tenga cuidado. La respuesta puede sorprenderle.)

28. Se carga una moneda para que la probabilidad de las caras sea 0.7 y la probabilidad de las cruces sea 0.3. Supongamos que se lanza una moneda diez veces y que los resultados de las tiradas son mutuamente independientes.
   a. ¿Cuál es la probabilidad de obtener exactamente siete caras?
   b. ¿Cuál es la probabilidad de obtener exactamente diez caras?
   c. ¿Cuál es la probabilidad de no obtener caras?
   d. ¿Cuál es la probabilidad de obtener al menos una cara?

29. Supongamos que se eligen aleatoriamente diez elementos de un gran lote entregado a una empresa. El fabricante afirma que sólo 3% de los elementos del lote son defectuosos. Suponga que el lote es grande, lo suficiente para que a pesar de que la selección se realiza sin reemplazo, se pueda utilizar el número de 0.03 para aproximar la probabilidad de que uno de los diez elementos es defectuoso. Además, se supone que ya que los elementos son elegidos aleatoriamente, los resultados de las elecciones son mutuamente independientes. Por último, suponga que la reclamación del fabricante es correcta.
   a. ¿Cuál es la probabilidad de que ninguno de los diez sea defectuoso?
   b. ¿Cuál es la probabilidad de que al menos uno de los diez es defectuoso?
   c. ¿Cuál es la probabilidad de que exactamente cuatro de los diez son defectuosos?
   d. ¿Cuál es la probabilidad de que al menos dos de los diez son defectuosos?

30. Supongamos que la probabilidad de un resultado falso positivo en una mamografía es de 4% y que las interpretaciones radiológicas de las mamografías son mutuamente independientes en el sentido de que si un radiólogo encuentra un resultado positivo en una mamografía no influye si, sí o no, el radiólogo encuentre un resultado positivo en otra mamografía. Supongamos que una mujer se hace una mamografía cada año durante diez años.
   a. ¿Cuál es la probabilidad de que no tendrá ningún resultado falso positivo durante ese tiempo?
   b. ¿Cuál es la probabilidad de que tendrá al menos un resultado falso positivo durante ese tiempo?
   c. ¿Cuál es la probabilidad de que tendrá exactamente dos resultados falsos positivos durante ese tiempo?
   d. Supongamos que la probabilidad de un resultado falso negativo en una mamografía es de 2% y suponga que la probabilidad de que una mujer elegida aleatoriamente tenga cáncer de mama es 0.0002.
      i) Si una mujer tiene un resultado positivo un año, ¿cuál es la probabilidad de que realmente tenga cáncer de mama?
      ii) Si una mujer tiene un resultado negativo un año, ¿cuál es la probabilidad de que realmente tenga cáncer de mama?

31. Datos empíricos indican que aproximadamente 103 de cada 200 niños nacidos son hombres. Por tanto la probabilidad de que un recién nacido sea varón es aproximadamente de 51.5%. Suponga que una familia tiene seis hijos y suponga que los géneros de todos los niños son mutuamente independientes.
   H a. ¿Cuál es la probabilidad de que ninguno de los hijos sea un hombre?
   b. ¿Cuál es la probabilidad de que al menos uno de los hijos sea un hombre?
   c. ¿Cuál es la probabilidad de que exactamente cinco de los hijos sean varones?

32. Una persona toma un examen de opción múltiple en el que cada pregunta tiene cuatro respuestas posibles. Suponga que la persona no tiene ni idea acerca de las respuestas a tres de las preguntas y simplemente elige aleatoriamente cada una.
   a. ¿Cuál es la probabilidad de que la persona responderá las tres preguntas correctamente?
   b. ¿Cuál es la probabilidad de que la persona responderá exactamente dos preguntas correctamente?
   c. ¿Cuál es la probabilidad de que la persona responderá exactamente una pregunta correctamente?
   d. ¿Cuál es la probabilidad de que la persona no responderá ninguna pregunta correctamente?
   e. Suponga que la persona obtiene un punto de crédito por cada respuesta correcta y se deduce $1/3$ punto por cada respuesta incorrecta. ¿Cuál es el valor esperado de puntuación de la persona para las tres preguntas?

33. En el ejercicio 23 de la sección 9.8, sea C_k sea el evento que el jugador que tiene k dólares, gane el siguiente tiro de los dados y finalmente se arruine y sea D_k el evento que el jugador que tiene k dólares, pierda el siguiente tiro de dados y finalmente se arruine y sea P_n la probabilidad de que el jugador finalmente se arruine. Utilice los axiomas de probabilidad y la definición de probabilidad condicional para deducir la ecuación

$$P_{k-1} = \frac{1}{6}P_k + \frac{5}{6}P_{k-2}.$$

Respuestas del autoexamen

1. $\dfrac{P(A \cap B)}{P(A)}$ 2. $P(B_k \mid A) = \dfrac{P(A \mid B_k)P(B_k)}{P(A \mid B_1)P(B_1) + P(A \mid B_2)P(B_2) + \cdots + P(A \mid B_n)P(B_n)}$ 3. $P(A \cap B) = P(A) \cdot P(B)$

4. $P(A \cap B) = P(A) \cdot P(B)$; $P(A \cap C) = P(A) \cdot P(C)$; $P(B \cap C) = P(B) \cdot P(C)$; $P(A \cap B \cap C) = P(A) \cdot P(B) \cdot P(C)$

CAPÍTULO 10

GRAFOS Y ÁRBOLES

Ya se han presentado antes en este libro grafos y árboles como convenientes visualizaciones. Por ejemplo, un árbol de probabilidad muestra todos los posibles resultados de una operación de varios pasos con un número finito de resultados para cada paso, el grafo dirigido de una relación en un conjunto muestra qué elementos del conjunto están relacionados, un diagrama de Hasse ilustra las relaciones entre los elementos de un conjunto que está parcialmente ordenado y un diagrama PERT muestra las tareas que deben realizarse antes de la ejecución de un proyecto.

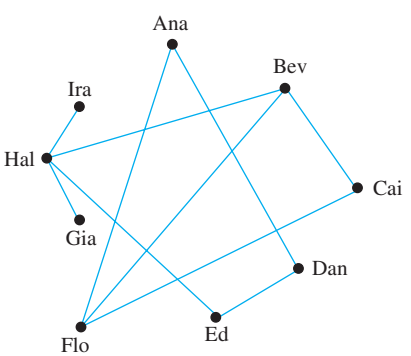
En este capítulo presentamos algo de las matemáticas de grafos y de árboles, se analizan conceptos como el grado de un vértice, conectividad, circuitos de Euler y hamiltonianos, representación de grafos con matrices, isomorfismos de grafos, la relación entre el número de vértices y el número de aristas de un árbol, propiedades de las raíces de los árboles, los árboles expandidos y las trayectorias más cortas en los grafos. Las aplicaciones incluyen el uso de grafos y árboles en el estudio de inteligencia artificial, química, problemas de programación y sistemas de transporte.

10.1 Grafos: definiciones y propiedades básicas

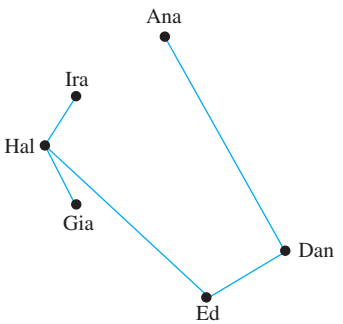
La totalidad de las matemáticas consiste en la organización de una serie de ayudas a la imaginación en el proceso de razonamiento. —Alfred North Whitehead, 1861-1947

Imagine una organización que quiere establecer equipos de tres para trabajar en algunos proyectos. A fin de maximizar el número de personas en cada equipo que tengan experiencia trabajando juntos con éxito, el director pidió a los miembros proporcionar los nombres de sus anteriores socios. Esta información se muestra a continuación tanto en una tabla como en un diagrama.

Nombre	Socios anteriores
Ana	Dan, Flo
Bev	Cai, Flo, Hal
Cai	Bev, Flo
Dan	Ana, Ed
Ed	Dan, Hal
Flo	Cai, Bev, Ana
Gia	Hal
Hal	Gia, Ed, Bev, Ira
Ira	Hal



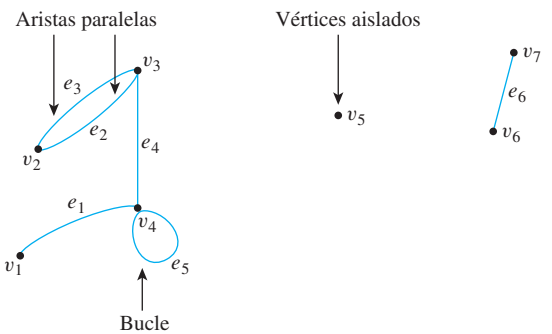
Del diagrama, es fácil ver que Bev, Cai y Flo, son un grupo de tres socios anteriores y así se debe formar uno de estos equipos. La figura en la página siguiente muestra el resultado cuando se eliminan estos tres nombres del diagrama.



Este dibujo muestra que colocar a Hal en el mismo equipo que Ed dejaría a Gia y a Ira en un equipo sin socios anteriores. Sin embargo, si se coloca a Hal en un equipo con Gia e Ira, entonces el equipo restante consistiría de Ana, Dan y Ed y ambos equipos contienen al menos un par de socios anteriores.

Dibujos como los que acabamos de mostrar son ejemplos de una estructura conocida como *grafo*. Los puntos se denominan *vértices* (plural de *vértice*) y los segmentos de recta que unen los vértices se llaman *aristas*. Como puede ver de los dibujos, es posible que dos aristas se crucen en un punto que no es un vértice. Observe también que el tipo de grafo que se describe aquí es muy diferente de la "gráfica de una ecuación" o la "gráfica de una función".

En general, un grafo consiste de un conjunto de vértices y un conjunto de aristas que conectan varios pares de vértices. Las aristas pueden ser rectas o curvas y deben conectar ya sea un vértice con otro vértice o consigo misma, como se muestra a continuación.



En este dibujo, los vértices se han etiquetado con v y las aristas con e. Cuando una arista conecta un vértice consigo mismo (como e_5), se llama un *bucle*. Cuando dos aristas conectan el mismo par de vértices (como e_2 y e_3), se dice que son *paralelas*. Es muy posible que un vértice no esté conectado por una arista con cualquier otro vértice en el grafo (como v_5) y en ese caso se dice que el vértice está *aislado*. A continuación se presenta la definición formal de un grafo.

• Definición

Un **grafo** G consiste de dos conjuntos finitos: un conjunto no vacío $V(G)$ de **vértices** y un conjunto de **aristas** $E(G)$, donde cada arista está asociada a un conjunto compuesto por uno o dos vértices llamados **puntos extremos**. La correspondencia de aristas a puntos finales se llama la **función de arista a punto extremo**.

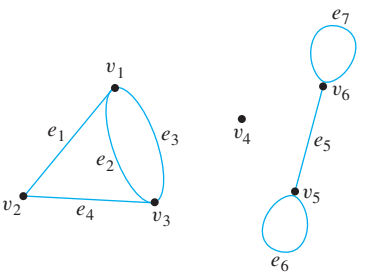
Una arista con un sólo punto extremo se llama un **bucle** y dos o más aristas distintas con el mismo conjunto de puntos extremos se dicen que son **paralelas**. Se dice que una arista **conecta** sus puntos finales; dos vértices que se conectan por una arista se denominan **adyacentes**; y un vértice que es un punto final de un bucle se dice que es **adyacente a sí mismo**.

Se dice que una arista **incide sobre** cada uno de sus puntos extremos y dos aristas que inciden en el mismo punto se llaman **adyacentes**. Un vértice en el que no incide arista alguna se llama **aislado**.

Las gráficas tienen representaciones pictóricas en las que los vértices se representan por puntos y las aristas por segmentos de recta. Una representación pictórica dada determina unívocamente una gráfica.

Ejemplo 10.1.1 Terminología

Considere la gráfica siguiente:



a. Escriba el conjunto de vértices y el conjunto de aristas y presente una tabla que muestre la función punto extremo-arista.

b. Determine todas las aristas que inciden en v_1, todos los vértices que son adyacentes a v_1, todas las aristas adyacentes a e_1, todos los bucles, todas las aristas paralelas, todos los vértices adyacentes a sí mismos y todos los vértices aislados.

Solución

a. conjunto de vértices $= \{v_1, v_2, v_3, v_4, v_5, v_6\}$
conjunto de aristas $= \{e_1, e_2, e_3, e_4, e_5, e_6, e_7\}$
función punto extremo-arista:

Arista	Punto extremo-arista
e_1	$\{v_1, v_2\}$
e_2	$\{v_1, v_3\}$
e_3	$\{v_1, v_3\}$
e_4	$\{v_2, v_3\}$
e_5	$\{v_5, v_6\}$
e_6	$\{v_5\}$
e_7	$\{v_6\}$

Observe que el vértice aislado v_4 no aparece en esta tabla. Aunque cada arista debe tener uno o dos puntos extremos, un vértice no necesita ser el punto extremo de una arista.

b. e_1, e_2 y e_3 inciden sobre v_1.
v_2 y v_3 son adyacentes a v_1.
e_2, e_3 y e_4 son adyacentes a e_1.
e_6 y e_7 son bucles.
e_2 y e_3 son paralelos.
v_5 y v_6 son adyacentes a sí mismos.
v_4 es un vértice aislado. ■

Como ya se indicó, una determinada representación pictórica determina unívocamente una gráfica. Sin embargo, una gráfica puede tener más de una representación pictórica. Cosas como las longitudes o curvaturas de las aristas y la posición relativa de los vértices en la página pueden variar de una representación a otra.

Ejemplo 10.1.2 Dibujo de más de una imagen de una gráfica

Considere la gráfica que se especifica de la forma siguiente:

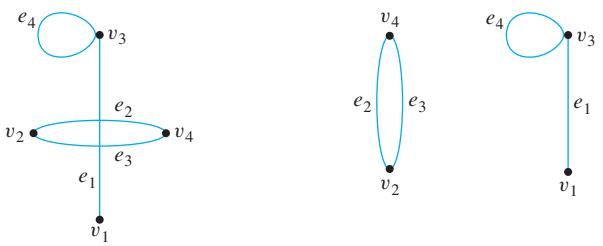
conjunto de vértices $= \{v_1, v_2, v_3, v_4\}$

conjunto de aristas $= \{e_1, e_2, e_3, e_4\}$

función punto extremo-arista:

Arista	Puntos extremos
e_1	$\{v_1, v_3\}$
e_2	$\{v_2, v_4\}$
e_3	$\{v_2, v_4\}$
e_4	$\{v_3\}$

Los dos dibujos *a*) y *b*) que se muestran a continuación son representaciones pictóricas de esta gráfica.



■

Ejemplo 10.1.3 Etiquetado de dibujos para demostrar que representan la misma gráfica

Considere los dos dibujos que se muestran en la figura 10.1.1. Etiquete los vértices y las aristas de tal manera que ambos dibujos representen la misma gráfica.

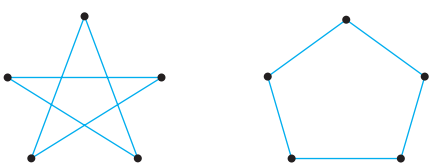
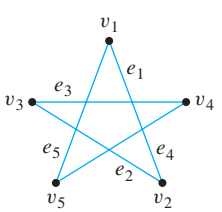
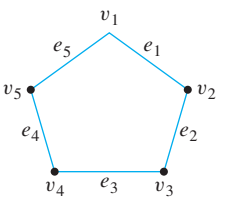


Figura 10.1.1

Solución Imagine poner el extremo de un pedazo de cuerda en el vértice superior de la figura 10.1.1*a*) (llame a este vértice v_1), después la cuerda cae al siguiente vértice adyacente en la parte inferior derecha (llame a este vértice v_2), después cae al siguiente vértice adyacente la parte superior izquierda (v_3) y así sucesivamente, regresando finalmente al vértice superior v_1. Llame a la primera arista e_1, a la segunda e_2 y así sucesivamente, como se muestra a continuación.



Ahora imagine juntar el pedazo de cuerda, junto con sus etiquetas y cambiar a la posición siguiente:



Ésta es igual a la figura 10.1.1*b*), por lo que ambos dibujos son representaciones de la gráfica con conjunto de vértices $\{v_1, v_2, v_3, v_4, v_5\}$, conjunto de aristas $\{e_1, e_2, e_3, e_4, e_5\}$ y la función de punto extremo-arista como sigue:

Arista	Punto extremo-arista
e_1	$\{v_1, v_2\}$
e_2	$\{v_2, v_3\}$
e_3	$\{v_3, v_4\}$
e_4	$\{v_4, v_5\}$
e_5	$\{v_5, v_1\}$

En el capítulo 8 analizamos el grafo dirigido de una relación binaria sobre un conjunto. La definición general de grafo dirigido es similar a la definición de grafo, salvo que se asocia un *par ordenado* de vértices a cada arista en lugar de un *conjunto* de vértices. Así cada arista de un grafo dirigido se puede dibujar como una flecha que va del primer vértice al segundo vértice del par ordenado.

• Definición

Un **grafo dirigido** o **digráfica**, consiste en dos conjuntos finitos: un conjunto no vacío $V(G)$ de vértices y un conjunto de aristas dirigidas $D(G)$, donde cada uno está asociado con un par ordenado de vértices llamado sus **puntos extremos**. Si el arista e está asociada con el par de vértices (v, w), entonces se dice que e es la arista (dirigida) de v a w.

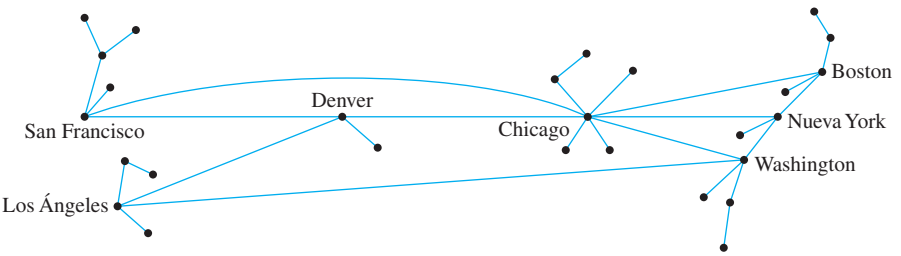
Observe que cada grafo dirigido tiene un grafo (no dirigido) ordinario asociado, que se obtiene ignorando las direcciones de las aristas.

Ejemplos de grafos

Los grafos son una poderosa herramienta para resolver problemas ya que nos permiten representar una situación compleja con una sola imagen que puede analizarse tanto visualmente y con la ayuda de una computadora. A continuación presentamos unos pocos ejemplos y en los ejercicios se incluyen otros.

Ejemplo 10.1.4 Uso de un grafo para representar una red

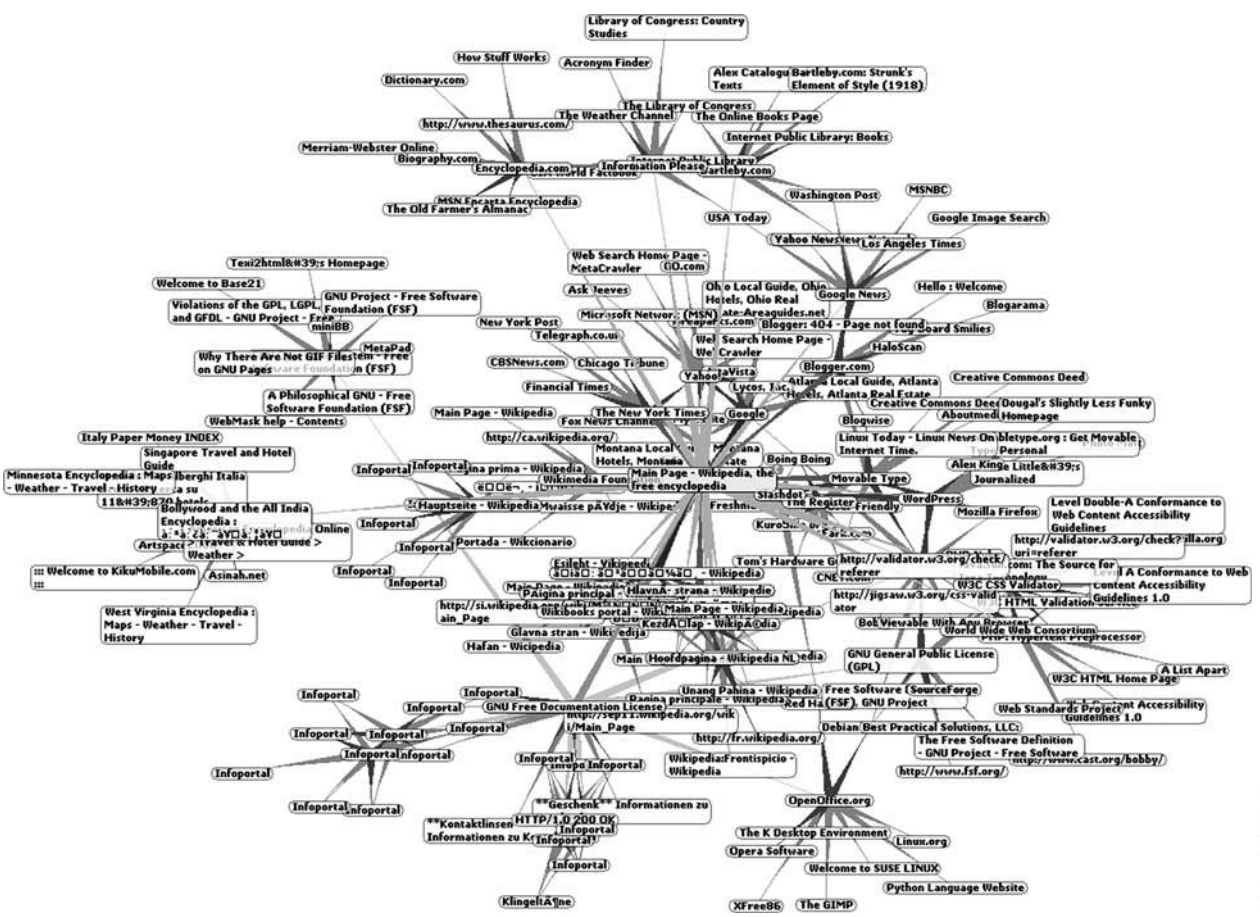
Telefonía, energía eléctrica, tuberías de gas y sistemas de transporte aéreo todos se pueden representar mediante grafos, como redes de computadoras, desde una red pequeña de área local al sistema mundial de internet que conecta a millones de computadoras en todo el mundo. Cuestiones que se plantean en el diseño de estos sistemas implican elegir aristas conectadas para minimizar los costos, optimizar un cierto tipo de servicio, etcétera. En la siguiente página, se muestra una red típica llamada un modelo radial.



Ejemplo 10.1.5 Uso de un grafo para representar a la red mundial

La red mundial (World Wide Web, www), o web, es un sistema de documentos vinculados entre sí, o páginas web, contenidas en el internet. Los usuarios empleando exploradores web, como internet Explorer, Google Chrome, Apple Safari y Opera, puede pasar rápidamente de una página web a otra haciendo clic en los hipervínculos, que utilicen versiones de software llamados protocolos de transferencia de hipertexto (HTTP). Las personas y las empresas particulares crean páginas, que transmiten a los servidores que contienen software capaz de enviarlas a quienes las solicitan a través de un navegador web. Debido a que la cantidad de información en la web es muy vasta, motores de búsqueda como Google, Yahoo y Bing, tienen algoritmos para encontrar información muy eficientemente.

La siguiente imagen muestra una fracción de minuto de las conexiones de hipervínculo en el internet que radian hacia dentro y hacia fuera de la página principal de Wikipedia.



Wikipedia/Chris 73

Ejemplo 10.1.6 Uso de un grafo para representar conocimiento

En muchas aplicaciones de inteligencia artificial, se recopila una base de conocimientos de información y se representa en una computadora. Debido a la forma del conocimiento se representa y debido a las propiedades que rigen el programa de inteligencia artificial, la computadora no se limita a recuperar los datos de la misma forma que los introdujo; también pueden deducir nuevos hechos en base a los conocimientos mediante el uso de ciertas reglas de inferencia integradas. Por ejemplo, a partir de conocer que *Los Angeles Times* es diario de una gran ciudad y que un diario de una gran ciudad contiene noticias nacionales, un programa de inteligencia artificial puede inferir que *Los Angeles Times* contiene noticias nacionales. El grafo dirigido que se muestra en la figura 10.1.2 es una representación gráfica de una base de datos simplificada de publicaciones periódicas.

De acuerdo con esta base de conocimientos, ¿qué acabado de papel utiliza el *Nueva York Times*?

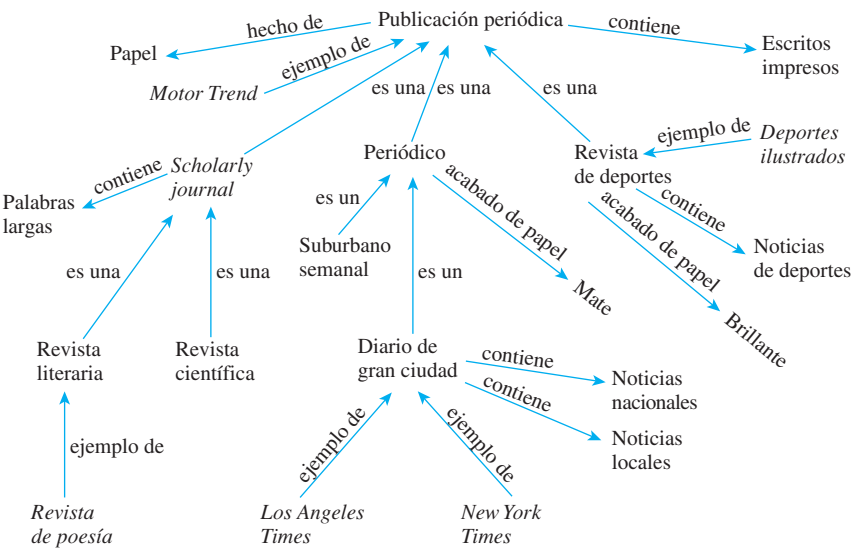


Figura 10.1.2

Solución La flecha que va del *New York Times* al diario de la gran ciudad (etiquetada como "ejemplo de") muestra que el *New York Times* es un diario de gran ciudad. La flecha va de diario de gran ciudad a periódico (con la etiqueta "es un") muestra que un diario de gran ciudad es un periódico. La flecha va de periódico a mate (etiquetada "acabado del papel") indica que el acabado del papel en un periódico es mate. Por tanto se puede inferir que el acabado de papel en el *New York Times* es mate. ■

Ejemplo 10.1.7 Uso de un grafo para resolver un problema: vegetarianos y caníbales

La siguiente es una variación de un famoso rompecabezas usado con frecuencia como un ejemplo en el estudio de inteligencia artificial. Se trata de una isla en la que todas las personas son de uno de dos tipos, vegetarianos o caníbales. Inicialmente, dos vegetarianos y dos caníbales están en la orilla izquierda del río. Con ellos está un barco que puede contener un máximo de dos personas. El objetivo del rompecabezas es encontrar una forma de transportar a todos los vegetarianos y caníbales a la orilla derecha del río. Lo que hace difícil es que en ningún momento puede el número de caníbales en cualquier orilla superar al número de vegetarianos. De lo contrario, les ¡sucedería un desastre a los vegetarianos!

Solución Una forma sistemática de abordar este problema es introducir una notación que puede indicar todos los posibles arreglos de vegetarianos, caníbales y el barco a orillas

del río. Por ejemplo, podría escribir (vvc/Bc) para indicar que hay dos vegetarianos y un caníbal en la orilla izquierda y un caníbal y el barco en la orilla derecha. Entonces $(vvccB/)$ indicaría la posición inicial en la que tanto dos vegetarianos, como dos caníbales y el barco se encuentran en la orilla izquierda del río. El objetivo del rompecabezas es entender una secuencia de movimientos para alcanzar la posición $(/Bvvcc)$ en la que tanto dos vegetarianos, como dos caníbales y el barco se encuentran en la orilla derecha del río.

Para construir un grafo cuyos vértices son los diferentes arreglos a los que se pueden llegar en una secuencia de movimientos válidos a partir de la posición inicial. Conecte al vértice x con el vértice y si es posible alcanzar al vértice y con un movimiento válido desde el vértice x. Por ejemplo, desde la posición inicial hay cuatro movimientos válidos: un vegetariano y un caníbal pueden tomar el barco en la orilla derecha; dos caníbales pueden tomar el barco en la orilla derecha; un caníbal puede tomar el barco en la orilla derecha; o los dos vegetarianos pueden tomar el barco en la orilla derecha. Puede mostrar esto dibujando aristas que conecten los vértices $(vvccB/)$ con los vértices (vc/Bvc), (vv/Bcc), $(vvcBc)$ y (cc/Bvv). (Puede parecer natural dibujar flechas en lugar de rectas de un vértice a otro. La justificación para dibujar flechas es que cada movimiento válido es reversible.) De la posición (vc/Bvc), los movimientos válidos sólo son volver a $(vvccB/)$ o ir a $(vvcB/c)$. También se pueden mostrar dibujando aristas. Continúe este proceso hasta que finalmente llegue a $(/Bvvcc)$. De la figura 10.1.3 resulta evidente que una secuencia exitosa de movimientos es $(vvccB/) \rightarrow (vc/Bvc) \rightarrow (vvcB/c) \rightarrow (c/Bvvc) \rightarrow (ccB/vv) \rightarrow (/Bvvcc)$.

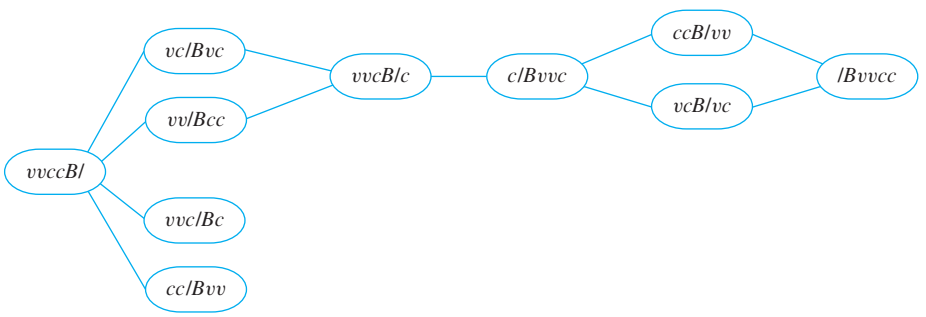


Figura 10.1.3

Grafos especiales

Una clase importante de grafos se compone de aquellas que no tienen ningún bucle o aristas paralelas. Estos grafos se denominan *simples*. En un grafo simple, no hay dos aristas que compartan el mismo conjunto de puntos extremos, para especificar los dos puntos extremos es suficiente con determinar una arista.

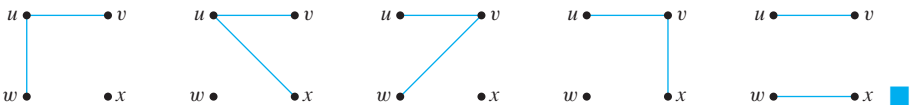
• Definición y notación

Un **grafo simple** es un grafo que no tiene ningún bucle o aristas paralelas. En un grafo simple, una arista con puntos extremos v y w se denota por $\{v, w\}$.

Ejemplo 10.1.8 Un grafo simple

Dibuje todos los grafos simples con cuatro vértices $\{u, v, w, x\}$ y dos aristas, una de los cuales es $\{u, v\}$.

Solución Cada posible arista de un grafo simple corresponde a un subconjunto de dos vértices. Dados cuatro vértices, hay $\binom{4}{2} = 6$ de dichos subconjuntos en total: $\{u, v\}$, $\{u, w\}$, $\{u, x\}$, $\{v, w\}$, $\{v, x\}$ y $\{w, x\}$. Ahora se especifica una arista del grafo como $\{u, v\}$, por lo que cualquiera de las restantes cinco de esta lista se puede elegir como la segunda arista. En la página siguiente se muestran las posibilidades.



Otra clase importante de grafos consiste de aquellas que están "completas" en el sentido de que todos los pares de vértices están conectados por aristas.

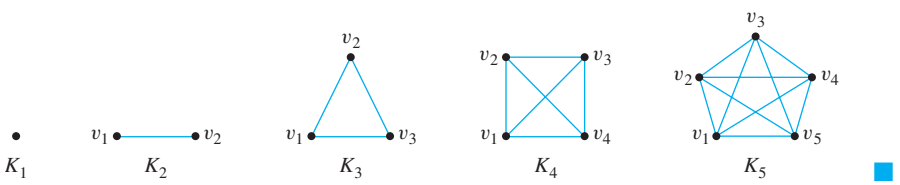
Nota La K se pone por la palabra alemana *komplett*, que significa "completo".

• Definición

Sea n un entero positivo. Un **grafo completo de n vértices**, que se denota por $\boldsymbol{K_n}$, es un grafo simple con n vértices y exactamente una arista conectando a cada par de vértices distintos.

Ejemplo 10.1.9 Grafos completos en n vértices: K_1, K_2, K_3, K_4, K_5

Los grafos completos K_1, K_2, K_3, K_4 y K_5 se pueden dibujar como:



En otra clase de grafos, los vértices de conjunto pueden separarse en dos subconjuntos: Cada vértice en uno de los subconjuntos está conectado por exactamente una arista para cada vértice en el otro subconjunto, pero no a cualquier vértice en su propio subconjunto. Dicho grafo se llama *completa bipartita*.

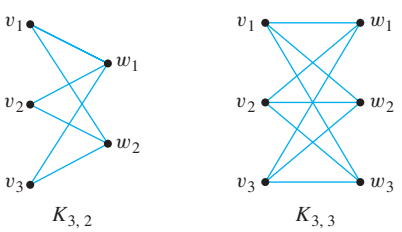
• Definición

Sean m y n enteros positivos. Un **grafo completo bipartito de vértices (m, n)**, que se denota por $\boldsymbol{K_{m,\,n}}$, es un grafo simple con vértices distintos $v_1, v_2, \ldots, v_m$ y $w_1, w_2, \ldots, w_n$ que satisface las siguientes propiedades: Para todos $i, k = 1, 2, \ldots, m$ y para todos $j, l = 1, 2, \ldots, n$,

1. Hay una arista de cada vértice v_i, a cada vértice w_j.
2. No hay arista de cualquier vértice v_i a cualquier otro vértice v_k.
3. No hay arista de cualquier vértice w_j a cualquier otro vértice w_l.

Ejemplo 10.1.10 Gráficas bipartitas completas: $K_{3,2}$ y $K_{3,3}$

A continuación se muestran, las gráficas bipartitas completas $K_{3,2}$ y $K_{3,3}$.



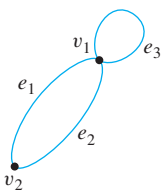
• Definición

Se dice que un grafo H es un **subgrafo** de un grafo G si y sólo si, cada vértice en H es también un vértice en G, cada arista en H es también una arista en G y cada arista en H tiene los mismos puntos extremos de G.

Ejemplo 10.1.11 Subgrafos

Enumere todos los subgrafos del grafo G con conjunto de vértices $\{v_1, v_2\}$ y conjunto de aristas $\{e_1, e_2, e_3\}$, donde los puntos extremos de e_1 son v_1 y v_2, los puntos extremos de e_2 son v_1 y v_2 y e_3 es un bucle en v_1.

Solución G se puede dibujar como se muestra a continuación.



Hay 11 subgrafos de G, que pueden agruparse de acuerdo con aquellas que no tienen arista, a aquellas que tienen una arista, a aquellas que tienen dos aristas y a aquellas que tienen tres aristas. En la figura 10.1.4 se muestran las 11 subgráficas.

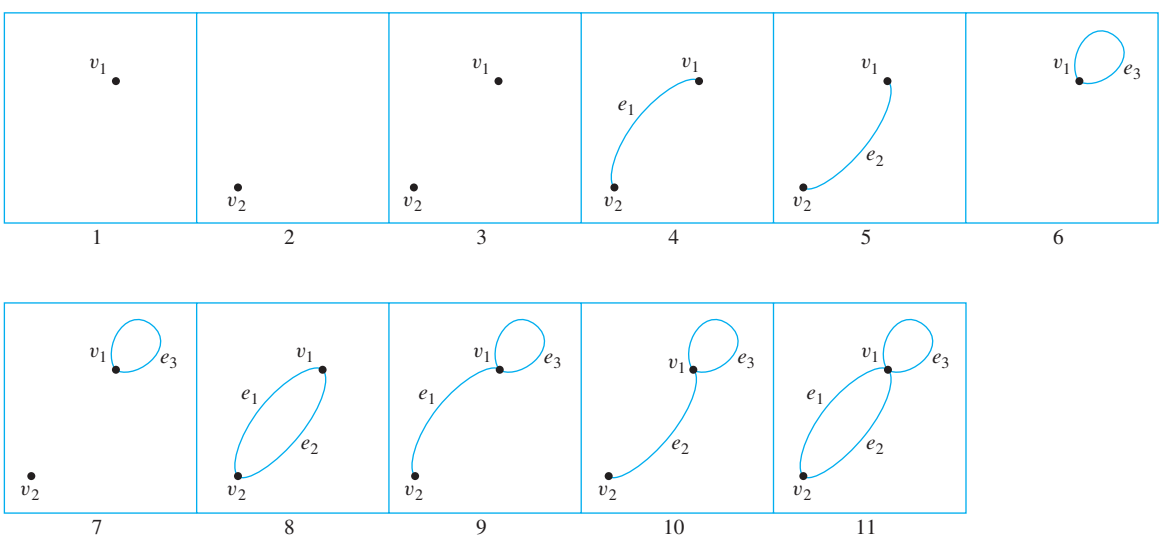


Figura 10.1.4

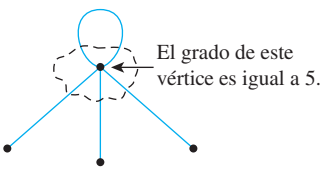
El concepto de grado

El *grado de un vértice* es el número de segmentos extremos de aristas que "salen del" vértice. Vamos a demostrar que la suma de los grados de todos los vértices en un grafo es dos veces el número de aristas en el grafo.

• Definición

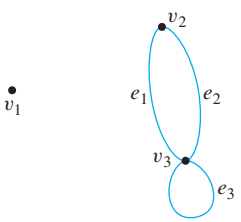
Sea G un grafo y v un vértice de G. El **grado de v**, que se denota por **deg(v)**, es igual al número de aristas que inciden en v, con una arista que es un bucle contado dos veces; El **grado total de G** es la suma de los grados de todos los vértices de G.

Ya que una arista que es un bucle se cuenta dos veces, el grado de un vértice puede obtenerse dibujando un grafo contando cuántos segmentos finales de aristas están incidiendo en el vértice. Esto se ilustra a continuación.



Ejemplo 10.1.12 Grado de un vértice y el grado total de un grafo

Encuentre el grado de cada vértice de la gráfica G que se muestra a continuación. Después encuentre el grado total de G.



Solución

$\deg(v_1) = 0$ ya no hay arista que incida en v_1 (v_1 está aislado).

$\deg(v_2) = 2$ ya que tanto e_1 como e_2 inciden en v_2.

$\deg(v_3) = 4$ ya que tanto e_1 como e_2 inciden en v_3 y el bucle e_3 también incide en v_3 (y contribuye con 2 al grado de v_3).

Grado total de $G = \deg(v_1) + \deg(v_2) + \deg(v_3) = 0 + 2 + 4 = 6$. ■

Observe que el grado total del grafo G del ejemplo 10.1.12, que es 6, equivale a dos veces el número de aristas de G, que es 3. En términos generales, esto es porque cada arista tiene dos segmentos extremos y cada segmento final se cuenta una vez para el grado de algunos vértices. Este resultado se generaliza en cualquier grafo.

De hecho, para cualquier grafo sin bucles, el resultado general se puede explicar como sigue: Imagine un grupo de personas en una fiesta. Dependiendo de cuántos amigos tiene, cada persona saluda de mano a otras diferentes personas. Por lo que cada persona participa en un cierto número de saludos de mano —quizá muchas, quizá ninguna— pero ya que cada saludo se da por dos personas diferentes, si se suman los números experimentados por cada persona, la suma será igual a dos veces el número total de saludos de mano. Esto es una forma de entender el porqué el teorema siguiente se llama el *lema del saludo de mano* o el *teorema del saludo de mano*. Como muestra la demostración, la conclusión es verdadera aún si el grafo contiene bucles.

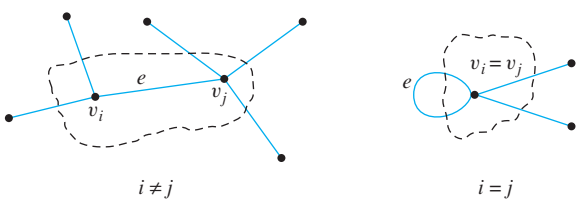
Teorema 10.1.1 El teorema del saludo de mano

Si G es cualquier grafo, entonces la suma de los grados de todos los vértices de G es dos veces el número de aristas de G. Específicamente, si los vértices de G son v_1, $v_2, \ldots, v_n$, donde n es un entero no negativo, entonces

$$\begin{aligned}\text{el grado total de } G &= \deg(v_1) + \deg(v_2) + \cdots + \deg(v_n)\\ &= 2 \cdot (\text{el número de aristas de } G).\end{aligned}$$

Demostración:

Sea G un grafo particular que se elige arbitrariamente y suponga que G tiene n vértices $v_1, v_2, \ldots, v_n$ y m aristas, donde n es un entero positivo y m es un entero no negativo. Pretendemos que cada arista de G contribuya en 2 al grado total de G. Se supone que e es una arista arbitrariamente elegida con puntos extremos v_i y v_j. Esta arista contribuye con 1 al grado de v_i y con 1 al grado v_j. Como se muestra a continuación, es verdadero aún si $i = j$ ya que se cuenta dos veces una arista que es un bucle en el cálculo del grado del vértice en el que incide.



Por tanto, e contribuye con 2 al grado total de G. Ya que e se escogió arbitrariamente, esto muestra que *cada* arista de G contribuye con 2 al grado total de G. Por tanto

$$\text{el grado total de } G = 2 \cdot (\text{el número de aristas de } G).$$

El corolario siguiente es una consecuencia inmediata del teorema 10.1.1.

Corolario 10.1.2

El grado total de un grafo es par.

Demostración:

Por el teorema 10.1.1 el grado total de G es igual a 2 veces el número de aristas, que es un entero y así el grado total de G es par.

Ejemplo 10.1.13 Determinación de si ciertos grafos existen

Dibuje un grafo con las propiedades dadas o muestre que ese grafo no existe.

a. Un grafo con cuatro vértices de grado 1, 1, 2 y 3

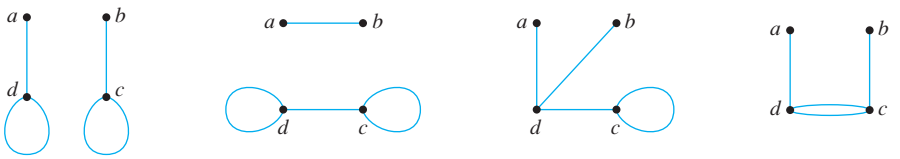
b. Un grafo con cuatro vértices de grados 1, 1, 3 y 3

c. Un grafo simple con cuatro vértices de grados 1, 1, 3 y 3

Solución

a. No es posible dicho grafo. Por el corolario 10.1.2, el grado total de un grafo es par. Pero un grafo con cuatro vértices de grados 1, 1, 2 y 3 tendría un grado total de $1 + 1 + 2 + 3 = 7$, que es impar.

b. Sea G cualquiera de los grafos que se muestra a continuación.

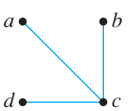


En cada caso, independientemente de cómo se etiquetan las aristas, $\deg(a) = 1$, $\deg(b) = 1$, $\deg(c) = 3$ y $\deg(d) = 3$.

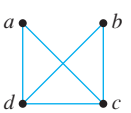
c. No hay grafo simple con cuatro vértices de grado 1, 1, 3 y 3.

Demostración (por contradicción):

Suponga que había un grafo simple G con cuatro vértices de grado 1, 1, 3 y 3. Llame a a y b los vértices de grado 1 y llame a c y d los vértices de grado 3. Ya que $\deg(c) = 3$ y G no tiene bucles o aristas paralelas (porque es simple), debe haber aristas que conecten c con a, b y d.



Por el mismo razonamiento, debe haber aristas que conectan a d con a, b y c.



Pero entonces $\deg(a) \geq 2$ y $\deg(b) \geq 2$, lo que contradice la suposición de que estos vértices tienen grado 1. Por tanto la suposición es falsa y en consecuencia no existe algún grafo simple con cuatro vértices de grado 1, 1, 3 y 3. ■

Ejemplo 10.1.14 Aplicación de un grafo conocido

¿Es posible formar en un grupo de nueve personas para cada cinco amigos con otros cinco exactamente?

Solución La respuesta es no. Imagine que construye un "grafo conocido" cada una de las nueve personas se representan con un vértice y dos vértices se unen con una arista si y sólo si, los que representan son amigos. Suponga que cada una de las personas eran amigos con otras cinco exactamente. Entonces cinco sería el grado de cada uno de los nueve vértices del grafo y así el grado total del grafo sería 45. Pero esto contradice el corolario 10.1.2, que dice que el grado total de un grafo es par. Esta contradicción muestra que la suposición es falsa y por tanto es imposible que cada persona en un grupo de nueve personas sean amigos de otras cinco exactamente. ■

La siguiente proposición se deduce fácilmente del corolario 10.1.2 utilizando las propiedades de los enteros pares e impares.

Proposición 10.1.3

En cualquier grafo hay un número par de vértices de grado impar.

Demostración:

Suponga que G es cualquier grafo y suponga que G tiene n vértices de grado impar y m vértices de grado par, donde n es un entero positivo y m es un entero no negativo. *[Tenemos que demostrar que n es par.]* Sea E la suma de los grados de todos los vértices de grado par, O la suma de los grados de todos los vértices de grado impar y T el grado total de G. Si $u_1, u_2, \ldots, u_m$ son los vértices de grado par y $v_1, v_2, \ldots, v_n$ son los vértices de grado impar, entonces

$$E = \deg(u_1) + \deg(u_2) + \cdots + \deg(u_m),$$
$$O = \deg(v_1) + \deg(v_2) + \cdots + \deg(v_n) \quad \text{y}$$
$$T = \deg(u_1) + \cdots + \deg(u_m) + \deg(v_1) + \cdots + \deg(v_n) = E + O.$$

Ahora T, el grado total de G, es un entero par por el corolario 10.1.2. También E es par ya que E es cero, que es par, o E es una suma de los números $\deg(u_i)$, cada uno de los cuales es par. Pero

$$T = E + O,$$

y por tanto

$$O = T - E.$$

Por lo que O es una diferencia de dos enteros pares y así O es par.

Suponiendo que, $\deg(v_i)$ es impar para toda $i = 1, 2, \ldots, n$. Por tanto O, entero par, es una suma de n enteros impares, $\deg(v_1), \deg(v_2), \ldots, \deg(v_n)$. Pero si una suma de enteros n impares es par, entonces n es par (vea el ejercicio 32 del final de esta sección). Por tanto, n es par *[como se quería demostrar]*.

Ejemplo 10.1.15 Aplicación del hecho de que el número de vértices con grado impar es par

¿Hay un grafo con diez vértices de grado 1, 1, 2, 2, 2, 3, 4, 4, 4 y 6?

Solución No. Dicho grafo tendría tres vértices de grado impar, lo que es imposible por la proposición 10.1.3.

Observe que este mismo resultado se podría deducir directamente del corolario 10.1.2 calculando el grado total ($1 + 1 + 2 + 2 + 2 + 3 + 4 + 4 + 4 + 6 = 29$) y observando que es impar. Sin embargo, usando la proposición 10.1.3 se obtiene el resultado sin necesidad de realizar esta suma. ■

Autoexamen

Las respuestas a las preguntas del autoexamen se encuentran al final de cada sección.

1. Un grafo consiste de dos conjuntos finitos: _____ y _____ donde cada arista está asociada con un conjunto compuesto de _____.
2. Un bucle en un grafo es _____.
3. Dos aristas distintas en un grafo son paralelas si y sólo si, _____.
4. Dos vértices se denominan adyacentes si y sólo si _____.
5. Una arista está incidiendo sobre _____.
6. Dos aristas que inciden en el mismo punto extremo son _____.
7. Un vértice en el que no hay aristas que sean incidentes es _____.
8. En un grafo dirigido, cada arista está asociada con _____.
9. Un grafo simple es _____.
10. Un grafo completo de n vértices es un _____.
11. Un grafo bipartito completo de vértices (m, n) es un grafo simple cuyos vértices se pueden particionar en dos conjuntos disjuntos

V_1 y V_2 de tal manera que (1) cada uno de los m vértices en V_1 es _____ para cada uno de los n vértices en V_2, ningún vértice en V_1 está conectado a _____ y ningún vértice en V_2 está conectado a_____.

12. Un grafo H es un subgrafo de un grafo G si y sólo si, (1) _____, (2) _____ y (3) _____.

13. El grado de un vértice en un grafo es _____.

14. El grado total de un grafo se define como _____.

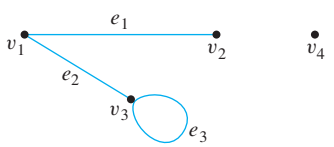
15. El teorema del saludo de mano dice que el grado total de un grafo es _____.

16. En cualquier grafo el número de vértices de grado impar es _____.

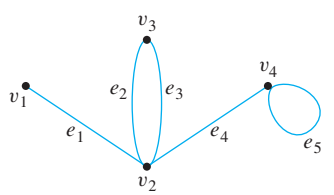
Conjunto de ejercicios 10.1*

En los ejercicios 1 y 2, los grafos se representan con dibujos. Defina cada grafo formalmente especificando su conjunto de vértices, su conjunto de aristas y una tabla que dé la función de punto extremo-arista.

1.



2.



En los ejercicios 3 y 4, dibuje las imágenes de los grafos dados.

3. El grafo G tiene el conjunto de vértices $\{v_1, v_2, v_3, v_4, v_5\}$ y el conjunto de aristas $[e_1, e_2, e_3, e_4\}$, con la función de punto extremo-arista definida como sigue:

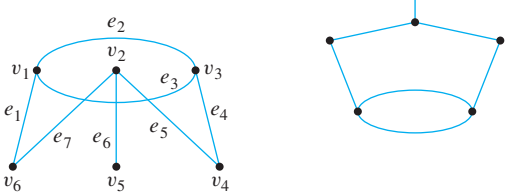
Arista	Puntos extremos
e_1	$\{v_1, v_2\}$
e_2	$\{v_1, v_2\}$
e_3	$\{v_2, v_3\}$
e_4	$\{v_2\}$

4. El grafo H tiene el conjunto de vértices $\{v_1, v_2, v_3, v_4, v_5\}$ y el conjunto de aristas $[e_1, e_2, e_3, e_4\}$, con la función de punto extremo-arista definida como sigue:

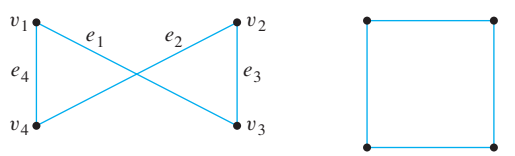
Arista	Puntos extremos
e_1	$\{v_1\}$
e_2	$\{v_2, v_3\}$
e_3	$\{v_2, v_3\}$
e_4	$\{v_1, v_5\}$

En los ejercicios del 5 al 7, demuestre que los dos dibujos representan la misma gráfica etiquetando los vértices y las aristas del lado derecho para dibujar los correspondientes a los del dibujo de la izquierda.

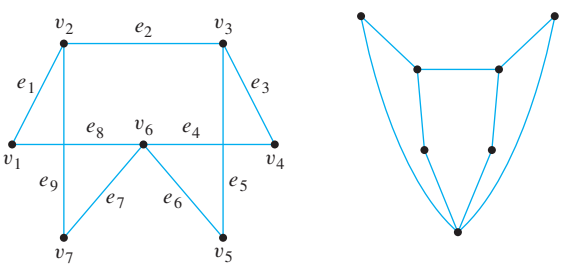
5.



6.



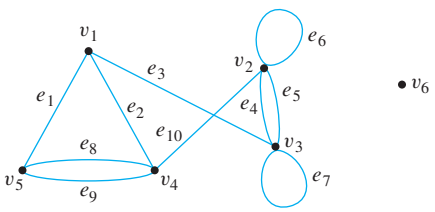
7.



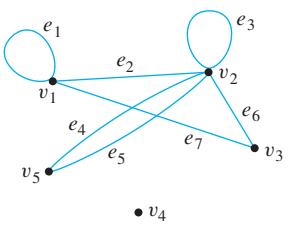
*Para los ejercicios con números o letras azules, las soluciones están dadas en el apéndice B. El símbolo ***H*** indica que sólo se da una sugerencia o una solución parcial. El símbolo ✶ indica que el ejercicio es más difícil de lo normal.

Para cada uno de los grafos en los ejercicios 8 y 9:
i) Determine todas las aristas que inciden en v_1.
ii) Encuentre todos los vértices adyacentes a v_3.
iii) Busque todas las aristas adyacentes a e_1.
iv) Determine todos los bucles.
v) Encuentre todas las aristas paralelas.
vi) Encuentre todos los vértices aislados,
vii) Determine el grado de v_3.
viii) Encuentre el grado total del grafo.

8.



9.



10. Use el grafo del ejemplo 10.1.6 para determinar
a. si *Deportes ilustrados* contiene escritos impresos;
b. si *Revista de poesía* contiene palabras largas.

11. Encuentre tres otras secuencias ganadoras de movimientos para los vegetarianos y los caníbales en el ejemplo 10.1.7.

12. Otro rompecabezas famoso utilizado como un ejemplo en el estudio de inteligencia artificial parece que primero apareció en una colección de problemas, *Problemas para el desafío de la mente*, que fue compilado en el 775 d.C. Implica un lobo, una cabra, una bolsa de col y un barquero. Desde una posición inicial en la orilla izquierda del río, el barquero está transportando al lobo, a la cabra y la col a la orilla derecha. La dificultad es que la nave del barquero sólo es lo suficientemente grande como para que él se transporte con un objeto, además de sí mismo a la vez. Sin embargo, por razones obvias, el lobo no se puede quedar solo con la cabra y la cabra no puede quedarse sola con la col. ¿Cómo debe proceder el barquero?

13. Resuelva el rompecabezas de los vegetarianos y caníbales para el caso donde hay tres vegetarianos y tres caníbales transportándose de un lado de un río al otro.

***H* 14.** Dos jarras A y B tienen capacidades de 3 cuartos y 5 cuartos de galón, respectivamente. ¿Puede utilizar las jarras para medir exactamente 1 litro de agua, mientras que sigue las siguientes restricciones? Puede llenar una jarra con la capacidad de un grifo de agua; puede vaciar el contenido de una jarra en un desagüe; y puede verter agua de una jarra en el otro.

15. Un grafo tiene vértices de grados 0, 2, 2, 3 y 9. ¿Cuántas aristas tiene el grafo?

16. Un grafo tiene vértices de grado 1, 1, 4 y 6. ¿Cuántas aristas tiene el grafo?

En cada uno de los ejercicios de los 17 al 25, dibuje un grafo con las propiedades dadas o explique por qué no existe dicho grafo.

17. Trace el grafo con cinco vértices de grados 1, 2, 3, 3 y 5.

18. Trace el grafo con cuatro vértices de grados 1, 2, 3 y 3.

19. Trace el grafo con cuatro vértices de grado 1, 1, 1 y 4.

20. Trace el grafo con cuatro vértices de grados 1, 2, 3 y 4.

21. Trace el grafo simple con cuatro vértices de grados 1, 2, 3 y 4.

22. Trace el grafo simple con cinco vértices de grados 2, 3, 3, 3 y 5.

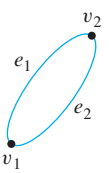
23. Trace el grafo simple con cinco vértices de grado 1, 1, 1, 2 y 3.

24. Trace el grafo simple con seis aristas y todos los vértices de grado 3.

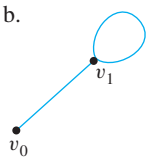
25. Trace el grafo simple con nueve aristas y todos los vértices de grado 3.

26. Determine todos los subgrafos de cada uno de los grafos siguientes.

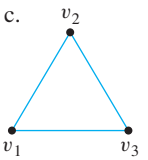
a.



b.



c.



27. **a.** En un grupo de 15 personas, ¿es posible que cada persona tenga exactamente 3 amigos? Explique. (Suponga que la amistad es una relación simétrica: Si x es un amigo de y, entonces y es un amigo de x).
b. En un grupo de cuatro personas, ¿es posible que cada persona tenga exactamente 3 amigos? ¿Por qué?

28. En un grupo de 25 personas, ¿es posible que cada uno salude de mano exactamente a otras 3 personas? Explique.

29. ¿Existe un grafo simple, cada uno de cuyos vértices tiene grado par? Explique.

30. Supongamos que G es un grafo con vértices v y aristas e y el grado de cada vértice es al menos $d_{\text{mín}}$ y a lo más $d_{\text{máx}}$. Demuestre que

$$\frac{1}{2}d_{\text{mín}} \cdot v \leq e \leq \frac{1}{2}d_{\text{máx}} \cdot v,$$

31. Demuestre que cualquier suma de un número impar de enteros impares es impar.

***H* 32.** Deduzca el ejercicio 31 que para cualquier entero positivo n, si hay una suma de n enteros impares que es par, entonces n es par.

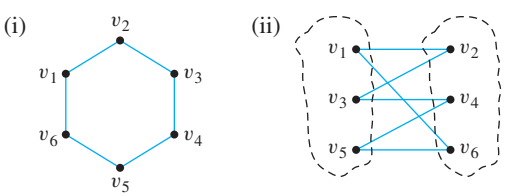
33. Recuerde que K_n denota un grafo completo con n vértices.
a. Dibuje K_6.
***H* b.** Demuestre que para todos los enteros $n \geq 1$, el número de aristas de K_n es $\dfrac{n(n-1)}{2}$.

34. Utilice el resultado del ejercicio 33 para demostrar que el número de aristas de un grafo simple con n vértices es menor o igual a $\dfrac{n(n-1)}{2}$.

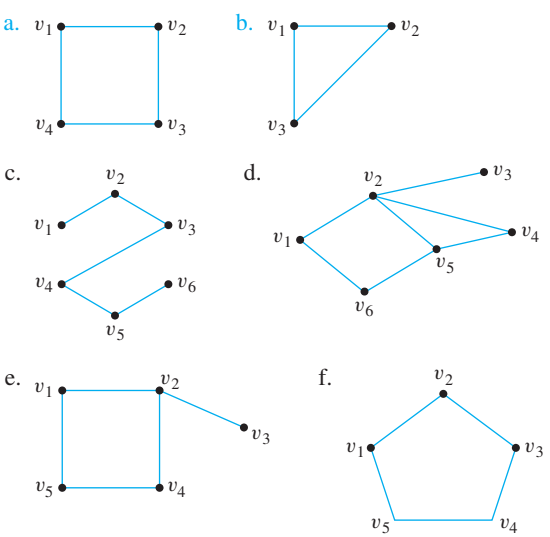
35. ¿Hay un grafo simple con el doble de aristas que de vértices? Explique. (Puede encontrar útil usar el resultado del ejercicio 34).

36. Recuerde que $K_{m,n}$ denota un grafo bipartito completo de vértices (m, n).
   a. Dibuje $K_{4,2}$
   b. Dibuje $K_{1,3}$
   c. Dibuje $K_{3,4}$
   d. ¿Cuántos vértices de $K_{m,n}$ tienen grado m?, ¿grado n?
   e. ¿Cuál es el grado total de $K_{m,n}$?
   f. Encuentre una fórmula de m y n el número de aristas de $K_{m,n}$. Explique.

37. Un **grafo bipartito** G es un grafo simple cuyos vértices de conjunto pueden dividirse en dos subconjuntos no vacíos disjuntos V_1 y V_2 los vértices en V_1 se pueden conectar con los vértices en V_2, pero ningún vértice en V_1 está conectado con otros vértices en V_1 y ningún vértice en V_2 está conectado con otros vértices en V_2. Por ejemplo, el grafo G que se muestra en (i) se puede dibujar como se muestra en (ii). Del dibujo en (ii), se puede ver que G es bipartita con conjuntos de vértice mutuamente disjuntos $V_1 = \{v_1, v_3, v_5\}$ y $V_2 = \{v_2, v_4, v_6\}$.

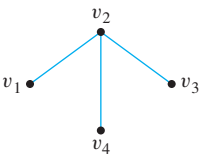


Encuentre cuál de los siguientes grafos son bipartitos. Vuelva a dibujar los grafos bipartitos que su naturaleza bipartita es evidente.

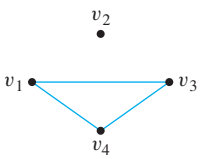


38. Suponga que r y s son enteros positivos cualesquiera. ¿Existe un grafo G con la propiedad de que G tenga vértices de grados r y s y de ningún otro grado? Explique.

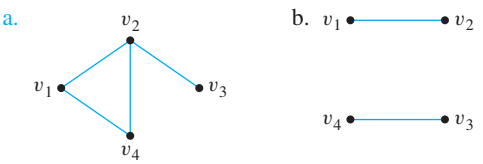
Definición: Si G es un grafo simple, el **complemento de G**, se denota G', se obtiene como sigue: El conjunto de vértices de G' es idéntico al conjunto de vértices G. Sin embargo, dos vértices distintos v y w de G' están conectados por una arista si y sólo si, v y w no están conectados por una arista en G. Por ejemplo, si G es el grafo



entonces G' es



39. Encuentre el complemento de cada una de los siguientes grafos.



40. a. Encuentre el complemento del grafo K_4, el grafo completo en cuatro vértices. (Vea el ejemplo 10.1.9.)
   b. Determine el complemento del grafo $K_{3,2}$, el grafo bipartito completo en los vértices (3, 2). (Vea el ejemplo 10.1.10.)

41. Suponga que en un grupo de cinco personas A, B, C, D y E los siguientes pares de personas se conocen entre sí: A y C, A y D, B y C, C y D, C y E.
   a. Dibuje un grafo para representar esta situación.
   b. Dibuje un grafo que muestre quienes entre estas cinco personas que *no* se conocen. Es decir, dibuje una arista entre dos personas si y sólo si, no se conocen.

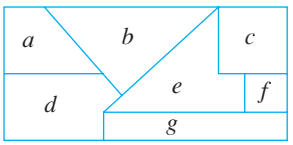
***H* 42.** Sea G un grafo simple con n vértices. ¿Cuál es la relación entre el número de aristas de G y el número de aristas del complemento del G'?

43. Demuestre que en una fiesta con al menos dos personas, hay al menos dos conocidos mutuos o por lo menos dos extraños mutuos.

44 a. En un grafo simple, ¿debe cada vértice tener un grado menor que el número de vértices en el grafo? ¿Por qué?
   b. ¿Puede haber un grafo simple que tenga cuatro vértices de diferentes grados?
***H* ✶ c.** Puede existir un grafo simple que tenga n vértices de diferentes grados?

***H* ✶ 45.** En un grupo de dos o más personas, ¿siempre deben por lo menos dos personas conocerse con el mismo número de personas dentro del grupo? ¿Por qué?

46. Imagine que el diagrama que se muestra a continuación es un mapa con los países etiquetados de *a* a *g*. ¿Es posible colorear el mapa con sólo tres colores de modo que no hay dos países adyacentes que tengan el mismo color? Para responder a esta pregunta, dibuje y analice un grafo en el que cada país está representado por un vértice y dos vértices están conectados por una arista si y sólo si los países comparten una frontera común.



***H* 47.** En este ejercicio se utiliza un grafo para ayudar a resolver un problema de programación. Doce miembros de la facultad de matemática dan servicio en los siguientes comités:

Educación de pregrado: Tenner, Peterson, Kashina, Cohen

Educación de graduados: Gatto, Yang, Cohen, Catoiu

Coloquio: Sahin, McMurry, Ash

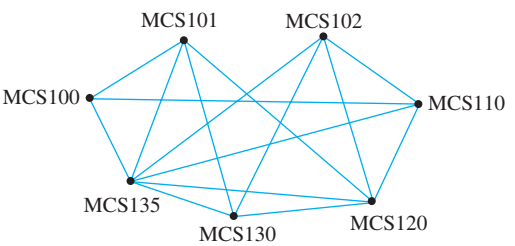
Biblioteca: Cortzen, Tenner, Sahin

Contratación: Gatto, McMurry, Yang, Peterson

Personal: Yang, Wang, Cortzen

Todos los comités se deben reunir durante la primera semana de clases, pero hay sólo tres intervalos de tiempo. Determine un horario que permita a todos los miembros de la Facultad asistir a las reuniones de las comisiones en las que se encuentran. Para ello, represente cada comité como vértice de un grafo y trace una arista entre dos vértices si los dos comités tienen un miembro común. Determine una forma para colorear los vértices utilizando sólo tres colores de manera que no haya dos comités que tengan el mismo color y explique cómo utilizar el resultado para programar las reuniones.

48. Un departamento quiere programar exámenes finales así que ningún estudiante tiene más de un examen en un día determinado. Los vértices del grafo que se presenta a continuación muestran los cursos que están siendo tomados por más de un estudiante, con una arista que conecta dos vértices si hay un estudiante en ambos cursos. Encuentre una forma para colorear los vértices del grafo con sólo cuatro colores así que no hay dos vértices adyacentes que tengan el mismo color y explique cómo utilizar el resultado para programar los exámenes finales.



Autoexamen

1. un conjunto finito no vacío de vértices; un conjunto de aristas; uno o dos vértices llamados sus puntos extremos 2. una arista con un solo extremo 3. tienen el mismo conjunto de puntos extremos 4. están conectados por una arista 5. cada uno de sus puntos extremos 6. adyacente 7. aislado 8. un par ordenado de vértices llamados sus puntos extremos 9. un grafo sin bucles o aristas paralelas 10. grafo simple con n vértices cuyo conjunto de aristas contiene exactamente una arista para cada par de vértices 11. conectados por una arista; cualquier otro vértice en V_1; cualquier otro vértice en V_2 12. cada vértice en H también es un vértice en G; cada arista en H también es una arista en G; cada arista en H tiene los mismos puntos extremos que en G 13. el número de aristas que incide sobre el vértice, con una arista que es un bucle contados dos veces 14. la suma de los grados de todos los vértices del grafo 15. igual al doble del número de aristas del grafo 16. un número par

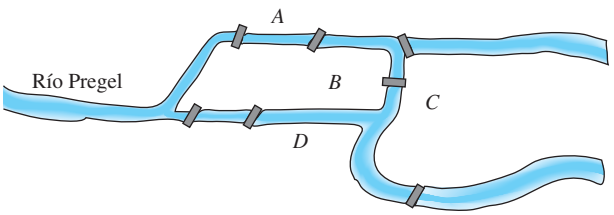
10.2 Senderos, rutas y circuitos

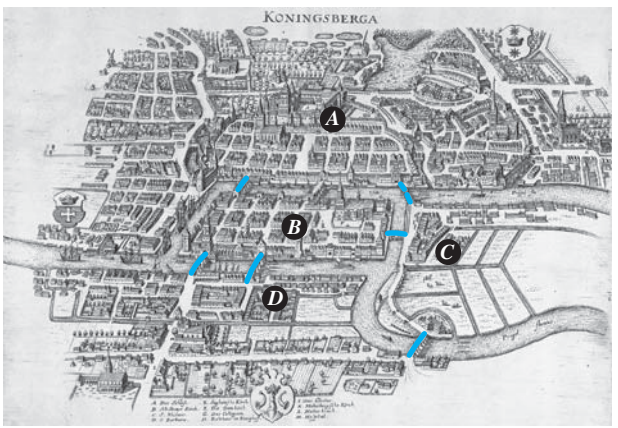
Uno puede comenzar a razonar sólo cuando se ha imaginado una imagen clara.
—W. W. Sawyer, *Mathematician's Delight*, 1943

El tema de la teoría de grafos comenzó en el año 1736 cuando el gran matemático Leonhard Euler publicó un documento presentando la solución del siguiente rompecabezas:

> La ciudad de Königsberg en Prusia (ahora Kaliningrado en Rusia) fue construida en un punto donde dos ramas del río Pregel vienen juntas. Consistía en una isla y algunas tierras a lo largo de las orillas del río. Estas se conectaron por siete puentes, como se muestra en la figura 10.2.1.
>
> La pregunta es: ¿es posible que una persona dé un recorrido por la ciudad, comenzando y terminando en la misma ubicación y cruzando cada uno de los siete puentes exactamente una vez?*

*En su artículo original, Euler no necesitaba el camino para iniciar y terminar en el mismo punto. Sin embargo, se simplifica el análisis del problema mediante la adición de esta condición. Más adelante en esta sección, analizamos caminos que comienzan y terminan en diferentes puntos.





Merian-Erben

Figura 10.2.1 **Los siete puentes de Königsberg**

Bettmann/CORBIS

Leonhar Euler
(1707-1783)

Para resolver este rompecabezas, Euler tradujo el problema en una teoría de grafos. Se dio cuenta de que todos los puntos de un terreno dado se pueden identificar con otros ya que una persona puede viajar desde cualquier punto a cualquier otro punto del mismo terreno sin cruzar un puente. Así, con el fin de resolver el rompecabezas, el mapa de Königsberg se puede identificar con el grafo que se muestra en la figura 10.2.2, en la que los vértices *A*, *B*, *C* y *D* representan terrenos y las siete aristas los siete puentes.

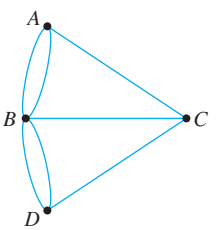


Figura 10.2.2 **Versión en grafo del mapa de Königsberg**

En términos de este grafo, la pregunta es la siguiente:

> ¿Es posible encontrar una ruta en el grafo que comience y termine en algún vértice, uno de *A*, *B*, *C* o D y que atraviese cada arista exactamente una vez?

Equivalente:

> ¿Es posible trazar este grafo, comenzando y terminando en el mismo punto, sin jamás levantar el lápiz del papel?

Dedique unos minutos para pensar la pregunta. ¿Puede encontrar una ruta que cumpla los requisitos? ¡Inténtelo!

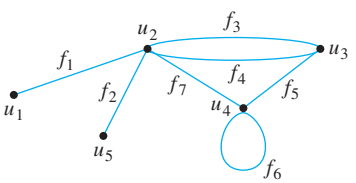
Buscar una ruta es frustrante porque se encuentra continuamente en un vértice que no tiene una arista no utilizada que dejar, mientras que en otros lugares hay aristas no utilizadas que aún se deben atravesar. Si por ejemplo, empieza en un vértice A, cada vez que atraviese el vértice *B*, *C* o *D*, utiliza hasta dos aristas porque llega en una arista y sale a otra diferente. Así, si es posible encontrar una ruta que utilice todas las aristas del grafo y que comience y termine en A, entonces el número total de llegadas y salidas de cada vértice *B*, *C* y *D* debe ser un múltiplo de 2. O, en otras palabras, los grados de los

vértices B, C y D deben ser pares. Pero no lo son: $\deg(B) = 5$, $\deg(C) = 3$ y $\deg(D) = 3$. Por lo que no hay ninguna ruta que resuelva el problema, que comience y termine en A. Se puede utilizar un razonamiento similar para mostrar que no hay rutas que resuelvan el problema, que comiencen y terminen en B, C, o D. Por tanto, es imposible viajar alrededor de la ciudad cruzando cada puente exactamente una vez.

Definiciones

Se logra viajar en un grafo moviéndose de un vértice a otro a lo largo de una sucesión de aristas adyacentes. En el grafo siguiente, por ejemplo, se puede ir de u_1 a u_4 tomando f_1 a u_2 y después, f_7 a u_4. Esto se representa escribiendo

$$u_1 f_1 u_2 f_7 u_4.$$



O usted podría tomar todo el camino

$$u_1 f_1 u_2 f_3 u_3 f_4 u_2 f_3 u_3 f_5 u_4 f_6 u_4 f_7 u_2 f_3 u_3 f_5 u_4.$$

Ciertos tipos de sucesiones de vértices adyacentes y aristas son de especial importancia en teoría de grafos: aquellos que no tienen una arista repetida, los que no tienen un vértice repetido y los que comienzan y terminan en el mismo vértice.

• Definición

Sea G un grafo y sean v y w vértices en G.

Un **camino de *v* a *w*** es una sucesión finita alternada de vértices adyacentes y aristas de G. Por tanto un camino tiene la forma

$$v_0 e_1 v_1 e_2 \cdots v_{n-1} e_n v_n,$$

donde las v representan vértices, las e representan aristas, $v_0 = v$, $v_n = w$ y para toda $i = 1, 2, \ldots n$, v_{i-1} y v_i son los puntos extremos de e_i. **El camino trivial de *v* a *v*** consiste del único vértice v.

Un **sendero de *v* a *w*** es un camino de v a w que no contiene una arista repetida.

Una **trayectoria de *v* a *w*** es un sendero que no contienen un vértice repetido.

Un **camino cerrado** es un camino que comienza y termina en el mismo vértice.

Un **circuito** es un camino cerrado que contiene al menos una arista y no contiene una arista repetida.

Un **circuito simple** es un circuito que no tiene cualquier otro vértice repetido excepto el primero y el último.

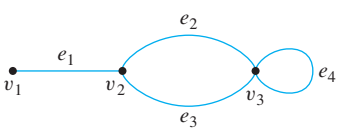
Para referencia fácil, estas definiciones se resumen en la tabla siguiente:

	¿Arista repetida?	¿Vértice repetido?	¿Inicia y finaliza en el mismo punto?	¿Debe contener al menos una arista?
Camino	permitido	permitido	permitido	no
Sendero	no	permitido	permitido	no
Trayectoria	no	no	no	no
Camino cerrado	permitido	permitido	sí	no
Circuito	no	permitido	sí	sí
Circuito simple	no	sólo primero y último	sí	sí

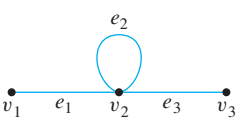
A menudo un camino se puede especificar claramente con una sucesión de aristas o una sucesión de vértices. Los siguientes ejemplos muestran cómo se hace.

Ejemplo 10.2.1 Notación para caminos

a. En el grafo que se muestra a continuación, la notación $e_1e_2e_4e_3$, se refiere claramente al camino siguiente: $v_1e_1v_2e_2v_3e_4v_3e_3v_2$. Por otro lado, la notación e_1 es ambigua si se utiliza para referirse a un camino. Podría significar $v_1e_1v_2$ o $v_2e_1v_1$.



b. En el grafo del inciso *a*), la notación v_2v_3 es ambigua, si se utiliza para referirse a un camino. Podría significar $v_2e_2v_3$ o $v_2e_3v_3$. Por otra parte, en el grafo siguiente, la notación $v_1v_2v_2v_3$ se refiere claramente al camino $v_1e_1v_2e_2v_2e_3v_3$.



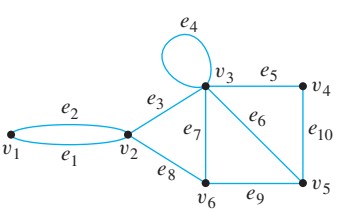
■

Observe que si una gráfica G no tiene ningunas aristas paralelas, entonces cualquier camino en G está únicamente determinado por su sucesión de vértices.

Ejemplo 10.2.2 Caminos, senderos, trayectorias y circuitos

En el grafo siguiente, determine cuáles de los siguientes caminos son senderos, trayectorias, circuitos o circuitos simples.

a. $v_1e_1v_2e_3v_3e_4v_3e_5v_4$
b. $e_1e_3e_5e_5e_6$
c. $v_2v_3v_4v_5v_3v_6v_2$
d. $v_2v_3v_4v_5v_6v_2$
e. $v_1e_1v_2e_1v_1$
f. v_1



Solución

a. Este camino tiene un vértice repetido, pero no tiene una arista repetida, así que es un sendero de v_1 a v_4, pero no una trayectoria.

b. Esto es sólo un camino de v_1 a v_5. No es un sendero porque tiene una arista repetida.

c. Este camino comienza y termina en v_2, contiene al menos una arista y no tiene una arista repetida, así que es un circuito. Ya que el vértice v_3 se repite en medio, no es un circuito simple.

d. Este camino empieza y termina en v_2, contiene al menos una arista, no tiene una arista repetida y no tiene un vértice repetido. Por tanto es un circuito simple.

e. Esto es sólo un camino cerrado comenzando y terminando en v_1. No es un circuito porque se repite la arista e_1.

f. El primer vértice de este camino es el mismo que su último vértice, pero no contiene una arista y así no es un circuito. Es un camino cerrado de v_1 a v_1. (También es un sendero de v_1 a v_1). ■

Ya que la mayoría de las principales novedades en teoría de grafos ha ocurrido relativamente recientemente y en una variedad de contextos diferentes, no se han estandarizado los términos utilizados del tema. Por ejemplo, lo que este libro llama un *grafo* a veces se denomina un *multígrafo*, lo que este libro llama un *grafo simple* a veces se llama un *grafo*, lo que este libro llama un *vértice* es llamado a veces un *nodo* y lo que este libro llama una arista se denomina un *arco*. Del mismo modo, en lugar de la palabra *sendero*, a veces se utiliza la palabra *trayectoria*; en lugar de la palabra *trayectoria*, se utilizan las palabras *trayectoria simple* y en lugar de las palabras *circuito simple*, a veces se utiliza la palabra *ciclo*. La terminología de este libro es una de las más comunes, pero si consulta otras fuentes, asegúrese de comprobar sus definiciones.

Conectividad

Es fácil comprender el concepto de conectividad a un nivel intuitivo. En términos generales, un grafo está conectada si es posible viajar desde cualquier vértice a cualquier otro vértice a lo largo de una sucesión de aristas adyacentes del grafo. La definición formal de conectividad se expresa en caminos.

• Definición

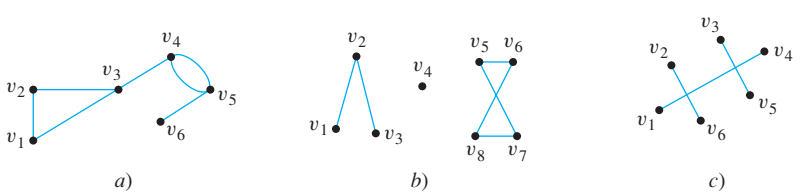
Sea G un grafo. Dos vértices v **y** w **de** G **son conexos** si y sólo si, existe un camino de v a w. El **grafo** G **es conexo** si y sólo si, dados *cualesquiera* dos vértices v y w en G, hay que un camino de v a w. Simbólicamente,

$$G \text{ es conexo} \quad \Leftrightarrow \quad \forall \text{ vértices } u, w \in V(G), \exists \text{ un camino de } v \text{ a } w.$$

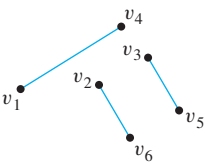
Si se toma la negación de esta definición, verá que un grafo G *no es conexo* si y sólo si, hay dos vértices de G que no están conectados por cualquier camino.

Ejemplo 10.2.3 ¿Grafos conexos y no conexos?

¿Cuáles de los siguientes grafos son conexos?



Solución El grafo representado en *a*) es conexo, mientras que los de *b*) y *c*) no lo son. Para entender por qué no es conexo *c*), recuerde que en un dibujo de un grafo, dos aristas pueden cruzar en un punto que no es un vértice. Por tanto puede redibujar el grafo en *c*) como sigue:



■

Algunos datos útiles sobre circuitos y conectividad se reúnen en el siguiente lema. Las demostraciones de *a*) y *b*) se dejan para los ejercicios. La demostración de *c*) se encuentra en la sección 10.5.

Lema 10.2.1

Sea G un grafo.

a. Si G es conexa, entonces cualesquiera dos vértices distintos de G pueden conectarse con una trayectoria.

b. Si los vértices v y w forman parte de un circuito en G y se quita una arista del circuito, entonces aún existe un sendero de v a w en G.

c. Si G es conexa y G contiene un circuito, entonces se puede eliminar una arista del circuito sin desconectar a G.

Revise de nuevo el ejemplo 10.2.3. Los grafos en *b*) y *c*) constan de tres partes, cada una de cuales es en sí misma un grafo conexo. *Un componente conexo* de un grafo es un subgrafo conexo del mayor tamaño posible.

• Definición

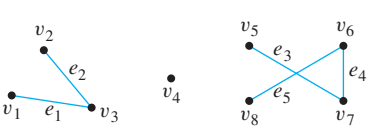
Un grafo H es un **componente conexo** de una gráfica G si y sólo si,

1. H es subgráfica de G;
2. H es conexo; y
3. Un subgrafo no conexo de G tiene a H como un subgrafo y contiene vértices o aristas que no están en H.

El hecho es que cualquier grafo es un tipo de unión de sus componentes conexos.

Ejemplo 10.2.4 Componentes conexos

Encuentre todos los componentes conexos de la gráfica siguiente G.



Solución G tiene tres componentes conexos: H_1, H_2 y H_3 con conjuntos de vértices V_1, V_2 y V_3 y conjuntos de aristas E_1, E_2 y E_3, donde

$$V_1 = \{v_1, v_2, v_3\}, \qquad E_1 = \{e_1, e_2\},$$
$$V_2 = \{v_4\}, \qquad E_2 = \emptyset,$$
$$V_3 = \{v_5, v_6, v_7, v_8\}, \qquad E_3 = \{e_3, e_4, e_5\}.$$

Circuitos de Euler

Ahora volvemos a considerar problemas generales similares al problema de los puentes de Königsberg. Se hace la siguiente definición en honor de Euler.

• Definición

Sea G un grafo. Un **circuito de Euler** para G es un circuito que contiene cada vértice y cada arista de G. Es decir, un circuito de Euler para G es una sucesión de vértices adyacentes y aristas en G que tiene al menos una arista, que comienza y termina en el mismo vértice, utiliza cada vértice de G por lo menos una vez y cada arista de G exactamente una vez.

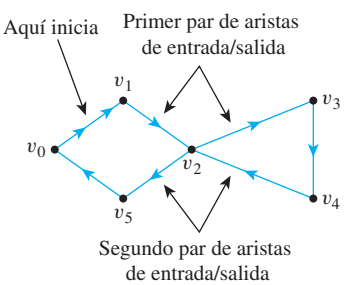
El análisis utilizado anteriormente para resolver el problema de los puentes de Königsberg generaliza la demostración del teorema siguiente:

Teorema 10.2.2

Si un grafo tiene un circuito de Euler, entonces todos los vértices del grafo tienen grado positivo par.

Demostración:

Suponga que G es un grafo que tiene un circuito de Euler. *[Debemos demostrar que dado cualquier vértice v de G, el grado de v es par.]* Sea v cualquier vértice particular arbitrariamente elegido de G. Puesto que el circuito de Euler contiene cada arista de G, contiene todas las aristas que inciden en v. Ahora imagine que toma un viaje que comienza en el centro de una de las aristas adyacentes al inicio del circuito de Euler y continúa en el circuito de Euler para terminar en el centro de la arista de partida. (Vea la figura 10.2.3. Existe dicha arista de partida ya que el circuito de Euler tiene al menos una arista.) Cada vez que v se introduce viajando a lo largo de una arista, inmediatamente se sale del viaje a lo largo de otra arista (ya que el viaje termina *en medio* de una arista).



En este ejemplo, el circuito de Euler es $v_0v_1v_2v_3v_4v_5v_0$ y v es v_2. Cada vez se introduce v_2 por una arista y se sale por otra arista.

Figura 10.2.3 Ejemplo para la demostración del teorema 10.2.2

Debido a que el circuito de Euler utiliza exactamente una vez cada arista de G, cada arista incidente en v se atraviesa exactamente una vez en este proceso. Por lo que las aristas que inciden en v ocurren en pares de entrada/salida y en consecuencia el grado de v debe ser un múltiplo positivo de 2. Pero eso significa que v tiene un grado positivo par *[como se quería demostrar]*.

Recordemos que el contrapositivo de un enunciado es lógicamente equivalente al enunciado. El contrapositivo del teorema 10.2.2 es el siguiente:

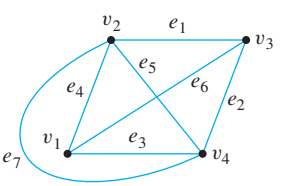
Versión contrapositiva del teorema 10.2.2

Si algún vértice de un grafo tiene grado impar, entonces el grafo no tiene un circuito de Euler.

Esta versión del teorema 10.2.2 es útil para mostrar que un grafo dado *no* tiene un circuito de Euler.

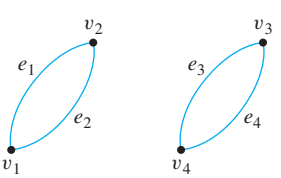
Ejemplo 10.2.5 Demostración de que un grafo no tiene un circuito de Euler

Demuestre que el grafo siguiente no tiene un circuito de Euler.



Solución Los dos vértices v_1 y v_3 tienen grado 3, que es impar. Por lo que por (la forma contrapositiva del) teorema 10.2.2, este grafo no tiene un circuito de Euler. ■

Ahora considere el converso del teorema 10.2.2: Si cada vértice de un grafo tiene grado par, entonces el grafo tiene un circuito de Euler. ¿Esto es verdad? La respuesta es no. Existe un grafo G tal que cada vértice de G tiene grado par pero G tiene un circuito de Euler. De hecho, hay muchas de tales grafos. La siguiente figura muestra un ejemplo.



Cada vértice tiene grado par, pero el grafo tiene un circuito de Euler.

Observe que el grafo en el dibujo anterior no es conexo. Resulta que aunque el converso del teorema 10.2.2 es falso, un converso modificado es verdadero: si cada vértice de un grafo tiene grado par positivo y si el grafo es conexo, entonces el grafo tiene un circuito de Euler. La demostración de este hecho es constructiva: Contiene un algoritmo para encontrar un circuito de Euler para cualquier grafo conexo en el que cada vértice tiene grado par.

Teorema 10.23

Si un grafo G es conexo y el grado de cada vértice de G es un entero positivo par, G tiene un circuito de Euler.

Demostración:

Suponga que G es cualquier grafo conexo y suponga que cada vértice de G es un entero positivo par. *[Debemos encontrar un circuito de Euler para G.]* Construya un circuito C con el algoritmo siguiente:

Paso 1: Seleccione cualquier vértice v de G en el que inicia.
[Este paso puede realizarse porque el conjunto G de vértices es no vacío, por suposición.]

Paso 2: Elija cualquier sucesión de vértices adyacentes y aristas, comenzando y terminando en v y nunca repita una arista. Llame al circuito resultante C.
[Este paso puede realizarse por las siguientes razones: ya que el grado de cada vértice de G es un entero positivo par, cada vértice de G se introduce por viajar en una arista ya sea el vértice es v mismo y no hay otra arista adyacente a v no utilizada o el vértice puede salir para viajar en otra arista no utilizada anteriormente. Dado que el número de aristas del grafo es finito (por definición de grafo), la sucesión de las distintas aristas no puede ser infinita. La sucesión puede eventualmente regresar a v ya que el grado de v es un entero positivo par y así si una arista conecta v con otro vértice, debe haber una arista diferente que se conecta de nuevo a v.]

Paso 3: Compruebe si C contiene cada arista y vértice de G. Si es así, C es un circuito de Euler y hemos terminado. Si no es así, realice los siguientes pasos.

Paso 3a: Quite todas las aristas C de G y también los vértices que sean aislados cuando se eliminan las aristas de C. Llame al subgrafo resultante G'.
[Observe que G' no se puede conectar (como se muestra en la figura 10.2.4), pero cada vértice de G' tiene grado positivo par (ya que quitar las aristas de C, quita un número par de aristas de cada vértice, la diferencia de dos enteros pares es par y los vértices aislados de grado 0 se han eliminado).]

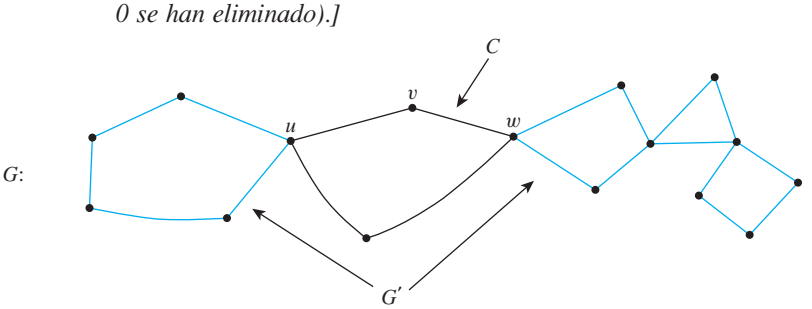


Figura 10.2.4

Paso 3b: Elija cualquier w vértice común a C y G'.
[Debe haber al menos un vértice de estos ya que G es conexo. (Consulte ejercicio 44.) (En la figura 10.2.4 existen dos de esos vértices: u y w.)]

Paso 3c: Elija cualquier sucesión de vértices adyacentes y aristas de G', comenzando y terminando en w y nunca repita una arista. Llame al circuito resultante C'. *[Esto se puede hacer ya que cada vértice de G' tiene grado positivo par y G' es finito. Consulte la justificación del paso 2.]*

Paso 3d: Remiende C y C' juntas para crear un nuevo circuito C'' como sigue: Inicie en v y siga a C todo el camino a w. Después siga a C' todo el camino de vuelta a w. Después de eso, continúe a lo largo de la parte no viajada de C para regresar a v. *[El efecto de la ejecución de los pasos 3c y 3d para el grafo de la figura 10.2.4 se muestra en la figura 10.2.5.]*

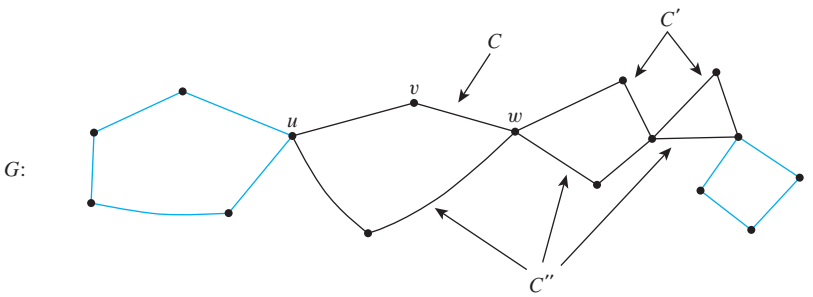


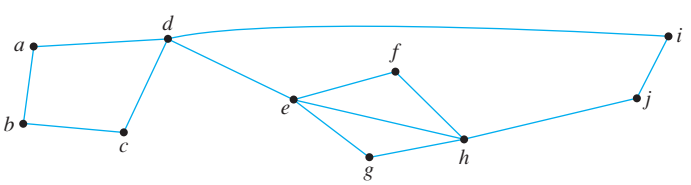
Figura 10.2.5

Paso 3e: Haga $C = C''$ y regrese al paso 3.

Ya que el grafo G es finito, finalmente debe terminar la ejecución de los pasos descritos en este algoritmo. En ese momento se habrá construido un circuito de Euler para G. (Observe que por el elemento seleccionado en los pasos 1, 2, 3b y 3c, se pueden producir una variedad de diferentes circuitos de Euler con este algoritmo).

Ejemplo 10.2.6 Determinación de un circuito de Euler

Utilice el teorema 10.2.3 para comprobar que el grafo que se presenta a continuación tiene un circuito de Euler. Después utilice el algoritmo de demostración del teorema para encontrar un circuito de Euler para el grafo.



Solución Observe que

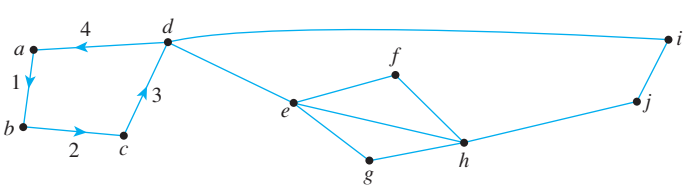
$$\deg(a) = \deg(b) = \deg(c) = \deg(f) = \deg(g) = \deg(i) = \deg(j) = 2$$

y que $\deg(d) = \deg(e) = \deg(h) = 4$. Por lo que todos los vértices tienen grado par. También, el grafo es conexo. Así, por el teorema 10.2.3, el grafo tiene un circuito de Euler.

Para construir un circuito de Euler usando el algoritmo del teorema 10.2.3, sea $v = a$ y sea C

$$C\text{: } abcda.$$

C está representado por las aristas etiquetadas que se muestran a continuación.



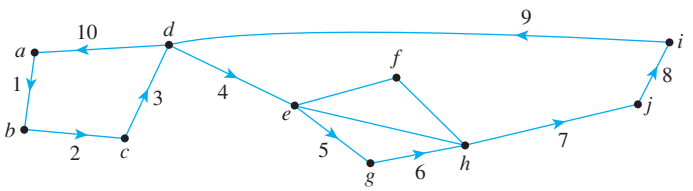
Observe que C no es un circuito de Euler para el grafo, pero C cruza el resto del grafo en d. Sea C'

$$C'\text{: } deghjid.$$

Parche C' en C para obtener

$$C''\text{: } abcdeghjida.$$

Sea $C = C''$. Entonces C está representado por las aristas etiquetados que se muestran a continuación.



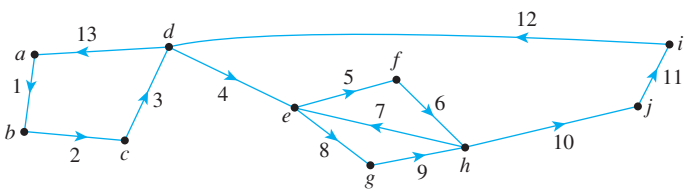
Observe que C no es un circuito de Euler para el grafo pero éste intersecta al resto del grafo en e. Sea C'

$$C'\text{: } efhe.$$

Parche C' en C para obtener

$$C'\text{: } abcdefheghjida.$$

Sea $C = C''$. Entonces C se representa por las aristas etiquetadas que se muestran a continuación.



Puesto que C incluye exactamente una vez cada arista del grafo, C es un circuito de Euler para el grafo. ■

En el ejercicio 45 del final de esta sección se debe mostrar que cualquier grafo con un circuito de Euler es conexo. Este resultado puede combinarse con los teoremas 10.2.2 y 10.2.3 para dar una completa caracterización de los grafos que tienen circuitos de Euler, como se indica en el teorema 10.2.4.

Teorema 10.2.4

Un grafo G tiene un circuito de Euler si y sólo si, G es conexo y cada vértice de G tiene grado par positivo.

Un corolario del teorema 10.2.4 da un criterio para determinar cuándo es posible encontrar un camino de un vértice de un grafo a otro, pasando por todos los vértices del grafo al menos una vez y por cada arista del grafo exactamente una sola vez.

• Definición

Sea G un grafo y sean v y w dos vértices distintos de G. Un **sendero de Euler de v a w** es una sucesión de aristas adyacentes y vértices que comienza en v, termina en w, pasa a través de cada vértice de G por lo menos una vez y atraviesa cada arista de G exactamente una vez.

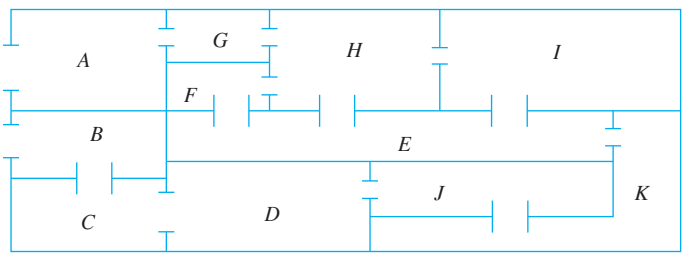
Corolario 10.2.5

Sea G un grafo y sea v y w dos vértices distintos de G. Existe una trayectoria de Euler de v a w si y sólo si G es conexo, u y w tienen grado impar y todos los otros vértices de G tienen grado par positivo.

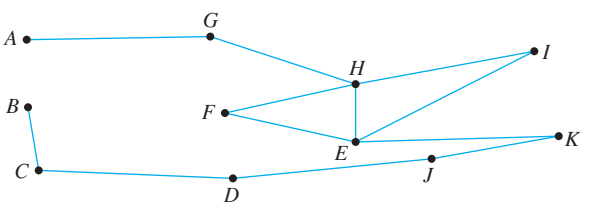
La demostración de este corolario queda como un ejercicio.

Ejemplo 10.2.7 Determinación de un sendero de Euler

El plano que se muestra a continuación es una casa abierta para vista del público. ¿Es posible encontrar un sendero que inicie en el cuarto A, termina en el cuarto B y pase exactamente una vez por cada puerta interior de la casa? Si es así, determine dicho sendero.



Solución Sea la planta de la casa representada por el grafo que se muestra a continuación.

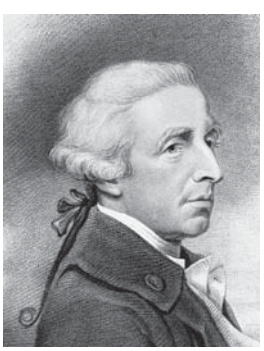


Cada vértice de este grafo tiene grado par excepto para A y B, cada uno de los cuales tiene grado 1. Por el corolario 10.2.5, existe una trayectoria de Euler de A a B. Una de dichas trayectorias es

$$AGHFEIHEKJDCB.$$

■

Circuitos hamiltonianos



Bettmann/CORBIS

Sir Wm. Hamilton (1805-1865)

El teorema 10.2.4 responde completamente a la pregunta siguiente: dado un grafo G, ¿es posible encontrar un circuito G en el que todas las *aristas* de G se presenten exactamente una vez? Una pregunta relacionada es la siguiente: Dado el grafo G, ¿es posible encontrar un circuito para G en la que todos los vértices de G (excepto el primero y el último) se presenten exactamente una vez?

En 1859, el matemático irlandés Sir William Rowan Hamilton presentó un enigma en forma de un dodecaedro (do-de-cae-dro). (La figura 10.2.6 contiene un dibujo de un dodecaedro, que es una figura sólida con 12 caras pentagonales idénticas).

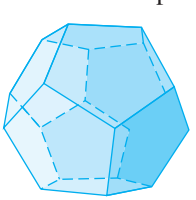
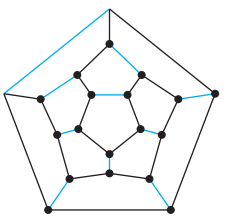


Figura 10.2.6 Dodecaedro

Cada vértice se etiqueta con el nombre de una ciudad: Londres, París, Hong Kong, Nueva York etc. El problema que planteó Hamilton fue iniciar en una ciudad y recorrer el mundo visitando otra ciudad exactamente una vez y regresar a la ciudad de partida. Una forma de resolver el problema es imaginar la superficie del dodecaedro estirada y puesta plana en el plano, como se muestra:



El circuito denotado con líneas negras es una solución. Observe que, aunque cada ciudad se visita, muchas aristas se omiten en el circuito. (Versiones más difíciles del problema requieren que ciertas ciudades se visiten en un orden dado.)

La siguiente definición se realiza en honor de Hamilton.

• Definición

Dado un grafo G, un **circuito hamiltoniano** para G es un circuito simple que incluye todos los vértices de G. Es decir, un circuito hamiltoniano para G es una sucesión de vértices adyacentes y aristas distintas en las que aparece exactamente una vez cada vértice de G, excepto el primero y el último, que son los mismos.

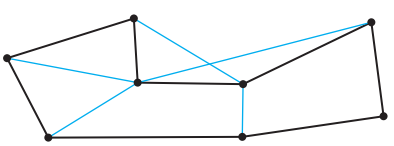
Observe que aunque un circuito de Euler para un grafo G debe incluir todos los vértices de G, puede visitar algunos vértices más de una vez y por lo que no puede ser un circuito hamiltoniano. Por otro lado, un circuito hamiltoniano para G no tiene que incluir todas las aristas de G y por lo que no puede ser un circuito de Euler.

A pesar de las definiciones parecidas de los circuitos de Euler y hamiltoniano, las matemáticas de los dos son muy diferentes. El teorema 10.2.4 da un simple criterio para especificar si un determinado grafo tiene un circuito de Euler. Lamentablemente, no hay ningún criterio análogo para especificar si un determinado grafo tiene un circuito hamiltoniano, no existe aún un algoritmo eficiente para determinar dicho circuito. Sin embargo, es una técnica simple que se puede utilizar en muchos casos para mostrar que un grafo *no* tiene un circuito hamiltoniano. Esto se deduce de las consideraciones siguientes:

Supongamos que un grafo G con al menos dos vértices tiene un circuito hamiltoniano C dado concretamente como

$$C\colon v_0e_1v_1e_2 \cdots v_{n-1}e_nv_n.$$

Ya que C es un circuito simple, todos los e_i son distintos y todos los v_i son distintos excepto $v_0 = v_n$. Sea H el subgrafo de G que se formó con los vértices y aristas de C. A continuación se muestra un ejemplo de dicha H.



H se indica con las líneas negras.

Observe que H tiene el mismo número de aristas que de vértices ya que todas estas n aristas son distintas y así son sus n vértices $v_1, v_2, \ldots, v_n$. También, por definición del

circuito hamiltoniano, cada vértice de G es un vértice de H y H es conexo ya que cualesquiera dos de sus vértices se encuentran en un circuito. Además, cada vértice de H tiene grado 2. La razón de esto es que hay exactamente dos aristas incidentes en cualquier vértice. Estos son e_i y e_{i+1} para cualquier vértice v_i excepto $v_0 = v_n$ y son e_1 y e_n para $v_0 (= v_n)$. Estas observaciones han establecido la verdad de la siguiente propuesta en todos los casos donde G tiene al menos dos vértices.

Proposición 10.2.6

Si un grafo G tiene un circuito hamiltoniano, entonces G tiene un subgrafo H con las propiedades siguientes:

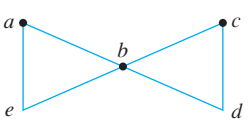
1. H contiene todos los vértices de G.
2. H es conexo.
3. H tiene el mismo número de aristas que de vértices.
4. Cada vértice de H tiene grado 2.

Observe que si G contiene sólo un vértice y G tiene un circuito hamiltoniano, entonces el circuito tiene la forma $v\ e\ v$, donde v es el vértice de G y e es una arista que incide en v. En este caso, el subgrafo H consiste de v y e satisface las condiciones de la l) a la 4) de la proposición 10.2.6.

Recordemos que el contrapositivo de un enunciado es lógicamente equivalente al enunciado. El contrapositivo de la proposición 10.2.6 dice que si un grafo G *no* tiene un subgrafo H con las propiedades de la 1) a la 4), entonces G *no* tiene un circuito hamiltoniano.

Ejemplo 10.2.8 Demostración de que un grafo no tiene un circuito hamiltoniano

Demuestre que el grafo G que se muestra a continuación no tiene un circuito hamiltoniano.

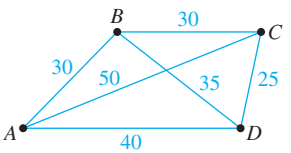


Solución Si G tiene un circuito hamiltoniano, entonces por la proposición 10.2.6, G tiene un subgrafo H que 1) contiene todos los vértices de G, 2) es conexo, 3) tiene el mismo número de aristas que de vértices y 4) es tal que cada vértice tiene grado 2. Supongamos que existe dicho subgrafo H. En otras palabras, suponga que hay un subgrafo H conexo de G tal que H tiene cinco vértices (a, b, c, d, e) y cinco aristas y tal que cada vértice de H tiene grado 2. Dado que el grado de b en G es 4 y cada vértice de H tiene grado 2, se deben remover dos aristas que inciden en b de G para crear a H. La arista $\{a, b\}$ no puede eliminarse porque si se hiciera, el vértice a tendría un grado menor que 2 en H. Un razonamiento similar muestra que las aristas $\{e, b\}$, $\{b, a\}$ y $\{b, d\}$ no pueden ser eliminadas. En consecuencia, el grado de b en H debe ser 4, lo que contradice la condición de que cada vértice en H tiene grado 2 en H. Por lo que no existe tal subgrafo H y así G no tiene un circuito hamiltoniano. ■

El ejemplo siguiente muestra un tipo de problema conocido como el **problema del agente viajero**. Es una variación del problema para encontrar un circuito hamiltoniano para un grafo.

Ejemplo 10.2.9 Un problema del agente viajero

Imagine que el dibujo que se muestra a continuación es un mapa que muestra cuatro ciudades y las distancias en kilómetros entre éstas. Supongamos que un vendedor debe viajar a cada ciudad exactamente una vez, comenzando y terminando en la ciudad A. ¿Qué ruta de ciudad a ciudad minimizará la distancia total que debe recorrer?



Solución Este problema se puede resolver mediante la escritura de todos los circuitos hamiltonianos posibles comenzando y terminando en A y calculando la distancia total recorrida para cada uno.

Ruta	Distancia total (en kilómetros)
$ABCDA$	$30 + 30 + 25 + 40 = 125$
$ABDCA$	$30 + 35 + 25 + 50 = 140$
$ACBDA$	$50 + 30 + 35 + 40 = 155$
$ACDBA$	140 [$ABDCA$ hacia atrás]
$ADBCA$	155 [$ACBDA$ hacia atrás]
$ADCBA$	125 [$ABCDA$ hacia atrás]

Así la ruta ya sea $ABCDA$ o $ADCBA$ da una distancia total mínima de 125 kilómetros. ■

El problema general del agente viajero implica encontrar un circuito hamiltoniano para minimizar la distancia total recorrida por un grafo arbitrario con n vértices en los que cada arista está marcada con una distancia. Una forma de resolver el problema general es utilizar el método de ejemplo 10.2.9; escriba todos los circuitos hamiltonianos comenzando y terminando en un vértice particular, calculando la distancia total para cada uno y eligiendo uno para que esta cifra sea mínima. Sin embargo, incluso para valores de tamaño mediano de n este método es poco práctico. Para una gráfica completa con 30 vértices, serían $(29!)/2 \cong 4.42 \times 10^{30}$ circuitos hamiltonianos comenzando y terminando en un vértice particular para comprobar. Aún si se encontró cada circuito y su distancia total se calculó en un solo nanosegundo, requeriría aproximadamente 1.4×10^{14} años terminar el cálculo. En la actualidad, no existe ningún algoritmo conocido para resolver el problema general del agente viajero que sea más eficiente. Sin embargo, existen algoritmos eficientes que encuentran soluciones "bastante bien", es decir, circuitos que, aunque no necesariamente tengan distancias totales lo menor posibles, tienen distancias total menores que la mayoría de otros circuitos hamiltonianos.

Autoexamen

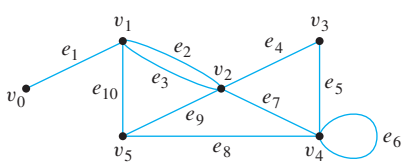
1. Sea G un grafo y sean v y w vértices en G.
   a) Un camino de v a w es _____.
   b) Un sendero de v a w es _____.
   c) Una trayectoria de v a w es _____.
   d) Un camino cerrado es _____.
   e) Un circuito es _____.
   f) Un circuito simple es _____.
   g) Un camino trivial es _____.
   h) Los vértices v y w están conectados si y sólo si, _____.

2. Un grafo es conexo si y sólo si, _____.
3. La eliminación de una arista de un circuito en un grafo no _____.
4. Un circuito de Euler, en un grafo es _____.
5. Un grafo tiene un circuito de Euler si y sólo si, _____.
6. Dados los vértices v y w en un grafo, existe una trayectoria de Euler de v a w si y sólo si _____.
7. Un circuito hamiltoniano en un grafo es _____.
8. Si un grafo G tiene un circuito hamiltoniano, entonces G tiene un subgrafo H con las siguientes propiedades: _____, _____, _____ y _____.
9. Un problema del agente viajero consiste en encontrar un _____ que minimice la distancia total recorrida por un grafo en la que cada arista está marcada con una distancia.

Conjunto de ejercicios 10.2

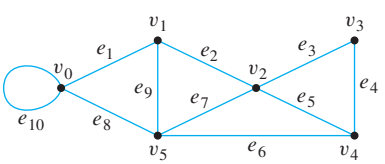
1. En el grafo siguiente, determine si los caminos siguientes son senderos, trayectorias, caminos cerrados, circuitos, circuitos simples o caminos simples.

a. $v_0e_1v_1e_{10}v_5e_9v_2e_2v_1$ b. $v_4e_7v_2e_9v_5e_{10}v_1e_3v_2e_9v_5$
c. v_2 d. $v_5v_2v_3v_4v_4v_5$
e. $v_2v_3v_4v_5v_2v_4v_3v_2$ f. $e_5e_8e_{10}e_3$

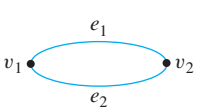


2. En el grafo siguiente, determine si los caminos siguientes son senderos, rutas, caminos cerrados, circuitos, circuitos simples o caminos simples.

a. $v_1e_2v_2e_3v_3e_4v_4e_5v_2e_2v_1e_1v_0$ b. $v_2v_3v_4v_5v_2$
c. $v_4v_2v_3v_4v_5v_2v_4$ d. $v_2v_1v_5v_2v_3v_4v_2$
e. $v_0v_5v_2v_3v_4v_2v_1$ f. $v_5v_4v_2v_1$



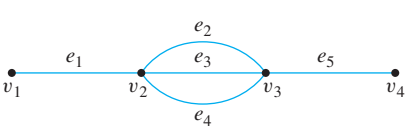
3. Sea G el grafo



y considere el camino $v_1e_1v_2e_2v_1$.

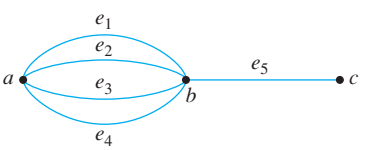
a. ¿Este camino se puede escribir sin ambigüedades como $v_1v_2v_1$? ¿Por qué?
b. ¿Este camino se puede escribir sin ambigüedades como e_1e_2? ¿Por qué?

4. Considere la siguiente gráfica.



a. ¿Cuántas trayectorias existen de v_1 a v_4?
b. ¿Cuántos senderos existen de v_1 a v_4?
c. ¿Cuántos caminos existen de v_1 a v_4?

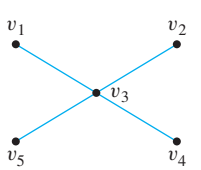
5. Considere el siguiente grafo.



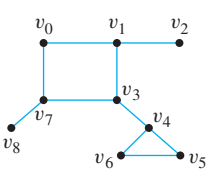
a. ¿Cuántas trayectorias hay de a a c?
b. ¿Cuántos senderos existen de a a c?
c. ¿Cuántos caminos existen de a a c?

6. Una arista cuya eliminación desconecta a la gráfica de la que es parte se llama un **puente**. Encuentre todos los puentes para cada uno de los siguientes grafos.

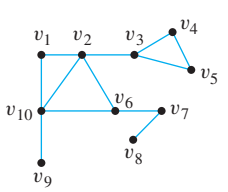
a.



b.



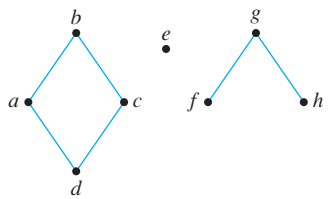
c.



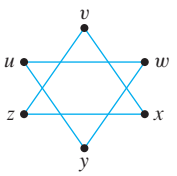
7. Dado cualquier entero positivo n, *a*) encuentre un grafo conexo con n aristas tal que la eliminación de una arista desconecte la gráfica; *b*) encuentre un grafo conexo con n aristas que no se pueda desconectar por la eliminación de cualquier arista.

8. Encuentre el número de componentes conectados de cada uno de los siguientes grafos.

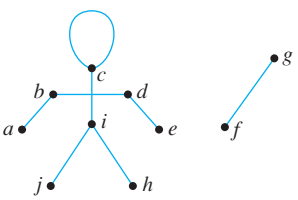
a.



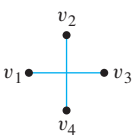
b.



c.



d.



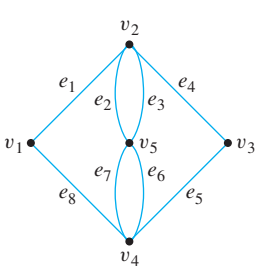
9. Cada uno de los incisos del *a*) al *c*) describe un grafo. En cada caso responda *sí*, *no*, o *no necesariamente* a esta pregunta: ¿el grafo tiene un circuito de Euler? Justifique sus respuestas.
   a. *G* es un grafo conexo con cinco vértices de grados 2, 2, 3, 3 y 4.
   b. *G* es un grafo conexo con cinco vértices de grados 2, 2, 4, 4 y 6.
   c. *G* es un grafo con cinco vértices de grados 2, 2, 4, 4 y 6.

10. La solución del ejemplo 10.2.5 muestra un grafo para que cada vértice tenga grado par, pero que no tiene un circuito de Euler. Dé otro ejemplo de un grafo que satisfaga estas propiedades.

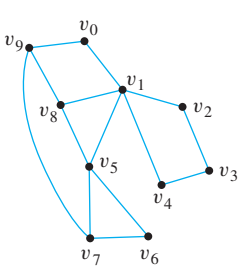
11. ¿Es posible para un ciudadano de Königsberg realizar un recorrido por la ciudad y cruzar cada puente exactamente dos veces? (Vea la figura 10.2.l.) ¿Por qué?

Determine cuál de los grafos en 12-17 tienen circuitos de Euler. Si el grafo no tiene un circuito de Euler, explique por qué no. Si tiene un circuito de Euler, describa uno.

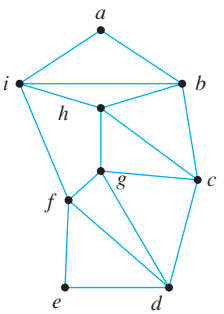
12.



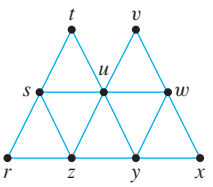
13.



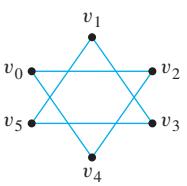
14.



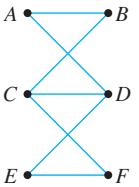
15.



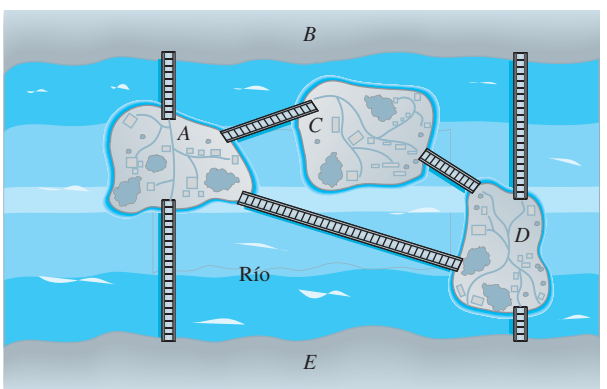
16.



17.

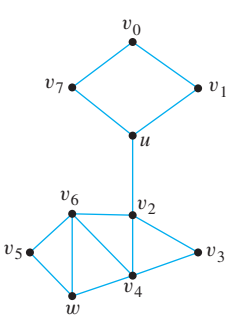


18. ¿Es posible hacer un camino alrededor de la ciudad cuyo mapa se muestra a continuación, comenzando y terminando en el mismo punto y cruzando cada puente exactamente una vez? Si es así, ¿cómo puede hacerse?

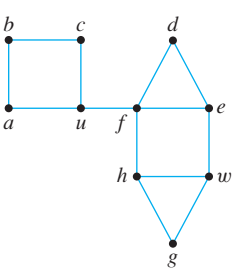


Para cada uno de los grafos en los ejercicios del 19 al 21, determine si hay una trayectoria de Euler de *u* a *w*. Si existe, encuentre dicha trayectoria.

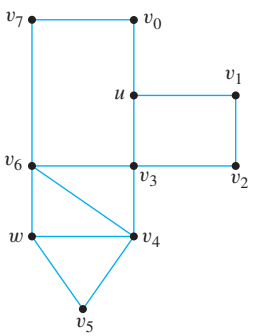
19.



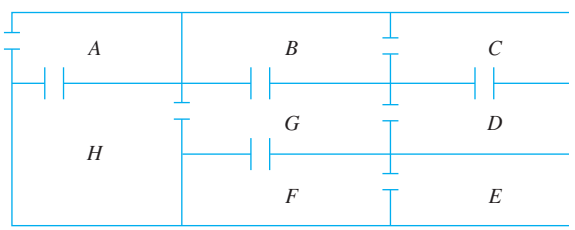
20.



21.

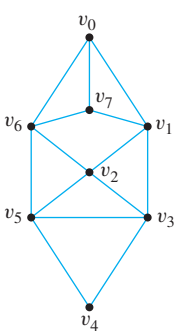


22. El siguiente es mapa de la planta de una casa. ¿Es posible entrar en la casa en el cuarto A, viajar a cada puerta interior de la casa exactamente una sola vez y salir por el cuarto E? Si es así, ¿cómo puede hacerse?

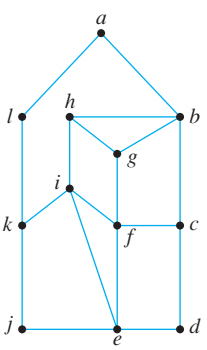


Encuentre circuitos hamiltonianos para cada uno de los grafos en 23 y 24.

23.

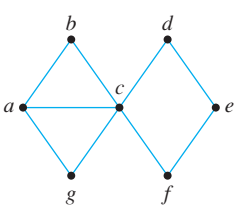


24.

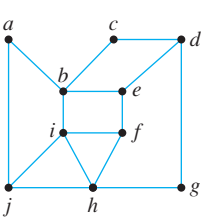


Muestre que ninguno de los grafos en los ejercicios del 25 al 27 tiene un circuito hamiltoniano.

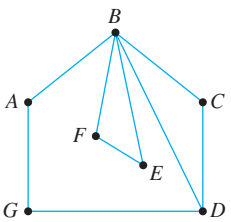
25.



26.

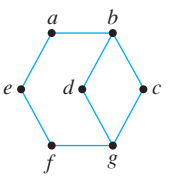


27.

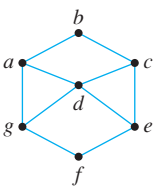


En los ejercicios del 28 al 31 encuentre los circuitos hamiltonianos para los grafos que los tengan. Explique por qué los otros grafos no los tienen.

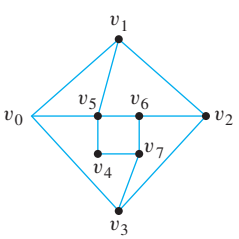
H 28.



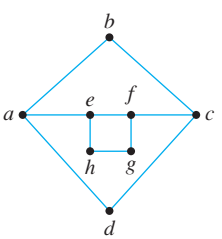
29.



30.



31.



H 32. Dé dos ejemplos de grafos que tengan circuitos de Euler, pero no circuitos hamiltonianos.

H 33. Dé dos ejemplos de grafos que tengan circuitos hamiltonianos, pero no circuitos de Euler.

H 34. Dé dos ejemplos de grafos que tengan tanto circuitos de Euler como circuitos hamiltonianos.

H 35. Dé dos ejemplos de grafos que tengan circuitos de Euler y circuitos hamiltonianos que no sean los mismos.

36. Un viajero en Europa quiere visitar cada una de las ciudades que se muestra en el mapa una sola vez, comenzando y terminando en Bruselas. La distancia (en kilómetros) entre cada par de ciudades se da en la tabla. Encuentre un circuito hamiltoniano que minimice la distancia total recorrida. (Utilice el mapa para limitar los posibles circuitos a algunos. Después utilice la tabla para encontrar la distancia total para cada una de ellas).

	Berlín	Bruselas	Düsseldorf	Luxemburgo	Munich
Bruselas	783				
Düsseldorf	564	223			
Luxemburgo	764	219	224		
Munich	585	771	613	517	
París	1 057	308	497	375	832

37. **a.** Demuestre que si un camino en un grafo contiene una arista repetida, el camino contiene un vértice repetido.
    b. Explique cómo se deduce del inciso *a*) que cualquier camino con ningún vértice repetido no tiene ninguna arista repetida.

38. Demuestre el lema 10.2.1*a*): si G es un grafo conexo, entonces los dos vértices distintos de G se pueden conectar con una trayectoria.

39. Demuestre el lema 10.2.1*b*): Si los vértices v y w son parte de un circuito en un grafo G y se quita una arista del circuito, entonces aún existe un sendero de v a w en G.

40. Dibuje una imagen para ilustrar el lema 10.2.1*c*): si un grafo G es conexo y G contiene un circuito, entonces se puede eliminar una arista del circuito sin desconectar G.

41. Demuestre que si hay un sendero en un grafo G de un vértice v a un vértice w, entonces hay un sendero de w a v.

***H* 42.** Si un grafo contiene un circuito que comienza y termina en un vértice v, ¿el grafo contiene un circuito simple que comienza y termina en v? ¿Por qué?

43. Demuestre que si hay un circuito en un grafo que comienza y termina en un vértice v y si w es otro vértice en el circuito, entonces existe un circuito en el grafo que comienza y termina en w.

44. Sea G un grafo conexo y C sea cualquier circuito en G que no contiene todos los vértices de C. Sea G' el subgrafo obtenido mediante la eliminación de todas las aristas C de G y también los vértices que se aíslan cuando se eliminan las aristas de C. Demuestre que existe un vértice v tal que v este tanto en C como en G'.

45. Demuestre que cualquier grafo con un circuito de Euler es conexo.

46. Demuestre el corolario 10.2.5.

47. ¿Para qué valores de n tiene el grafo completo K_n con n vértices tiene: *a*) un circuito de Euler? *b*) un circuito hamiltoniano? Justifique sus respuestas.

✶ 48. ¿Para los valores de m y n tiene el grafo bipartito completo de vértices (m, n) tiene: *a*) un circuito de Euler? *b*) un circuito hamiltoniano? Justifique sus respuestas.

✶ 49. ¿Cuál es el número máximo de aristas que puede tener un grafo simple desconectado con n vértices? Demuestre su respuesta.

✶ 50. Demuestre que un grafo es bipartito si y sólo si, no tiene un circuito con un número impar de aristas. (Consulte el ejercicio 37 de la sección 10.1 para la definición de grafo bipartito.)

Respuestas del autoexamen

1. *a*) una sucesión finita alternando vértices y aristas adyacentes de G *b*) a camino que no contiene una arista repetida *c*) un sendero que no contiene un vértice repetido *d*) un camino que comienza y termina en el mismo vértice *e*) un camino cerrado que contiene al menos una arista y no contiene ninguna arista repetida *f*) un circuito que no tenga algún vértice repetido excepto el primero y el último *g*) un camino que consta de un único vértice y ninguna arista *h*) existe un camino de v a w 2. dados cualesquiera dos vértices en el grafo, hay un camino de uno a los otros 3. desconecta el grafo 4. un circuito que contiene cada vértice y cada arista del grafo 5. el grafo es conexo y cada vértice tiene grado positivo par 6. el grafo es conexo, v y w tienen grado impar y todos los demás vértices tienen grado par positivo 7. un circuito simple que incluye todos los vértices del grafo 8. H contiene todos los vértices de G; H es conexo; H tiene el mismo número de aristas que de vértices; cada vértice de H tiene grado 2 9. circuito hamiltoniano

10.3 Representaciones matriciales de grafos

Orden y simplificación son los primeros pasos hacia el dominio de un tema.
—Thomas Mann, *La montaña mágica*, 1924

¿Cómo pueden representarse los grafos en una computadora? Ocurre que toda la información necesaria para especificar un grafo se puede transmitir por una estructura llamada *matriz* y las matrices (matrices es el plural de *matriz*) son fáciles de representar dentro de las computadoras. Esta sección contiene algunas definiciones básicas acerca de las matrices y de las operaciones entre matrices, una descripción de la relación entre grafos, matrices y algunas aplicaciones.

Matrices

Las matrices son analogías de sucesiones bidimensionales. También se les llaman arreglos bidimensionales.

• Definición

Una **matriz A *m* × *n*** (se lee "*m* por *n*") **sobre un conjunto *S*** es un arreglo rectangular de elementos de S dispuestos en m renglones y n columnas:

$$\mathbf{A} = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1j} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2j} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{i1} & a_{i2} & \dots & a_{ij} & \dots & a_{in} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{m1} & a_{m2} & \dots & a_{mj} & \dots & a_{mn} \end{bmatrix} \leftarrow i\text{-ésimo renglón de } \mathbf{A}$$

$$\uparrow$$

j-ésima columna de **A**

Se escribe $\mathbf{A} = (a_{ij})$.

El ***i*-ésimo renglón de A** es

$$[a_{i1} \quad a_{i2} \quad \cdots \quad a_{in}]$$

y la ***j*-ésima columna de A** es

$$\begin{bmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{bmatrix}.$$

La entrada a_{ij} en el i-ésimo renglón y la j-ésima columna de **A** se llama la ***ij*-ésima entrada de A**. Se dice que una matriz $m \times n$ tiene **tamaño *m* × *n***. Si **A** y **B** son matrices, entonces $\mathbf{A} = \mathbf{B}$ si y sólo si, **A** y **B** tienen el mismo tamaño y las entradas correspondientes de **A** y **B** son todas iguales; es decir,

$$a_{ij} = b_{ij} \quad \text{para toda } i = 1, 2, \dots, m \text{ y } j = 1, 2, \dots, n.$$

Una matriz para la que los números de renglones y de columnas son iguales se llama una **matriz cuadrada**. Si **A** es una matriz cuadrada de tamaño $n \times n$, entonces la **diagonal principal de A** consta de todas las entradas $a_{11}, a_{22}, \dots, a_{nn}$:

$$\begin{bmatrix} a_{11} & a_{12} & \dots & a_{1i} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2i} & \dots & a_{2n} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{i1} & a_{i2} & \dots & a_{ii} & \dots & a_{in} \\ \vdots & \vdots & & \vdots & & \vdots \\ a_{n1} & a_{n2} & \dots & a_{ni} & \dots & a_{nn} \end{bmatrix}$$

matriz diagonal de **A**

Ejemplo 10.3.1 Terminología de la matriz

La siguiente es una matriz de 3×3 en el conjunto de números enteros.

$$\begin{bmatrix} 1 & 0 & -3 \\ 4 & -1 & 5 \\ -2 & 2 & 0 \end{bmatrix}$$

a. ¿Cuál es la entrada en el renglón 2, columna 3?

b. ¿Cuál es la segunda columna de **A**?

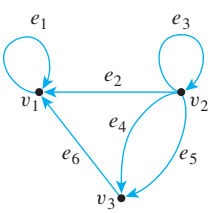
c. ¿Cuáles son las entradas de la diagonal principal de **A**?

Solución

a. 5 b. $\begin{bmatrix} 0 \\ -1 \\ 2 \end{bmatrix}$ c. 1, −1 y 0 ■

Matrices y grafos dirigidos

Considere el grafo dirigido que se muestra en la figura 10.3.1. Este grafo se puede representar por la matriz $\mathbf{A} = (a_{ij})$ para la que a_{ij} = número de flechas de v_i a v_j, para toda $i = 1, 2, 3$ y $j = 1, 2, 3$. Así $a_{11} = 1$ porque hay una flecha de v_1 a v_1, $a_{12} = 0$ porque no hay flecha de v_1 a v_2, $a_{23} = 2$ porque hay dos flechas de v_2 a v_3 y así sucesivamente. **A** se llama la *matriz de adyacencia* del grafo dirigido. Para referencia, los renglones y las columnas de **A** se etiquetan con frecuencia con los vértices del grafo G.



Grafo dirigido G

a)

$$\mathbf{A} = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \end{array} \begin{array}{c} \begin{array}{ccc} v_1 & v_2 & v_3 \end{array} \\ \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 2 \\ 1 & 0 & 0 \end{bmatrix} \end{array}$$

Matriz de adyacencia

b)

Figura 10.3.1 Un grafo dirigido y su matriz de adyacencia

• Definición

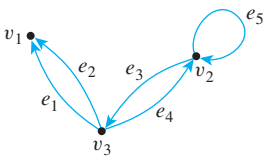
Sea G un grafo dirigido con vértices ordenados $v_1, v_2, \dots, v_n$. La **matriz de adyacencia de G** es la matriz $n \times n$ $\boldsymbol{A} = (\boldsymbol{a_{ij}})$ sobre el conjunto de enteros no negativos tales que

a_{ij} = al número de flechas de v_i a v_j para toda $i, j = 1, 2, \dots, n$.

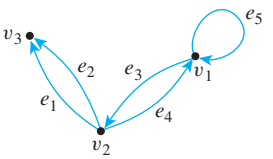
Observe que las entradas distintas de cero a lo largo de la diagonal principal de una matriz de adyacencia indican la presencia de bucles y las entradas mayores que 1 corresponden a aristas paralelas. Además, si se reordenan los vértices de un grafo dirigido, entonces se mueven las entradas de los renglones y columnas de la correspondiente matriz de adyacencia.

Ejemplo 10.3.2 La matriz de adyacencia de un grafo

Los dos grafos dirigidos que se muestran a continuación difieren sólo en el orden de sus vértices. Encuentre sus matrices de adyacencia.



a)



b)

Solución Ya que ambos grafos tienen tres vértices, ambas matrices de adyacencia son matrices 3×3. Para *a*), todas las entradas en el primer renglón son 0 ya no hay ninguna flecha de v_1 a cualquier otro vértice. Para *b*), las dos primeras entradas en el primer renglón son 1 y la tercera entrada es 0 ya que de v_1 salen flechas sencillas a v_1 y v_2 y no hay flechas a v_3. Continuando con el análisis de este modo, obtendrá las siguientes dos matrices de adyacencia:

$$\begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \end{array}\!\!\begin{array}{c} \begin{array}{ccc} v_1 & v_2 & v_3 \end{array} \\ \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 1 \\ 2 & 1 & 0 \end{bmatrix} \end{array} \qquad \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \end{array}\!\!\begin{array}{c} \begin{array}{ccc} v_1 & v_2 & v_3 \end{array} \\ \begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 2 \\ 0 & 0 & 0 \end{bmatrix} \end{array}$$

a) *b)*

Si le dan una matriz cuadrada con entradas de números enteros no negativos, puede construir un grafo dirigido con la matriz como su matriz de adyacencia. Sin embargo, la matriz no le dice cómo etiquetar las aristas, así el grafo dirigido no está determinado de manera única.

Ejemplo 10.3.3 Determinación de un grafo dirigido de una matriz

Sea

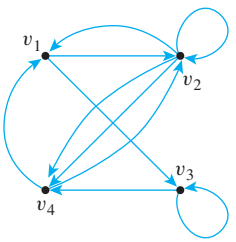
$$\mathbf{A} = \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 2 \\ 0 & 0 & 1 & 1 \\ 2 & 1 & 0 & 0 \end{bmatrix}.$$

Dibuje un grafo dirigido que tiene a $\mathbf{A}$ como su matriz de adyacencia.

Solución Sea G el grafo correspondiente de $\mathbf{A}$ y sean v_1, v_2, v_3, v_4 los vértices de G. Etiquete a $\mathbf{A}$ a lo largo de la parte superior y del lado izquierdo con los nombres de los vértices, como se muestra a continuación.

$$\mathbf{A} = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \end{array}\!\!\begin{array}{c} \begin{array}{cccc} v_1 & v_2 & v_3 & v_4 \end{array} \\ \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 2 \\ 0 & 0 & 1 & 1 \\ 2 & 1 & 0 & 0 \end{bmatrix} \end{array}$$

Entonces, por ejemplo, el 2 en el cuarto renglón y la primera columna significa que hay dos flechas de v_4 a v_1. El 0 en el primer renglón y la cuarta columna significa que no hay flecha de v_1 a v_4. Un correspondiente grafo dirigido se muestra en la siguiente página (sin etiquetas de las aristas ya que no las determina la matriz).



Matrices y grafos no dirigidos

Una vez que sepa cómo asociar una matriz con un grafo dirigido, la definición de la matriz correspondiente a un grafo no dirigido le debe parecer natural. Como antes, debe ordenar los vértices del grafo, pero en este caso simplemente hará la ij-ésima entrada de la matriz de adyacencia igual al número de aristas que conectan los i-ésimo y j-ésimo vértices del grafo.

• Definición

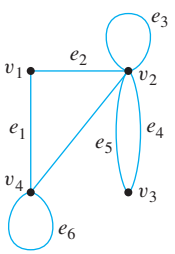
Sea G un grafo no dirigido con vértices ordenados $v_1, v_2, \ldots, v_n$. La **matriz de adyacencia de G** es la matriz $n \times n$, $\mathbf{A} = (a_{ij})$ sobre el conjunto de los enteros no negativos tales que

$$a_{ij} = \text{número de aristas que conectan } v_i \text{ con } v_j$$

para todas $i, j = 1, 2, \ldots, n$.

Ejemplo 10.3.4 Determinación de la matriz de adyacencia de un grafo

Encuentre la matriz de adyacencia para el grafo G que se muestra a continuación.



Solución

$$\mathbf{A} = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \end{array} \begin{array}{c} \begin{array}{cccc} v_1 & v_2 & v_3 & v_4 \end{array} \\ \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 1 & 2 & 1 \\ 0 & 2 & 0 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix} \end{array}$$

Observe que si la matriz $\mathbf{A} = (a_{ij})$ en el ejemplo 10.3.4 se voltea con respecto a su diagonal principal es ella misma: $a_{ij} = a_{ji}$, para $i, j = 1,2,\ldots, n$. Se dice que dicha matriz es *simétrica*.

• Definición

Una matriz cuadrada $n \times n$, $\mathbf{A} = (a_{ij})$ se llama **simétrica**, si y sólo si, para toda i, $j = 1, 2,\ldots, n$,

$$a_{ij} = a_{ji}.$$

Ejemplo 10.3.5 Matrices simétricas

¿Cuáles de las siguientes matrices son simétricas?

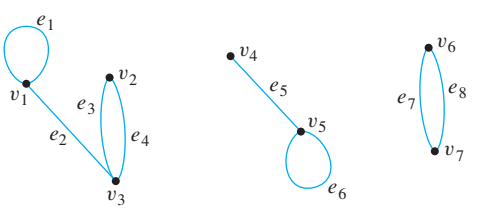
a. $\begin{bmatrix} 1 & 0 \\ 1 & 2 \end{bmatrix}$ b. $\begin{bmatrix} 0 & 1 & 2 \\ 1 & 1 & 0 \\ 2 & 0 & 3 \end{bmatrix}$ c. $\begin{bmatrix} 2 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$

Solución Sólo *b*) es simétrica. En *a*) la entrada en el primer renglón y la segunda columna difiere de la entrada en el segundo renglón y la primera columna; la matriz en *c*) no es cuadrada. ■

Es fácil ver que la matriz de *cualquier* grafo no dirigido es simétrica ya que siempre es el caso de que el número de aristas que unen a v_i con v_j es igual al número de aristas que unen a v_j con v_i, para todas $i, j = 1, 2, \ldots, n$.

Matrices y componentes conexos

Considere un grafo G, como los que se muestran a continuación, que consta de varios componentes conexos.



La matriz de adyacencia de G es

$$\mathbf{A} = \left[\begin{array}{ccc:ccc:cc} 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ 1 & 2 & 0 & 0 & 0 & 0 & 0 \\ \hdashline 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ \hdashline 0 & 0 & 0 & 0 & 0 & 0 & 2 \\ 0 & 0 & 0 & 0 & 0 & 2 & 0 \end{array}\right].$$

Como puede ver, $\mathbf{A}$ consta de bloques de matriz cuadrada (de diferentes tamaños) fuera de los bloques de su diagonal y las entradas son iguales a 0. La razón es que los vértices en cada componente conexo no comparten aristas con los vértices de otros componentes conexos. Por ejemplo ya que, v_1, v_2 y v_3 no comparten aristas con v_4, v_5, v_6 o v_7, todas las entradas en los tres renglones superiores a la derecha de la tercera columna son 0 y todas las entradas en las tres columnas de la izquierda debajo del tercer renglón son también 0. A veces, las matrices, cuyas entradas son todas 0 se denotan por 0. Si seguimos esta convención aquí, $\mathbf{A}$ se escribe como

$$\mathbf{A} = \left[\begin{array}{ccc:c:c} 1 & 0 & 1 & & \\ 0 & 0 & 2 & & \\ 1 & 2 & 0 & & \\ \hdashline & & & \begin{matrix} 0 & 1 \\ 1 & 1 \end{matrix} & \\ \hdashline & & & & \begin{matrix} 0 & 2 \\ 2 & 0 \end{matrix} \end{array}\right]$$

El razonamiento anterior puede generalizarse para demostrar el teorema siguiente:

Teorema 10.3.1

Sea G un grafo con componentes conexos $G_1, G_2, \ldots, G_k$. Si hay n_i vértices en cada componente conexa G_i y estos vértices están numerados consecutivamente, entonces la matriz de adyacencia de G tiene la forma

$$\begin{bmatrix} A_1 & O & O & \cdots & O & O \\ O & A_2 & O & \cdots & O & O \\ O & O & A_3 & \cdots & O & O \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ O & O & O & \cdots & O & A_k \end{bmatrix}$$

donde cada A_i es la matriz de adyacencia $n_i \times n_j$ de G_i, para toda $i = 1, 2, \ldots, k$ y los O representan matrices cuyas entradas son todas 0.

Multiplicación de matrices

La multiplicación de matrices es una operación enormemente útil que se plantea en muchos contextos, incluyendo la investigación de caminos en grafos. Aunque la multiplicación de matrices puede definirse en forma muy abstracta, la definición de matrices, cuyas entradas son números reales será suficiente para nuestras aplicaciones. El producto de dos matrices se construye de productos *escalares* o *punto* de sus columnas y renglones.

• Definición

Suponga que todas las entradas de las matrices **A** y **B** son números reales. Si el número de elementos, n, en el i-ésimo renglón de **A** es igual el número de elementos en la j-ésima columna de **B**, entonces el **producto escalar** o **producto punto** del i-ésimo renglón de **A** y la j-ésima columna de **B** es el número real que se obtiene como:

$$[a_{i1} \quad a_{i2} \quad \cdots \quad a_{in}] \begin{bmatrix} b_{1j} \\ b_{2j} \\ \vdots \\ b_{nj} \end{bmatrix} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{in}b_{nj}.$$

Ejemplo 10.3.6 Multiplicación de un renglón y de una columna

$$\begin{aligned} [3 \quad 0 \quad -1 \quad 2] \begin{bmatrix} -1 \\ 2 \\ 3 \\ 0 \end{bmatrix} &= 3 \cdot (-1) + 0 \cdot 2 + (-1) \cdot 3 + 2 \cdot 0 \\ &= -3 + 0 - 3 + 0 = -6 \end{aligned}$$

■

Más generalmente, si **A** y **B** son matrices, cuyas entradas son números reales y si **A** y **B** tienen *tamaños compatibles* en el sentido de que el número de columnas de **A** es igual al número de renglones de **B**, entonces se define el producto **AB**. Esta es la matriz cuya ij-ésima entrada es el producto escalar del i-ésimo renglón de **A** por la j-ésima columna de **B**, para todos los valores posibles de i y de j.

• Definición

Sea $\mathbf{A} = (a_{ij})$ una matriz $m \times k$ y $\mathbf{B} = (b_{ij})$ una matriz $k \times n$ con entradas reales. El producto (matricial), de **A** por **B**, que se denota por **AB**, es la matriz (c_{ij}) que se define como sigue:

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1k} \\ a_{21} & a_{22} & \cdots & a_{2k} \\ \vdots & \vdots & & \vdots \\ a_{i1} & a_{i2} & \cdots & a_{ik} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mk} \end{bmatrix} \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1j} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2j} & \cdots & b_{2n} \\ & \cdot & & \cdot & & \cdot \\ & \cdot & & \cdot & & \cdot \\ & \cdot & & \cdot & & \cdot \\ b_{k1} & b_{k2} & \cdots & b_{kj} & \cdots & b_{kn} \end{bmatrix}$$

$$= \begin{bmatrix} c_{11} & c_{12} & \cdots & c_{1j} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2j} & \cdots & c_{2n} \\ \vdots & \vdots & & \vdots & & \vdots \\ c_{i1} & c_{i2} & \cdots & c_{ij} & \cdots & c_{in} \\ \vdots & \vdots & & \vdots & & \vdots \\ c_{m1} & c_{m2} & \cdots & c_{mj} & \cdots & c_{mn} \end{bmatrix}$$

donde

$$c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots + a_{ik}b_{kj} = \sum_{r=1}^{k} a_{ir}b_{rj},$$

para toda $i = 1, 2, \ldots, m$ y $j = 1, 2, \ldots, n$.

Ejemplo 10.3.7 Cálculo de un producto matricial

Sea $\mathbf{A} = \begin{bmatrix} 2 & 0 & 3 \\ -1 & 1 & 0 \end{bmatrix}$ y $\mathbf{B} = \begin{bmatrix} 4 & 3 \\ 2 & 2 \\ -2 & -1 \end{bmatrix}$. Calcule **AB**.

Solución **A** tiene tamaño 2×3 y **B** tiene tamaño 3×2, así el número de columnas de **A** es igual al número de renglones de **B** y se puede calcular el producto matricial de **A** y **B**. Entonces,

$$\begin{bmatrix} 2 & 0 & 3 \\ -1 & 1 & 0 \end{bmatrix} \begin{bmatrix} 4 & 3 \\ 2 & 2 \\ -2 & -1 \end{bmatrix} = \begin{bmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{bmatrix},$$

donde

$$c_{11} = 2\cdot 4 + 0\cdot 2 + 3\cdot(-2) = 2 \qquad \begin{bmatrix} \boxed{2} & \boxed{0} & \boxed{3} \\ -1 & 1 & 0 \end{bmatrix} \begin{bmatrix} \boxed{4} & 3 \\ \boxed{2} & 2 \\ \boxed{-2} & -1 \end{bmatrix}$$

$$c_{12} = 2\cdot 3 + 0\cdot 2 + 3\cdot(-1) = 3 \qquad \begin{bmatrix} \boxed{2} & \boxed{0} & \boxed{3} \\ -1 & 1 & 0 \end{bmatrix} \begin{bmatrix} 4 & \boxed{3} \\ 2 & \boxed{2} \\ -2 & \boxed{-1} \end{bmatrix}$$

$$c_{21} = (-1)\cdot 4 + 1\cdot 2 + 0\cdot(-2) = 2 \qquad \begin{bmatrix} 2 & 0 & 3 \\ \boxed{-1} & \boxed{1} & \boxed{0} \end{bmatrix} \begin{bmatrix} \boxed{4} & 3 \\ \boxed{2} & 2 \\ \boxed{-2} & -1 \end{bmatrix}$$

$$c_{22} = (-1)\cdot 3 + 0\cdot 2 + 3\cdot(-1) = -1 \qquad \begin{bmatrix} 2 & 0 & 3 \\ \boxed{-1} & \boxed{1} & \boxed{0} \end{bmatrix} \begin{bmatrix} 4 & \boxed{3} \\ 2 & \boxed{2} \\ -2 & \boxed{-1} \end{bmatrix}.$$

Por tanto

$$\mathbf{AB} = \begin{bmatrix} 2 & 3 \\ -2 & -1 \end{bmatrix}. \qquad \blacksquare$$

La multiplicación de matrices es similar a y distinta de la multiplicación de los números reales. Una diferencia es que aunque puede ser el producto de dos números, sólo pueden multiplicarse matrices con tamaños compatibles. También, la multiplicación de números reales es conmutativa (para todos los números reales a y b, $ab = ba$), mientras que la multiplicación de matrices no lo es. Por ejemplo,

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 2 \\ 0 & 1 \end{bmatrix}, \quad \text{pero} \quad \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 1 \end{bmatrix}.$$

Por otra parte, tanto las multiplicaciones de números reales como de matrices son asociativas $(ab)c = a(bc)$, para todos los elementos a, b y c para los que los productos están definidos). Esto se demuestra en el ejemplo 10.3.8 para los productos de matrices 2×2. En los ejercicios se presentan más propiedades de la multiplicación de matrices.

Ejemplo 10.3.8 Asociatividad de la multiplicación de matrices para matrices 2 × 2

Demuestre si **A**, **B** y **C** son matrices de 2×2 en el conjunto de números reales, entonces **(AB)C** = **A(BC)**.

Solución Suponga que $\mathbf{A} = (a_{ij})$, $\mathbf{B} = (b_{ij})$ y $\mathbf{C} = (c_{ij})$ son matrices 2×2, particulares arbitrariamente elegidas con entradas reales. Dado que el número de renglones y columnas son todos iguales, están definidos **AB**, **BC**, **(AB)C** y **A(BC)**. Sea $\mathbf{AB} = (d_{ij})$ y $\mathbf{BC} = (e_{ij})$. Entonces para todos los enteros $i = 1, 2$ y $j = 1, 2$,

$$\begin{aligned} \text{la } ij\text{-ésima entrada de } \mathbf{(AB)C} &= \sum_{r=1}^{2} d_{ir}c_{rj} && \text{por definición del producto de } \mathbf{AB} \text{ y } \mathbf{C} \\ &= d_{i1}c_{1j} + d_{i2}c_{2j} && \text{por definición de } \Sigma \\ &= \left(\sum_{r=1}^{2} a_{ir}b_{r1}\right)c_{1j} + \left(\sum_{r=1}^{2} a_{ir}b_{r2}\right)c_{2j} && \text{por definición del producto de } \mathbf{A} \text{y } \mathbf{B} \\ &= (a_{i1}b_{11} + a_{i2}b_{21})c_{1_j} && \text{por definición de } \Sigma \\ &\qquad + (a_{i1}b_{12} + a_{i2}b_{22})c_{2j} \\ &= a_{i1}b_{11}c_{1j} + a_{i2}b_{21}c_{1j} + a_{i1}b_{12}c_{2j} + a_{i2}b_{22}c_{2j}. \end{aligned}$$

Similarmente la ij-ésima entrada de $\mathbf{A}(\mathbf{BC})$ es

$$\begin{aligned}(\mathbf{A}(\mathbf{BC}))_{ij} &= \sum_{r=1}^{2} a_{ir}e_{rj} \\ &= a_{i1}e_{1j} + a_{i2}e_{2j} \\ &= a_{i1}\left(\sum_{r=1}^{2} b_{1r}c_{rj}\right) + a_{i2}\left(\sum_{r=1}^{2} b_{2r}c_{rj}\right) \\ &= a_{i1}(b_{11}c_{1j} + b_{12}c_{2j}) + a_{i2}(b_{21}c_{1j} + b_{22}c_{2j}) \\ &= a_{i1}b_{11}c_{1j} + a_{i1}b_{12}c_{2j} + a_{i2}b_{21}c_{1j} + a_{i2}b_{22}c_{2j} \\ &= a_{i1}b_{11}c_{1j} + a_{i2}b_{21}c_{1j} + a_{i1}b_{12}c_{2j} + a_{i2}b_{22}c_{2j}.\end{aligned}$$

Comparando los resultados de los dos cálculos se encuentra que para todas i y j,

la ij-ésima entrada de $(\mathbf{AB})\mathbf{C}$ = la ij-ésima entrada de $\mathbf{A}(\mathbf{BC})$.

Puesto que todas las entradas correspondientes son iguales, $(\mathbf{AB})\mathbf{C} = \mathbf{A}(\mathbf{BC})$, como se demostró. ■

Con respecto a las identidades multiplicativas, hay similitudes y diferencias entre los números reales y las matrices. Sabe que el número 1 actúa como una identidad multiplicativa para productos de números reales. Resulta que hay ciertas matrices, llamadas *matrices identidad*, que actúan como identidades multiplicativas para determinados productos de la matriz. Por ejemplo, realice mentalmente las siguientes multiplicaciones matriciales para comprobar que para cualesquiera números reales a, b, c, d, e, f, g, h e i,

$$\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\begin{bmatrix}a & b & c\\ d & e & f\end{bmatrix} = \begin{bmatrix}a & b & c\\ d & e & f\end{bmatrix}$$

y

$$\begin{bmatrix}a & b & c\\ d & e & f\\ g & h & i\end{bmatrix}\begin{bmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{bmatrix} = \begin{bmatrix}a & b & c\\ d & e & f\\ g & h & i\end{bmatrix}.$$

Estos cálculos muestran que $\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$ actúa como una identidad en el lado izquierdo de la multiplicación con las matrices 2×3 y que $\begin{bmatrix}1 & 0 & 0\\ 0 & 1 & 0\\ 0 & 0 & 1\end{bmatrix}$ actúa como una identidad en el lado derecho de la multiplicación con matrices 3×3. Observe que $\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$ no puede actuar como una identidad en el lado derecho de la multiplicación con matrices 2×3 porque los tamaños no son compatibles.

David Eugene Smith Collection, Rare Book and Manuscript Library, Columbia University

Leopold Kronecker (1823-1891)

• Definición

Para cada entero positivo n, la **matriz identidad $n \times n$**, que se denota por $\mathbf{I}_n = (\delta_{ij})$ o simplemente $\mathbf{I}$ (si el tamaño de la matriz es obvio del contexto), es la matriz de $n \times n$ en la que todas las entradas de la diagonal principal son 1 y todas las demás entradas son 0. En otras palabras,

$$\delta_{ij} = \begin{cases}1 & \text{si } i = j\\ 0 & \text{si } i \neq j\end{cases}, \quad \text{para toda } i, j = 1, 2, \ldots, n.$$

El matemático alemán Leopold Kronecker introdujo el símbolo δ_{ij} para hacer los cálculos matriciales más fáciles. En su honor, este símbolo se llama la *delta de Kronecker*.

Ejemplo 10.3.9 Una matriz identidad actúa como una identidad

Demuestre que si $\mathbf{A}$ es cualquier matriz $m \times n$ e $\mathbf{I}$ es la matriz identidad $n \times n$, entonces $\mathbf{AI} = \mathbf{A}$. (En el ejercicio 14 al final de esta sección se le pide demostrar que si $\mathbf{I}$ es la matriz identidad $m \times m$, entonces $\mathbf{IA} = \mathbf{A}$.)

Demostración:

Sea $\mathbf{A}$ cualquier matriz $n \times n$ y sea a_{ij} la ij-ésima entrada de $\mathbf{A}$ para todos los enteros $i = 1, 2, \ldots, m$ y $j = 1, 2, \ldots, n$. Considere el producto $\mathbf{AI}$, donde $\mathbf{I}$ es la matriz identidad $n \times n$. Observe que

$$\begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & 2_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix} \begin{bmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \cdots & 1 \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{bmatrix}$$

ya que

$$\begin{aligned} \text{la } ij\text{-ésima entrada de } \mathbf{AI} &= \sum_{r=1}^{n} a_{ir}\delta_{rj} && \text{por definición de 1} \\ &= a_{i1}\delta_{1j} + a_{i2}\delta_{2j} + \cdots && \text{por definición de } \Sigma \\ &\quad + a_{ij}\delta_{jj} + \cdots + a_{in}\delta_{nj} \\ &= a_{ij}\delta_{jj} && \text{ya que } \delta_{kj} = 0 \text{ siempre que } k \neq j \text{ y} \\ &= a_{ij} && \delta_{jj} = 1 \\ &= \text{la } ij\text{-ésima entrada de } \mathbf{A}. \end{aligned}$$

Así $\mathbf{AI} = \mathbf{A}$, como se quería demostrar. ■

También hay similitudes y diferencias entre los números reales y las matrices con respecto al cálculo de potencias. Cualquier número se puede elevar a una potencia de entero no negativo, pero una matriz se puede multiplicar por sí misma, sólo si tiene el mismo número de renglones que de columnas. Como para los números reales, sin embargo, la definición de las potencias de la matriz es recursiva. Como cualquier número a la potencia cero se define como 1, así cualquier matriz $n \times n$ a la potencia cero se define como la matriz identidad $n \times n$. La enésima potencia de una matriz $n \times n$ se define como el producto de $\mathbf{A}$ con su $(n - 1)$-ésima potencia.

• Definición

Para cualquier matriz $n \times n$, las **potencias de A** se definen como:

$$\mathbf{A}^0 = \mathbf{I} \quad \text{donde } \mathbf{I} \text{ es la matriz identidad } n \times n$$
$$\mathbf{A}^n = \mathbf{A}\mathbf{A}^{n-1} \quad \text{para todos los enteros } n \geq 1$$

Ejemplo 10.3.10 Potencias de una matriz

Sea $\mathbf{A} = \begin{bmatrix} 1 & 2 \\ 2 & 0 \end{bmatrix}$. Calcule $\mathbf{A}^0$, $\mathbf{A}^1$, $\mathbf{A}^2$ y $\mathbf{A}^3$.

Solución

$$\mathbf{A}^0 = \text{matriz identidad } 2 \times 2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$
$$\mathbf{A}^1 = \mathbf{A}\mathbf{A}^0 = \mathbf{A}\mathbf{I} = \mathbf{A}$$

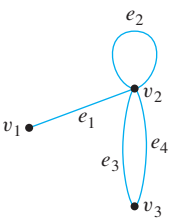
$$\mathbf{A}^2 = \mathbf{A}\mathbf{A}^1 = \mathbf{A}\mathbf{A} = \begin{bmatrix} 1 & 2 \\ 2 & 0 \end{bmatrix}\begin{bmatrix} 1 & 2 \\ 2 & 0 \end{bmatrix} = \begin{bmatrix} 5 & 2 \\ 2 & 4 \end{bmatrix}$$

$$\mathbf{A}^3 = \mathbf{A}\mathbf{A}^2 = \begin{bmatrix} 1 & 2 \\ 2 & 0 \end{bmatrix}\begin{bmatrix} 5 & 2 \\ 2 & 4 \end{bmatrix} = \begin{bmatrix} 9 & 10 \\ 10 & 4 \end{bmatrix}$$

■

Conteo de caminos de longitud N

Un camino en un grafo consta de una sucesión alternada de vértices y aristas. Si se repiten aristas se cuentan cada vez que se produzcan, el número de aristas en la sucesión se llama la **longitud** del camino. Por ejemplo, el camino $v_2 e_3 v_3 e_4 v_2 e_2 v_2 e_3 v_3$ tiene longitud 4 (contando e_3 dos veces). Considere el siguiente grafo G:



¿Cuántos distintos caminos de longitud 2 conectan a v_2 y v_2? Puede enlistar las posibilidades sistemáticamente como sigue: De v_1, la primera arista del camino debe ir a *algún* vértice de G: v_1, v_2 o v_3. Hay un camino de longitud 2 de v_2 a v_2 que comienza al pasar de v_2 a v_1:

$$v_2 e_1 v_1 e_1 v_2 .$$

Hay un camino de longitud 2 de v_2 a v_2 que comienza al ir de v_2 a v_2:

$$v_2 e_2 v_2 e_2 v_2 .$$

Y hay cuatro caminos de longitud 2 de v_2 a v_2 que inicia yendo de v_2 a v_3,

$$v_2 e_3 v_3 e_4 v_2 ,$$
$$v_2 e_4 v_3 e_3 v_2 ,$$
$$v_2 e_3 v_3 e_3 v_2 ,$$
$$v_2 e_4 v_3 e_4 v_2 .$$

Por tanto, la respuesta es seis.

La cuestión general es encontrar el número de caminos que tienen una longitud dada y que conecten dos vértices dados de un grafo puede responderse fácilmente mediante la multiplicación de matrices. Considere la matriz de adyacencia $\mathbf{A}$ de la gráfica G de la página anterior:

$$\mathbf{A} = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \end{array}\begin{array}{c} \begin{array}{ccc} v_1 & v_2 & v_3 \end{array} \\ \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 2 \\ 0 & 2 & 0 \end{bmatrix} \end{array}.$$

Calcule $\mathbf{A}^2$ como:

$$\begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 2 \\ 0 & 2 & 0 \end{bmatrix}\begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 2 \\ 0 & 2 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 2 \\ 1 & 6 & 2 \\ 2 & 2 & 4 \end{bmatrix}.$$

Observe que la entrada en el segundo renglón y la segunda columna es 6, que es igual al número de caminos de longitud 2 de v_2 a v_2. ¡Esto no es casualidad! Para calcular a_{22}, multiplique el segundo renglón de $\mathbf{A}$ por la segunda columna de $\mathbf{A}$ para obtener una suma de tres términos:

$$\begin{bmatrix} 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 2 \end{bmatrix} = 1 \cdot 1 + 1 \cdot 1 + 2 \cdot 2.$$

Observe que

$$\begin{bmatrix} \text{el primer término} \\ \text{de esta suma} \end{bmatrix} = \begin{bmatrix} \text{número de} \\ \text{aristas de} \\ v_2 \text{ a } v_1 \end{bmatrix} \cdot \begin{bmatrix} \text{número de} \\ \text{aristas de} \\ v_1 \text{ a } v_2 \end{bmatrix} = \begin{bmatrix} \text{número de pares de} \\ \text{aristas de} \\ v_2 \text{ a } v_1 \text{ y } v_1 \text{ a } v_2 \end{bmatrix}.$$

Ahora considere el i-ésimo término de esta suma, para cada $i = 1, 2$ y 3. Es igual al número de aristas de v_2 a v_i por el número de aristas de v_i a v_2. Por la regla de multiplicación esto es igual al número de pares de aristas de v_2 a v_i y de v_i de regreso a v_2. Pero esto es igual al número de caminos de longitud 2 que comienzan y terminan en v_2 y pasan por v_i. Ya que este análisis vale para cada término de la suma para $i = 1, 2$ y 3, el número total de caminos es igual al número total de caminos de longitud 2 que comienzan y terminan en v_2:

$$1 \cdot 1 + 1 \cdot 1 + 2 \cdot 2 = 1 + 1 + 4 = 6.$$

Más generalmente, si $\mathbf{A}$ es la matriz de adyacencia de una gráfica G, la ij-ésima entrada de $\mathbf{A}^2$ es igual al número de caminos de longitud 2 que conectan el i-ésimo vértice con el j-ésimo vértice de G. Aún más generalmente, si n es cualquier entero positivo, la ij-ésima entrada de $\mathbf{A}^n$ es igual a la cantidad de caminos de longitud n que conectando el i-ésimo y el j-ésimo vértices de G.

Teorema 10.3.2

Si G es un grafo con vértices $v_1, v_2, \ldots, v_m$ y $\mathbf{A}$ es la matriz de adyacencia de G, entonces para cada entero positivo n y para todos los enteros $i, j = 1, 2, \ldots, m$,

la ij-ésima entrada de $\mathbf{A}^n$ = número de caminos de longitud n de v_i a v_j.

Demostración:

Suponga que G es un grafo con vértices $v_1, v_2, \ldots, v_m$ y $\mathbf{A}$ es la matriz de adyacencia de G. Sea $P(n)$ la frase

Para todos los enteros $i, j = 1, 2, \ldots, m$, ← $P(n)$
la entrada ij-ésima de $\mathbf{A}^n$ = número de caminos de longitud n de v_i a v_j.

Utilizaremos inducción matemática para demostrar que la $P(n)$ es verdadera para todos los enteros $n \geq 1$.

Demostración de que P(1) es verdadera:

La ij-ésima entrada de $\mathbf{A}^1$	= la ij-ésima entrada de $\mathbf{A}$	ya que $\mathbf{A}^1 = \mathbf{A}$
	= número de aristas que conectan a v_i con v_j	por la definición de matriz de adyacencia
	= número de caminos de longitud 1 de v_i a v_j	ya que un camino de longitud 1 contiene una única arista.

Demostración de que para todos los enteros k con k ≥ 1, si P(k) es verdadera entonces P(k + 1) es verdadera:

Sea k un entero con $k \geq 1$ y suponga que

Para todos los enteros $i, j = 1, 2, \ldots, m$, ← $P(k)$
la ij-ésima entrada de $\mathbf{A}^k$ = el número de caminos de longitud k de v_i a v_j. hipótesis de inducción

Debemos demostrar que

Para todos los enteros $i, j = 1, 2, \ldots, m$, ← $P(k+1)$
la ij-ésima entrada de $\mathbf{A}^{k+1}$ = el número de caminos de longitud $k+1$ de v_i a v_j.

Sea $\mathbf{A} = (a_{ij})$ y $\mathbf{A}^k = (b_{ij})$. De $\mathbf{A}^{k+1} = \mathbf{A}\mathbf{A}^k$, la ij-ésima entrada de $\mathbf{A}^{k+1}$ se obtiene multiplicando el i-ésimo renglón por la j-ésima columna de $\mathbf{A}^k$:

$$ij\text{-ésima entrada de } \mathbf{A}^{k+1} = a_{i1}b_{1j} + a_{i2}b_{2j} + \cdots a_{im}b_{mj} \qquad 10.3.1$$

para toda $i, j = 1, 2, \ldots, m$. Ahora considere cada uno de los términos de esta suma: a_{i1} es el número de aristas de v_i a v_1 y, por la hipótesis de inducción, b_{1j} es el número de caminos de longitud k de v_1 a v_j. Pero cualquier arista de v_i a v_1 puede combinarse con cualquier camino de longitud k de v_1 a v_j para crear un camino de longitud $k+1$ de v_i a v_j con v_1 como su segundo vértice. Así, por la regla de multiplicación,

$$a_{i1}b_{1j} = \left[\begin{array}{l}\text{número de caminos de longitud } k+1 \text{ de} \\ v_i \text{ a } v_j \text{ que tienen } v_1 \text{ como su segundo vértice}\end{array}\right].$$

Más generalmente, para cada entero $r = 1, 2, \ldots, m$,

$$a_{ir}b_{rj} = \left[\begin{array}{l}\text{número de caminos de longitud } k+1 \text{ de} \\ v_i \text{ a } v_j \text{ que tienen } v_r \text{ como su segundo vértice}\end{array}\right].$$

Puesto que cualquier camino de longitud $k+1$ de v_i a v_j debe tener *uno* de los vértices $v_1, v_2, \ldots, v_m$ como su segundo vértice, el número total de caminos de longitud $k+1$ de v_i a v_j es igual a la suma en (10.3.1), que es igual a la ij-ésima entrada de $\mathbf{A}^{k+1}$. Por lo que

la ij-ésima entrada de $\mathbf{A}^{k+1}$ = el número de caminos de longitud $k+1$ de v_i a v_j

[como se quería demostrar].
[Ya se han demostrado el paso básico y el paso de inducción, la frase P(n) es verdadera para todo entero $n \geq 1$.]

Autoexamen

1. En la matriz de adyacencia para un grafo dirigido, la entrada en el i-ésimo renglón y j-ésima columna es _____.
2. En la matriz de adyacencia para un grafo no dirigido, la entrada en el i-ésimo renglón y j-ésima columna es _____.
3. Una matriz $n \times n$ se llama simétrica si y sólo si, para todos los enteros i y j de 1 a n, la entrada en el renglón _____ y en la columna _____ es igual a la entrada en el renglón _____ y en la columna _____.
4. La ij-ésima entrada en el producto de dos matrices $\mathbf{A}$ y $\mathbf{B}$ se obtiene multiplicando renglón _____ de $\mathbf{A}$ por renglón _____ de $\mathbf{B}$.
5. En una matriz identidad $n \times n$ las entradas de la diagonal principal son las entradas de todas _____ y fuera de la diagonal son todas _____.
6. Si G es un grafo con vértices, $v_1, v_2, \ldots, v_m$ y $\mathbf{A}$ es la matriz de adyacencia de G, entonces para cada entero positivo n y para todos los enteros, i y j con $i, j = 1, 2, \ldots, m$, la ij-ésima entrada de $\mathbf{A}^n$ = _____.

Conjunto de ejercicios 10.3

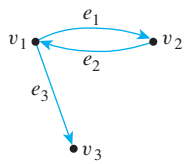
1. Encuentre los números reales a, b y c tales que las siguientes expresiones sean verdaderas.

a. $\begin{bmatrix} a+b & a-c \\ c & b-a \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ -1 & 3 \end{bmatrix}$

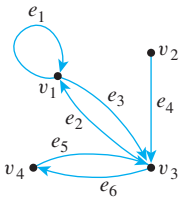
b. $\begin{bmatrix} 2a & b+c \\ c-a & 2b-a \end{bmatrix} = \begin{bmatrix} 4 & 3 \\ 1 & -2 \end{bmatrix}$

2. Encuentre las matrices de adyacencia para los siguientes grafos dirigidos.

a.



b.

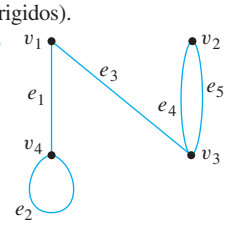


3. Encuentre los grafos dirigidos que tienen las siguientes matrices de adyacencia.

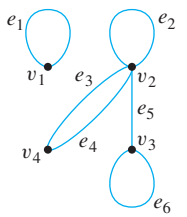
a. $\begin{bmatrix} 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 0 \\ 0 & 2 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$ b. $\begin{bmatrix} 0 & 1 & 0 & 0 \\ 2 & 0 & 1 & 0 \\ 1 & 2 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$

4. Determine las matrices de adyacencia para los siguientes grafos (no dirigidos).

a.



b.



c. K_4, el grafo completo de cuatro vértices
d. $K_{2,3}$ el grafo bipartito completo en los vértices (2, 3)

5. Encuentre los grafos que tengan las siguientes matrices de adyacencia.

a. $\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 2 \\ 1 & 2 & 0 \end{bmatrix}$ b. $\begin{bmatrix} 0 & 2 & 0 \\ 2 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$

6. Las siguientes son matrices de adyacencia de grafos. En cada caso determine si el grafo es conexo mediante el análisis de la matriz sin dibujar el grafo.

a. $\begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$ b. $\begin{bmatrix} 0 & 2 & 0 & 0 \\ 2 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$

7. Suponga que para todos los enteros positivos i, todas las entradas en el i-ésimo renglón y en la i-ésima columna de la matriz de adyacencia de un grafo son 0. ¿Qué puede concluir acerca del grafo?

8. Encuentre cada uno de los siguientes productos.

a. $\begin{bmatrix} 2 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 3 \end{bmatrix}$ b. $\begin{bmatrix} 4 & -1 & 7 \end{bmatrix} \begin{bmatrix} 1 \\ 2 \\ 0 \end{bmatrix}$

9. Encuentre cada uno de los siguientes productos.

a. $\begin{bmatrix} 3 & 0 \\ 1 & -2 \end{bmatrix} \begin{bmatrix} 1 & -1 & 4 \\ 0 & 2 & 1 \end{bmatrix}$

b. $\begin{bmatrix} 2 & 0 & 1 \\ 0 & -1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 3 \\ 5 & -4 \\ -2 & 2 \end{bmatrix}$

c. $\begin{bmatrix} -1 \\ 2 \end{bmatrix} \begin{bmatrix} 2 & 3 \end{bmatrix}$

10. Sea $\mathbf{A} = \begin{bmatrix} 1 & 1 & -1 \\ 0 & -2 & 1 \end{bmatrix}$, $\mathbf{B} = \begin{bmatrix} -2 & 0 \\ 1 & 3 \end{bmatrix}$ y $\mathbf{C} = \begin{bmatrix} 0 & -2 \\ 3 & 1 \\ 1 & 0 \end{bmatrix}$.

Para cada una de las expresiones siguientes, determine si el producto indicado existe y calcúlelo si existe.

a. $\mathbf{AB}$ **b.** $\mathbf{BA}$ c. $\mathbf{A}^2$ d. $\mathbf{BC}$ e. $\mathbf{CB}$
f. $\mathbf{B}^2$ g. $\mathbf{B}^3$ h. $\mathbf{C}^2$ **i.** $\mathbf{AC}$ j. $\mathbf{CA}$

11. Dé un ejemplo diferente que en el libro para mostrar que la multiplicación de matrices no es conmutativa. Es decir, encuentre matrices 2×2, $\mathbf{A}$ y $\mathbf{B}$ tales que $\mathbf{AB}$ y $\mathbf{BA}$ existen pero $\mathbf{AB} \neq \mathbf{BA}$.

12. Sea O la matriz $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$. Encuentre matrices 2×2, $\mathbf{A}$ y $\mathbf{B}$ tales que $\mathbf{A} \neq \mathrm{O}$ y $\mathbf{B} \neq \mathrm{O}$ pero $\mathbf{AB} = \mathrm{O}$.

13. Sea O la matriz $\begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$. Encuentre matrices 2×2, $\mathbf{A}$ y $\mathbf{B}$ tales que $\mathbf{A} \neq \mathbf{B}$, $\mathbf{B} \neq \mathrm{O}$ y $\mathbf{AB} \neq \mathrm{O}$, pero $\mathbf{BA} = \mathrm{O}$.

En los ejercicios del 14 al 18 suponga que las entradas de todas las matrices son números reales.

***H* 14.** Demuestre que si $\mathbf{I}$ es la matriz identidad $m \times m$ y $\mathbf{A}$ es cualquier matriz $m \times n$, entonces $\mathbf{IA} = \mathbf{A}$.

15. Demuestre que si $\mathbf{A}$ es una matriz simétrica $m \times m$, $\mathbf{A}^2$ es simétrica.

16. Demuestre que el producto de matrices es asociativo: si $\mathbf{A}$, $\mathbf{B}$ y $\mathbf{C}$ son matrices cualesquiera $m \times k$, $k \times r$ y $r \times n$, respectivamente, entonces $(\mathbf{AB})\mathbf{C} = \mathbf{A}(\mathbf{BC})$.

17. Utilice inducción matemática y el resultado del ejercicio 16 para demostrar que si $\mathbf{A}$ es cualquier matriz $m \times m$, entonces $\mathbf{A}^n\mathbf{A} = \mathbf{A}\mathbf{A}^n$ para todos los enteros $n \geq 1$.

18. Utilice inducción matemática para demostrar que si $\mathbf{A}$ es una matriz simétrica $m \times m$, entonces para cualquier entero $n \geq 1$, $\mathbf{A}^n$ también es simétrica.

19. **a.** Sea $\mathbf{A} = \begin{bmatrix} 1 & 1 & 2 \\ 1 & 0 & 1 \\ 2 & 1 & 0 \end{bmatrix}$. Encuentre $\mathbf{A}^2$ y $\mathbf{A}^3$.

b. Sea G el grafo con vértices v_1, v_2 y v_3 y con $\mathbf{A}$ como su matriz de adyacencia. Utilice las respuestas del inciso *a*) para encontrar el número de caminos de longitud 2 de v_1 a v_3 y el número de caminos de longitud 3 de v_1 a v_3. No dibuje G para resolver este problema.

c. Examine los cálculos que realizó para responder el inciso *a*) para encontrar cinco caminos de longitud 2 de v_3 a v_3. Después dibuje G y encuentre los caminos por inspección visual.

20. La siguiente es una matriz de adyacencia para un grafo:

$$\begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \end{array} \begin{array}{c} \begin{array}{cccc} v_1 & v_2 & v_3 & v_4 \end{array} \\ \begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 0 & 2 & 1 \\ 1 & 2 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix} \end{array}$$

Responda las siguientes preguntas mediante el examen de la matriz y sus potencias, no dibuje el grafo:

a. ¿Cuántos caminos de longitud 2 existen de v_2 a v_3?
b. ¿Cuántos caminos de longitud 2 existen de v_3 a v_4?
c. ¿Cuántos caminos de longitud 3 existen de v_1 a v_4?
d. ¿Cuántos caminos de longitud 3 existen de v_2 a v_3?

21. Sea $\mathbf{A}$ la matriz de adyacencia para K_3, el grafo completo en tres vértices. Utilice inducción matemática para demostrar que para cada entero positivo n, todas las entradas a lo largo de la diagonal principal de $\mathbf{A}^n$ son iguales entre sí y todas las entradas que no se encuentran en la diagonal principal son iguales entre sí.

22. a. Dibuje un grafo que tenga a

$$\begin{bmatrix} 0 & 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 2 & 1 \\ 1 & 1 & 2 & 0 & 0 \\ 2 & 1 & 1 & 0 & 0 \end{bmatrix}$$

como su matriz de adyacencia. ¿Es este grafo bipartito? (Para una definición de bipartito, vea el ejercicio 37 en la sección 10.1.)

Definición: Dada una matriz $\mathbf{A}$, $m \times n$ cuya ij-ésima entrada se denota por a_{ij}, la **traspuesta de** $\mathbf{A}$ es la matriz $\mathbf{A}^t$ cuya ij-ésima entrada es a_{ji}, para todas $i = 1, 2, \ldots, m$ y $j = 1, 2, \ldots, n$.

Observe que el primer renglón de $\mathbf{A}$ se convierte en la primera columna de $\mathbf{A}'$, el segunda renglón de $\mathbf{A}$ se convierte en la segunda columna de $\mathbf{A}'$ y así sucesivamente. Por ejemplo,

$$\text{si } \mathbf{A} = \begin{bmatrix} 0 & 2 & 1 \\ 1 & 2 & 3 \end{bmatrix}, \text{ entonces } \mathbf{A}^t = \begin{bmatrix} 0 & 1 \\ 2 & 2 \\ 1 & 3 \end{bmatrix}.$$

H **b.** Demuestre que un grafo con n vértices es bipartito si y sólo si, para algunos etiquetados de sus vértices, su matriz de adyacencia tiene la forma

$$\begin{bmatrix} \mathbf{O} & \mathbf{A} \\ \mathbf{A}^t & \mathbf{O} \end{bmatrix}$$

donde $\mathbf{A}$ es una matriz $k \times (n - k)$ para algún entero k tal que $0 < k < n$, la parte superior izquierda de O representa una matriz $k \times k$ todas cuyas entradas son 0, $\mathbf{A}^t$ es la transpuesta de $\mathbf{A}$ y la parte inferior derecha O representa una matriz $(n - k) \times (n - k)$ cuyas entradas son 0.

23 a. Sea G un grafo con n vértices y sean v y w distintos vértices de G. Pruebe que si hay un camino de v a w, entonces hay un camino de v a w que tiene longitud inferior o igual a $n - 1$.

H **b.** Si $\mathbf{A} = (a_{ij})$ y $\mathbf{B} = (b_{ij})$ son matrices cualesquiera $m \times n$, la matriz $\mathbf{A} + \mathbf{B}$ es la matriz $m \times n$ cuya ij-ésima entrada es $a_{ij} + b_{ij}$ para todas $i = 1, 2, \ldots, m$ y $j = 1, 2, \ldots, n$. Sea G un grafo con n vértices, donde $n > 1$ y sea $\mathbf{A}$ la matriz de adyacencia de G. Demuestre que G es conexo si y sólo si, cada entrada del $\mathbf{A} + \mathbf{A}^2 + \cdots + \mathbf{A}^{n-1}$ es positivo.

Respuestas del autoexamen

1. el número de flechas de v_i (el vértice i-ésimo) para v_j (el vértice j-ésimo) 2. el número de aristas que conectan a v_i (el vértice i-ésimo) y v_j (el vértice j-ésimo) 3. i; j; j; i 4. i; j 5. 1; 0 6. el número de caminos de longitud n de v_i a v_j

10.4 Isomorfismos de grafos

El pensamiento es un despido momentáneo de irrelevantes. —R. Buckminster Fuller, 1969

Recuerde del ejemplo 10.1.3 que los dos dibujos que se muestran en la figura 10.4.1 ambos representan el mismo grafo: Sus conjuntos de aristas y de vértices son idénticos y sus funciones arista-punto extremo son las mismas. Se le llama a este grafo G.

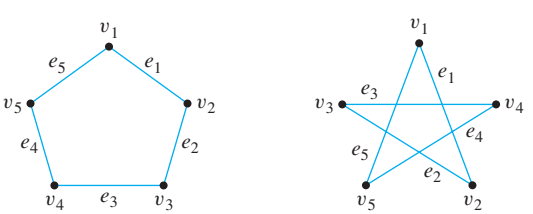


Figura 10.4.1

Ahora considere el grafo G' que se representa en la figura 10.4.2.

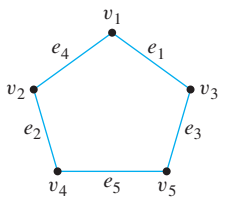


Figura 10.4.2

Observe que G' es un grafo diferente de G (por ejemplo, en G los puntos extremos de e_1 son v_1 y v_2, mientras que en G' los puntos extremos de e_1 son v_1 y v_3). Sin embargo, G' es, sin duda, muy similar a G. De hecho, si los vértices y aristas de G' son re-etiquetados por las funciones que se muestran en la figura 10.4.3, entonces G' se convierte en la misma G.

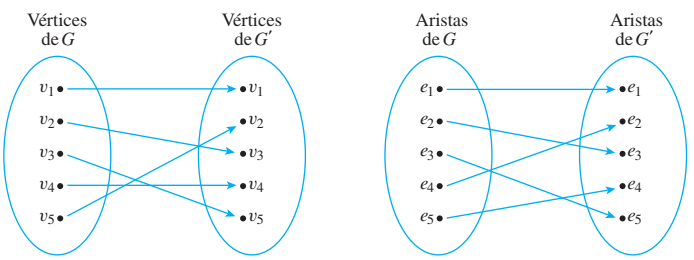


Figura 10.4.3

Observe que estas funciones re-etiquetadas son inyectivas y sobreyectivas.

Dos grafos que son iguales excepto para el etiquetado de sus vértices y aristas se llaman *isomorfos*. La palabra *isomorfismo* proviene del griego, que significa "misma forma". Los grafos isomorfos son aquellos que tienen esencialmente la misma forma.

• Definición

Sean G y G' grafos con conjuntos de vértices $V(G)$ y $V(G')$ y conjuntos de aristas, $E(G)$ y $E(G')$, respectivamente. **G es isomorfo a G'** si y sólo si, existe una correspondencia uno a uno g: $V(G) \to V(G')$ y h: $E(G) \to E(G')$ que preserva las funciones de punto extremo-aristas de G y G' en el sentido que para todo $v \in V(G)$ y $e \in E(G)$,

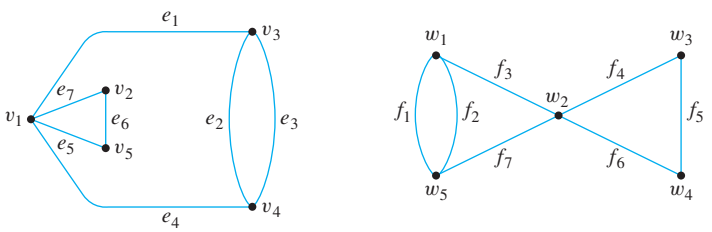
$$v \text{ es un punto extremo de } e \iff g(v) \text{ es un punto extremo de } h(e). \qquad 10.4.1$$

En palabras, G es isomorfa a G' si y sólo si, los vértices y aristas de G y G' se pueden igualar por funciones inyectivas y sobreyectivas tales que las aristas y los vértices se correspondan entre sí.

Es común en matemáticas identificar los objetos que son isomorfos. Por ejemplo, si se nos da un grafo G con cinco vértices tal que cada par de vértices está conectado por una arista, entonces podemos identificar G con K_5, diciendo que G es K_5, en lugar de que G es isomorfa con K_5.

Ejemplo 10.4.1 Demostración de que dos grafos son isomorfos

Demuestre que los siguientes dos grafos son isomorfos.

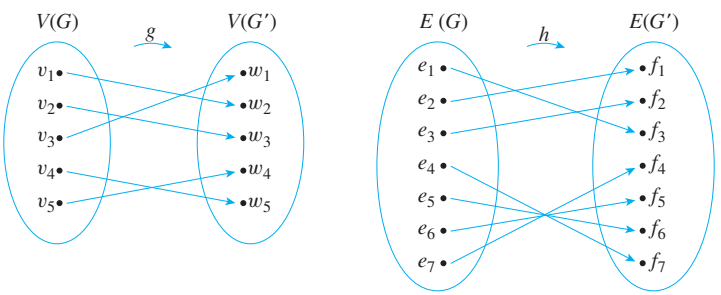


G G'

Solución Para resolver este problema, debe encontrar funciones $g: V(G) \to V(G')$ y h: $E(G) \to E(G')$ tales que para toda $v \in V(G)$ y $e \in E(G)$, v es un punto extremo de e si y sólo si, $g(v)$ es un punto extremo de $h(e)$. La configuración de las funciones es en parte una cuestión de ensayo y error y en parte una cuestión de deducción. Por ejemplo, puesto que e_2 y e_3 son paralelas (tienen los mismos puntos extremos), $h(e_2)$ y $h(e_3)$ también deben ser paralelas. Así $h(e_2) = f_1$ y $h(e_3) = f_2$ o $h(e_2) = f_2$ y $h(e_3) = f_1$. También, los puntos extremos de e_2 y e_3 deben corresponder a los puntos extremos de f_1 y f_2 y así $g(v_3) = w_1$ y $g(v_4) = w_5$ o $g(v_3) = w_5$ y $g(v_4) = w_1$.

Similarmente ya que v_1 es el punto extremo de cuatro aristas distintas (e_1, e_7, e_5 y e_4), $g(v_1)$ también debe ser el punto extremo de cuatro aristas distintas (porque cada arista que incide en $g(v_1)$ es la imagen bajo h de una arista que incide en v_1 y h es inyectiva y sobreyectiva). Pero el único vértice en G' que tiene cuatro aristas saliendo de él es w_2 y así $g(v_1) = w_2$. Ahora si $g(v_3) = w_1$, entonces ya que v_1 y v_3, son puntos extremos de e_1 en G, $g(v_1) = w_2$ y $g(v_3) = w_1$ deben ser puntos extremos de $h(e_1)$ en G'. Esto implica que $h(e_1) = f_3$.

Continuando de esta manera, posiblemente haciendo algunas decisiones arbitrarias conforme avanza, eventualmente puede encontrar las funciones g y h para definir el isomorfismo entre G y G'. Un par de funciones (hay varias) es el siguiente:



■

No es difícil demostrar que ese isomorfismo gráfico es una relación de equivalencia en un conjunto de grafos; en otras palabras, es reflexiva, simétrica y transitiva.

Teorema 10.4.1 El isomorfismo gráfico es una relación de equivalencia

Sea S un conjunto de grafos y sea R la relación de isomorfismo gráfico en S. Entonces R es una relación de equivalencia en S.

Demostración:

R es reflexiva: Dado cualquier grafo G en S, defina un isomorfismo gráfico de G a G mediante las funciones identidad en el conjunto de vértices y en el conjunto de aristas de G.

R es simétrica: Dados los grafos cualesquiera G y G' en S tales que G es isomorfa a G', debemos demostrar que G' es isomorfa a G.

continúa en la página 678

Pero esto es así porque si g y h son las correspondencias de vértice y arista de G a G' que preservan las funciones de punto final-aristas, entonces g^{-1} y h^{-1} son las correspondencias de vértice y arista de G' G que preservan las funciones de punto final-aristas.

R es transitiva: Dadas los grafos cualesquiera G, G' y G'' en S tal que G es isomórfica a G' y G' es isomórfica a G'', debemos demostrar que G es isomórfica a G''.

Pero esto se deduce del hecho que si g_1 y h_1 son los vértices y aristas correspondientes de G a G' que preservan las funciones de punto final-aristas de G y G' y g_2 y h_2 son los vértices y aristas correspondientes de G' a G'' que preservan las funciones punto final-aristas de G' y G'', entonces g_2 o g_1 y h_2 o h_1 son vértices y correspondencias de G a G'' que preservan las funciones de punto final-aristas de G y G''.

Nota Como una consecuencia de la propiedad de simetría podemos simplemente decir que "G y G' son isomorfas" en lugar de "G es isomorfa a G''' o "G' es isomorfa a G".

Ejemplo 10.4.2 Encuentre representantes de las clases de isomorfismo

Encuentre todos los grafos no isomorfos que tienen dos vértices y dos aristas. En otras palabras, encuentre una colección de grafos representativos con dos vértices y dos aristas tales que todos esos grafos son isomorfos a una en la colección.

Solución Hay cuatro grafos no isomorfos que tienen dos vértices y dos aristas. Estos se pueden dibujar sin etiquetas de vértice y arista porque cualesquiera dos etiquetados de grafos isomorfos.

a) *b*) *c*) *d*)

Para ver que estos cuatro dibujos demuestran todos los grafos no isomorfos que tienen dos vértices y dos aristas, primero observe si una de las aristas une los dos vértices o no. Si lo hace, hay dos posibilidades: la otra arista también puede unir los dos vértices (como en *a*) o puede ser un bucle incidiendo en uno de ellos (como en *b*, no hay ninguna diferencia en *cuál* vértice se elija que esté el bucle ya que al intercambiar las dos etiquetas del vértice se obtienen grafos isomorfos). Si ninguna de las dos aristas se unen a los dos vértices, ambas aristas son bucles. En este caso, hay dos posibilidades: O ambos bucles están incidiendo en el mismo vértice (como en *c*) o los dos bucles están incidiendo en vértices independientes (como en *d*). Cuando ya no hay ninguna otra posibilidad de colocar las aristas, la lista está completa. ■

Ahora considere la pregunta, ¿existe un método general para averiguar si los grafos G y G' son isomorfos? En otras palabras, ¿existe algún algoritmo que aceptará grafos G y G' como entrada y produzca un enunciado acerca de si son isomorfos? De hecho, existe tal algoritmo. Consiste en generar todas las funciones inyectivas, sobreyectivas del conjunto de vértices de G al conjunto de vértices de G' y del conjunto de aristas de G para el conjunto de aristas de G' y comprobar cada par determinando si se conservan la función de punto extremo-aristas de G y G'. El problema con este algoritmo es que tarda un tiempo excesivamente largo realizarlo, aún en una computadora de alta velocidad. Si G y G' cada una tiene n vértices y m aristas, el número de correspondencias uno a uno de vértices a vértices es $n!$ y el número de correspondencias uno a uno de aristas a aristas es $m!$, así el número total de pares de funciones para comprobar es $n! \cdot m!$ Por ejemplo, si $m = n = 20$, habrá $20! \cdot 20! \cong 5.9 \times 10^{36}$ pares para comprobar. Suponiendo que cada comprobación lleva sólo 1 nanosegundo, ¡el tiempo total sería aproximadamente 1.9×10^{20} años!

Lamentablemente, no hay método conocido más eficiente para comprobar si dos grafos son isomorfos. Sin embargo, hay algunas pruebas sencillas que se pueden utilizar para mostrar que ciertos pares de grafos *no* son isomorfos. Por ejemplo, si dos grafos son isomorfos, entonces tienen el mismo número de vértices (porque hay una correspondencia uno a uno del conjunto de vértices de un grafo al conjunto de vértices de otro). Se tiene que si le dan dos grafos, una con 16 vértices y la otra con 17, usted puede inmediatamente concluir que los dos no son isomorfos. Más generalmente, una propiedad que conserva de isomorfismo de un grafo se llama *invariante isomorfo*. Por ejemplo, "tener 16 vértices" es un invariante isomorfo: si un grafo tiene 16 vértices, entonces cualquier grafo que es isomorfo también los tiene.

• Definición

Una propiedad P se llama una **invariante del isomorfismo del grafo** si y sólo si, dados los grafos cualesquiera G y G', si G tiene la propiedad P y G' es isomorfa a G, entonces G' tiene la propiedad P.

Teorema 10.4.2

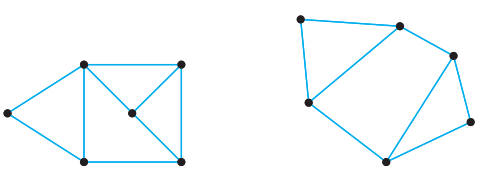
Cada una de las siguientes propiedades es un invariante del isomorfismo del grafo, donde n, m y k son todos enteros no negativos:

1. tiene n vértices;
2. tiene m aristas;
3. tiene un vértice de grado k;
4. tiene m vértices de grado k;
5. tiene un circuito de longitud k;
6. tiene un circuito simple de longitud k;
7. tiene m circuitos simples de longitud k;
8. es conexo;
9. tiene un circuito de Euler;
10. tiene un circuito hamiltoniano.

Ejemplo 10.4.3 Demostración de que dos grafos no son isomorfos

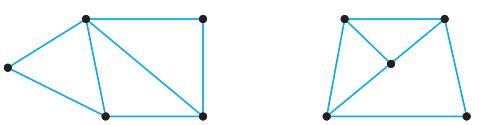
Demuestre que los siguientes pares de grafos no son isomorfos encontrando un invariante isomorfo que no comparten.

a.



G G'

b.



H H'

Solución

a. G tiene nueve aristas; G' tiene sólo ocho.

b. H tiene un vértice de grado 4; H' no. ■

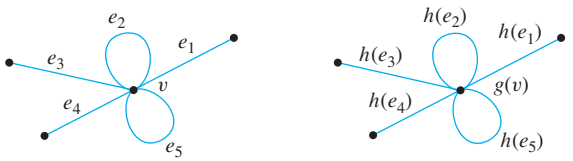
Demostraremos la parte 3) del teorema 10.4.2 en la página siguiente y dejaremos las demostraciones de las otras partes como ejercicios.

Ejemplo 10.4.4 Demostración del teorema 10.4.2, parte (3)

Demostración de que si G es un grafo que tiene un vértice de grado k y G' es isomorfo a G, entonces G' tiene un vértice de grado k.

Demostración:

Suponga que G y G' son grafos isomorfos y que G tiene un vértice v de grado k, donde k es un entero no negativo. *[Debemos demostrar que G' tiene un vértice de grado k.]* Puesto que G y G' son isomorfos, existen las funciones inyectivas, sobreyectivas g y h de los vértices de G a los vértices de G' y de las aristas de G a las aristas de G' que preservan las funciones de punto extremo-aristas en el sentido que para todas las aristas e y todos los vértices u de G, u es un punto extremo de e si y sólo si, $g(u)$ es un punto extremo de $h(e)$. A continuación se muestra un ejemplo de un vértice particular v.



Grado $v = 3 + 2 \cdot 2 = 7$ Grado $g(v) = 3 + 2 \cdot 2 = 7$

Sean $e_1, e_2, \ldots, e_m$ m aristas distintas que inciden en un vértice v en G, donde m es un entero no negativo. Entonces $h(e_1), h(e_2), \ldots, h(e_m)$ son m aristas distintas que inciden sobre $g(v)$ en G'. *[La razón por qué $h(e_1), h(e_2), \ldots, h(e_m)$ son distintas es que h es inyectiva y $e_1, e_2, \ldots, e_m$ son distintas. Y la razón de por qué $h(e_1), h(e_2), \ldots, h(e_m)$ inciden en $g(v)$ es que g y h preservan la función de punto extremo-aristas de G y G' y $e_1, e_2, \ldots, e_m$ inciden en v.]*

También, no hay ningún arista que incida en $g(v)$ distinta de las que son imágenes bajo g de aristas que inciden sobre v *[ya que g es sobreyectiva y g y h conservan la función de punto extremo-aristas de G y G']*. Por tanto el número de aristas que inciden en v es igual al número de aristas que incide en $g(v)$.

Por último, una arista e es un bucle en v si y sólo si, $h(e)$ es un bucle en $g(v)$, así el número de bucles que inciden en v es igual al número de bucles que inciden en $g(v)$. [*Ya que g y h conservan las funciones de punto extremo-aristas de G y G', un vértice w es un punto extremo de e en G si y sólo si, $g(w)$ es un punto extremo de $h(e)$ en G'. De lo que se deduce que v es el único punto extremo de e en G si y sólo si, $g(v)$ es el único punto extremo de $h(e)$ en G'.*]

Ahora el grado de v, que es k, es igual al número de aristas que inciden en v más el número de aristas que inciden en v que son bucles (ya que cada bucle contribuye en 2 al grado de v). Pero ya hemos demostrado que el número de aristas que inciden en v es igual al número de arista que inciden en $g(v)$ y que el número de bucles que inciden en v es igual al número de bucles que inciden en $g(v)$. Por lo que $g(v)$ también tiene grado k. ■

Isomorfismo gráfico para grafos simples

Cuando los dos grafos G y G' son ambos simples, la definición de que G sea isomorfo a G' se puede escribir sin hacer referencia a la correspondencia entre las aristas de G y las aristas de G'.

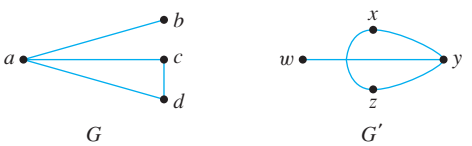
• Definición

Si G y G' son grafos simples, entonces **G es isomorfo a G'** si y sólo si, existe una correspondencia g uno a uno del conjunto de vértices $V(G)$ de G al conjunto de vértices $V(G')$ de G' que conserva las funciones de punto extremo-aristas de G y G' en el sentido que para todos los vértices u y v de G,

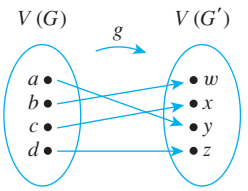
$$\{u, v\} \text{ es una arista en } G \iff \{g(u), g(v)\} \text{ es una arista en } G'. \qquad 10.4.2$$

Ejemplo 10.4.5 Isomorfismo de grafos simples

¿Los dos grafos que se muestran a continuación son isomorfos? Si es así, defina un isomorfismo.



Solución Sí. Se define $f: V(G) \to V(G')$ por el diagrama de flecha que se muestra a continuación.



Entonces g es inyectiva y sobreyectiva por inspección. El hecho de que g conserva las funciones de punto extremo-aristas de G y G' se muestra en la siguiente tabla:

Aristas de G	Aristas de G'
$\{a, b\}$	$\{y, w\} = \{g(a), g(b)\}$
$\{a, c\}$	$\{y, x\} = \{g(a), g(c)\}$
$\{a, d\}$	$\{y, z\} = \{g(a), g(d)\}$
$\{c, d\}$	$\{x, z\} = \{g(c), g(d)\}$

■

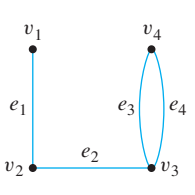
Autoexamen

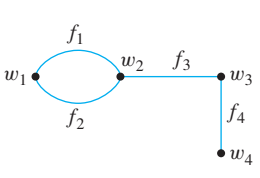
1. Si G y G' son grafos, entonces G es isomorfo a G' si y sólo si, hay una correspondencia g uno a uno del conjunto de vértices de G al conjunto de vértice de G' y una correspondencia h uno a uno del conjunto de aristas de G al conjunto de aristas de G' tal que para todos de vértices v y aristas e en G, v es un punto extremo de e si y sólo si, _____.
2. Una propiedad P es una invariante para isomorfismo gráfico si y sólo si, dados cualesquiera grafos G y G', si G tiene la propiedad P y G' es isomorfo a G entonces _____.
3. Algunos invariantes para los isomorfismos gráficos son ____, ____, ____, ____, ____, ____, ____, ____, ____ y ____.

Conjunto de ejercicios 10.4

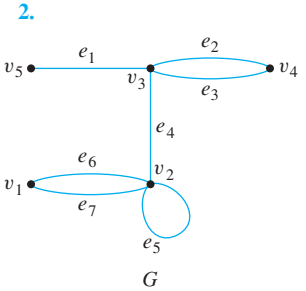
Para cada par de grafos G y G' en los ejercicios del 1 al 5, determine si G y G' son isomorfos. Si es así, de las funciones $g: V(G) \to V(G')$ y $h: E(G) \to E(G')$ que definen el isomorfismo. Si no son, de un invariante que no compartan

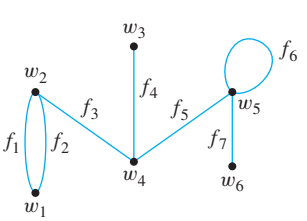
1.



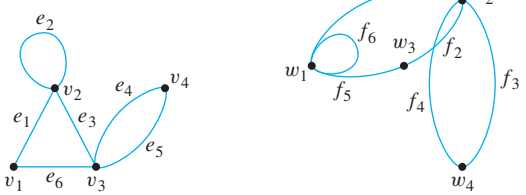


2.



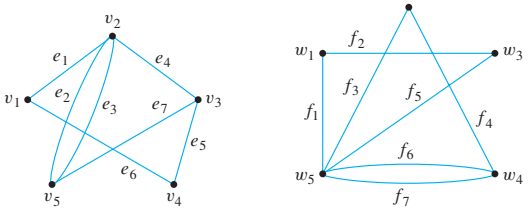


3.



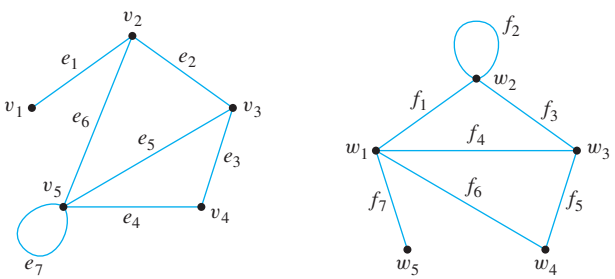
G $\quad$ G'

4.



G $\quad$ G'

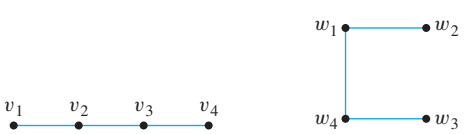
5.



G $\quad$ G'

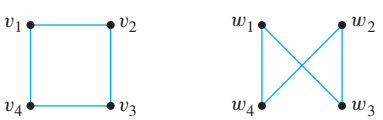
Para cada par de grafos simples G y G' en los ejercicios del 6 al 13, determine si G y G' son isomorfos. Si es así, de una función $g\colon V(G) \to V(G')$ que defina el isomorfismo. Si no es así, de un invariante para el isomorfismo gráfico que no compartan.

6.



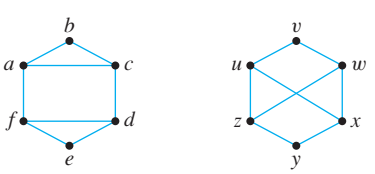
G $\quad$ G'

7.



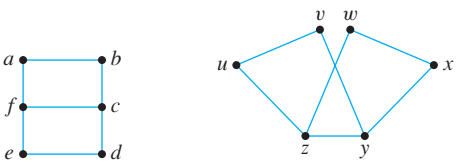
G $\quad$ G'

8.



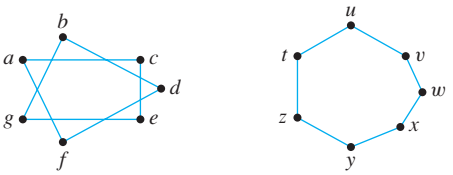
G $\quad$ G'

9.



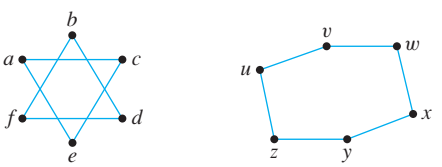
G $\quad$ G'

10.



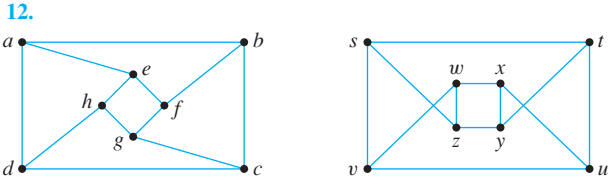
G $\quad$ G'

11.



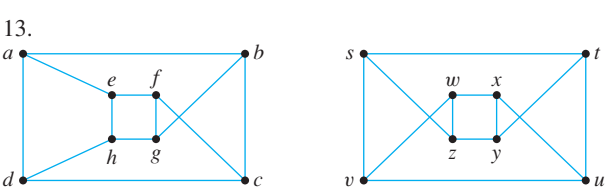
G $\quad$ G'

12.



G $\quad$ G'

13.



G $\quad$ G'

14. Dibuje todos los grafos simples no isomorfos con tres vértices.

15. Dibuje todos los grafos simples no isomorfos con cuatro vértices.

16. Dibuje todos los grafos no isomorfos con tres vértices y aristas no más de dos.

17. Dibuje todos los grafos no isomorfos con cuatro vértices y no más de dos aristas.

***H* 18.** Dibuje todos los grafos no isomorfos con cuatro vértices y tres aristas.

19. Dibuje todos los grafos no isomorfos con seis vértices, todos con grado 2.

20. Dibuje cuatro grafos no isomorfos con seis vértices, dos de grado 4 y cuatro de grado 3.

Demuestre que cada una de las propiedades en los ejercicios del 21 al 29 es un invariante de isomorfismo gráfico. Se supone que n, m y k son todos enteros no negativos.

21. Tiene n vértices

22. Tiene m aristas

23. Tiene un circuito de longitud k

24. Tiene un circuito simple de longitud k

H 25. Tiene m vértices de grado k

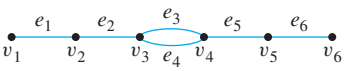
26. Tiene m circuitos simples de longitud k

H 27. Es conexo

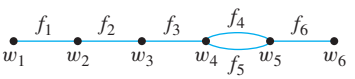
28. Tiene un circuito de Euler

29. Tiene un circuito hamiltoniano

30. Demuestre que los siguientes dos grafos no son isomorfos suponiendo que son isomorfos y deduciendo una contradicción.



G



G'

Respuestas del autoexamen

1. $g(v)$ es un punto extremo de $h(e)$ 2. G' tiene la propiedad P 3. tiene n vértices; tiene m aristas; tiene un vértice de grado k; tiene m vértices de grado k; tiene un circuito de longitud k; tiene un circuito simple de longitud k; tiene m circuitos simples de longitud k; es conexo; tiene un circuito de Euler; tiene un circuito hamiltoniano

10.5 Árboles

No estamos muy contentos cuando nos vemos obligados a aceptar una verdad matemática en virtud de una cadena complicada de conclusiones formales y cálculos, que se recorren a ciegas, punto por punto, sintiendo nuestro camino por contacto. En primer lugar queremos una visión general del objetivo y de la carretera; queremos entender la idea de la demostración, el contexto más profundo.

—Hermann Weyl, 1885-1955

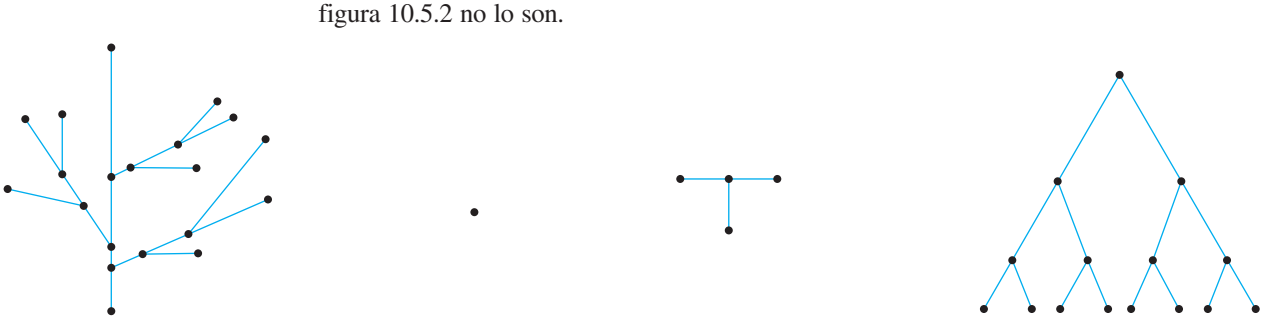
Si un amigo le pregunta lo que están estudiando y responde "árboles", su amigo es probable a inferir que está tomando un curso en botánica. Pero los árboles también son objeto de investigación matemática. En matemáticas, un árbol es un grafo conexo que no tiene ningún circuito. Los árboles matemáticos son similares en cierta forma a sus tocayos botánicos.

• Definición

Se dice que un grafo está **libre de circuitos** si y sólo si, no tiene circuitos. Un grafo se llama **árbol** si y sólo si, está libre de circuitos y es conexo. Un **árbol trivial** es un grafo que consta de un único vértice. Un grafo se llama un **bosque** si y sólo si, está libre de circuitos y no es conexo.

Ejemplo 10.5.1 Árboles y no árboles

Todos los grafos que se muestra en la figura 10.5.1 son árboles, mientras que los de la figura 10.5.2 no lo son.



a) *b*) *c*) *d*)

Figura 10.5.1 Árboles. Todos los grafos en *a*) a *d*) son conexos y libres de circuitos.

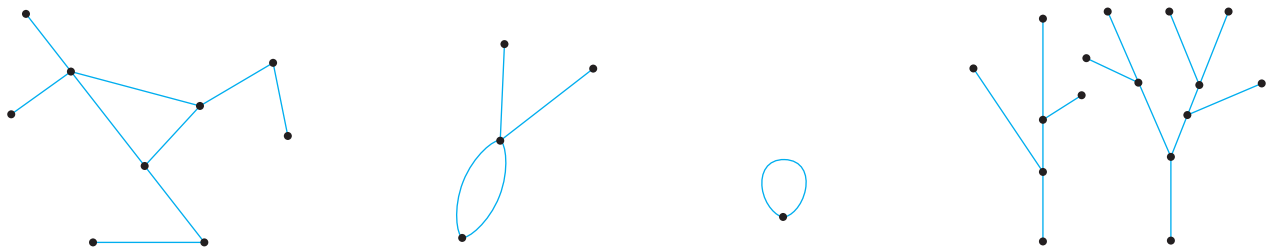


Figura 10.5.2 **No árboles. Los grafos en *a*), *b*) y *c*) todos tienen circuitos y el grafo en *d*) no es conexo.** ■

Ejemplos de árboles

Los siguientes ejemplos ilustran algunas de las muchas y variadas situaciones en las que surgen los árboles matemáticos.

Ejemplo 10.5.2 Un árbol de decisión

Durante la semana de orientación, un colegio aplica un examen a todos los estudiantes que ingresan para ubicarlos en el currículo de matemáticas. El examen consta de dos partes y se colocan recomendaciones para indicarles con el árbol que se muestra en la figura 10.5.3. Lea el árbol de izquierda a derecha para decidir qué curso se recomienda para un estudiante que obtuvo 9 en la parte I y 7 en la parte II.

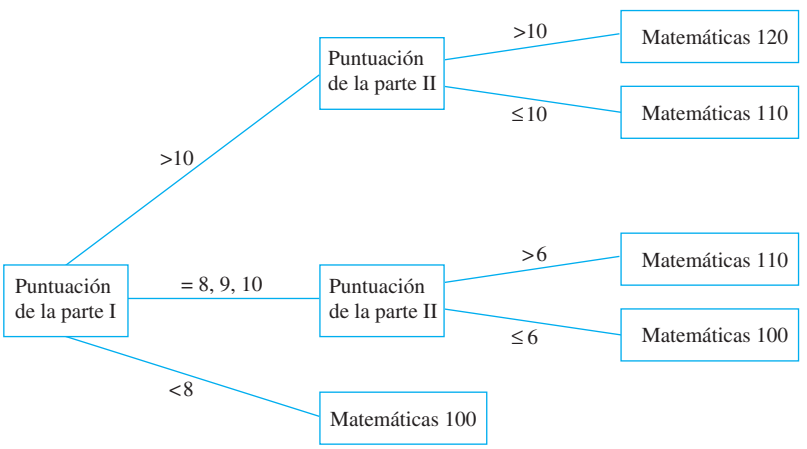


Figura 10.5.3

Solución Ya que el estudiante obtuvo 9 en la parte I, la calificación en la parte II se comprueba. Ya que es superior a 6, se le aconseja al alumno que tome Matemáticas 110. ■

Ejemplo 10.5.3 Análisis de un árbol

En los últimos 30 años, Noam Chomsky y otros han desarrollado nuevas formas para describir la sintaxis (o estructura gramatical) de lenguajes naturales como el inglés. Como se describe brevemente en el capítulo 12, este trabajo ha resultado útil para construir los compiladores de lenguajes de cómputo de alto nivel. En el estudio de las gramáticas, los árboles a menudo se utilizan para mostrar la deducción de oraciones gramaticalmente correctas a partir de algunas normas básicas. Esos árboles son llamados **árboles de deducción sintáctica** o **árboles analizados**.

Un pequeño subconjunto de gramática inglesa, por ejemplo, específica que

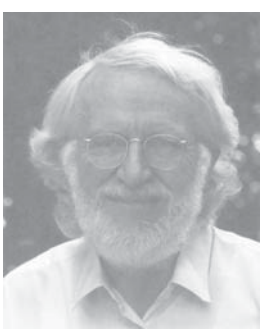
1. una frase se puede producir escribiendo primero una frase nominal y después una frase verbal;
2. una frase nominal se puede producir escribiendo un artículo y después un sustantivo;
3. una frase nominal también se puede producir escribiendo un artículo, después un adjetivo y después sustantivo;
4. una frase verbal se puede producir escribiendo un verbo y después una frase nominal;
5. un artículo es "el";
6. un adjetivo es "joven";
7. un verbo es "atrapa";
8. un sustantivo es "hombre";
9. un (otro) sustantivo es "pelota".

Cortesía de IBM Corporation

John Backus
(1924-1998)

Las reglas de gramática se llaman **producciones**. Se acostumbra expresarlos usando notación abreviada como se muestra a continuación. Esta notación, introducida por John Backus en 1959 y modificada por Peter Naur en 1960, fue usada para describir el lenguaje de programación Algol y se llama la **notación de Backus-Naur**. En la notación, el símbolo | representa la palabra *o* y los corchetes ⟨ ⟩ se utilizan para incluir términos a ser definido (por ejemplo, una frase o frase nominal).

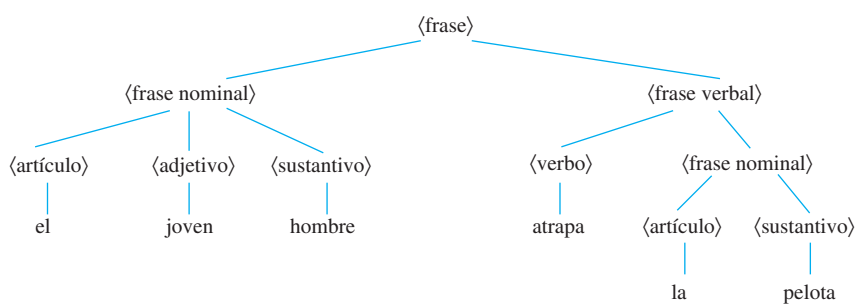
1. ⟨frase⟩ → ⟨frase nominal⟩ ⟨frase verbal⟩
2., 3. ⟨frase nominal⟩ → ⟨artículo⟩⟨sustantivo⟩ | ⟨artículo⟩⟨adjetivo⟩⟨sustantivo⟩
4. ⟨frase verbal⟩ →⟨verbo⟩⟨frase nominal⟩
5. ⟨artículo⟩ → el
6. ⟨adjetivo⟩ → joven
7., 8. ⟨sustantivo⟩ → hombre | pelota
9. ⟨verbo⟩ → atrapa



Cortesía de Peter Naur

Peter Naur
(nació en 1928)

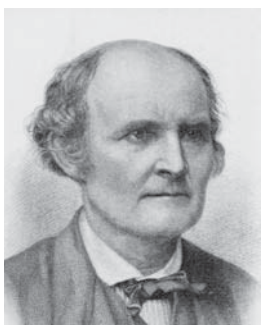
La deducción de la frase "El joven atrapa la pelota" con las reglas anteriores se describe por el árbol que se muestra a continuación.



En el estudio de la lingüística, la **sintaxis** se refiere a la estructura gramatical de las oraciones y **semántica** a los significados de las palabras y sus interrelaciones. Una frase puede ser sintácticamente correcta pero semánticamente incorrecta, como en la frase sin sentido "la joven pelota atrapa al hombre", que se puede deducir de las reglas antes dadas. O una frase puede contener errores sintácticos pero no semánticos que, como, por ejemplo, cuando un niño de dos años, dice, ¡mi hambre! ■

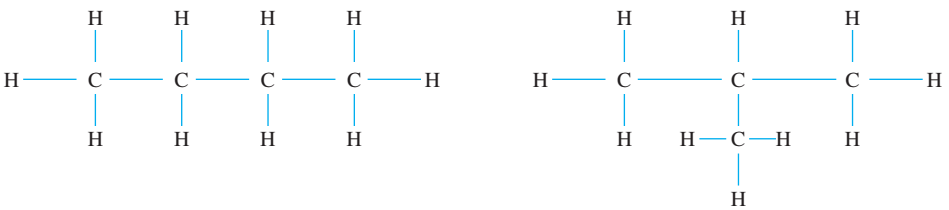
Ejemplo 10.5.4 Estructura de moléculas de hidrocarburos

El físico alemán Gustav Kirchhoff (1824-1887) fue el primero en analizar el comportamiento de árboles matemáticos en relación con la investigación de circuitos eléctricos. Poco después (e independiente), el matemático inglés Arthur Cayley utilizaron la matemática de árboles para enumerar todos los isómeros de determinados hidrocarburos. Las moléculas de hidrocarburos están compuestas de carbono e hidrógeno; cada átomo de carbono puede formar hasta cuatro enlaces químicos con otros átomos y cada átomo de hidrógeno puede formar un enlace con otro átomo. Por tanto la estructura de las moléculas de hidrocarburos se pueden representar por grafos, como los que aparecen después, en las que los vértices representan átomos de hidrógeno y carbono, denotados por H y C y las aristas representan los enlaces químicos entre ellos.



Bettmann/CORBIS

Arthur Cayley (1821-1895)

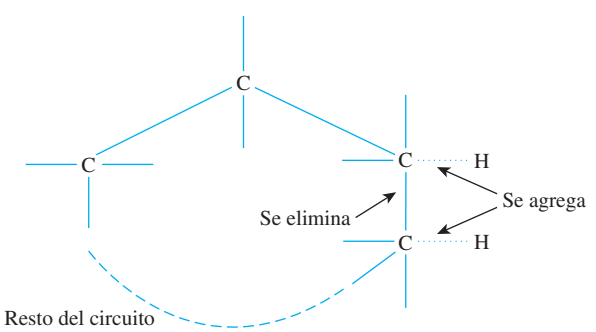


Butano Isobutano

Observe que cada uno de estos grafos tiene cuatro átomos de carbono y diez átomos de hidrógeno, pero los dos grafos muestran diferentes configuraciones de átomos. Cuando dos moléculas tienen las mismas fórmulas químicas (en este caso C_4H_{10}) pero diferentes enlaces químicos, se denominan *isómeros*.

Ciertas moléculas de *hidrocarburos saturados* contienen el máximo número de átomos de hidrogeno para un determinado número de átomos de carbono. Cayley demostró que si dicha molécula de hidrocarburos saturados tiene k átomos de carbono, entonces tiene $2k + 2$ átomos de hidrógeno. El primer paso para hacerlo es demostrar que el grafo de una molécula de hidrocarburos saturados de éstas es un árbol. Demuéstrelo mediante la demostración de contradicción. (Se debe finalizar la deducción del resultado de Cayley en el ejercicio 4 al final de esta sección).

Solución Suponga que hay una molécula de hidrocarburos que contiene el número máximo de átomos de hidrógeno para el número de sus átomos de carbono y cuyo grafo G no es un árbol. *[Se debe deducir una contradicción.]* Ya que G no es un árbol, G no es conexo o G tiene un circuito. Pero el grafo de cualquier molécula es conexo (todos los átomos en una molécula deben estar conectados entre sí) y así G tiene un circuito no trivial. Ahora las aristas del circuito pueden enlazar sólo los átomos de carbono porque cada vértice de un circuito tiene grado mínimo de 2 y un vértice del átomo de hidrógeno tiene grado 1. Elimine una arista del circuito y agregue dos aristas nuevas a cada uno de los vértices del átomo de carbono recién desconectado de un vértice del átomo de hidrógeno, como se muestra a continuación.



La molécula resultante tiene dos átomos de hidrógeno más que la molécula dada, pero no se ha modificado el número de átomos de carbono. Esto contradice la suposición de que la molécula dada tiene el máximo número de átomos de hidrógeno para el número de átomos de carbono. Por lo que la suposición es falsa y así G es un árbol. ■

Caracterización de árboles

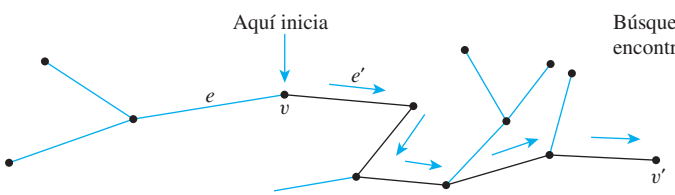
Hay una relación un poco sorprendente entre el número de vértices y el número de aristas de un árbol. Resulta que si n es un entero positivo, entonces cualquier árbol con n vértices (no importa su forma) tiene $n - 1$ aristas. Tal vez incluso más sorprendente, un converso parcial de este hecho también es verdadero; es decir, cualquier grafo *conexo* con n vértices y $n - 1$ aristas es un árbol. Se deduce de estos hechos que si incluso una arista nueva (pero no nuevo vértice) se agrega a un árbol, el grafo resultante debe contener un circuito. También, del hecho de que la eliminación de una arista de un circuito no desconecta un grafo, se puede demostrar que cada grafo conexo tiene una subgrafo que es un árbol. Resulta que si n es un entero positivo, cualquier grafo con n vértices y *menos* de $n - 1$ aristas no es conexo.

Un pequeño pero muy importante hecho necesario para obtener el primer teorema principal acerca de los árboles es que cualquier árbol no trivial debe tener al menos un vértice de grado 1.

Lema 6.5.1

Cualquier árbol que tiene más de un vértice tiene al menos un vértice de grado 1.

Una forma constructiva de entender este lema es imaginar un árbol T dado con más de un vértice. Elija un vértice v al azar y busque hacia fuera a lo largo de una trayectoria de v en busca de un vértice de grado 1. Cómo llegar a cada vértice nuevo, compruebe si tiene grado 1. Si lo hace, habrá terminado. Si no es así, salga del vértice a lo largo de una arista diferente de la que entró él. Ya que T está libre de circuito, los vértices que se incluyen en la trayectoria nunca se repiten. Y dado que el número de vértices de T es finito, finalmente el proceso de construcción de una trayectoria debe terminar. Cuando esto sucede, el vértice final v' de la trayectoria debe tener grado 1. Este proceso se muestra a continuación.



Este análisis es una forma precisa en la siguiente demostración.

Demostración:

Sea T un árbol particular arbitrariamente elegido que tiene más de un vértice y considere el algoritmo siguiente:

Paso 1: Seleccione un vértice v de T y sea e una arista que incide en v.
[Si no hubiera ninguna arista que incida en v, entonces v sería un vértice aislado. Pero esto contradice la suposición de que T es conexo (ya que es un árbol) y tiene al menos dos vértices.]

Paso 2: Mientras que $\deg(v) > 1$, repita los pasos 2a, 2b y 2c:

continúa en la página 688

Paso 2a: Elija e' como una arista que incide en v tal que $e' \neq e$. *[Tal que una arista existe porque deg(v) > 1 y así hay al menos dos aristas que inciden en v.]*

Paso 2b: Sea v' el vértice en el otro extremo de e' para v. *[Ya que T es un árbol, e' no puede ser un bucle y por tanto e' tiene dos puntos distintos extremos.]*

Paso 2c: Sea $e = e'$ y $v = v'$. *[Esto es sólo un proceso de cambio de nombre en preparación para una repetición del paso 2.]*

El algoritmo que se acaba de describir debe terminar finalmente porque el conjunto de vértices del árbol T es finito y T está libre de circuitos. Cuando se hace, se habrá encontrado un vértice v de grado 1.

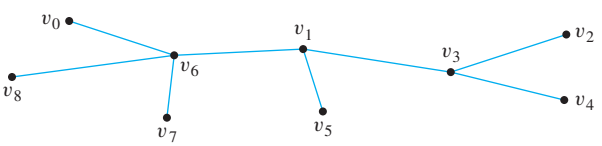
Usando el lema 10.5.1 no es difícil demostrar que, de hecho, cualquier árbol que tiene más de un vértice, tiene al menos *dos* vértices de grado 1. Esta extensión del lema 10.5.1 se deja en los ejercicios del final de esta sección.

• Definición

Sea T un árbol. Si T tiene sólo uno o dos vértices, cada uno se llama un **vértice terminal**. Si T tiene al menos tres vértices, entonces un vértice de grado 1 en T se denomina un **vértice terminal** (o una **hoja**) y un vértice de grado superior a 1 en T es un **vértice interno** (o un **vértice de rama**).

Ejemplo 10.5.5 Vértices terminales e internos

Encuentre todos los vértices terminales y todos los vértices internos en el siguiente árbol:



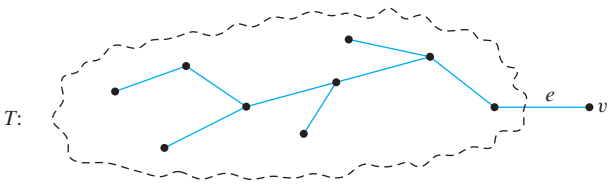
Solución Los vértices terminales son v_0, v_2, v_4, v_5, v_7 y v_8. Los vértices internos son v_6, v_1 y v_3. ■

El siguiente es el primero de los dos principales teoremas sobre árboles:

Teorema 10.5.2

Para cualquier entero positivo n, cualquier árbol con n vértices tiene $n - 1$ aristas.

La demostración es por inducción matemática. Para hacer el paso inductivo, suponga que el teorema es verdadero para un entero positivo k y después demuestre que es verdadero para $k + 1$. Por tanto, suponga que tiene un árbol T con $k + 1$ vértices y debe demostrar que T tiene $(k + 1) - 1 = k$ aristas. Para hacerlo, es libre de utilizar la hipótesis de inducción de que *cualquier* árbol con vértices k tiene $k - 1$ aristas. Para hacer uso de la hipótesis de inducción, necesita reducir el árbol T con $k + 1$ vértices a un árbol con sólo k vértices. Pero por el lema 10.5.1, T tiene un vértice v de grado 1 y puesto que T es conexo, v está unida al resto de T por una sola arista e como se esboza en la página siguiente.



Ahora si se quitan e y v de T, lo que queda es un árbol T' con $(k + 1) - 1 = k$ vértices. Por hipótesis de inducción, entonces, T' tiene $k - 1$ aristas. Pero el árbol original T tiene un vértice más y una arista más que T'. Por lo que T debe tener $(k - 1) + 1 = k$ aristas, como se ha demostrado. A continuación se muestra una versión formal de este argumento. ■

Demostración (por inducción matemática):

Sea la propiedad $P(n)$ la frase

Cualquier árbol con n vértices tiene $n - 1$ aristas. ← $P(n)$

Utilizamos inducción matemática para demostrar que esta propiedad es verdadera para todos los enteros $n \geq 1$.

Demostración de que P(1) es verdadero: Sea T cualquier árbol con un vértice. Entonces T tiene cero aristas (ya que no contiene bucles). Pero $0 = 1 - 1$, así $P(1)$ es verdadera.

Demostración de que para todos los enteros k ≥ 1, si P(k) es verdadera entonces P(k + 1) es verdadera:
Suponga que k es cualquier entero positivo para el que $P(k)$ es verdadera. Con otras palabras, supongamos que

Cualquier árbol con k vértices tiene $k - 1$ aristas. ← $P(k)$ hipótesis de inducción

Debemos demostrar que $P(k + 1)$ es verdadera. O sea debemos demostrar que

Cualquier árbol con $k + 1$ vértices tiene $(k + 1) - 1 = k$ aristas. ← $P(k + 1)$

Sea T un árbol particular pero arbitrariamente elegido con $k + 1$ vértices. *[Debemos demostrar que T tiene k aristas.]* Ya que k es un entero positivo $(k + 1) \geq 2$ y así T tiene más de un vértice. Por lo que por el lema 10.5.1, T tiene un vértice v de grado 1. También, como T tiene más de un vértice, hay al menos otro vértice de T además de v. Así hay una arista e que conecta a v con el resto de T. Defina un subgrafo T' a T así que,

$$V(T') = V(T) - \{v\}$$

entonces

$$E(T') = E(T) - \{e\}.$$

1. El número de vértices de T' es $(k + 1) - 1 = k$.
2. T' está libre de circuitos (ya que T está libre de circuitos y quitar una arista y un vértice no crea un circuito).
3. T' es conexo (vea el ejercicio 24 al final de esta sección).

Por lo que, por la definición del árbol, T' es un árbol. Ya que T' tiene k vértices, por la hipótesis de inducción

$$\begin{aligned}\text{el número de aristas de } T' &= (\text{el número de vértices de } T') - 1\\ &= k - 1\end{aligned}$$

continúa en la página 690

Pero entonces

el número de aristas de T = (el número de aristas de T') + 1

$= (k - 1) + 1$

$= k$.

[Esto es lo que se quería demostrar.]

Ejemplo 10.5.6 Determine si un grafo es un árbol

Un grafo G tiene diez vértices y doce aristas. ¿Es un árbol?

Solución No. Por el teorema 10.5.2, cualquier árbol con diez vértices tiene nueve aristas, no doce. ■

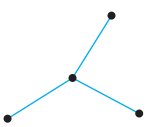
Ejemplo 10.5.7 Encuentre los árboles que satisfacen las condiciones dadas

Encuentre todos los árboles no isomorfos con cuatro vértices.

Solución Por el teorema 10.5.2, cualquier árbol con cuatro vértices tiene tres aristas. Por tanto el grado total de un árbol con cuatro vértices debe ser 6. Además, cada árbol con más de un vértice tiene al menos dos vértices de grado 1 (vea el siguiente comentario del lema 10.5.1 y los ejercicios 5 y 29 del final de esta sección). Por tanto las siguientes combinaciones de grados para los vértices son los únicos posibles:

$$1, 1, 1, 3 \quad \text{y} \quad 1, 1, 2, 2.$$

Hay dos árboles no isomorfos correspondientes a cada una de estas posibilidades, como se muestra a continuación.


y

■

Para demostrar el segundo teorema importante acerca de los árboles, necesitamos otro lema.

Lema 10.5.3

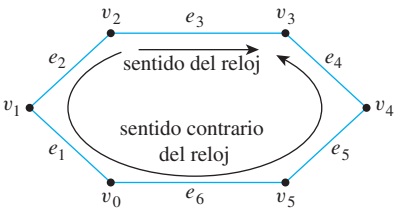
Si G es cualquier grafo conexo, C es cualquier circuito en G y una de las aristas de C se quita de G, entonces el grafo restante es conexo.

Esencialmente, la razón de por qué el lema 10.5.3 es verdadero es que los dos vértices están conectados en un circuito por dos trayectorias distintas. Es posible dibujar el grafo así que uno de ellos va "hacia la derecha" y la otra va "a la izquierda" en el circuito. Por ejemplo, en el circuito que se muestra en la siguiente página, la trayectoria va hacia la derecha de v_2 a v_3 es

$$v_2 e_3 v_3$$

y la trayectoria en el sentido contrario de las manecillas del reloj de v_2 a v_3 es

$$v_2 e_2 v_1 e_1 v_0 e_6 v_5 e_5 v_4 e_4 v_3.$$



Demostración:

Supongamos que G es un grafo conexo, C es un circuito en G y e es una arista de C. Forme una subgrafo G' de G eliminando e de G. Así,

$$V(G') = V(G)$$
$$E(G') = E(G) - \{e\}.$$

Debemos demostrar que G' es conexa. *[Para demostrar que un grafo es conexo, debemos demostrar que si u y w son vértices cualesquiera del grafo, entonces existe un camino en G' de u a w.]* Suponga que u y w son los dos vértices de G'. *[Debemos encontrar un camino de u a w.]* Ya que los conjuntos de vértices de G y G' son iguales, u y w son dos vértices de G y ya que G es conexa, hay un camino W en G de u a w.

Caso 1 (e no es una arista de W): La única arista en G que no está en G' es e, así en este caso W es también un camino en G'. Por lo que u está conectado a w por un camino en G'.

Caso 2 (e es una arista de W): en este caso el camino W de u a w incluye una sección del circuito C que contiene a e. Sea C que se denota como sigue:

$$C\colon\ v_0 e_1 v_1 e_2 v_2 \cdots e_n v_n\ (= v_0).$$

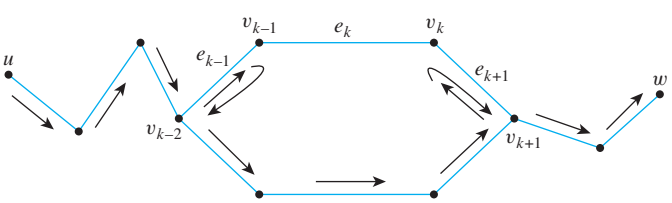
Ahora e es una de las aristas de C, así, en concreto, sea $e = e_k$. Entonces, el camino W contiene ya sea la sucesión

$$v_{k-1} e_k v_k \quad \text{o} \quad v_k e_k v_{k-1}.$$

Si W contiene $v_{k-1}e_k v_k$, conecta a v_{k-1} con v_k tomando el camino "en sentido contrario a las manecillas del reloj" W' definido como sigue:

$$W'\colon\ v_{k-1} e_{k-1} v_{k-2} \cdots v_0 e_n v_{n-1} \cdots e_{k+1} v_k.$$

Un ejemplo muestra cómo ir desde u a w evitando a e_k en la figura 10.5.4.



Para ir de u a w evitando a e_k, vaya en sentido contrario al reloj alrededor del circuito.

Figura 10.5.4 **Un ejemplo de un camino de u a w que no incluye a la arista e_k**

Si W contiene a $v_k e_k v_{k-1}$, conecta a v_k con v_{k-1} tomando el camino "en el sentido de las manecillas del reloj" W'' que se define como sigue:

$$W''\colon\ v_k e_{k+1} v_{k+1} \cdots v_n e_1 v_1 e_2 \cdots e_{k-1} v_{k-1}.$$

continúa en la página 692

Ahora parche ya sea W' o W'' en W para formar un nuevo camino de u a w. Por ejemplo, para parchar a W' en W, empiece por la sección de W de u a v_{k-1}, después tome W' de v_{k-1} a v_k y por último tome la sección de W de v_k a w. Si este nuevo camino aún contiene una ocurrencia de e, sólo repita el proceso descrito anteriormente hasta que se eliminen todas las ocurrencias. *[Esto debe suceder eventualmente ya que el número de ocurrencias de e en C es finito.]* El resultado es un camino de u a w que no contienen a e por lo que es un camino en G'.

Los argumentos anteriores muestran que en el caso 1 y en el caso 2 hay un camino en G' de u a w. Ya que la elección de u y w fue arbitraria, G' es conexo.

El segundo teorema importante acerca de los árboles es un recíproco modificado del teorema 10.5.2.

Teorema 10.5.4

Para cualquier entero positivo n, si G es un grafo conexo con n vértices y $n - 1$ aristas, entonces G es un árbol.

Demostración:

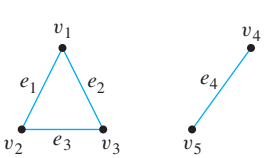
Sea n un entero positivo y suponga que G es un grafo particular arbitrariamente elegido que es conexo y tiene n vértices y $n - 1$ aristas. *[Debemos demostrar que G es un árbol. Ahora un árbol es un grafo conexo, libre de circuitos. Puesto que ya sabemos que G es conexo, es suficiente demostrar que está libre de circuitos.]* Suponga que G no está libre de circuitos. Es decir, suponga que G tiene un circuito C. *[Debemos deducir una contradicción.]* Por el lema 10.5.3, se puede quitar una arista de C de G para obtener un grafo G' que es conexo. Si G' tiene un circuito, repita este proceso: quite una arista del circuito de G' para formar un nuevo grafo conexo. Siga repitiendo el proceso de eliminación de aristas de circuitos hasta que eventualmente se obtenga una gráfica G'' que es conexo y está libre de circuitos. Por definición, G'' es un árbol. Ya no se quitaron vértices de G para formar G'', G'' tiene n vértices igual que G. Así, por el teorema 10.5.2, G'' tiene $n - 1$ aristas. Pero la suposición de que G tiene un circuito implica que al menos se quita una arista de G para formar G''. Por lo que G'' no tiene más de $(n - 1) - 1 = n - 2$ aristas, que contradice que tiene $n - 1$ aristas. Así la suposición es falsa. Por lo que G está libre de circuitos y por tanto G es un árbol *[como se quería demostrar]*.

El teorema 10.5.4 no es un completo converso del teorema 10.5.2. Aunque es verdadero para cada grafo *conexo* con n vértices y $n - 1$ aristas (donde n es un entero positivo) es un árbol, no es verdad que *cada* grafo con n vértices y $n - 1$ aristas es un árbol.

Ejemplo 10.5.8 Un grafo con n vértices y $n - 1$ aristas que no es un árbol

Dé un ejemplo de un grafo con cinco vértices y cuatro aristas que no es un árbol.

Solución Por el teorema 10.5.4, dicho grafo no puede conectarse. A continuación se muestra un ejemplo de dicho grafo no conexo.



Autoexamen

1. Un grafo de un circuito libre es un grafo con _____.
2. Un bosque es un grafo que es _____ y un árbol es un grafo que es _____.
3. Un árbol trivial es un grafo que consta de _____.
4. Cualquier árbol con al menos dos vértices tiene al menos un vértice de grado _____.
5. Si un árbol T tiene al menos dos vértices, entonces un vértice terminal (u hoja) en T es un vértice de grado _____ y un vértice interno (o rama de vértice) en T es un vértice de grado _____.
6. Para cualquier entero positivo n, cualquier árbol con n vértices tiene _____.
7. Para cualquier entero positivo n, si G es un grafo conexo con n vértices y $n - 1$ aristas entonces _____.

Conjunto de ejercicios 10.5

1. ¿Lea el árbol en el ejemplo 10.5.2 de izquierda a derecha para responder a las preguntas siguientes:
   a. ¿Qué curso debería tomar un estudiante que obtuvo 12 en la parte I y 4 en la parte II?
   b. ¿Qué curso debería tomar un estudiante que obtuvo 8 en la parte I y 9 en la parte II?

2. Dibuje árboles para mostrar las deducciones de las siguientes frases de las reglas del ejemplo 10.5.3.
   a. la joven pelota captura al hombre.
   b. el hombre capturó a la joven pelota.

3. ¿Cuál es el grado total de un árbol con n vértices? ¿Por qué?

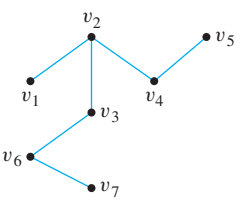
4. Sea G el grafo de una molécula de hidrocarburos con el máximo número de átomos de hidrógeno para el número de sus átomos de carbono.
   a. Dibuje el grafo de G si G tiene tres átomos de carbón y ocho átomos de hidrógeno.
   b. Dibuje los grafos de tres isómeros de C_5H_{12}.
   c. Use el ejemplo 10.5.4 y el ejercicio 3 para demostrar que si los vértices de G consisten de k átomos de carbón y m átomos de hidrógeno, entonces G tiene un grado total de $2k + 2m - 2$.
   ***H* d.** Demuestre que si los vértices de G se componen de átomos de carbono k y m átomos de hidrógeno, entonces G tiene un grado total de $4k + m$.
   e. Iguale los resultados de (c) y (d) para demostrar el resultado de Cayley que una molécula de hidrocarburos saturados con átomos de carbono k y un número máximo de átomos de hidrógeno tiene $2k + 2$ átomos de hidrógeno.

***H* 5.** Amplíe el argumento dado en la demostración del lema 10.5.1 para demostrar que un árbol con más de un vértice tiene al menos dos vértices de grado 1.

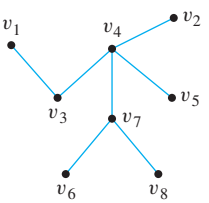
6. Si los grafos pueden tener un número infinito de vértices y aristas, entonces el lema 10.5.1 es falso. Dé un contraejemplo que lo demuestre. En otras palabras, dé un ejemplo de un "árbol infinito" (un grafo conexo, libre de circuitos con un número infinito de vértices y aristas) que no tenga un vértice de grado 1.

7. Encuentre todos los vértices terminales y todos los vértices internos para los siguientes árboles.

a.



b.



En cada uno de los ejercicios del 8 al 21, dibuje un grafo con las especificaciones dadas o explique por qué ese grafo no existe.

8. Árbol, nueve vértices, nueve aristas

9. Grafo, conexo, nueve vértices, nueve aristas

10. Grafo, libre de circuitos, nueve vértices, seis aristas

11. Árbol, seis vértices, grado total 14

12. Árbol, cinco vértices, grado total 8

13. Grafo, conexo, seis vértices, cinco aristas, tiene un circuito no trivial

14. Grafo, dos vértices, una arista, no es un árbol

15. Grafo, libre de circuitos, siete vértices, cuatro aristas

16. Árbol, doce vértices, quince aristas

17. Grafo, seis vértices, cinco aristas, no es un árbol

18. Árbol, cinco vértices, grado total 10

19. Grafo, conexo, diez vértices, nueve aristas, tiene un circuito no trivial

20. Grafo simple, conexo, seis vértices, seis aristas

21. Árbol, diez vértices, grado total 24

22. Un grafo conexo tiene doce vértices y once aristas. ¿Tiene un vértice de grado 1? ¿Por qué?

23. Un grafo conexo tiene nueve vértices y doce aristas. ¿Tiene un circuito no trivial? ¿Por qué?

24. Suponga que v es un vértice de grado 1 en un grafo conexo G y e es la arista que incide en v. Sea G' el subgrafo G obtenida al eliminar v y e de G. ¿Debe G' ser conexo? ¿Por qué?

25. Un grafo tiene ocho vértices y seis aristas. ¿Es conexo? ¿Por qué?

H 26. ¿Si un grafo tiene vértices n y $n - 2$ o menos aristas, puede ser conexo? ¿Por qué?

27. Un grafo libre de circuitos tiene diez vértices y nueve aristas. ¿Es conexo? ¿Por qué?

H 28. ¿Es un grafo libre de circuitos con n vértices y al menos $n - 1$ aristas conectada? ¿Por qué?

29. Demuestre que cada árbol no trivial tiene al menos dos vértices de grado 1 completando los detalles y completar el siguiente argumento: Sea T un árbol no trivial y sea S el conjunto de todas las trayectorias de un vértice a otro de T. Entre todas las trayectorias en S, elija una trayectoria P con más aristas. (¿Por qué es posible encontrar dicha P?) ¿Qué puede decir sobre los vértices iniciales y finales de P? ¿Por qué?

30. Encuentre todos los árboles no isomorfos con cinco vértices.

31. a. Demuestre que el siguiente es un invariante de isomorfismo gráfico: un vértice de grado i es adyacente a un vértice de grado j.

H b. Encuentre todos los árboles no isomorfos con seis vértices.

Respuestas del autoexamen

1. no circuitos 2. libre de circuitos y no conexo; conexo y libres de circuito 3. un único vértice (y sin aristas) 4. 1 5. 1; mayor que 1 (O: al menos 2). 6. $n - 1$ aristas 7. G es un árbol

10.6 Árboles enraizados

Lo que nos concede la búsqueda de las matemáticas es una locura divina del espíritu humano, un refugio de la urgencia de crear acontecimientos fortuitos. —Alfred North Whitehead, 1861-1947

Un árbol al aire libre está enraizado y así es el tipo de árbol que muestra todos los descendientes de una persona en particular. La terminología y notación de árboles enraizados combina el idioma de los árboles botánicos y de árboles de la familia. En matemáticas, un árbol enraizado es un árbol en el que un vértice se ha distinguido de los demás y se designa como la *raíz*. Dado que cualquier otro vértice v en el árbol, existe una trayectoria única de la raíz a v. (Después de todo, si hubiera dos trayectorias distintas, se podría construir un circuito.) El número de aristas en esta trayectoria se llama el *nivel* de v y la *altura* del árbol es la longitud de la más larga trayectoria. Es tradicional al dibujar árboles enraizados colocar la raíz en la parte superior (como se hace con los árboles familiares) y mostrar las ramas que descienden de ésta.

• Definición

Un **árbol enraizado** es un árbol en el que hay un vértice que se distingue de los demás y se le llama **raíz**. El **nivel** de un vértice es el número de aristas a lo largo de la trayectoria única entre éste y la raíz. La **altura** de un árbol enraizado es el nivel máximo de cualquier vértice del árbol. Dada la raíz o cualquier vértice interno v de un árbol, los **hijos** de v son todos los vértices adyacentes a v y están a un nivel de la raíz que v. Si w es un hijo de v, entonces v se llama el **padre** de w y dos vértices diferentes que son ambos hijos del mismo padre se llaman **hermanos**. Dados dos vértices diferentes v y w, si v se encuentra en la única trayectoria entre w y la raíz, entonces v es un **ancestro** de w y w es un **descendiente** de v.

Estos términos se muestran en la figura 10.6.1.

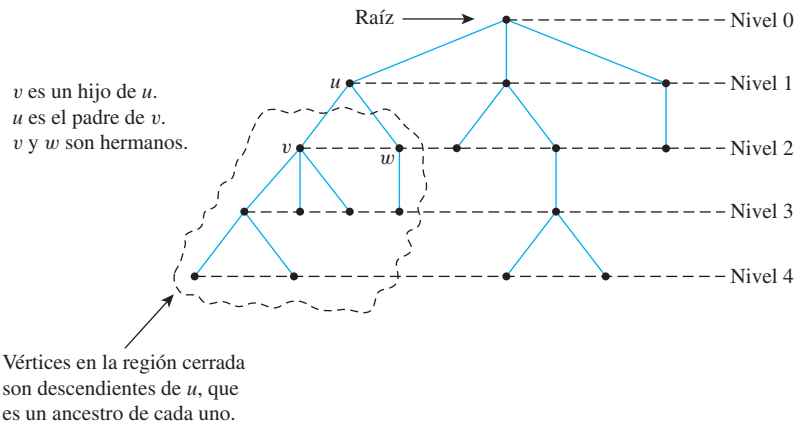
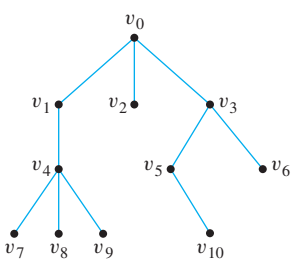


Figura 10.4.1 **Un árbol enraizado**

Ejemplo 10.6.1 Árboles enraizados

Considere el árbol con raíz v_0 que se muestra a continuación.

a. ¿Cuál es el nivel de v_5?
b. ¿Cuál es el nivel de v_0?
c. ¿Cuál es la altura de este árbol?
d. ¿Cuáles son los hijos de v_3?
e. ¿Quién es el padre de v_2?
f. ¿Cuáles son los hermanos de v_8?
g. ¿Cuáles son los descendientes de v_3?



Solución

a. 2 b. 0 c. 3 d. v_5 y v_6 e. v_0 f. v_7 y v_9 g. v_5, v_6, v_{10}

■

Observe que en el árbol con raíz v_0 que se muestra a continuación, v_1 tiene nivel 1 y es el hijo de v_0 y tanto v_0 como v_1 son vértices terminales.

Árboles binarios

Cuando cada vértice en un árbol enraizado tiene a lo más dos hijos y cada hijo se designa como el hijo izquierdo (único) o el hijo derecho (único), el resultado es un *árbol binario*.

• Definición

Un **árbol binario** es un árbol enraizado en el que todo padre tiene como máximo dos hijos. Cada hijo en un árbol binario se designa como un **hijo izquierdo** o como un **hijo derecho** (pero no ambos) y cada padre tiene a lo más un hijo izquierdo y un hijo derecho. Un **árbol binario completo** es un árbol binario en el que cada padre tiene exactamente dos hijos.

Dado cualquier padre v en un árbol binario T, si v tiene un hijo izquierdo, entonces el **subárbol izquierdo** de v es el árbol binario cuya raíz es el hijo izquierdo de v, cuyos vértices consisten en el hijo izquierdo de v y todos sus descendientes y cuyas aristas consisten en todas las aristas de T que conectan los vértices del subárbol izquierdo. El **subárbol derecho** de v se define análogamente.

Estos términos se muestran en la figura 10.6.2.

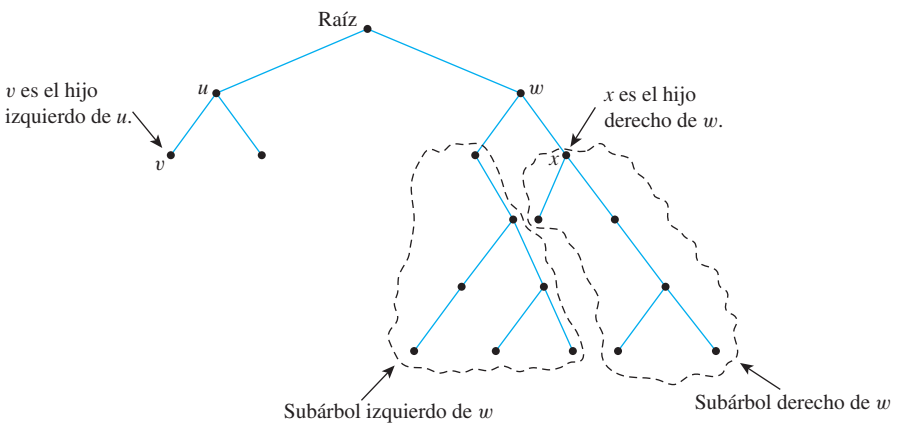
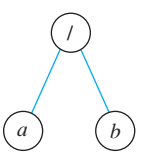


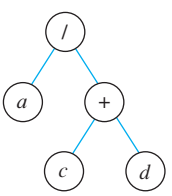
Figura 10.6.2 Árbol binario

Ejemplo 10.6.2 Representación de expresiones algebraicas

Los árboles binarios se usan en muchas formas en ciencias de la computación. Un uso es para representar expresiones algebraicas con anidamiento arbitrario de paréntesis balanceados. Por ejemplo, el siguiente árbol binario (etiquetado) representa la expresión a/b: el operador está en la raíz y actúa en los hijos izquierdo y derecho de la raíz en el orden izquierdo-derecho.

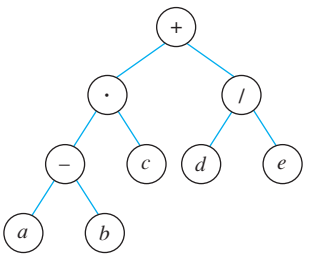


Más generalmente, el árbol binario que se muestra a continuación representa la expresión $a/(c + d)$. En una representación, los vértices internos son operadores aritméticos, los vértices terminales son variables y el operador en cada vértice actúa sobre sus subárboles izquierdo y derecho de izquierda a derecha.



Dibuje un árbol binario para representar la expresión $((a - b) \cdot c) + (d/e)$.

Solución



■

Un teorema interesante sobre árboles binarios dice que si sabe el número de vértices internos de un árbol binario completo, entonces se pueden calcular el número total de vértices y el número de vértices terminales y a la inversa. Más específicamente, un árbol binario con k vértices internos tiene un total de $2k + 1$ vértices de los cuales $k + 1$ son los vértices terminales.

Teorema 10.6.1

Si k es un entero positivo y T es un árbol binario completo con k vértices internos, entonces T tiene un total de $2k + 1$ vértices y tiene $k + 1$ vértices terminales.

Demostración:

Suponga que k es un entero positivo y T es un árbol binario con k vértices internos. Observe que el conjunto de todos los vértices de T se puede particionar en dos subconjuntos disjuntos: el conjunto de todos los vértices que tienen un padre y el conjunto de todos los vértices que no tienen un padre. Ahora existe sólo un vértice que no tiene un padre, a saber la raíz. También ya que cada vértice interno de un árbol binario tiene exactamente dos hijos, el número de vértices que tienen un padre es el doble de los padres, o $2k$ ya que cada padre es un vértice interno. Por lo que

$$\begin{bmatrix}\text{el número total}\\ \text{de vértices de } T\end{bmatrix} = \begin{bmatrix}\text{el número de}\\ \text{vértices que}\\ \text{tienen un padre}\end{bmatrix} + \begin{bmatrix}\text{el número de}\\ \text{vértices que}\\ \text{no tienen un padre}\end{bmatrix}$$
$$= \quad 2k \quad + \quad 1.$$

Pero también es cierto que el número total de vértices de T es igual al número de vértices internos más el número de vértices terminales. Así,

$$\begin{bmatrix}\text{el número total}\\ \text{de vértices de } T\end{bmatrix} = \begin{bmatrix}\text{el número de}\\ \text{vértices internos}\end{bmatrix} + \begin{bmatrix}\text{el número de}\\ \text{vértices terminales}\end{bmatrix}$$
$$= \quad k \quad + \begin{bmatrix}\text{el número de}\\ \text{vértices terminales}\end{bmatrix}$$

Ahora igualando las dos expresiones para el número total de vértices de T:

$$2k + 1 = k + \begin{bmatrix}\text{el número de}\\ \text{vértices terminales}\end{bmatrix}$$

Resolviendo esta ecuación se obtiene

$$\begin{bmatrix}\text{el número de}\\ \text{vértices terminales}\end{bmatrix} = (2k + 1) - k = k + 1.$$

Así el número total de vértices es $2k + 1$ y el número de vértices terminales es $k + 1$ *[como se quería demostrar]*.

Ejemplo 10.6.3 Determinación de si un cierto árbol binario completo existe

¿Existe un árbol binario que tiene 10 vértices internos y 13 vértices terminales?

Solución No. Por el teorema de 10.6.1, un árbol binario completo con 10 vértices internos tiene $10 + 1 = 11$ vértices terminales, no 13. ■

Otro teorema interesante sobre árboles binarios especifica el número máximo de vértices terminales de un árbol binario de una altura determinada. Específicamente, el número máximo de vértices terminales de un árbol binario de altura h es 2^h. Otra forma de decir esto es que un árbol binario con t vértices terminales tiene al menos una altura de $\log_2 t$.

Teorema 10.6.2

Para todos los enteros $h \geq 0$, si t es cualquier árbol binario de altura h y t vértices terminales, entonces,

$$t \leq 2^h.$$

Equivalentemente, $\log_2 t \leq h$.

Demostración (por inducción matemática fuerte):

Sea $P(h)$ la frase

> Si T es cualquier árbol binario de altura h, entonces el número de vértices terminales de T es a lo más 2^h. ← $P(h)$

Demuestre que P(0) es verdadero: Debemos demostrar que si T es cualquier árbol binario de altura 0, entonces el número de vértices terminales de T es a lo más 2^0. Suponga que T es un árbol de altura 0. Entonces T consta de un único vértice, la raíz. Esta es por definición un vértice terminal y así el número de vértices terminales es $t = 1 = 2^0 = 2^h$. Por lo que $t \leq 2^h$ *[como se quería demostrar]*.

Demuestre que para todos los enteros k ≥ 0, si P(i) es válido para todos los enteros i de 0 a k, entonces es verdadero para k + 1:
Sea k cualquier entero con $k \geq 0$ y se supone que

> Para todos los enteros i de 0 a k, si T es cualquier árbol binario de altura i, entonces el número de vértices terminales de T es a lo más 2^i. ← hipótesis de inducción

Tenemos que demostrar que

> Si T es cualquier árbol binario de altura $k + 1$, entonces el número de vértices terminales de T es 2^{k+1}. ← $P(k + 1)$

Sea T un árbol binario de altura $k + 1$, raíz v y vértices terminales t. Como $k \geq 0$, tenemos que $k + 1 \geq 1$ y así v tiene al menos un hijo.

Caso 1 (v tiene sólo un hijo): En este caso podemos suponer sin pérdida de generalidad que v hijo es un hijo izquierdo y se denota por v_L. Sea T_L el subárbol izquierdo de v. Entonces v_L es la raíz de T_L. (Esta situación se muestra en la figura 10.6.3.) Ya que v tiene sólo un hijo, v es en sí mismo un vértice terminal, así el número total de vértices terminales en T es igual al número de vértices terminales en T_L más 1. Por tanto si T_L es el número de vértices terminales en T_L, entonces $t = t_L + 1$.

Ahora por hipótesis de inducción, $t_L < 2^k$ por la altura de T_L es k, uno menos que la altura de T. También ya que v tiene un hijo, $k + 1 \geq 1$ y así $2^k \geq 2^0 = 1$. Por tanto,

$$t = t_L + 1 \leq 2^k + 1 \leq 2^k + 2^k = 2 \cdot 2^k = 2^{(k+1)}.$$

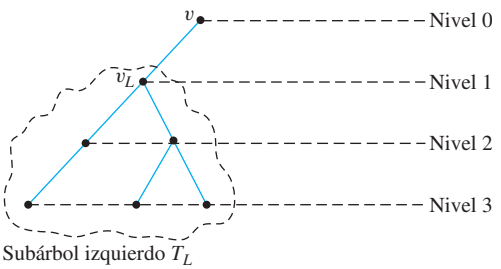


Figura 10.6.3 **Un árbol binario cuya raíz tiene un hijo**

Caso 2 (v tiene dos hijos): En este caso, v tiene un hijo izquierdo, v_L un hijo de derecho, v_R y v_L y v_R son raíces de un subárbol izquierdo T_L y del subárbol derecho T_R. Observe que T_L y T_R son árboles binarios porque T es un árbol binario. (Esta situación se ilustra en la figura 10.6.4.)

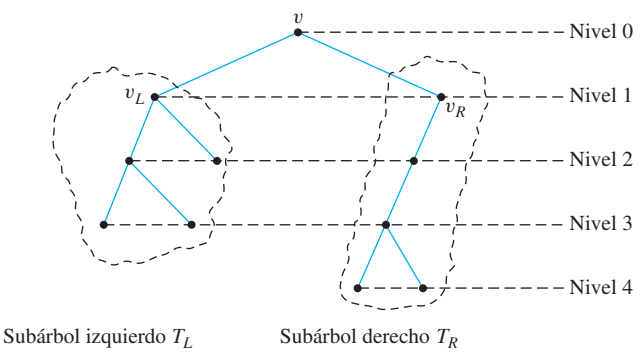


Figura 10.6.4 **Un árbol binario cuya raíz tiene dos hijos**

Ahora v_L y v_R son las raíces de los subárboles izquierdo y derecho de v, que se denotan con T_L y T_R, respectivamente. Observe que T_L y T_R son árboles binarios porque T es un árbol binario. Sea h_L y h_R las alturas de T_L y T_R, respectivamente. Entonces $h_L \leq k$ y $h_R \leq k$ ya que T se obtiene de unir a T_L y T_R y agregar un nivel. Sean t_L y t_R los números de vértices terminales de T_L y T_R, respectivamente. Entonces ya T_L y T_R tienen alturas menores que $k + 1$, por hipótesis de inducción

$$t_L \leq 2^{h_L} \quad \text{y} \quad t_R \leq 2^{h_R}.$$

Pero los vértices terminales de T consisten exactamente de los vértices terminales de T_L junto con los vértices terminales de T_R. Por tanto

$$t = t_L + t_R \leq 2^{h_L} + 2^{h_R}$$

por hipótesis de inducción y ya que $h_L \leq k$ y $h_R \leq k$

continúa en la página 700

Por tanto,

$$t < 2^k + 2^k = 2 \cdot 2^k = 2^{k+1} \qquad \text{por álgebra básica.}$$

Así el número de vértices terminales es a lo más $2k + 1$ *[como se quería demostrar]*.

Puesto que ya se han demostrado tanto el paso básico como el paso inductivo, se concluye que para todos los enteros $h \geq 0$, si T es cualquier árbol binario con altura h y t vértices terminales, entonces $t \leq 2^h$.

La desigualdad equivalente $\log_2 t \leq h$ se deduce del hecho que está aumentando la función logarítmica con base 2. En otras palabras, para todos los números reales positivos x y y,

$$\text{si } x < y \text{ entonces } \log_2 x < \log_2 y.$$

Así, si se aplica la función logarítmica con base 2 a ambos lados de

$$t \leq 2^h,$$

obtenemos

$$\log_2 t \leq \log_2(2^h).$$

Ahora por definición de logaritmo, $\log_2(2^h) = h$ *[ya que $\log_2(2^h)$ es el exponente al que se debe elevar 2 para obtener 2^h]*. Por lo que

$$\log_2 t \leq h$$

[como se quería demostrar].

Ejemplo 10.6.4 Determinar si existe cierto árbol binario

¿Existe un árbol binario que tiene una altura de 5 y 38 vértices terminales?

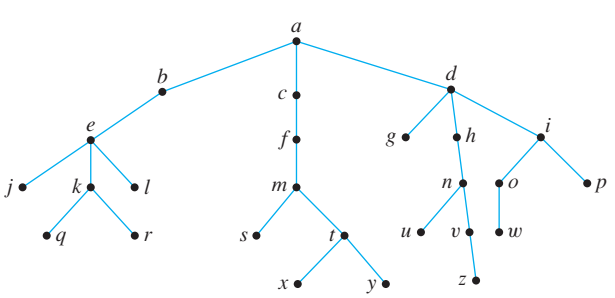
Solución No. Por el teorema 10.6.2, cualquier árbol binario T con altura 5 tiene a lo más $2^5 = 32$ vértices terminales, por lo que dicho árbol no pueden tener 38 vértices terminales. ■

Autoexamen

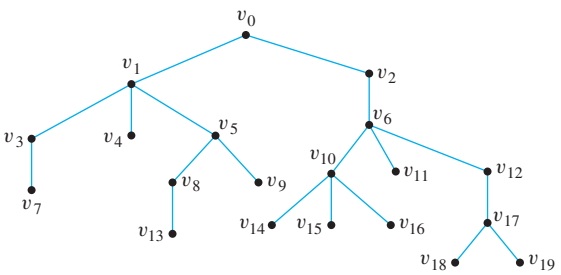
1. Un árbol enraizado es un árbol que _____. El nivel de un vértice en un árbol enraizado es _____. La altura de un árbol enraizado es _____.
2. Un árbol binario es un árbol en el que _____.
3. Un árbol binario es un árbol en el que _____.
4. Si k es un entero positivo y T es un árbol binario con k vértices internos, entonces T tiene un total de _____ vértices _____ tiene _____ vértices terminales.
5. Si T es un árbol binario que tiene t vértices terminales y altura h, entonces t y h están relacionados por la desigualdad _____.

Conjunto de ejercicios 10.6

1. Considere el árbol que se muestra a la derecha con raíz a.
   a. ¿Cuál es el nivel de n?
   b. ¿Cuál es el nivel de a?
   c. ¿Cuál es la altura de este árbol enraizado?
   d. ¿Quiénes son los hijos de n?
   e. ¿Quién es el padre de g?
   f. ¿Cuáles son los hermanos de j?
   g. ¿Cuáles son los descendientes de j?



2. Considere el árbol que se muestra a continuación con raíz v_0.
   a. ¿Cuál es el nivel de v_8?
   b. ¿Cuál es el nivel de v_0?
   c. ¿Cuál es la altura de este árbol enraizado?
   d. ¿Cuáles son los hijos de v_{10}?
   e. ¿Quién es el padre de v_5?
   f. ¿Quiénes son los hermanos de v_1?
   g. ¿Quiénes son los descendientes de v_{12}?



3. Dibuje árboles binarios para representar las expresiones siguientes:
   a. $a \cdot b - (c/(d + e)$ b. $a/(b - c \cdot d)$

En cada uno de los ejercicios del 4 al 20, dibuje un grafo con las especificaciones dadas o explique por qué no existe dicho grafo.

4. Árbol binario completo, cinco vértices internos

5. Árbol binario completo, cinco vértices internos, siete vértices terminales

6. Árbol binario completo, siete vértices, de los cuales cuatro son vértices internos

7. Árbol binario completo, doce vértices

8. Árbol binario completo, nueve vértices

9. Árbol binario, altura 3, siete vértices terminales

10. Árbol binario completo, altura 3, seis vértices terminales

11. Árbol binario, altura 3, nueve vértices terminales

12. Árbol binario completo, ocho vértices internos, siete vértices terminales.

13. Árbol binario, altura 4, ocho vértices terminales

14. Árbol binario completo, siete vértices

15. Árbol binario completo, nueve vértices, cinco vértices internas

16. Árbol binario completo, cuatro vértices internos

17. Árbol binario, altura 4, dieciocho vértices terminales

18. Árbol binario completo, 16 vértices

19. Árbol binario, altura 3, siete vértices terminales

20. ¿Qué puede deducir acerca de la altura de un árbol binario si sabe que tiene las propiedades siguientes?
   a. Veinticinco vértices terminales
   b. Cuarenta vértices terminales
   c. Sesenta vértices terminales

Respuestas del autoexamen

1. un vértice se distingue de los demás y se denomina la raíz; el número de aristas a lo largo de la trayectoria única entre éste y la raíz; el nivel máximo de cualquier vértice del árbol 2. cada padre tiene a lo más dos hijos 3. cada padre tiene exactamente dos hijos 4. $2k + 1$; $k + 1$ 5. $t \leq 2^h$ o equivalente, $\log_2 t \leq h$

10.7 Expansión de árboles y trayectorias más cortas

Sostengo que cada ciencia es una ciencia real en la medida en que es matemáticas.
—Immanuel Kant, 1724-1804

La compañía aérea de la Costa Este quiere ampliar el servicio al medio oeste y ha recibido permiso de la Autoridad Federal de Aviación para volar a cualquiera de las rutas que se muestra en la figura 10.7.1.

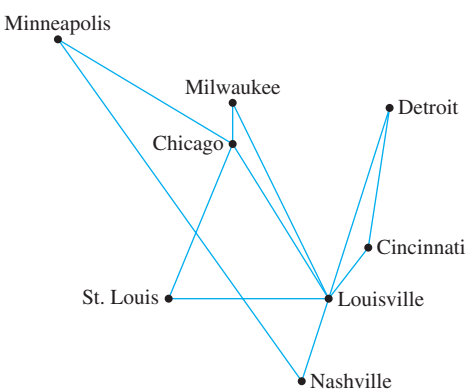


Figura 10.7.1

La empresa desea legítimamente brindar el servicio a todas las ciudades que se muestran pero, por razones de economía, quiere usar el menor número posible de rutas individuales para conectarlas. Un sistema de ruta posible se indica en la figura 10.7.2.

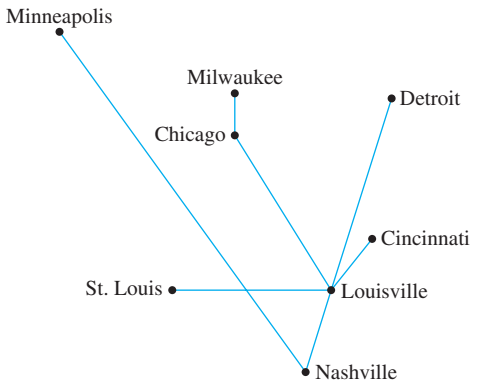


Figura 10.7.2

Este sistema une claramente a todas las ciudades. ¿Es el número de rutas individuales mínima? La respuesta es sí y la razón puede sorprenderle.

El hecho es que el grafo de cualquier sistema de rutas que satisface los deseos de la empresa es un árbol, porque si el grafo contiene un circuito, entonces una de las rutas en el circuito podría eliminarse sin desconectar el grafo (por el lema 10.5.3) y que daría un número reducido de rutas. Pero cualquier árbol con ocho vértices tiene siete bordes. Por tanto, cualquier sistema de rutas que conecta todos los ocho vértices y aún minimiza el número total de rutas consta de siete rutas.

• Definición

Un **árbol expandido** para un grafo G es un subgrafo de G que contiene cada vértice de G y es un árbol.

El análisis anterior contiene la esencia de la demostración de la siguiente propuesta:

Proposición 10.7.1

1. Cada grafo conexo tiene un árbol expandido.
2. Cualesquiera dos árboles expandidos para un grafo tienen el mismo número de aristas.

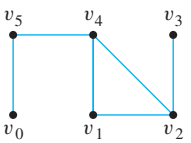
Demostración de (l):

Suponga que G es un grafo conexo. Si G está libre de circuito, entonces G es su propio árbol expandido y terminamos. Si no es así, entonces G tiene al menos un circuito C_1. Por el lema 10.5.3, la subgrafo de G obtenido mediante la eliminación de una arista de C_1 es conexo. Si este subgrafo está libre de circuitos, entonces es un árbol expandido y terminamos. Si no es así, tiene al menos un circuito C_2 y que, como anteriormente, se puede eliminar una arista de C_2 para obtener un subgrafo conexo. Continuando de esta manera, podemos quitar aristas sucesivas de circuitos, hasta que finalmente obtengamos un subgrafo conexo, libre de circuitos T de G. *[Esto debe suceder en el mismo punto porque el número de aristas de G es finito y en ningún momento se elimina una arista para desconectar el subgrafo.]* También, T contiene todos los vértices de G porque no se eliminaron vértices de G en esta construcción. Por tanto es un árbol expandido de G.

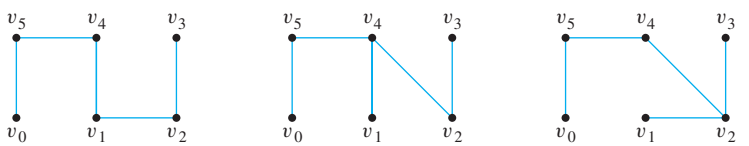
La demostración del inciso 2) queda como un ejercicio.

Ejemplo 10.7.1 Árboles expandidos

Encuentre todos árboles expandidos para el grafo G que se muestra a continuación.



Solución El grafo G tiene un circuito $v_2v_1v_4v_2$ y la eliminación de cualquiera de las aristas del circuito da un árbol. Por tanto, como se muestra a continuación, hay tres árboles expandidos para G.



■

Arboles expandidos mínimos

Al grafo de las rutas permitidas por la Autoridad Federal de Aviación que se muestra en la figura 10.7.1 se le puede anotar las distancias (en millas) entre cada par de ciudades. Esto está hecho en la figura 10.7.3.

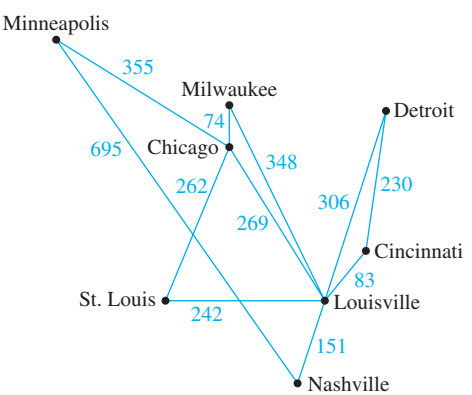


Figura 10.7.3

Ahora supongamos que la compañía aérea quiere servir a todas las ciudades que se muestran, pero con un sistema de ruta que minimice el kilometraje total. Observe que este sistema es un árbol, porque si el sistema contiene un circuito, la eliminación de una arista del circuito no afectaría la capacidad de una persona para llegar a todas las ciudades en el sistema de todos los demás (otra vez, por lema 10.5.3), pero reduciría el kilometraje total del sistema.

Más generalmente, un grafo cuyas aristas están etiquetadas con números (conocidos como *pesos*) se llama un *grafo pesado*. Un *árbol recubridor de mínimo peso*, o simplemente *árbol expandido mínimo*, es un árbol expandido en el que la suma de los pesos de todas las aristas es tan pequeña como sea posible.

• Definición

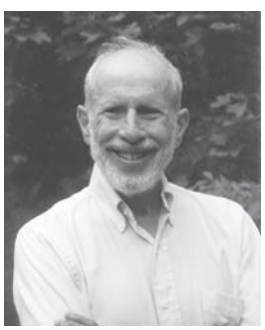
Un **grafo pesado** es un grafo en el que cada arista tiene un **peso**, número real positivo asociado. La suma de los pesos de todas las aristas es el **peso total** del grafo. Un **árbol expandido mínimo** para un grafo conexo pesado es un árbol expandido que tiene el menor peso total posible en comparación con otros árboles expandidos para el grafo.

Si G es un grafo pesado y e es una arista de G, entonces $\boldsymbol{w(e)}$ denota el peso de e y $\boldsymbol{w(G)}$ denota el peso total de G.

El problema de encontrar un árbol expandido mínimo para un grafo es ciertamente soluble. Una solución es listar todos los árboles expandidos del grafo, calcular el peso total de cada uno y elegir uno para el que esta cifra sea un mínimo. (Observe que el principio del buen orden para los enteros garantiza la existencia de dicho mínimo total.) Sin embargo esta solución, es ineficiente en su uso de tiempo de computación porque el número de árboles expandidos distintos es muy grande. Por ejemplo, un grafo completo con n vértices tiene n^{n-2} árboles expandidos. Incluso con los equipos más rápidos disponibles hoy en día, examinar todos estos árboles en un grafo con aproximadamente 100 vértices requeriría más tiempo del que se estima que resta en la vida del universo.

En 1956 y 1957, Joseph B. Kruskal y Robert C. Prim cada uno describió algoritmos mucho más eficientes para construir árboles expandidos mínimos. Incluso para grafos grandes, ambos algoritmos se pueden implementar para tener tiempos de computación relativamente cortos.

Algoritmo de Kruskal



Cortesía de Joseph Kruskal

Joseph Kruskal (nacido en 1928)

En el algoritmo de Kruskal, las aristas de un grafo conexo pesado son examinadas una por una en orden creciente de peso. En cada etapa la arista que se está examinando se agrega a lo que será el árbol expandido mínimo, siempre que esta adición hace no cree un circuito. Después de que se han agregado $n - 1$ aristas (donde n es el número de vértices del grafo), estas aristas, junto con los vértices del grafo, forman un árbol expandido mínimo para el grafo.

Algoritmo 10.7.1 Kruskal

Entrada: *G [un grafo conexo pesado con n vértices, donde n es un entero positivo]*

Cuerpo del algoritmo:
[Construya un subgrafo T de G que consista de todos los vértices de G con aristas agregadas en orden creciente de peso. En cada etapa, sea m el número de aristas de T.]

1. Inicialice T para tener todos los vértices de G y sin aristas.
2. Sea E el conjunto de todas las aristas de G y sea $m := 0$.
3. **while** $(m < n - 1)$
   - 3a. Encuentre una arista e en E de menor peso.
   - 3b. Elimine e de E.
   - 3c. **Si** la adición de e al conjunto de aristas de T no produce un circuito
     entonces agregar e al conjunto de las aristas de T y se hace $m := m + 1$

   end while

Salida: *T [T es un árbol expandido mínimo para G.]*

En el ejemplo siguiente se muestra cómo el algoritmo de Kruskal funciona para el grafo del sistema de rutas de la aerolínea.

Ejemplo 10.7.2 Acción del algoritmo de Kruskal

Describa la acción del algoritmo de Kruskal en el grafo que se muestra en la figura 10.7.4, donde $n = 8$.

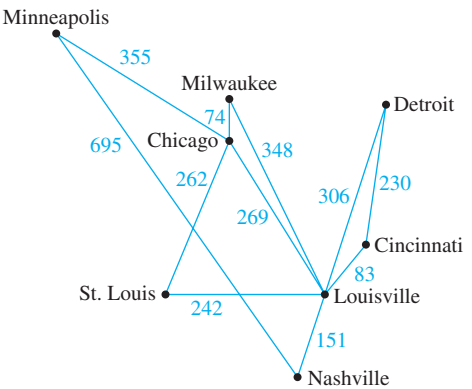


Figura 10.7.4

Solución

Número de iteración	Arista considerada	Peso	Acción tomada
1	Chicago–Milwaukee	74	agregada
2	Louisville–Cincinnati	83	agregada
3	Louisville–Nashville	151	agregada
4	Cincinnati–Detroit	230	agregada
5	St. Louis–Louisville	242	agregada
6	St. Louis–Chicago	262	agregada
7	Chicago–Louisville	269	no agregada
8	Louisville–Detroit	306	no agregada
9	Louisville–Milwaukee	348	no agregada
10	Minneapolis–Chicago	355	agregada

En la figura 10.7.5 se muestra el árbol producido por el algoritmo de Kruskal.

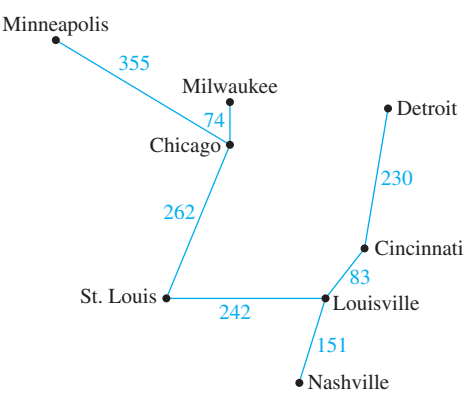


Figura 10.7.5 ■

Cuando se utiliza el algoritmo de Kruskal en un grafo en el que algunas aristas tienen el mismo peso que otras, más de un árbol expandido mínimo puede ocurrir como resultado.

Para realizar la salida única, las aristas del grafo pueden colocarse en una matriz y pueden agregar bordes con el mismo peso en el orden en que aparecen en la matriz.

No resulta evidente de la descripción del algoritmo de Kruskal que hace lo que se tenga que hacer. ¿Para ser específicos, qué garantiza que es posible en cada etapa encontrar una arista de peso menor cuya adición no produzca un circuito? ¿Y si pueden encontrarse esas aristas, qué garantiza que todo finalmente se conectará? ¿Y si se conectan, qué garantiza que el árbol resultante tenga peso mínimo? Por supuesto, el mero hecho de que el algoritmo de Kruskal está impreso en este libro puede llevarle a creer que todo funciona. Pero las preguntas de arriba son reales y merecen respuestas serias.

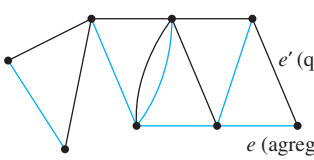
Teorema 10.7.2 Corrección del algoritmo de Kruskal

Cuando un grafo conexo, pesado es la entrada al algoritmo de Kruskal, el resultado es un árbol expandido mínimo.

Demostración:

Supongamos que G es un grafo conexo, pesado con n vértices y que T es un subgrafo de G producido cuando G es una entrada para el algoritmo de Kruskal. Claramente está libre de circuito *[ya que nunca se agrega ninguna arista que complete un circuito a T]*. También T es conexo. T tiene más de un componente conectado, el conjunto de aristas de G que se pueden agregar a T sin crear un circuito es no vacío. *[La razón es que como G es conexo, dado cualquier vértice v_1 en uno de los componentes conectado C_1 de T y cualquier vértice v_2 en otro componente conectado C2, hay una trayectoria en G de v_1 a v_2. Ya que C_1 y C_2 son distintos, hay una arista e de esta trayectoria que no está en T. Agregar e a T no crea un circuito en T, porque la eliminación de una arista de un circuito no desconecta un grafo y la eliminación podría.]* Los argumentos anteriores muestran que T está libre de circuitos y conexo. Ya que por construcción T contiene todos los vértices de G, T es un árbol expandido de G.

A continuación mostramos que T tiene peso mínimo. Sea T_1 cualquier árbol expandido mínimo de G tal que el número de aristas T_1 y T tienen en común un máximo. Supongamos que $T \neq T_1$. Entonces hay una arista e en T que no es una arista de T_1. *[Ya que los árboles T y T_1 tienen el mismo conjunto de vértices, si difieren en todo, deben tener seis diferentes conjuntos de aristas, pero del mismo tamaño.]* Ahora agregando e a T_1 se produce un grafo con un único circuito (vea el ejercicio 19 al final de esta sección). Sea e' una arista de este circuito, tal que e' no está en T. *[Dicha arista debe existir porque T es un árbol y, por tanto, está libre de circuito.]* Sea T_2 el grafo que se obtiene de T_1 eliminando e' y agregando e. Esta situación se ilustra a continuación.



El grafo entero es G. T_1 tiene aristas negras. e está en T pero no en T_1. e' está en T_1 pero no T.

Observe que T_2 tiene $n - 1$ aristas y n vértices y que T_2 es conexo *[ya que por el lema 10.5.3 está conectada al subgrafo obtenido mediante la eliminación de una arista de un circuito en un grafo conexo]*. En consecuencia, T_2 es un árbol expandido de G. Además,

$$w(T_2) = w(T_1) - w(e') + w(e).$$

Ahora $w(e) \leq w(e')$ porque en la etapa del algoritmo de Kruskal cuando se agregó e a T, e' estaba disponible para agregar *[ya que no estaba ya en T y en ese momento su*

adición no podría producir un circuito e que no estaba en T] y e' habría sido añadido su peso había sido inferior al de e. Por tanto

$$w(T_2) = w(T_1) - \underbrace{[w(e') - w(e)]}_{\geq 0}$$
$$\leq w(T_1).$$

Pero T_1 es un árbol expandido mínimo. Dado que T_2 es un árbol expandido con peso inferior o igual al peso de T_1, T_2 también es un árbol expandido mínimo de G.

Por último, observe que, por construcción, T_2 tiene una arista más con T que T_1, lo que contradice la elección de T_1 como árbol expandido mínimo para G con un número máximo de aristas en común con T. Por tanto la suposición de que $T \neq T_1$ es falsa y por tanto T en sí misma es un árbol expandido mínimo de G.

Algoritmo de Prim

Cortesía de Alcatel-Lucent Technologies

Robert Prim (nacido en 1921)

El algoritmo de Prim funciona diferente del de Kruskal. Se construye un árbol expandido mínimo T expandiendo hacia el exterior con enlaces conectados en algunos vértices. En cada etapa se agregan una arista y un vértice. La arista añadida es la de menos peso que conecta los vértices que están en T con los no están en T y el vértice es el punto extremo de esta arista que ya no está en T.

Algoritmo 10.7.2

Entrada: *G [un grafo conexo pesado con vértices n, donde n es un entero positivo]*

Cuerpo del algoritmo:
[Construya un subgrafo T de G que inicie con cualquier vértice v de G y asocie las aristas (con sus puntos extremos) uno por uno conforme este un vértice desconectado de G cada vez que se elija una arista de menos peso que sea adyacente a un vértice de T.]

1. Seleccione un vértice v de G y sea T el grafo con un vértice v y sin aristas.
2. Sea V el conjunto de todos los vértices de G excepto v.
3. **for** $i := 1$ **a** $n - 1$
   - 3a. Encuentre una arista e de G tal que (1) e conecta a T con uno de los vértices en v y (2) e tiene el peso mínimo de todas las aristas que conectan a T con un vértice en V. Sea w el punto extremo de e que se encuentra en V.
   - 3b. Agregue e y w a los conjuntos de aristas y vértices de T y elimine w de V.

   next i

Salida: *T [T es un árbol expandido mínimo para G.]*

En el ejemplo siguiente se muestra cómo el algoritmo de Prim funciona para el grafo del sistema de rutas de la aerolínea.

Ejemplo 10.7.3 Acción del algoritmo de Prim

Describa la acción del algoritmo de Prim para el grafo en la figura 10.7.6 utilizando el vértice de Minneapolis como un punto de partida.

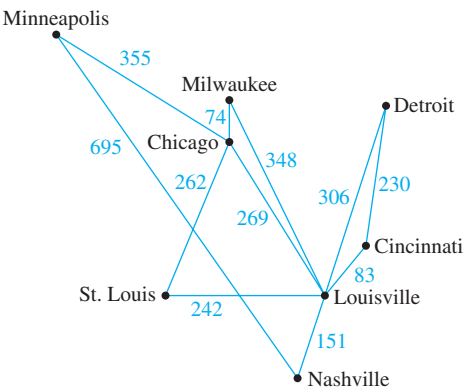


Figura 10.7.6

Solución

Número de iteración	Vértice agregado	Arista agregada	Peso
0	Minneapolis		
1	Chicago	Minneapolis–Chicago	355
2	Milwaukee	Chicago–Milwaukee	74
3	St. Louis	Chicago–St. Louis	262
4	Louisville	St. Louis–Louisville	242
5	Cincinnati	Louisville–Cincinnati	83
6	Nashville	Louisville–Nashville	151
7	Detroit	Cincinnati–Detroit	230

Observe que el árbol que se obtiene es igual al obtenido con el algoritmo de Kruskal, pero las aristas se agregan en un orden diferente.

Como con el algoritmo de Kruskal, a fin de garantizar una única salida, las aristas del grafo podrían colocarse en una matriz y los que tienen el mismo peso podrían agregarse en el orden en que aparecen en la matriz. No es difícil ver que cuando se conecta un grafo a la entrada al algoritmo de Prim, el resultado es un árbol expandido. Lo que no está tan claro es que este árbol expandido es un mínimo. La demostración del teorema siguiente establece que lo es.

Teorema 10.7.3 Corrección algoritmo de Prim

Cuando un grafo pesado, conexo G se introduce en el algoritmo de Prim, el resultado es un árbol expandido mínimo para G.

Demostración:

Sea G un grafo conexo, pesado y suponga que G es una entrada para el algoritmo de Prim. En cada etapa de ejecución del algoritmo, se debe encontrar una arista que conecte un vértice en un subgrafo con un vértice fuera del subgrafo. Mientras que haya vértices fuera del subgrafo, la conexión de G asegura que siempre se encuentran dicha arista. *[Por si se eligen uno de los vértices en el subgrafo y uno de los vértices fuera de ésta, por la conexión de G hay un camino en G para conectar a los dos. Conforme se viaja lo largo de este camino, en algún momento uno se mueve a lo largo de una arista de un vértice dentro del subgrafo a un vértice fuera del subgrafo.]*

Ahora está claro que la salida T del algoritmo de Prim es un árbol porque la arista y el vértice agregado a T en cada etapa se conectan con otras aristas y vértices de T

y porque en ninguna etapa se crea un circuito ya que cada arista agregada conecta vértices en dos conjuntos disjuntos. *[Por tanto, la eliminación de una arista recién agregada produce un grafo no conexo, mientras que por el lema 10.5.3, la eliminación de una arista de un circuito produce un grafo conexo.]* También, T incluye todos los vértices de G porque T, siendo un árbol con $n - 1$ aristas, tiene n vértices [y todos están en G]. Por tanto T es un árbol expandido de G.

A continuación mostramos que T tiene peso mínimo. Sea T_1 un árbol expandido mínimo de G tal que el número de aristas de T_1 y T tienen en común que es un máximo. Supongamos que $T \neq T_1$. Entonces hay una arista e en T que no se trata de una arista de T_1. *[Ya que los árboles T y T_1, ambos tienen el mismo vértice si difieren en todo, deben tener conjuntos de aristas diferentes, del mismo tamaño.]* De todos esos extremos, e será la última que se agregó cuando se construyó T mediante el algoritmo de Prim de e. Sea S el conjunto de vértices de T justo antes de la adición de e. Entonces un punto extremo, por ejemplo v de e, está en S y el otro, digamos w, no lo está. Dado que T_1 es un árbol expandido, existe una trayectoria en T_1 que une a v y w. Y puesto que $v \in S$ y $w \notin S$, conforme se viaja a lo largo de esta trayectoria, se debe encontrar una arista e' que une a un vértice en S con uno que no está en S y por lo tanto, no está en T, porque fue la última arista que se agrego a T. Ahora en la etapa cuando se agregó e a T, e' se podría también haber añadido y se habría agregado en lugar de e que tenía un peso menor que el de e. Como e' no se ha agregado en esa etapa, concluimos que

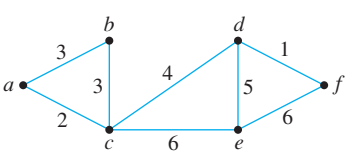
$$w(e') > w(e).$$

Sea T_2 el grafo que se obtuvo de T_1 eliminando e' y agregando e. *[Así T_2 tiene una arista más en común con T que T_1.]* Observe que T_2 es un árbol. La razón es que, como e' es parte de una trayectoria en T_1 de v a w y e conecta a v con w, agregando e a T_1 creando un circuito. Cuando e' se elimina de este circuito, el subgrafo resultante permanece conexo. De hecho, T_2 es un árbol expandido para G ya que no se retiraron vértices en la formación de T_2 de T_1. El argumento que muestre que $w(T_2) \leq w(T_1)$ queda como un ejercicio. *[Es prácticamente idéntico a la parte de la demostración del teorema 10.7.2.]* Se deduce que T_2 es árbol expandido mínimo de G.

Por construcción, T_2 tiene una arista más en común con T de T_1, hace que contradice la elección de T_1 como árbol expandido mínimo para G con un número máximo de aristas en común con T. De lo que se deduce que $T = T_1$ y por tanto T es un árbol expandido mínimo por ejemplo G.

Ejemplo 10.7.4 Encuentre árboles expandidos mínimos

Encuentre los árboles expandidos mínimos para el siguiente grafo. Use el algoritmo de Kruskal y el algoritmo de Prim a partir de vértices a. Indique el orden que se agregan las aristas para formar cada árbol.



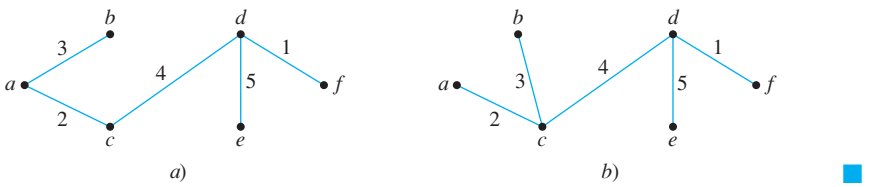
Solución Cuando se aplica el algoritmo de Kruskal, se agregan los aristas en uno de los siguientes dos órdenes:

1. $\{d, f\}$ $\{a, c\}$, $\{a, b\}$, $\{c, d\}$, $\{d, e\}$
2. $\{d, f\}$, $\{a, c\}$, $\{b, c\}$, $\{c, d\}$, $\{d, e\}$

Cuando se aplica el algoritmo de Prim a partir de a, se agregan las aristas a en uno de los siguientes dos órdenes:

1. $\{a, c\}, \{a, b\}, \{c, d\}, \{d, f\}, \{d, e\}$
2. $\{a, c\}\ \{b, c\}, \{c, d\}, \{d, f\}, \{d, e\}$

Así, como se muestra a continuación, hay dos distintos árboles expandidos mínimos para este grafo.



Algoritmo de la trayectoria más corta de Dijkstra

Aunque los árboles producidos por los algoritmos Kruskal y de Prim tienen el peso total lo menos posible en comparación con todos los demás árboles expandidos para el grafo, no siempre revelan la distancia más corta entre dos puntos en el grafo. Por ejemplo, de acuerdo al sistema de rutas completo que se muestra en la figura 10.7.3, uno puede volar directamente desde Nashville a Minneapolis una distancia de 695 km, mientras que utilice el árbol expandido mínimo que se muestra en la figura 10.7.5 es la única manera de volar desde Nashville a Minneapolis al pasar por Louisville, San Louis y Chicago, que da una distancia total $151 + 242 + 262 + 355 = 1\,010$ millas y la descortesía de tres cambios de avión.

En 1959 el pionero informático, Edsgar Dijkstra (vea la sección 5.5), desarrolló un algoritmo para encontrar la trayectoria más corta entre un vértice inicial y un vértice en un grafo pesado en el que todos los pesos son positivos. Es algo similar al algoritmo de Prim que trabaja hacia el exterior desde un vértice inicial a, agregando vértices y aristas uno por uno para construir un árbol T. Sin embargo, difiere del algoritmo de Prim en la forma en que se elige el siguiente vértice a agregar, asegurando que para cada vértice agregado v, la longitud de la ruta más corta de a a v se ha identificado.

En el inicio de la ejecución del algoritmo, a cada vértice u de G se le da una etiqueta $L(u)$, que indica la mejor estimación actual de la longitud de la ruta más corta de a a u. $L(a)$ se hace inicialmente igual a 0 ya que el camino más corto de a a a tiene longitud cero, pero, debido a que no existe ninguna información previa acerca de las longitudes de las trayectorias más cortas de a a cualquier otro vértice de G, la etiqueta $L(u)$ de cada vértice u diferente de a se hace inicialmente igual a un número, que se denota por ∞, que es mayor que la suma de los pesos de todas las aristas de G. Como la ejecución de los progresos de algoritmo, se cambian los valores de $L(u)$, convirtiéndose en las longitudes reales de las trayectorias más cortas de a a u en G.

Porque T se construye hacia el exterior desde a, en cada etapa de ejecución del algoritmo los únicos vértices que son candidatos a formar parte de T son los que están junto al menos un vértice de T. Así, en cada etapa del algoritmo de Dijkstra, el grafo G puede pensarse como dividido en tres partes: el árbol T que se está construyendo en el conjunto de vértices "marginales" que son adyacentes al menos a un vértice del árbol y el resto de los vértices de G. Cada franja de vértices es un candidato a ser el siguiente vértice agregado a T. El elegido es aquel para el que la longitud de la trayectoria más corta de a a T es un mínimo entre todos los vértices de la franja.

Una observación fundamental subyacente del algoritmo de Dijkstra es que después de cada adición de un vértice v a T, sólo los vértices de la franja para los que una trayectoria más corta de a se pueda encontrar son aquellas que son adyacentes a v *[ya que la longitud de la trayectoria de a a v fue un mínimo entre todas las trayectorias de a a los vértices que estaban entonces en la franja]*. Así después de cada adición de un vértice v a T, cada

vértice u de la franja adyacente a v; se examina y se comparan dos números: el valor actual de $L(u)$ y el valor de $L(v) + w(v, u)$, donde $L(v)$ es la longitud de la trayectoria más corta a v (en T) y $w(v, u)$ es el peso de la arista que une a v con u. Si $L(v) + w(v, u) < L(u)$, entonces el valor de $L(u)$ se cambia a $L(v) + w(v, u)$.

Al comienzo de la ejecución del algoritmo, el árbol consta sólo del vértice a y $L(a) = 0$. Cuando se termina la ejecución, $L(z)$ es la longitud de la trayectoria más corta de a a z.

Como con los algoritmos de Kruskal y Prim para encontrar árboles expandidos mínimos, hay una manera simple pero dramáticamente ineficiente para encontrar el camino más corto de a a z: calcular la longitud de todas las trayectorias y se elige la que sea más corta. El problema es que aún grafos relativamente pequeños que utilicen este método para encontrar una trayectoria más corta podría requerir miles de millones de años, mientras que el algoritmo de Dijkstra podría hacer el trabajo en unos segundos.

Algoritmo 10.7.3 Dijkstra

Entrada: *G [un grafo conexo simple con un peso positivo para cada arista], ∞ [un número mayor que la suma de los pesos de todas las aristas del grafo], $w(u, v)$ [el peso de la arista $\{u, v\}$], a [el vértice inicial], z [vértice final]*

Cuerpo del algoritmo:

1. Inicializa T como el grafo con el vértice a y sin aristas. Sea $V(T)$ el conjunto de los vértices de T y sea $E(T)$ el conjunto de aristas de T.
2. Sea $L(a) = 0$ y para todos los vértices en G excepto a, sea $L(u) = \infty$.
   [El número $L(x)$ se llama la etiqueta de x.]
3. Inicialice v a igual a a y F será $\{a\}$.
   [El símbolo v se utiliza para denotar el vértice agregado a T.]
4. **while** $(z \notin V(T))$
   - **4a.** $F := (F - \{v\}) \cup \{$vértices que son adyacentes a v y no están en $V(T)\}$
     [El conjunto F se llama la franja. Cada vez que se agrega un vértice a T, se elimina de la franja y se agregan los vértices adyacentes a la franja si ya no están en la franja o en el árbol T.]
   - **4b.** Para cada vértice u que es adyacente a v y no está en $V(T)$,
     if $L(u) + w(v, u) < L(u)$ **then**

     $$L(u) := L(v) + w(v, u)$$

     $$D(u) := v$$

     [Observe que agregar v a T no afecta las etiquetas de los vértices en la franja F excepto aquellas adyacentes a v. También, cuando $L(u)$ se cambia a un valor menor, se introduce la notación $D(u)$ para realizar un seguimiento de qué vértice en T dio lugar al menor valor.]
   - **4c.** Encuentre un vértice x en F con la etiqueta más pequeña
     Agregue el vértice x a $V(T)$ y se agrega una arista $\{D(x), x\}$ a $E(T)$
     $v := x$ *[Este enunciado establece la notación para la siguiente iteración del bucle.]*

   end while

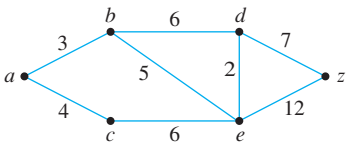
Salida: *$L(z)$ [$L(z)$, un entero no negativo, es la longitud de la trayectoria más corta de a a z.]*

Nota La única trayectoria en el árbol T de a a z es la trayectoria más corta en G de a a z.

La acción del algoritmo de Dijkstra se muestra con el flujo de los dibujos del ejemplo 10.7.5.

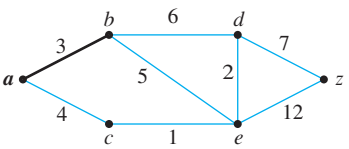
Ejemplo 10.7.5 Acción del algoritmo de Dijkstra

Mostrar los pasos en la ejecución del algoritmo de Dijkstra de la trayectoria más corta para el grafo que se muestra a continuación con vértice inicial a y final z.



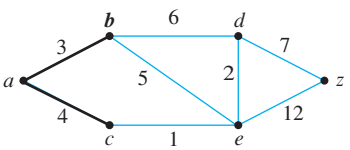
Solución

Paso 1: Va al bucle **while**: $V(T) = \{a\}$, $E(T) = \emptyset$ y $F = \{a\}$



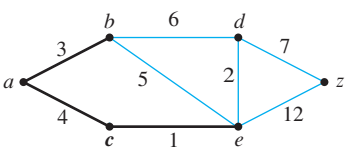
Durante la iteración:
$F = \{b, c\}$, $L(b) = 3$, $L(c) = 4$.
Ya que $L(b) < L(c)$, b se agrega a $V(T)$ y $\{a, b\}$ se agrega a $E(T)$.

Paso 2: Va al bucle **while**: $V(T) = \{a, b\}$, $E(T) = \{\{a, b\}\}$



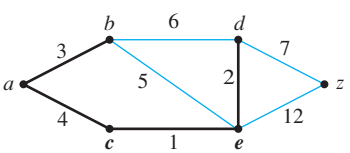
Durante la iteración:
$F = \{c, d, e\}$, $L(c) = 4$, $L(d) = 9$, $L(e) = 8$.
Puesto que $L(c) < L(d)$ y $L(c) < L(e)$, c se agrega a $V(T)$ y $\{a, c\}$ se agrega a $E(T)$.

Paso 3: Va al bucle **while**: $V(T) = \{a, b, c\}$, $E(T) = \{\{a, b\}, \{a, c\}\}$



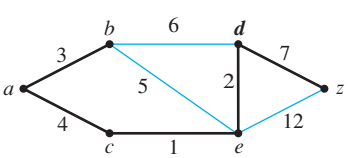
Durante la iteración:
$F = \{d, e\}$, $L(d) = 9$, $L(e) = 5$.
$L(e)$ se hace 5 porque ace, que tiene longitud 5, es una trayectoria más corta a e que abe, que tiene longitud 8.
Ya que $L(e) < L(d)$, e se agrega a $V(T)$ y $\{c, e\}$ se agrega a $E(T)$.

Paso 4: Va al bucle **while**: $V(T) = \{a, b, c, e\}$, $E(T) = \{\{a, b\}, \{a, c\}, \{c, e\}\}$



Durante la iteración:
$F = \{d, z\}$, $L(d) = 7$, $L(z) = 17$
$L(d)$ se hace 7 porque $aced$, que tiene longitud 7, es una trayectoria más corta a d que abd, que tiene la longitud 9.
Ya que $L(d) < L(z)$, d se agrega a $V(T)$ y $\{e, d\}$ se agrega a $E(T)$.

Paso 5: Va al bucle **while**: $V(T) = \{a, b, c, e, d\}$, $E(T) = \{\{a, b\}, \{a, c\}, \{c, e\}, \{e, d\}\}$



Durante la iteración: $F = \{z\}$, $L(z) = 14$
$L(z)$ se convierte en 14 porque $acedz$, que tiene longitud 14, es una trayectoria más corta a d que $abdz$, que tiene 17.
Puesto que z es el único vértice en F, su etiqueta es un mínimo y por lo que z se agrega a $V(T)$ y $\{e, z\}$ se agrega a $E(T)$.

La ejecución del algoritmo termina en este momento porque $z \in V(T)$. La trayectoria más corta de a a z tiene longitud $L(z) = 14$. ■

Siguiendo los pasos en una tabla es una forma conveniente de mostrar la acción de algoritmo de Dijkstra. La tabla 10.7.1 hace esto para el grafo del ejemplo 10.7.5.

Tabla 10.7.1

Paso	$V(T)$	$E(T)$	F	$L(a)$	$L(b)$	$L(c)$	$L(d)$	$L(e)$	$L(z)$
0	$\{a\}$	$\emptyset$	$\{a\}$	**0**	∞	∞	∞	∞	∞
1	$\{a\}$	$\emptyset$	$\{b, c\}$	0	**3**	4	∞	∞	∞
2	$\{a, b\}$	$\{\{a, b\}\}$	$\{c, d, e\}$	0	3	**4**	9	8	∞
3	$\{a, b, c\}$	$\{\{a, b\}, \{a, c\}\}$	$\{d, e\}$	0	3	4	9	**5**	∞
4	$\{a, b, c, e\}$	$\{\{a, b\}, \{a, c\}, \{c, e\}\}$	$\{d, z\}$	0	3	4	**7**	5	17
5	$\{a, b, c, e, d\}$	$\{\{a, b\}, \{a, c\}, \{c, e\}, \{e, d\}\}$	$\{z\}$	0	3	4	7	5	**14**
6	$\{a, b, c, e, d, z\}$	$\{\{a, b\}, \{a, c\}, \{c, e\}, \{e, d\}, \{e, z\}\}$							

Es claro que el algoritmo de Dijkstra mantiene agregar vértices a I hasta se que han agregado a z. La demostración del teorema siguiente muestra que cuando termina el algoritmo, la etiqueta z recorre la longitud de la trayectoria más corta de a.

Teorema 10.7.4 Corrección del algoritmo de Dijkstra

Cuando un grafo conexo simple, con un peso positivo para cada arista es la entrada al algoritmo de Dijkstra con vértice inicial a y vértice final z, la salida es la longitud de una trayectoria más corta de a a z.

Demostración:

Sea G un grafo conexo, pesado sin bucles o aristas paralelas y con un peso positivo para cada arista. Sea T el grafo creado por el algoritmo de Dijkstra y para cada vértice u en G, sea $L(u)$ la etiqueta dada por el algoritmo al vértice u. Para cada entero $n \geq 0$, que la propiedad $P(n)$ sea la frase

> Después de la enésima iteración del bucle while en el algoritmo de Dijkstra, 1) T es un árbol y 2) para cada vértice v en T, $L(v)$ es la longitud de una trayectoria más corta en G de a a v. ← $P(n)$

Mostraremos por inducción matemática que $P(n)$ es verdadera para todos los enteros n de 0 a la terminación del algoritmo.

Demostración de que P(0) es verdadero: Cuando $n = 0$, el grafo T es un árbol porque se define que consta sólo del vértice a y sin extremos. Además, $L(a)$ es la longitud de la trayectoria más corta de a a a ya que el valor inicial de $L(a)$ es 0.

Demostración de que para todos los enteros k ≥ 0, si P(k) es verdadero entonces P(k + 1) es también verdadero: Sea k cualquier entero con $k \geq 0$ y suponga que

> Después de la k-ésima iteración del bucle while en el algoritmo de Dijkstra, 1) T es un árbol y 2) para cada vértice v en T, $L(v)$ es la longitud de la trayectoria más corta en G de a a v. ← $P(k)$ hipótesis de inducción

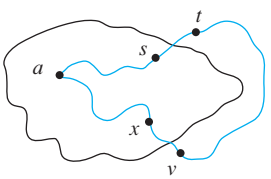
Debemos demostrar que

> Después de la $(k + 1)$ésima iteración del bucle **while** en el algoritmo de Dijkstra, 1) T es un árbol y 2) para cada vértice v en T, $L(v)$ es la longitud de la trayectoria más corta en G de a a v. ← $P(k + 1)$

continúa en la página 714

Así que suponga que después de la $(k + 1)$ésima iteración del bucle **while** en el algoritmo de Dikjstra, el vértice v y la arista $\{x, v\}$ se han agregado a T, donde x está en $V(T)$. Claramente el nuevo valor de T es un árbol porque agregar un vértice nuevo y arista a un árbol no crea un circuito y desconecta el árbol. Por hipótesis de inducción para cada vértice y en el árbol antes de la adición de v, $L(y)$ es la longitud de una trayectoria más corta de a a y. Así queda sólo mostrar que $L(v)$ es la longitud de una trayectoria más corta de a a v.

Ahora, de acuerdo con el algoritmo, el valor final de $L(v) = L(x) + w(x, v)$. Considere *cualquier* trayectoria más corta de a a v y $\{s, t\}$ la primer arista en esta trayectoria que sale de T, donde $s \in V(T)$ y $t \notin V(T)$. Este caso se muestra a continuación.



Sea $LSP(a, v)$ la longitud de la trayectoria más corta de a a v y sea $LSP(a, s)$ la longitud de la trayectoria más corta de a a s. Observe que

$$LSP(a, v) \geq LSP(a, s) + w(s, t)$$ ya que la trayectoria de t a v tiene longitud ≥ 0

$$\geq L(s) + w(s, t)$$ por hipótesis de inducción porque s es un vértice en T

$$\geq L(x) + w(x, v)$$ t está en la franja del árbol y así si $L(s) + w(s, t)$ eran menores que $L(x) + w(x, v)$ entonces se tendría que agregar t en lugar de v.

Por otro lado

$$L(x) + w(x, v) \geq LSP(a, v)$$ ya que $L(x) + w(x, v)$ es la longitud de una trayectoria de a a v y que es mayor o igual a la longitud de la trayectoria más corta de a a v.

Se deduce que $$LSP(a, v) = L(x) + w(x, v),$$

y puesto que $$L(v) = L(x) + w(x, v),$$

$L(v)$ es la longitud de la trayectoria más corta de a a v. Esto completa la demostración por inducción matemática.

El algoritmo termina tan pronto como z esté en T y ya hemos demostrado que la marca de cada vértice en el árbol indica la longitud de la trayectoria más corta de a, entonces, en particular, $L(z)$ es la longitud de una trayectoria más corta de a a z.

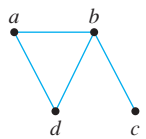
Autoexamen

1. Un árbol expandido para un grafo G es _____.
2. Un grafo pesado es un grafo para la que _____ y el peso total del grafo es _____.
3. Un árbol expandido mínimo para un grafo conexo pesada es _____.
4. En el algoritmo de Kruskal, las aristas de un grafo conexo, pesado se examinan uno por uno en orden de _____ comenzando con _____ .
5. En el algoritmo de Prim, un árbol expandido mínimo se construye por expansión hacia el exterior de un _____ en una sucesión de _____.
6. En el algoritmo de Dijkstra, un vértice está en la franja si es un vértice _____ en el árbol que se está construyendo.
7. En cada etapa del algoritmo de Dijkstra, el vértice que se agrega al árbol es un vértice en la franja cuya etiqueta es un _____.

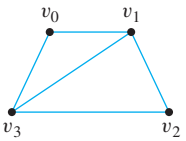
Conjunto de ejercicios 10.7

Encuentre todos los posibles árboles expandidos para cada uno de los grafos 1 y 2.

1.

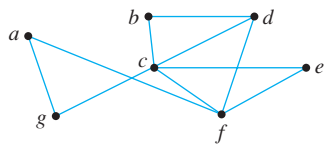


2.

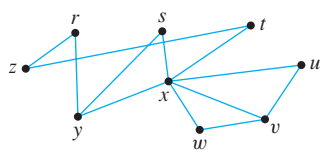


Encuentre un árbol expandido para cada una de los grafos en los ejercicios 3 y 4.

3.

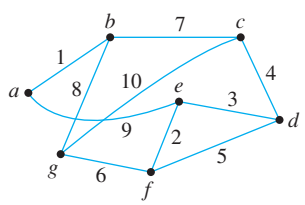


4.

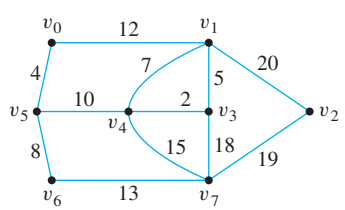


Utilice el algoritmo de Kruskal para encontrar un árbol expandido mínimo para cada una de los grafos en los ejercicios 5 y 6. Indique el orden en que las aristas se agregan para formar cada árbol.

5.



6.



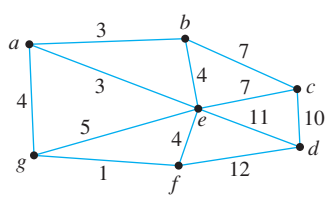
Uso del algoritmo de Prim partiendo del vértice a o v_0 encuentre un árbol expandido mínimo para cada una de los grafos en los ejercicios 7 y 8. Indique el orden en que se agregan las aristas para formar cada árbol.

7. El grafo del ejercicio 5.

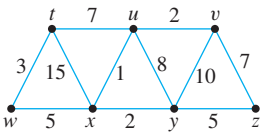
8. El grafo del ejercicio 6.

Para cada uno de los grafos en los ejercicios 9 y 10, encuentre todos los árboles de expansión mínimos que pueden obtenerse mediante *a*) el algoritmo de Kruskal y *b*) el algoritmo de Prim partiendo de un vértice a o t. Indique el orden en que se agregan las aristas para formar cada árbol.

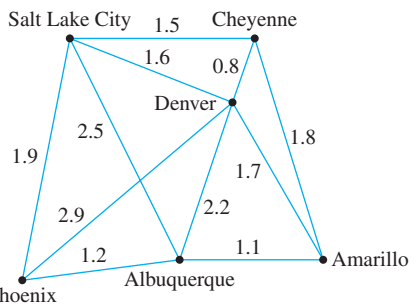
9.



10.



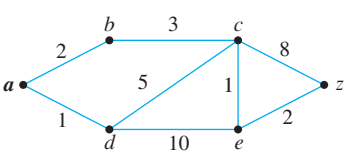
11. Se construye una tubería que enlaza seis ciudades. El costo (en cientos de millones de dólares) de la construcción de cada enlace potencial depende de la distancia, del terreno y se muestra en el siguiente grafo pesado. Encuentre un sistema de tuberías para conectar todas las ciudades y aún reducir al mínimo el costo total.



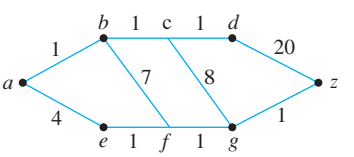
12. Utilice el algoritmo de Dijkstra para el sistema de ruta de la aerolínea de la figura 10.7.3 para encontrar la distancia más corta de Nashville a Minneapolis. Haga una tabla similar a la tabla 10.7.1 para mostrar la acción del algoritmo.

Utilizar el algoritmo de Dijkstra para encontrar el camino más corto de a a z para cada uno de los grafos en los ejercicios 13 al 16. En cada caso haga tablas similares a la tabla 10.7.1 para mostrar la acción del algoritmo.

13.



14.



15. El grafo del ejercicio 9 con $a = a$ y $z = f$

16. El grafo del ejercicio 10 con $a = u$ y $z = w$

17. Demuestre el inciso (2) de la proposición 10.7.1: cualesquiera dos árboles expandidos para un grafo tienen el mismo número de aristas.

18. Dados dos vértices distintos de un árbol, existe una única trayectoria de uno a otro.
   a. Dé una justificación informal para el enunciado anterior.
   ✶ **b.** Escriba una demostración formal del enunciado anterior.

19. Demuestre que si G es un grafo con árbol expandido T y e es una arista de G que no está en T, entonces el grafo obtenido por adición de e a T contiene sólo un conjunto de aristas que forman un circuito.

20. Suponga que G es un grafo conexo y T es un subgrafo libre de circuitos de G. Supongamos también que si cualquier arista e de G no está en T se agrega a T, el grafo resultante contiene un circuito. Demuestre que es un árbol expandido para G.

21. **a.** Supongamos que T_1 y T_2 son dos árboles expandidos diferentes para un grafo G. ¿Deben T_1 y T_2 tener una arista en común? Demuestre o dé un contraejemplo.
    b. Suponga que el grafo G en el inciso *a*) es simple. ¿Deben T_1 y T_2 tener una arista en común? Demuestre o dé un contraejemplo.

H 22. Demuestre que una arista e está contenida en cada árbol expandido de un grafo conexo G si y sólo si, se elimina e y se desconecta de G.

23. Considere los árboles expandidos T_1 y T_2 en la demostración del teorema 10.7.3. Demuestre que $w(T_2) \leq w(T_1)$.

24. Suponga que T es un árbol expandido mínimo para un grafo conexo, pesado y que G contiene una arista e (no un bucle) que no está en T. Sean v y w los puntos extremos de e. Por ejercicio 18 hay una ruta única en T de v a w. Sea e' cualquier arista de esta trayectoria. Demuestre que $w(e') \leq w(e)$.

H 25. Demuestre que si G es un grafo conexo, pesado y e es una arista de G (no un bucle) que tiene menor peso que cualquier otra arista de G, entonces e está en cada árbol expandido mínimo para G.

✶ 26. Si G es un grafo conexo, pesado y no dos aristas de G que tienen el mismo peso, ¿existe un único árbol expandido mínimo para G? Utilice el resultado del ejercicio 19 para justificar su respuesta.

✶ 27. Demuestre si G es un grafo conexo, pesado y e es una arista de G que: 1) tiene más peso que cualquier otra arista de G y 2) está en un circuito de G, entonces no hay ningún árbol expandido mínimo T para G tal que e está en T.

28. Suponga que un grafo no conexo es la entrada al algoritmo de Kruskal. ¿Cuál será el resultado?

29. Suponga que un grafo no conexo es la entrada al algoritmo de Prim. ¿Cuál será el resultado?

30. Demuestre que si un grafo G conexo, pesado, es la entrada al algoritmo 10.7.4 (que se muestra a continuación), el resultado es un árbol expandido mínimo para la entrada de algoritmo de G.

Algoritmo 10.7.4

Entrada: *G [un grafo conexo]*

Cuerpo del algoritmo:

1. $T := G$.

2. $E :=$ el conjunto de todas las aristas de G, $m :=$ número de aristas de G.

3. **while** $(m > 0)$.

3a. Encuentre una arista e en E que tiene peso máximo.
3b. Quite e de E y sea el conjunto $m := m - 1$.
3c. **If** el subgrafo obtenido cuando e se quita del conjunto de aristas de T, **entonces** se quita e del conjunto de arista de T

end while

Salida: *T [árbol expandido mínimo para G]*

31. Modifique el algoritmo 10.7.3 que consiste en la salida de la sucesión de las aristas de la trayectoria más corta de a a z.

Respuestas del autoexamen

1. una subgrafo de G que contiene cada vértice de G y es un árbol. 2. cada arista tiene un peso que es un número real positivo asociado; la suma de los pesos de todas las aristas del grafo 3. un árbol expandido que tiene el peso total lo menor posible en comparación con otros árboles expandidos para el grafo 4. peso; una arista de menor peso 5. vértice inicial; vértices adyacentes y aristas 6. adyacente de a 7. mínimo entre todos los de la franja

CAPÍTULO 11

ANÁLISIS DE LA EFICIENCIA DE UN ALGORITMO

Bettmann/CORBIS

René Descartes
(*1596-1650*)

En 1637 el matemático y filósofo francés René Descartes, publicó su gran trabajo filosófico *Discurso sobre el Método*. Un apéndice a este trabajo, llamado "Geometría", estableció el fundamento para el tema de la geometría analítica, en el cual los métodos geométricos son aplicados al estudio de objetos algebraicos, tales como funciones, ecuaciones y desigualdades y los métodos algebraicos son empleados para estudiar objetos geométricos, como rectas, circunferencias y semiplanos.

La geometría analítica de Descartes proporciona el fundamento para el tema principal de este capítulo: las notaciones O, Omega y Theta y su aplicación al análisis de algoritmos. En la sección 11.1 analizamos brevemente ciertas propiedades de las gráficas de funciones de variable real valuadas en los reales, las cuales son necesarias para entender esas notaciones. En la sección 11.2 definimos las notaciones y las aplicamos a funciones potencia y polinomiales y en la sección 11.3 mostramos cómo se emplean las notaciones para estudiar la eficiencia de los algoritmos. Como el análisis de algoritmos frecuentemente implica funciones logarítmicas y exponenciales, en la sección 11.4 desarrollamos las propiedades necesarias de esas funciones, que en la sección 11.5 son usadas para analizar varios algoritmos.

11.1 Funciones de valores reales de una variable real y sus gráficas

El primer precepto fue nunca aceptar una cosa como verdadera hasta que yo la conocí como tal sin duda alguna. —René Descartes, 1637

Un **plano cartesiano** o **sistema coordenado cartesiano bidimensional** es una representación pictórica de $\mathbf{R} \times \mathbf{R}$, obtenida al establecer una correspondencia uno a uno entre pares ordenados de números reales y puntos en un plano euclidiano. Para obtenerla, se dibujan en el plano, dos rectas perpendiculares, llamadas **ejes horizontal** y **vertical**. Su punto de intersección se llama el **origen** y se elige una unidad de distancia para cada eje. Un par ordenado (x, y) de números reales corresponde al punto P que está a $|x|$ unidades a la derecha o a la izquierda del eje vertical y a $|y|$ arriba o abajo del eje horizontal. Sobre cada eje la dirección positiva se indica con una flecha.

Una **función de variable real valuada en los reales** es una función entre dos conjuntos de números reales. Si f es tal función, entonces para cada número real x en el dominio de f, existe un único correspondiente número real $f(x)$. Así, es posible definir la *gráfica de f* como sigue:

• Definición

Sea f una función de variable real valuada en los reales. La **gráfica de *f*** es el conjunto de todos los puntos (x, y) en el plano cartesiano con la propiedad de que x está en el dominio de f y $y = f(x)$.

La definición de gráfica (vea la figura 11.1.1) significa que para todas las x en el dominio de f:

$$y = f(x) \quad \Leftrightarrow \quad \text{el punto } (x, y) \text{ está sobre la gráfica de } f.$$

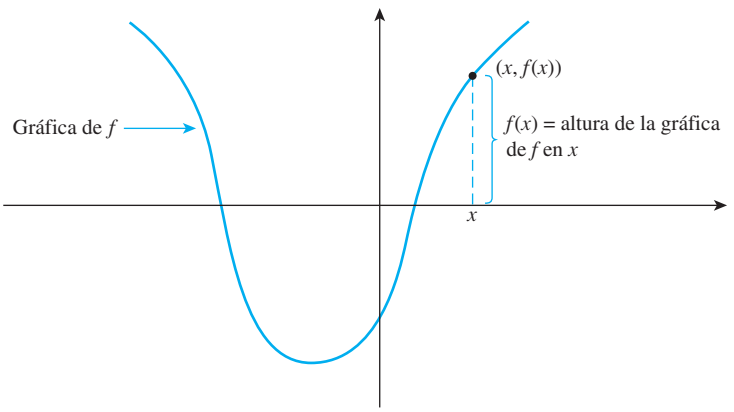


Figura 11.1.1 **Gráfica de una función f**

Observe que si $f(x)$ se puede escribir como una expresión algebraica en x, la gráfica de la función f es la misma que la gráfica de la ecuación $y = f(x)$ en donde x está restringida al dominio de f.

Funciones potencia

Una función que envía a un número real x a una potencia particular, x^a, es llamada una *función potencia*. En aplicaciones en ciencias computacionales, estamos casi invariablemente involucrados en situaciones en donde x y a son no-negativos y entonces restringimos nuestra definición a esos casos.

• Definición

Sea a cualquier número real no-negativo. Definimos p_a, la **función potencia con exponente *a***, como sigue:

$$p_a(x) = x^a \quad \text{para cada número real no-negativo } x.$$

Ejemplo 11.1.1 Gráficas de funciones potencia

Dibuje las gráficas de las funciones potencia p_0, $p_{1/2}$, p_1 y p_2 sobre los mismos ejes coordenados.

Solución La función potencia con exponente cero satisface $p_0(x) = x^0 = 1$ para todos los números no-negativos x,* entonces todos los puntos de la forma $(x, 1)$ están sobre la gráfica de p_0 para dichas x. Así la gráfica es justamente una semi-recta horizontal de altura 1 sobre el eje horizontal. Similarmente, $p_1(x) = x$ para todos los números no-negativos x y así la gráfica de p_1 consiste de todos los puntos de la forma (x, x) en donde x es no-negativo. Por tanto, la gráfica es una semi-recta de pendiente 1 que sale del (0, 0).

Para cada número no-negativo x, $p_{1/2}(x) = x^{1/2} = \sqrt{x}$, entonces cualquier punto con coordenadas $(x, \sqrt{x})$, en donde x es no-negativo, está sobre la gráfica de $p_{1/2}$. Por

* Como en la sección 9.7 (vea la página 598), por simplicidad definimos $0^0 = 1$.

ejemplo, la gráfica de $p_{1/2}$ contiene los puntos (0, 0), (1, 1), (4, 2) y (9, 3). Similarmente, $p_2(x) = x^2$, entonces cualquier punto con coordenadas (x, x^2) está sobre la gráfica de p_2. Así, por ejemplo, la gráfica de p_2 contiene los puntos (0, 0), (1, 1), (2, 4) y (3, 9).

Las gráficas de las cuatro funciones se muestran en la figura 11.1.2.

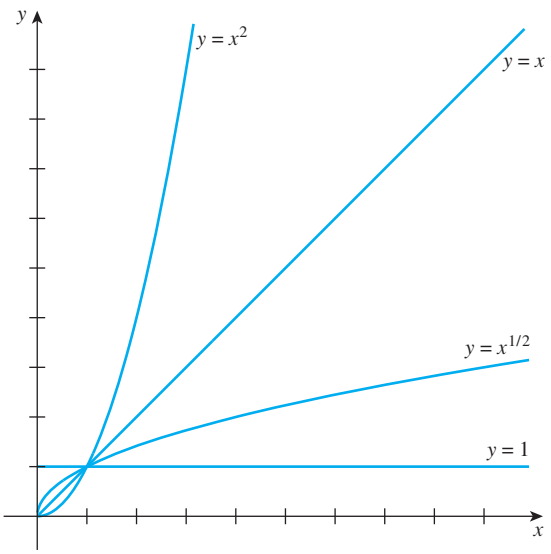


Figura 11.1.2 **Gráficas de algunas funciones potencia**

La función piso

Las funciones piso y techo aparecen en muchos contextos de ciencias computacionales. El ejemplo 11.1.2 muestra la gráfica de la función piso. En el ejercicio 6, al final de esta sección, se le pedirá graficar la función techo.

Ejemplo 11.1.2 Gráfica de la función piso

Recuerde que cada número real es un entero por sí mismo o está entre dos enteros consecutivos: Para cada número real x, existe un entero único n tal que $n \leq x < n + 1$. El piso de un número es el entero inmediatamente a su izquierda sobre la recta numérica. Más formalmente, la función F está definida por la regla:

Para cada número real x,

$$F(x) = \lfloor x \rfloor$$
$$= \text{el más grande entero que es menor o igual que } x$$
$$= \text{el único entero } n \text{ tal que } n \leq x < n + 1.$$

Grafique la función piso.

Solución Si n es cualquier entero, entonces para cada número real x en el intervalo $n \leq x < n + 1$, el piso de x, $\lfloor x \rfloor$, es igual a n. Así sobre cada uno de dichos intervalos, la gráfica de la función piso es horizontal; para cada x en el intervalo, la altura de la gráfica es n.

Se sigue que la gráfica de la función piso consiste de segmentos de recta horizontales, semejantes a una escalera, como se indica en la figura 11.1.3. Los círculos abiertos en el extremo derecho de cada escalón se utilizan para mostrar que esos puntos *no* están sobre la gráfica.

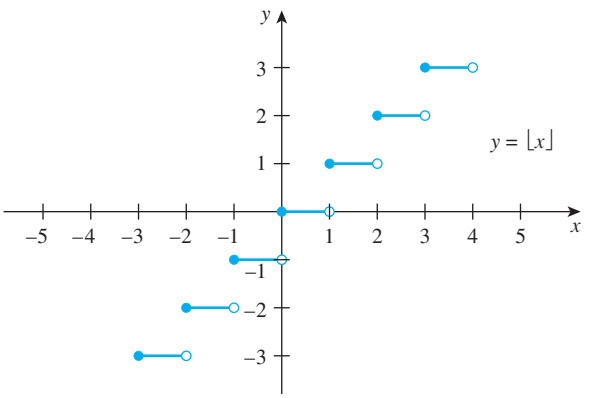
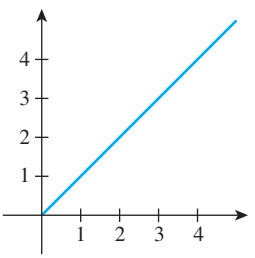


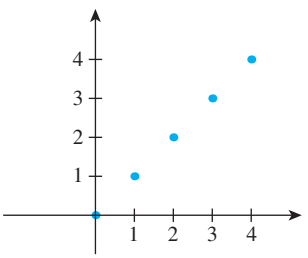
Figura 11.1.3 **Gráfica de la función piso**

Graficando funciones definidas sobre conjuntos de enteros

Muchas funciones valuadas en los reales, empleadas en ciencias computacionales, están definidas sobre conjuntos de enteros y no sobre intervalos de números reales. Supongamos que conoce la gráfica de una función dada por cierta fórmula sobre un intervalo de números reales. Puede obtener la gráfica de la función, definida por la misma fórmula, en los enteros en el intervalo si selecciona en la gráfica sólo aquellos puntos cuya primera coordenada es un entero. Por ejemplo, si f es la función definida por la misma fórmula que la función potencia p_1, pero teniendo como su dominio el conjunto de enteros no-negativos, entonces $f(n) = n$ para todos los enteros no-negativos n. Las gráficas de p_1, reproducidas del ejemplo 11.1.2 y f se muestran a continuación una junto a la otra.



Gráfica de p_1 en donde $p_1(x) = x$ para todos los números reales no-negativos x.

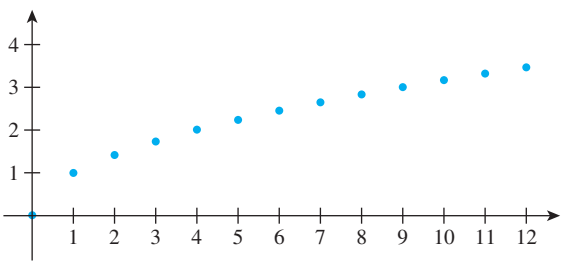


Gráfica de f en donde $f(n) = n$ para todos los enteros no-negativos n.

Ejemplo 11.1.3 Gráfica de una función definida sobre un conjunto de enteros

Considere la versión, valuada en los enteros, de la función potencia $p_{1/2}$. En otras palabras, defina una función g por la fórmula $g(n) = n^{1/2}$ para todos los enteros no-negativos n. Dibuje la gráfica de g.

Solución Observe la gráfica de $p_{1/2}$ indicada en la figura 11.1.2. Dibuje la gráfica de g reproduciendo sólo los puntos sobre la gráfica de $p_{1/2}$ cuyas primeras coordenadas sean enteros. Así, para cada entero no-negativo n, el punto $(n, n^{1/2})$ está sobre la gráfica de g.



Gráfica de g en donde $g(n) = n^{1/2}$ para todos los enteros no-negativos n.

Gráfica de un múltiplo de una función

Un *múltiplo* de una función se obtiene al multiplicar cada valor de la función por un número fijo. Para entender el concepto de la notación O (o la notación O), es útil comprender la relación entre la gráfica de una función y la gráfica de un múltiplo de la función.

• Definición

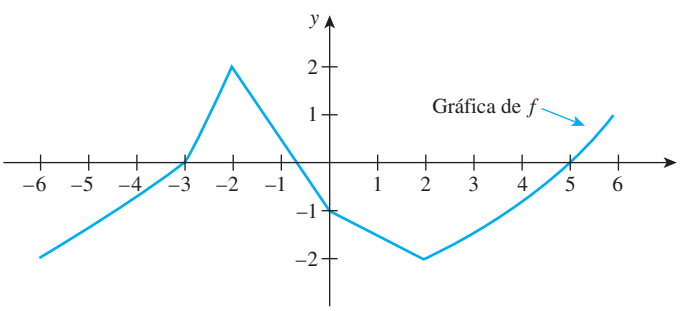
Sea f una función de una variable real valuada en los reales y sea M cualquier número real. La función Mf, llamada el **múltiplo de f por M** o **M veces f**, es la función valuada en los reales con el mismo dominio que f y definida por la regla

$$(Mf)(x) = M \cdot (f(x)) \quad \text{para todas las } x \in \text{dominio de } f.$$

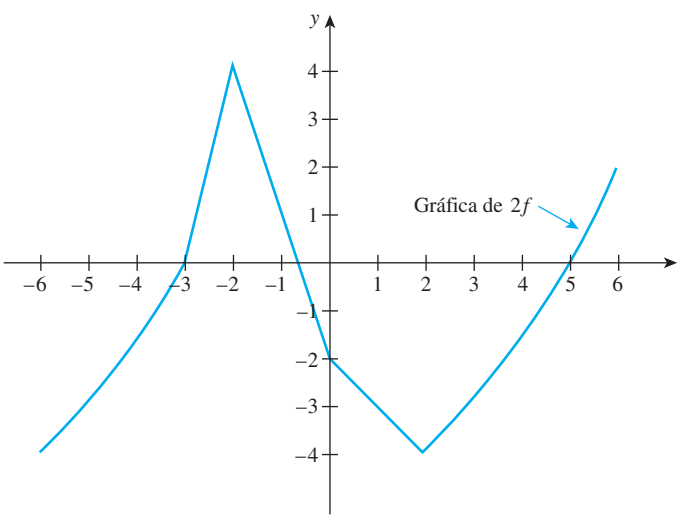
Si se conoce la gráfica de una función, entonces es fácil deducir la gráfica de cualquier múltiplo. Específicamente, si f es una función y M es un número real, la altura de la gráfica de Mf en cualquier número real x es M veces la cantidad $f(x)$. Para trazar la gráfica de Mf a partir de la gráfica de f, dibuje las alturas de $M \cdot (f(x))$ sobre la base del conocimiento de M y la inspección visual de las alturas $f(x)$.

Ejemplo 11.1.4 Gráfica de un múltiplo de una función

Sea f la función cuya gráfica se muestra a continuación. Trace la gráfica de $2f$.



Solución En cada número real x, obtenga la altura de la gráfica de $2f$ midiendo la altura de la gráfica de f en x y multiplicando ese número por 2. El resultado es la siguiente gráfica. Observe que en general las formas de f y $2f$ son muy similares, pero la gráfica de $2f$ está "extendida": las "alturas" son dos veces más altas y los "descensos" son dos veces más bajos.



■

Funciones crecientes y decrecientes

Considere la *función valor absoluto*, A, que se define como sigue:

$$A(x) = |x| = \begin{cases} x & \text{si } x \geq 0 \\ -x & \text{si } x < 0 \end{cases} \quad \text{para todos los números reales } x.$$

Cuando $x \geq 0$, la gráfica de A es la misma que la gráfica de $y = x$, la recta con pendiente 1 que pasa por el origen (0, 0). Para $x < 0$, la gráfica de A es la misma que la gráfica de $y = -x$, que es una recta con pendiente -1 que pasa por (0, 0). (Vea la figura 11.1.4.)

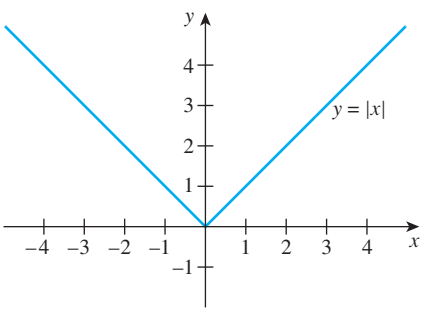


Figura 11.1.4 **Gráfica de la función valor absoluto**

Observe que conforme se traza de izquierda a derecha, la parte de la gráfica a la izquierda del origen, la altura de la gráfica *decrece* continuamente. Por esta razón, se dice que la función valor absoluto es *decreciente* sobre el conjunto de números reales menores que 0. Por otro lado, al trazar de izquierda a derecha la parte de la gráfica a la derecha del origen, la altura de la gráfica se *incrementa* continuamente. Así, se dice que la función valor absoluto es *creciente* sobre el conjunto de números reales mayores que 0.

La altura de la gráfica de una función f en un punto x es $f(x)$, entonces esos conceptos geométricos se trasladan a la siguiente definición analítica.

• Definición

Sea f una función valuada en los reales definida sobre un conjunto de números reales y supongamos que el dominio de f contiene al conjunto S. Decimos que f es **creciente en el conjunto S** si y sólo si,

para todos los números reales x_1 y x_2 en S, si $x_1 < x_2$ entonces $f(x_1) < f(x_2)$.

Decimos que f es **decreciente en el conjunto S** si y sólo si,

para todos los números reales x_1 y x_2 en S, si $x_1 < x_2$ entonces $f(x_1) > f(x_2)$.

Decimos que f es una **función creciente** (o **decreciente**) si y sólo si, f es creciente (o decreciente) en todo su dominio.

La figura 11.1.5 muestra las definiciones analíticas de creciente y decreciente.

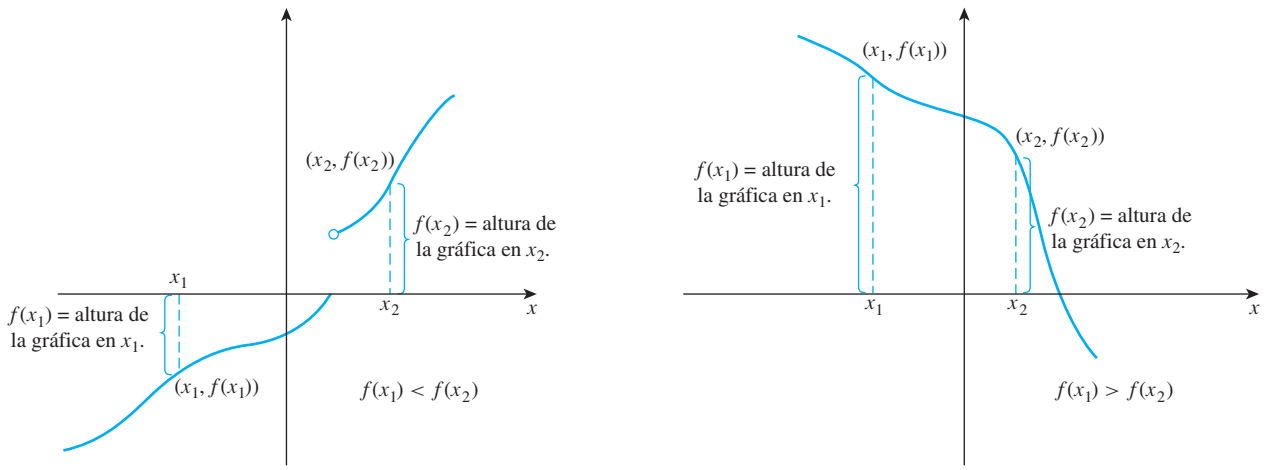


Figura 11.1.5

De las definiciones, se tiene casi inmediatamente, que las funciones creciente y decreciente son inyectivas. En los ejercicios se le pide demostrar esto.

Ejemplo 11.1.5 Un múltiplo positivo de una función creciente es creciente

Suponga que f es una función de una variable real valuada en los reales, la cual es creciente sobre un conjunto S de números reales y suponga que M es cualquier número real positivo. Demuestre que Mf también es creciente sobre S.

Solución Suponga que x_1 y x_2 son elementos particulares de S, arbitrariamente seleccionados, tales que

$$x_1 < x_2.$$

[Debemos demostrar que $(Mf)(x_1) < (Mf)(x_2)$*.]* De $x_1 < x_2$ y el hecho de que f es creciente, se sigue que

$$f(x_1) < f(x_2).$$

Entonces

$$Mf(x_1) < Mf(x_2),$$

porque al multiplicar ambos lados de la desigualdad por un número positivo no se altera la dirección de la desigualdad. Así que, por definición de Mf,

$$(Mf)(x_1) < (Mf)(x_2),$$

y, en consecuencia, Mf es creciente sobre S. ■

También es cierto que un múltiplo positivo de una función decreciente es decreciente, que un múltiplo negativo de una función creciente es decreciente y que un múltiplo negativo de una función decreciente es creciente. Las demostraciones de esos hechos se dejan como ejercicios.

Autoexamen

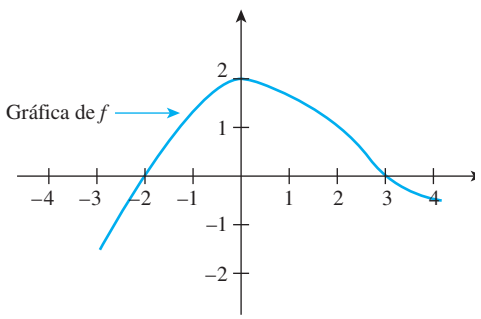
Las respuestas a las preguntas del autoexamen se localizan al final de cada sección.

1. Si f es una función valuada en los reales de una variable real, entonces el dominio y codominio de f son ambos _____.
2. Un punto (x, y) está sobre la gráfica de una función f valuada en los reales de una variable real si y sólo si, _____.

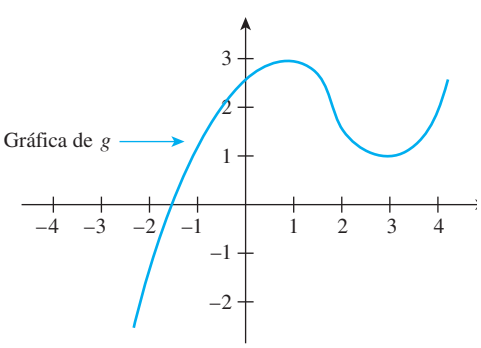
3. Si a es cualquier número real no-negativo, entonces la función potencia con exponente a, p_a, está definida por _____.
4. Dada una función $f: \mathbf{R} \to \mathbf{R}$ y un número real M, la función Mf está definida por _____.
5. Dada una función $f: \mathbf{R} \to \mathbf{R}$, para demostrar que f es creciente, supone que _____ y entonces demuestra que _____.
6. Dada una función $f: \mathbf{R} \to \mathbf{R}$, para demostrar que f es decreciente, supone que _____ y entonces demuestra que _____.

Conjunto de ejercicios 11.1*

1. A continuación se muestra la gráfica de una función f.
   a. ¿$f(0)$ es positiva o negativa?
   b. ¿Para qué valores de x se tiene $f(x) = 0$?
   c. Encuentre valores aproximados para x_1 y x_2 tales que $f(x_1) = f(x_2) = 1$ con $x_1 \neq x_2$.
   d. Obtenga un valor aproximado para x tal que $f(x) = 1.5$.
   e. Conforme x se incrementa de -3 a -1, ¿los valores de f crecen o decrecen?
   f. Conforme x se incrementa de 0 a 4, ¿los valores de f aumentan o disminuyen?



2. A continuación se muestra la gráfica de una función g.
   a. ¿$g(0)$ es positiva o negativa?
   b. Encuentre un valor de x aproximado tal que $g(x) = 0$.
   c. Determine valores aproximados para x_1 y x_2 tales que $g(x_1) = g(x_2) = 1$ con $x_1 \neq x_2$.
   d. Obtenga un valor aproximado para x tal que $g(x) = -2$.
   e. Conforme x se incrementa de -2 a 1, ¿los valores de g aumentan o disminuyen?
   f. Conforme x se incrementa de 1 a 3, ¿los valores de g crecen o decrecen?



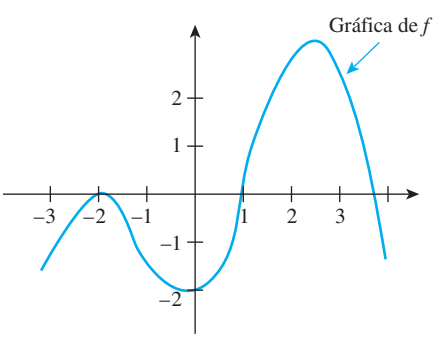
3. Dibuje las gráficas de las funciones potencia $p_{1/3}$ y $p_{1/4}$ sobre el mismo conjunto de ejes. Cuando $0 < x < 1$, ¿cuál es más grande: $x^{1/3}$ o $x^{1/4}$? Cuando $x > 1$, ¿cuál es mayor: $x^{1/3}$ o $x^{1/4}$?
4. Dibuje las gráficas de las funciones potencia p_3 y p_4 sobre el mismo conjunto de ejes. Cuando $0 < x < 1$, ¿cuál es más grande: x^3 o x^4? Cuando $x > 1$, ¿cuál es mayor: x^3 o x^4?
5. Dibuja las gráficas de $y = 2\lfloor x \rfloor$ y $y = \lfloor 2x \rfloor$ para todos los números reales x. ¿Qué puedes concluir de esas gráficas?

Grafique cada una de las funciones definidas en los ejercicios del 6 al 9.

6. $g(x) = \lceil x \rceil$ para todos los números reales x (recuerde que el techo de x, $\lceil x \rceil$, es el mínimo entero que es mayor o igual que x. Es decir, $\lceil x \rceil$ = el único entero n tal que $n - 1 < x \leq n$).
7. $h(x) = \lceil x \rceil - \lfloor x \rfloor$ para todos los números reales x.
8. $F(x) = \lfloor x^{1/2} \rfloor$ para todos los números reales x.
9. $G(x) = x - \lfloor x \rfloor$ para todos los números reales x.

En cada uno de los ejercicios del 10 al 13 se define una función. Grafique cada función.

10. $f(n) = |n|$ para cada entero n.
11. $g(n) = (n/2) + 1$ para cada entero n.
12. $h(n) = \lfloor n/2 \rfloor$ para cada entero $n \geq 0$.
13. $k(n) = \lfloor n^{1/2} \rfloor$ para cada entero $n \geq 0$.
14. A continuación se muestra la gráfica de una función f. Encuentre los intervalos en donde f es creciente y en los que f es decreciente.



15. Demuestre que la función $f: \mathbf{R} \to \mathbf{R}$ definida por la fórmula $f(x) = 2x - 3$ es creciente en el conjunto de todos los números reales.
16. Demuestre que la función $g: \mathbf{R} \to \mathbf{R}$ definida por la fórmula $g(x) = -(x/3) + 1$ es decreciente en todo el conjunto de números reales.

*Para los ejercicios con números o letras azules, las soluciones están dadas en el apéndice B. El símbolo **H** indica que sólo se da una sugerencia o una solución parcial. El símbolo ✶ indica que el ejercicio es más difícil de lo normal.

17. Sea h la función de $\mathbf{R}$ a $\mathbf{R}$ definida por la fórmula $h(x) = x^2$ para todos los números reales x.
    a. Demuestre que h es decreciente sobre el conjunto de todos los números reales menores que cero.
    b. Demuestre que h es creciente sobre el conjunto de todos los números reales mayores que cero.

18. Sea k: $\mathbf{R} \to \mathbf{R}$ la función definida por la fórmula $k(x) = (x-1)/x$ para todos los números reales $x \neq 0$.
    a. Demuestre que k es creciente para todos los números reales $x > 0$.
    b. ¿Es k creciente o decreciente para $x < 0$? Demuestre su respuesta.

19. Demuestre que si una función f: $\mathbf{R} \to \mathbf{R}$ es creciente, entonces f es inyectiva.

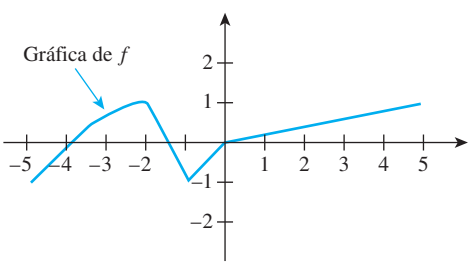
20. Dadas dos funciones f y g valuadas en los reales, con el mismo dominio D, la suma de f y g, que se denota por $f + g$, se define como sigue:

    Para todos los números reales x, $(f + g)(x) = f(x) + g(x)$.

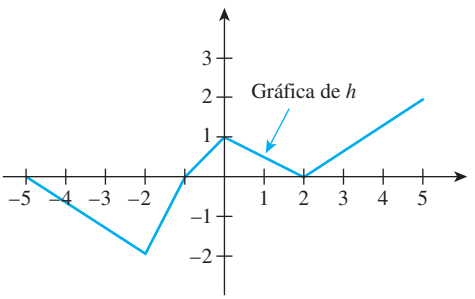
    Demuestre que si f y g son crecientes sobre un conjunto S, entonces $f + g$ también es creciente sobre S.

21. **a.** Sea m cualquier entero positivo y definimos $f(x) = x^m$ para todos los números reales no-negativos x. Use el teorema del binomio para demostrar que f es una función creciente.
    b. Sean m y n enteros positivos arbitrarios y $g(x) = x^{m/n}$ para todos los números reales no-negativos x. Demuestre que g es una función creciente.
    Los resultados de este ejercicio se emplean en los ejercicios de las secciones 11.2 y 11.4.

22. Sea f una función cuya gráfica se muestra abajo. Dibuje la gráfica de $3f$.



23. Sea h la función cuya gráfica se muestra abajo. Dibuje la gráfica de $2h$.



24. Sea f una función valuada en los reales, de una variable real. Demuestre que si f es decreciente sobre un conjunto S y si M es cualquier número real positivo, entonces Mf es decreciente sobre S.

25. Sea f una función de una variable real, valuada en los reales. Demuestre que si f es creciente sobre un conjunto S y si M es cualquier número real negativo, entonces Mf es decreciente sobre S.

26. Sea f una función valuada en los reales, de una variable real. Demuestre que si f es decreciente sobre un conjunto S y si M es cualquier número real negativo, entonces Mf es creciente sobre S.

En los ejercicios 27 y 28 se definen las funciones f y g. En cada caso dibuje las gráficas de f y $2g$ sobre el mismo conjunto de ejes y encuentre un número x_0 tal que $f(x) \leq 2g(x)$ para todos los $x > x_0$. Puede obtener un valor exacto para x_0 resolviendo una ecuación cuadrática o puede deducir un valor aproximado para x_0 empleando una graficadora.

27. $f(x) = x^2 + 10x + 11$ y $g(x) = x^2$ para todos los números reales $x \geq 0$.

28. $f(x) = x^2 + 125x + 254$ y $g(x) = x^2$ para todos los números reales $x \geq 0$.

Respuestas del autoexamen

1. conjuntos de números reales 2. $y = f(x)$ 3. $p_a(x) = x^a$ para todos los números reales x 4. $(Mf)(x) = M \cdot f(x)$ para $x \in \mathbf{R}$ 5. x_1 y x_2 son números reales arbitrarios tales que $x_1 < x_2; f(x_1) < f(x_2)$, 6. x_1 y x_2 son números reales arbitrarios tales que $x_1 < x_2; f(x_1) > f(x_2)$.

11.2 Notaciones O, Ω y Θ

No obstante que esto pueda parecer una paradoja, toda la ciencia exacta está dominada por la idea de aproximación. —Bertrand Russell, 1872-1970.

Frecuentemente ocurre que, de entre varios algoritmos, se podría emplear uno para ejecutar cierto trabajo, pero el tiempo o la capacidad de memoria que requieren varían dramáticamente. Las notaciones O, Ω y Θ dan aproximaciones que hace fácil evaluar

diferencias a gran escala en la eficiencia de un algoritmo, mientras que se ignoran diferencias de un factor constante y diferencias que suceden sólo para pequeños conjuntos de datos de entrada.

La más antigua de las notaciones, la O-notación (o la notación O), fue introducida por el matemático alemán Paul Bachmann en 1894 en un libro sobre teoría analítica de números. Las notaciones Ω (Omega) y Θ (Theta) fueron desarrolladas por Donald Knuth, uno de los pioneros de la ciencia de programación computacional.

La idea de las notaciones es esta. Suponga que f y g son funciones valuadas en los reales de una variable real x.

1. Si, para valores de x suficientemente grandes, los valores de $|f|$ son menores que los de un múltiplo de $|g|$, entonces f es de orden *a lo más* g, o $f(x)$ es $O(g(x))$.
2. Si, para valores de x suficientemente grandes, los valores de $|f|$ son más grandes que los de un múltiplo de $|g|$, entonces f es de orden *al menos* g, o $f(x)$ es $\Omega(g(x))$.
3. Si, para valores de x suficientemente grandes, los valores de $|f|$ están acotados por arriba y por abajo por valores múltiplos de $|g|$, entonces f es de orden g, o $f(x)$ es $\Theta(g(x))$.

Esas relaciones se ilustran en la figura 11.2.1.

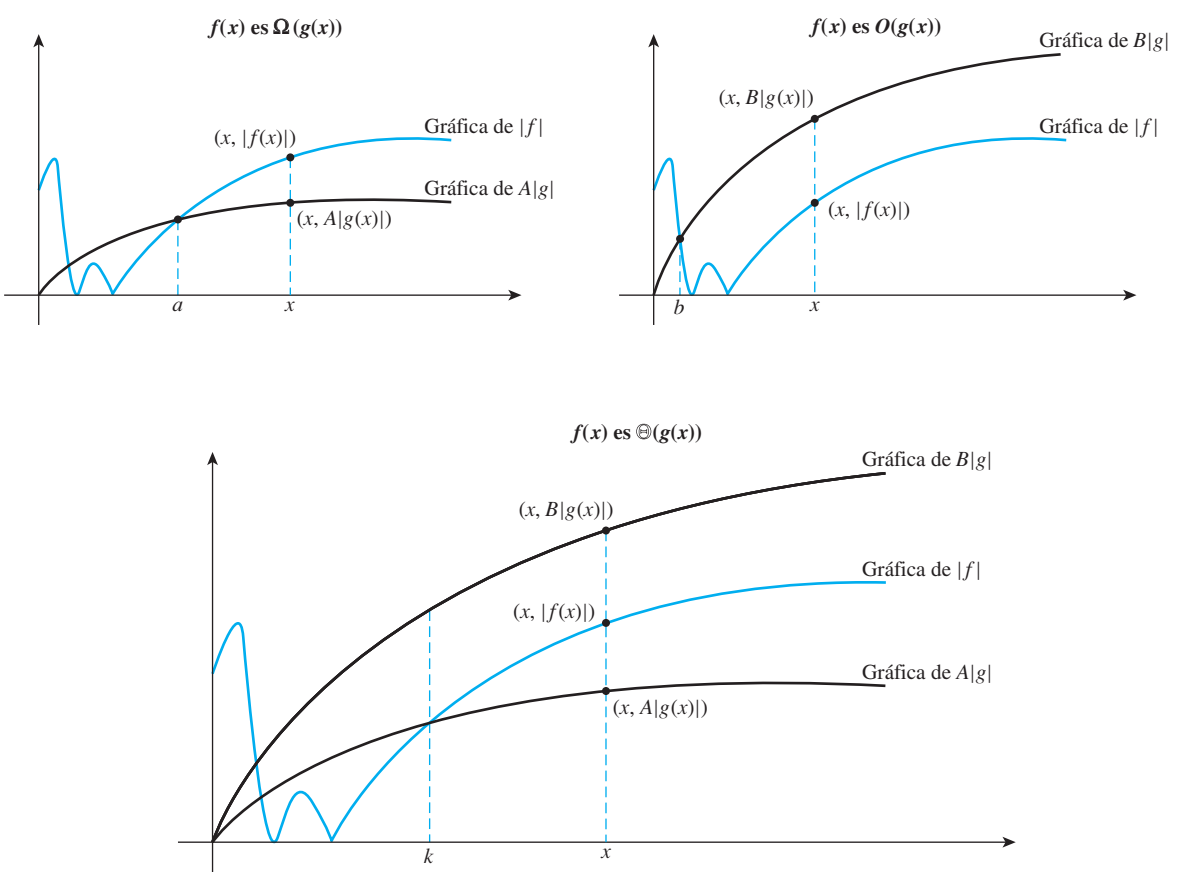


Figura 11.2.1

• Definición

Sean f y g funciones valuadas en los reales sobre el mismo conjunto de números reales no-negativos. Entonces

1. ***f* es de orden al menos *g*,** que se escribe $\boldsymbol{f(x)}$ **es** $\boldsymbol{\Omega(g(x))}$, si y sólo si, existen un número real positivo A y un número real no-negativo a tales que
$$A\,|g(x)| \le |f(x)| \quad \text{para todos los números reales } x > a.$$
2. ***f* es de orden a lo más *g*,** que se escribe $\boldsymbol{f(x)}$ **es** $\boldsymbol{O(g(x))}$, si y sólo si, existen un número real positivo B y un número real no-negativo b tales que
$$|f(x)| \le B\,|g(x)| \quad \text{para todos los números reales } x > b.$$
3. ***f* es de orden *g*,** que se escribe $\boldsymbol{f(x)}$ ***es*** $\boldsymbol{\Theta(g(x))}$, si y sólo si, existen números reales positivos A, B y un número real no-negativo k tal que
$$A\,|g(x)| \le |f(x)| \le B|g(x)| \quad \text{para todos los números reales } x > k.$$

Observación sobre la notación: En la sección 7.1 establecimos que generalmente haríamos una cuidadosa distinción entre la función f y su valor $f(x)$. El uso tradicional de la notación de orden viola esta regla general. Por ejemplo, en el enunciado "$f(x)$ es $\Theta(g(x))$," los símbolos $f(x)$ y $g(x)$ son entendidos a referirse a las funciones f y g definidas por las expresiones $f(x)$ y $g(x)$, respectivamente. Así el enunciado

$$3\sqrt{x} + 4 \text{ es } \Theta(x^{1/2})$$

significa que f es de orden g en donde f y g están definidas por $f(x) = 3\sqrt{x} + 4$ y $g(x) = x^{1/2}$ con algún dominio común (usualmente el conjunto más grande de números reales no-negativos para el cual ambas fórmulas están definidas).

Ejemplo 11.2.1 Traduciendo a la notación Θ

Use la notación Θ para expresar el enunciado

$$10|x^6| \le |17x^6 - 45x^3 + 2x + 8| \le 30|x^6|, \text{ para todos los números reales } x > 2.$$

Solución Sean $A = 10$, $B = 30$ y $k = 2$. Entonces el enunciado se traduce a

$$A|x^6| \le |17x^6 - 45\,x^3 + 2x + 8| \le B|x^6|, \text{ para todos los números reales } x > k.$$

Así, por definición de la notación Θ,

$$17x^6 - 45x^3 + 2x + 8 \text{ is } \Theta(x^6).$$

■

Ejemplo 11.2.2 Traduciendo a las notaciones O y Ω

a. Use las notaciones O y Ω para expresar los enunciados

(i) $15\,|\sqrt{x}| \le \left|\dfrac{15\sqrt{x}(2x+9)}{x+1}\right|$ para todos los números reales $x > 0$.

(ii) $\left|\dfrac{15\sqrt{x}(2x+9)}{x+1}\right| \le 45\,|\sqrt{x}|$ para todos los números reales $x > 7$.

b. Justifique el enunciado: $\dfrac{15\sqrt{x}(2x+9)}{x+1}$ es $\Theta\left(\sqrt{x}\right)$.

Solución

a. (i) Sean $A = 15$ y $a = 0$. El enunciado dado se traduce a

$$A|\sqrt{x}| \leq \left|\frac{15\sqrt{x}(2x+9)}{x+1}\right| \text{ para todos los números reales } x > a.$$

Así por definición de la notación Ω,

$$\frac{15\sqrt{x}(2x+9)}{x+1} \text{ es } \Omega(\sqrt{x}).$$

(ii) Sean $B = 45$ y $b = 7$. El enunciado dado se traduce a

$$\left|\frac{15\sqrt{x}(2x+9)}{x+1}\right| \leq B|\sqrt{x}| \text{ para todos los números reales } x > b$$

Así, por definición de la notación O,

$$\frac{15\sqrt{x}(2x+9)}{x+1} \text{ es } O(\sqrt{x}).$$

b. Sean $A = 15$, $B = 45$ y k sea el mayor de 0 y 7. Entonces cuando $x > k$, se cumplen ambas desigualdades en a(i) y en a(ii), por tanto

$$A|\sqrt{x}| \leq \left|\frac{15\sqrt{x}(2x+9)}{x+1}\right| \leq B|\sqrt{x}| \quad \text{para todos los números reales } x > k.$$

Entonces por definición de la notación Θ, $\dfrac{15\sqrt{x}(2x+9)}{x+1}$ es $\Theta(\sqrt{x})$. ■

El inciso *b*) del ejemplo 11.2.2 muestra el hecho de que si sabe que f es de orden a lo más g y que f es de orden a lo menos g, entonces puede tomar k como el mayor de los números a y b como se prometió en las definiciones de las notaciones omega y O y así concluir que f es de orden g. Inversamente, si f es de orden g, entonces a y b pueden tomarse como el número k prometido en la definición de la notación theta, para así demostrar que f es del orden a lo más g y que f es del orden a lo menos g. Esos resultados y una propiedad transitiva de orden, se establecen formalmente en el siguiente teorema. Útiles propiedades adicionales de las notaciones se incluyen en los ejercicios al final de cada sección.

Teorema 11.2.1 Propiedades de las notaciones O, Ω y Θ

Sean f y g funciones valuadas en los reales definidas sobre el mismo conjunto de números reales no-negativos.

1. $f(x)$ es $\Omega(g(x))$ y $f(x)$ es $O(g(x))$ si y sólo si, $f(x)$ es $\Theta(g(x))$.
2. $f(x)$ es $\Omega(g(x))$ si y sólo si, $g(x)$ es $O(f(x))$.
3. Si $f(x)$ es $O(g(x))$ y $g(x)$ es $O(h(x))$, entonces $f(x)$ es $O(h(x))$.

Demostración:

1. La demostración de esta propiedad fue dada antes de enunciar el teorema.
2. Primero demostramos que si $f(x)$ es $\Omega(g(x))$, entonces $g(x)$ es $O(f(x))$. Así, supongamos que $f(x)$ es $\Omega(g(x))$. Por definición de la notación Ω, existe un número real positivo A y un número real no-negativo a tales que

$$A|g(x)| \leq |f(x)| \quad \text{para todos los números reales } x > a.$$

Dividiendo ambos lados entre A se obtiene

$$|g(x)| \leq \frac{1}{A}|f(x)| \quad \text{para todos los números reales } x > a.$$

Sean $B = 1/A$ y $b = a$. Entonces B es un número real positivo y b es un número real no-negativo y

$$|g(x)| \leq B\,|f(x)| \text{ para todos los números reales } x > b,$$

y así $g(x)$ es $O(f(x))$ por definición de la notación O.

La demostración de que si $g(x)$ es $O(f(x))$ entonces $f(x)$ es $\Omega(g(x))$, se deja como ejercicio 10 al final de la sección.

3. Suponga que $f(x)$ es $O(g(x))$ y $g(x)$ es $O(h(x))$. Por definición de la notación O, existen números reales positivos B_1 y B_2 y números reales no-negativos b_1 y b_2 tales que

$$|f(x)| \leq B_1|g(x)| \text{ para todos los números reales } x > b_1,$$

y

$$|g(x)| \leq B_2|h(x)| \text{ para todos los números reales } x > b_2.$$

Sean $B = B_1\,B_2$, y sea b el mayor de b_1 y b_2. Entonces si $x > b$,

$$|f(x)| \leq B_1|g(x)| \leq B_1(B_2\,|h(x)|) \leq B\,|h(x)|.$$

Así, por definición de la notación O, $f(x)$ es $O(h(x))$

Órdenes de funciones potencia

Observe que si $1 < x$,

entonces $x < x^2$ multiplicando ambos lados por x (que es positivo)

y así $x^2 < x^3$ multiplicando otra vez por x.

Por tanto, si $1 < x$, entonces $1 < x < x^2 < x^3$.

La siguiente generalización de este resultado se desarrolla en los ejercicios 15 y 50 al final de esta sección.

Para cualesquiera números racionales r y s,

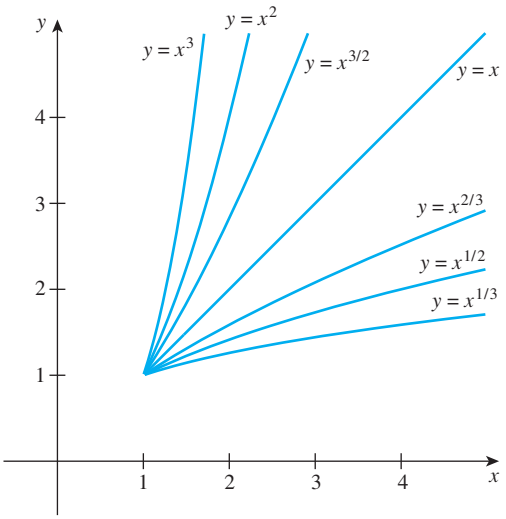
$$\text{si } x > 1 \text{ y } r < s, \text{ entonces } x^r < x^s. \qquad 11.2.1$$

La propiedad (11.2.1) tiene la siguiente consecuencia para los órdenes.

Para cualesquiera números racionales r y s,

$$\text{si } r < s, \text{ entonces } x^r \text{ es } O(x^s). \qquad 11.2.2$$

En la figura 11.2.2, de la siguiente página, se muestra geométricamente la relación entre las gráficas de varias funciones potencia positivas de x para $x \geq 1$.



Si $r < s$, la gráfica de $y = x^r$ se encuentra abajo de la gráfica de $y = x^s$ para $x > 1$.

Figura 11.2.2 **Gráficas de potencias de x para $x \geq 1$**

Órdenes de funciones polinomiales

El siguiente ejemplo muestra cómo emplear la propiedad (11.2.1) para deducir una desigualdad polinomial.

Ejemplo 11.2.3 Una desigualdad polinomial

Demuestre que para cualquier número real x,

$$\text{si } x > 1, \quad \text{entonces} \quad 3x^3 + 2x + 7 \leq 12x^3.$$

Solución Suponga que x es un número real y $x > 1$. Entonces por la propiedad (11.2.1),

$$x < x^3 \quad \text{y} \quad 1 < x^3.$$

Multiplique la desigualdad de la izquierda por 2 y la desigualdad de la derecha por 7 para obtener

$$2x < 2x^3 \quad \text{y} \quad 7 < 7x^3.$$

Ahora sume $3x^3 \leq 3x^3$, $2x < 2x^3$ y $7 < 7x^3$ para obtener

$$3x^3 + 2x + 7 \leq 3x^3 + 2x^3 + 7\,x^3 = 12x^3. \qquad \blacksquare$$

El método del ejemplo 11.2.3 se utiliza en el próximo ejemplo (más compactamente) para demostrar que una función polinomial tiene un cierto orden.

Ejemplo 11.2.4 Uso de las definiciones para demostrar que una función polinomial con coeficientes positivos tiene un cierto orden

Use las definiciones de omega mayúscula, O mayúscula y Theta mayúscula para demostrar que $2x^4 + 3x^3 + 5$ es $\Theta(x^4)$.

Solución Defina las funciones f y g como sigue. Para todos los números reales no-negativos x,

$$f(x) = 2x^4 + 3x^3 + 5 \text{ y}$$
$$g(x) = x^4.$$

Observe que para todos los números reales $x > 0$,

$$2x^4 \quad \leq \quad 2x^4 + 3x^3 + 5, \qquad \text{porque } 3x^3 + 5 > 0 \text{ para } x > 0.$$

y así

$$2\,|x^4| \;\le\; |2x^4 + 3x^3 + 5|$$

porque son positivos todos los términos en ambos lados de la desigualdad.

Sean $A = 2$ y $a = 0$. Entonces

$$A\,|x^4| \le |2x^4 + 3x^3 + 5| \quad \text{para toda } x > a,$$

por tanto, por definición de notación Ω, $2x^4 + 3x^3 + 5$ es $\Omega(x^4)$.

También para $x > 1$,

$$2x^4 + 3x^3 + 5 \;\le\; 2x^4 + 3x^4 + 5x^4$$

porque por (11.2.1), $x^3 < x^4$ y $1 < x^4$ y así $3x^3 < 3x^4$ y $5 < 5x^4$,

$$\Rightarrow \quad 2x^4 + 3x^3 + 5 \;\le\; 10x^4$$

porque $2 + 3 + 5 = 10$,

$$\Rightarrow \quad |2x^4 + 3x^3 + 5| \;\le\; 10|x^4|$$

porque todos los términos en ambos lados de la desigualdad son positivos.

Nota Cuando se coloca la flecha de implicación, ⇒, al inicio de un renglón, significa que cada número x que hace válida la desigualdad del renglón anterior, también hace verdadera la desigualdad del renglón dado.

Sean $B = 10$ y $b = 1$. Entonces

$$|2x^4 + 3x^3 + 5| \le B|x^4| \text{ para todo } x > b,$$

y así, por definición de la notación O, $2x^4 + 3x^3 + 5$ es $O(x^4)$.

Como $2x^4 + 3x^3 + 5$ es $\Omega(x^4)$ y $O(x^4)$, entonces por el teorema 11.2.1, también es $\Theta(x^4)$. ■

La técnica utilizada en el ejemplo 11.2.4 se puede generalizar para demostrar que cualquier polinomio con coeficientes no-negativos es la omega mayúscula de su término a la más alta potencia. Los dos ejemplos siguientes prueban que este resultado puede ser válido para un polinomio tanto para coeficientes negativos como positivos.

Ejemplo 11.2.5 Una aproximación *O* para un polinomio con algunos coeficientes negativos

a. Use la definición de la notación O para demostrar que $3x^3 - 1\,000x - 200$ es $O(x^3)$.

b. Demuestre que $3x^3 - 1\,000x - 200$ es $O(x^s)$ para todos los enteros $s > 3$.

Solución

a. De acuerdo a la desigualdad del triángulo para el valor absoluto (teorema 4.4.6),

$\lvert a + b\rvert \le \lvert a\rvert + \lvert b\rvert$ para todos los números reales a y b.

desigualdad del triángulo.

Si se sustituye $-b$ en lugar de b, el resultado es

$$|a - b| = |a + (-b)| \;\le\; |a| + |-b| = |a| + |b|, \text{ o}$$

$$|a - b| \;\le\; |a| + |b|.$$

Se tiene que para todos los números reales $x > 1$,

$$|3x^3 - 1000x - 200| \;\le\; |3x^3| + |1000x| + |200|$$

$$\Rightarrow \quad |3x^3 - 1000x - 200| \;\le\; 3x^3 + 1000x + 200$$

porque todos los términos en el lado derecho de la desigualdad son positivos cuando $x > 1$,

$$\Rightarrow \quad |3x^3 - 1000x - 200| \;\le\; 3x^3 + 1000x^3 + 200x^3$$

porque debido a (11.2.1), $x < x^3$ y $1 < x^3$ y así $1\,000x < 1\,000x^3$ y $200 < 200x^3$,

$$\Rightarrow \quad |3x^3 - 1000x - 200| \;\le\; 1203x^3$$

porque $3 + 1\,000 + 200 = 1\,203$,

$$\Rightarrow \quad |3x^3 - 1000x - 200| \;\le\; 1203|x^3|$$

porque x^3 es positivo.

Sean $b = 1$ y $B = 1\,203$. Entonces

$$|3x^3 - 1\,000x - 200| \leq B|x^3| \text{ para todos los números } x > b.$$

Así, por definición de la notación O, $3x^3 - 1\,000x - 200$ es $O(x^3)$.

b. Suponga que s es un entero con $s > 3$. Por la propiedad (11.2.1), $x^3 < x^s$ para todos los números reales $x > 1$. Así $B\,|x^3| < B\,|x^s|$ para todos los números reales $x > b$ (porque $b = 1$) y entonces por el inciso a),

$$|3x^3 - 1\,000x - 200| \leq B|x^s| \quad \text{para todos los números reales } x > b.$$

Por tanto, por definición de la notación O, $3x^3 - 1\,000x - 200$ es $O(x^s)$ para todos los enteros $s > 3$. ■

Ejemplo 11.2.6 Una aproximación omega mayúscula para un polinomio con algunos coeficientes negativos

a. Use la definición de la notación Ω para demostrar que $3x^3 - 1\,000x - 200$ es $\Omega(x^3)$.

b. Demuestre que $3x^3 - 1\,000x - 200$ es $\Omega(x^r)$ para todos los enteros $r < 3$.

Solución

a. Para demostrar que $3x^3 - 1\,000x - 200$ es $\Omega(x^3)$, necesita encontrar números a y A tales que $A|x^3| \leq |3x^3 - 1\,000x - 200|$ para todos los números reales $x > a$. El ejercicio 27, al final de la sección, muestra que el siguiente procedimiento para elegir a siempre producirá una A que dará el resultado deseado.

Elija a como sigue: Sume los valores absolutos de los coeficientes de los términos de más bajo orden de $3x^3 - 1\,000x - 200$, divida entre el valor absoluto del término de más alta potencia y multiplique el resultado por 2. El resultado es $a = 2(1\,000 + 200)/3$, el cual es igual a 800. Si sigue los pasos que se muestran a continuación verá que cuando a se elige de esta manera, A se puede tomar como la mitad del valor absoluto de la más alta potencia del polinomio. Entonces, suponga que $x > a$. Por tanto

$$x > 800$$

$$\Rightarrow \quad x > 2\left(\frac{1\,000 + 200}{3}\right) \qquad \text{porque } 2(1\,000 + 200)/3 = 800,$$

$$\Rightarrow \quad x > \frac{2 \cdot 1\,000}{3} + \frac{2 \cdot 200}{3} \qquad \text{por las reglas para sumar fracciones,}$$

$$\Rightarrow \quad x > \frac{2 \cdot 1\,000}{3} \cdot \frac{1}{x} + \frac{2 \cdot 200}{3} \cdot \frac{1}{x^2} \qquad \text{porque } x > 800 \text{ y así por (11.2.1), } 1 > \frac{1}{x} \text{ y } 1 > \frac{1}{x^2}$$

$$\Rightarrow \quad \frac{3}{2}x^3 > 1\,000x + 200 \qquad \text{multiplicando ambos lados por } \frac{3}{2}x^2$$

$$\Rightarrow \quad 3x^3 - \frac{3}{2}x^3 > 1\,000x + 200 \qquad \text{porque } \tfrac{3}{2} = 3 - \tfrac{3}{2}$$

$$\Rightarrow \quad 3x^3 - 1\,000x - 200 > \frac{3}{2}x^3 \qquad \text{sumando } \tfrac{3}{2}x^3 - 1\,000x - 200 \text{ en ambos lados,}$$

$$\Rightarrow \quad |3x^3 - 1\,000x - 200| > \frac{3}{2}|x^3| \qquad \text{ya que, cuando } x > 800, \text{ las expresiones en ambos lados de la desigualdad son positivas.}$$

Sean $A = \frac{3}{2}$ y $a = 800$. Entonces

$$A|x^3| \leq |3x^3 - 1\,000x - 200|, \quad \text{para todos los números reales } x > a.$$

Así, por definición de notación Ω, $3x^3 - 1\,000x - 200$ es $\Omega(x^3)$.

b. Suponga que r es un entero con $r < 3$. Por la propiedad (11.2.1), $x^r < x^3$ para todos los números reales $x > 1$. Entonces, como $a = 800 > 1$, $A|x^r| < A|x^3|$ para todos los números reales $x > a$. Así, por el inciso *a*),

$$A|x^r| \leq |3x^3 - 1\,000x - 200|, \quad \text{para todos los números reales } x > a.$$

En consecuencia, por definición de la notación Ω, $3x^3 - 1\,000x - 200$ es $\Omega(x^r)$ para todos los enteros $r < 3$. ■

Por el teorema 11.2.1, se sigue inmediatamente de los ejemplos 11.2.5*a*) y 11.2.6*a*), que $3x^3 - 1\,000x - 200$ es $\Theta(x^3)$ y que las técnicas empleadas en los ejemplos se pueden generalizar para demostrar que cada polinomio es Θ de la función potencia de su más alta potencia. Además, los resultados del inciso *b*) de los ejemplos, $3x^3 - 1\,000x - 200$, también es mayúscula $O(x^s)$ para cada entero s mayor que 3 y que es mayúscula $\Omega(x^r)$ para cada entero r menor que 3, también se puede generalizar todos los polinomios. Estos hechos se resumen en el próximo teorema.

Teorema 11.2.2 de órdenes de polinomios

Suponga que $a_0, a_1, a_2, \ldots, a_n$ son números reales con $a_n \neq 0$.

1. $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ es $O(x^s)$ para todos los enteros $s \geq n$.
2. $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ es $\Omega(x^r)$ para todos los enteros $r \leq n$.
3. $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ es $\Theta(x^n)$.

El teorema 11.2.2 se puede demostrar fácilmente utilizando cálculo. Sin embargo, como lo sugieren los ejemplos 11.2.5 y 11.2.6, también se puede deducir sin cálculo. (Vea los ejercicios 26, 27 y 49 al final de esta sección.)

Ejemplo 11.2.7 Cálculo de órdenes de polinomios utilizando el teorema de órdenes de polinomios

Use el teorema de órdenes de polinomios para encontrar órdenes para las funciones dadas por las siguientes fórmulas.

a. $f(x) = 7x^5 + 5x^3 - x + 4$, para todos los números reales x.

b. $g(x) = \dfrac{(x-1)(x+1)}{4}$, para todos los números reales x.

Solución

a. Por aplicación directa del teorema sobre órdenes de polinomios, $7x^5 + 5x^3 - x + 4$ es $\Theta(x^5)$.

b. $$g(x) = \frac{(x-1)(x+1)}{4}$$
$$= \frac{1}{4}(x^2 - 1)$$
$$= \frac{1}{4}x^2 - \frac{1}{4} \quad \text{por álgebra}$$

Así $g(x)$ es $\Theta(x^2)$ por el teorema de órdenes de polinomios. ■

Ejemplo 11.2.8 Demostración de que dos funciones potencia tengan órdenes diferentes

Demuestre que x^2 no es $O(x)$ y deduzca que x^2 no es $\Theta(x)$.

Solución *[Proceda por contradicción.]* Suponga que x^2 es $O(x)$. *[Obtenga una contradicción.]* Por la suposición de que x^2 es $O(x)$, existen un número real positivo B y un número real no-negativo b tales que

$$|x^2| \leq B\,|x| \quad \text{para todos los números reales } x > b. \tag{$*$}$$

Sea x un número real positivo mayor que B y b. Entonces

$$x \cdot x > B \cdot x \quad \text{multiplicando ambos lados de } x > B \text{ por } x \text{ que es positivo}$$

$$\Rightarrow |x^2| > B|x| \quad \text{porque } b \text{ es positivo.}$$

Así hay un número real $x > b$ tal que

$$|x^2| > B|x|.$$

Esto contradice $(*)$. Entonces la suposición es falsa y así x^2 no es $O(x)$.

Por el teorema 11.2.1, si x^2 es $\Theta(x)$, entonces x^2 es $O(x)$. Pero x^2 no es $O(x)$ y así x^2 no es $\Theta(x)$. ■

La técnica empleada en el ejemplo 11.2.8 se puede ampliar y generalizar para demostrar que cualquier función polinomial en x de grado n, *no* es O ni Θ mayúsculas de la función de la m-ésima potencia x^m para cualquier $m < n$. (Vea el ejercicio 53 al final de esta sección.)

Teorema 11.2.3 Limitación de órdenes de funciones polinomiales

Sean n un entero positivo y $a_0, a_1, a_2, \ldots, a_n$ números reales con $a_n \neq 0$. Si m es cualquier entero con $m < n$, entonces

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \text{ no es } O(x^m)$$

y

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \text{ no es } \Theta(x^m).$$

De los teoremas 11.2.2 y 11.2.3, se tiene que las funciones potencia enteras son convenientes estándares de comparación entre funciones polinomiales generales porque cada función polinomial tiene el mismo orden que alguna función potencia entera y ninguna función potencia tiene el mismo orden que cualquier otra.

Órdenes para funciones de variables enteras

Es tradicional usar el símbolo x para denotar un número real variable, mientras que n es empleado para representar un entero variable. Así, dado un enunciado de la forma

$$f(n) \quad \text{es} \quad \Theta(g(n)),$$

suponemos que f y g son funciones definidas sobre conjuntos de *enteros*. Si es verdad que

$$f(x) \quad \text{es} \quad \Theta(g(x)),$$

en donde f y g son funciones definidas para *números reales*, entonces es ciertamente verdadero que $f(n)$ es $\Theta(g(n))$. La razón es que si $f(x)$ es $\Theta(g(x))$, entonces una desigualdad

$$A|g(x)| \leq |f(x)| \leq B|g(x)|$$

es válida para todos los números reales $x > k$. Así, en particular, la desigualdad

$$A|g(n)| \leq |f(n)| \leq B|g(n)|$$

vale para todos los enteros $n > k$.

Ejemplo 11.2.9 Un orden para la suma de los primeros *n* enteros

Sumas de la forma $1 + 2 + 3 + \cdots + n$ se presentan en el análisis de algoritmos computacionales tales como tipos de selección. Demuestre que para un entero positivo variable n,

$$1 + 2 + 3 + \cdots + n \text{ es } \Theta(n^2).$$

Solución Por la fórmula para la suma de los primeros n enteros (ver teorema 5.2.2), para todos los enteros n positivos,

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}.$$

Pero

$$\frac{n(n+1)}{2} = \frac{1}{2}n^2 + \frac{1}{2}n \qquad \text{por álgebra básica.}$$

Y, por el teorema de órdenes polinomiales,

$$\frac{1}{2}n^2 + \frac{1}{2}n \text{ es } \Theta(n^2).$$

Así

$$1 + 2 + 3 + \cdots + n \text{ es } \Theta(n^2). \qquad \blacksquare$$

Extensión a funciones compuestas de funciones potencia racionales

Considere una función de la forma

$$\frac{(x^{3/2}+3)(x-2)^2}{x^{1/2}(2x^{1/2}+1)} = \frac{x^{7/2} - 4x^{5/2} + 4x^{3/2} + 3x^2 - 12x + 12}{2x + x^{1/2}}.$$

Cuando el numerador y denominador se expanden, cada uno de ellos es una suma de términos de la forma ax^r, en donde a es un número real y r es un número racional positivo. El grado de dicha suma puede tomarse como el mayor exponente de x que ocurre en unos de sus términos. Si la diferencia entre el grado del numerador y el del denominador se llama el grado de la función y se denota por d, entonces se puede demostrar que $f(x)$ es $\Theta(x^d)$, que $f(x)$ es $O(x^c)$ para todos los números reales $c > d$ y que $f(x)$ no es $O(x^c)$ para cualquier número real $c < d$. Para el ejemplo anterior, esto significa que $d = 7/2 - 1 = 5/2$ y que

$$\frac{(x^{3/2}+3)(x-2)^2}{x^{1/2}(2x^{1/2}+1)} \text{ es } \Theta(x^{5/2}),$$

$$\frac{(x^{3/2}+3)(x-2)^2}{x^{1/2}(2x^{1/2}+1)} \text{ es } O(x^c) \quad \text{para todos los números reales } c > 5/2,$$

y

$$\frac{(x^{3/2}+3)(x-2)^2}{x^{1/2}(2x^{1/2}+1)} \quad \text{no es } O(x^c) \quad \text{para cualquier número real } c < 5/2.$$

El resultado general lo establecemos como el teorema 11.2.4

Teorema 11.2.4 Órdenes de funciones compuestas de funciones potencia racionales

Sean m y n enteros positivos y sean $r_0, r_1, r_2, \ldots, r_n$ y $s_0, s_1, s_2, \ldots, s_m$ números racionales no-negativos con $r_0 < r_1 < r_2 < \cdots < r_n$ y $s_0 < s_1 < s_2 \cdots < s_m$. Sean $a_0, a_1, a_2, \ldots, a_n$ y $b_0, b_1, b_2, \ldots, b_m$ números reales con $a_n \neq 0$ y $b_m \neq 0$. Entonces

$$\frac{a_n x^{r_n} + a_{n-1}x^{r_{n-1}} + \cdots + a_1 x^{r_1} + a_0 x^{r_0}}{b_m x^{s_m} + b_{m-1}x^{s_{m-1}} + \cdots + b_1 x^{s_1} + b_0 x^{s_0}} \text{ es } \Theta(x^{r_n - s_m}).$$

$$\frac{a_n x^{r_n} + a_{n-1}x^{r_{n-1}} + \cdots + a_1 x^{r_1} + a_0 x^{r_0}}{b_m x^{s_m} + b_{m-1}x^{s_{m-1}} + \cdots + b_1 x^{s_1} + b_0 x^{s_0}} \text{ es } O(x^c) \quad \text{para todos los números reales } c > r_n - s_m.$$

$$\frac{a_n x^{r_n} + a_{n-1}x^{r_{n-1}} + \cdots + a_1 x^{r_1} + a_0 x^{r_0}}{b_m x^{s_m} + b_{m-1}x^{s_{m-1}} + \cdots + b_1 x^{s_1} + b_0 x^{s_0}} \text{ no es } O(x^c) \quad \text{para todos los números reales } c < r_n - s_m.$$

Autoexamen

1. Una frase de la forma "$A|g(x)| \leq |f(x)|$ para toda $x > a$" se traduce en la notación Ω como _____.
2. Una frase de la forma "$|f(x)| \leq B|g(x)|$ para toda $x > b$" se traduce en la notación O como _____.
3. Una frase de la forma "$A|g(x)| \leq |f(x)| \leq B|g(x)|$ para toda $x > k$" se traduce en la notación Θ como _____.
4. Cuando $x > 1$, x^2 _____ x y x^5 _____ x^2.
5. De acuerdo al teorema de órdenes de polinomios, si $p(x)$ es un polinomio en x, entonces $p(x)$ es $\Theta(x^n)$, en donde n es _____.
6. Si n es un entero positivo, entonces $1 + 2 + 3 + \cdots + n$ tiene orden _____.

Conjunto de ejercicios 11.2

1. La siguiente es una definición formal para la notación Ω, escrita empleando cuantificadores y variables: $f(x)$ es $\Omega(g(x))$ si y sólo si, $\exists$ números reales positivos a y A tales que para todo $\forall x > a$,

$$A\,|g(x)| \leq |f(x)|.$$

a. Utilizando los símbolos $\forall$ y $\exists$ escriba la negación formal de la definición.
b. Sin emplear los símbolos $\forall$ y $\exists$, establezca la negación, pero menos formalmente.

2. La siguiente es una definición formal para la notación O, escrita utilizando cuantificadores y variables: $f(x)$ es $O(g(x))$ si y sólo si, $\exists$ números reales positivos b y B tales que $\forall\, x > b$,

$$|f(x)| \leq B\,|g(x)|.$$

a. Utilizando los símbolos $\forall$ y $\exists$, escriba la negación formal de la definición.
b. Escriba la negación, pero menos formalmente, sin emplear los símbolos $\forall$ y $\exists$.

3. La siguiente es una definición formal para la notación Θ, escrita utilizando cuantificadores y variables: $f(x)$ es $\Theta(g(x))$ si y sólo si, $\exists$ números reales positivos k, A y B tales que $\forall\, x > k$,

$$A\,|g(x)| \leq |f(x)| \leq B\,|g(x)|.$$

a. Escriba la negación formal de la definición empleando los símbolos $\forall$ y $\exists$.
b. Sin usar los símbolos $\forall$ y $\exists$, redacte la negación, pero con menos formalidad.

En los ejercicios del 4 al 9, exprese cada enunciado empleando las notaciones Ω, O o Θ.

4. $|5x^8 - 9x^7 + 2x^5 + 3x - 1| \leq 6|x^8|$ para todos los números reales $x > 3$. (Use la notación O.)

5. $|x| \leq \left|\dfrac{(x^2 - 1)(12x + 25)}{3x^2 + 4}\right| \leq 6|x|$ para todos los números reales $x > 2$.

6. $|x^{7/2}| \leq \left|\dfrac{(x^2 - 7)^2(10x^{1/2} + 3)}{x + 1}\right|$ para todos los números reales $x > 4$. (Use la notación Ω.)

7. $|3x^6 + 5x^4 - x^3| \leq 9|x^6|$ para todos los números reales $x > 1$. (Use la notación O.)

8. $\frac{1}{2}x^4 \leq |x^4 - 50x^3 + 1|$ para todos los números reales $x > 101$. (Use la notación Ω.)

9. $\frac{1}{2}x^2 \leq |3x^2 - 80x + 7| \leq 3|x^2|$ para todos los números reales $x > 25$.

En cada ejercicio del 10 al 14 suponga que f y g son funciones valuadas en los reales definidas sobre el mismo conjunto de números reales no-negativos.

10. Demuestre que si $g(x)$ es $O(f(x))$, entonces $f(x)$ es $\Omega(g(x))$.

11. Demuestre que si $f(x)$ es $O(g(x))$ y c es cualquier número real diferente de cero, entonces $cf(x)$ es $O(g(x))$.

12. Demuestre que si $f(x)$ es $O(h(x))$ y $g(x)$ es $O(k(x))$, entonces $f(x) + g(x)$ es $O(G(x))$, en donde, para cada x en el dominio, $G(x) = \text{máx}(|h(x)|, |k(x)|)$.

13. Demuestre que $f(x)$ es $\Theta(f(x))$.

H 14. Demuestre que si $f(x)$ es $O(h(x))$ y $g(x)$ es $O(k(x))$, entonces $f(x)g(x)$ es $O(h(x)k(x))$.

15. a. Use inducción matemática para demostrar que si x es cualquier número real $x > 1$, entonces $x^n > 1$ para todos los enteros $n \geq 1$.

H b. Demuestre que si x es cualquier número real con $x > 1$, entonces $x^m < x^n$ para cualesquiera enteros m y n con $m < n$.

16. a. Demuestre que para cualquier número real x,

$$\text{si } x > 1 \text{ entonces } |x^2| \leq |2x^2 + 15x + 4|.$$

b. Demuestre que para cualquier número real x,

$$\text{si } x > 1 \text{ entonces } |2x^2 + 15x + 4| \leq 21|x^2|.$$

c. Use las notaciones Ω y O para expresar los resultados de los incisos *a*) y *b*).

d. ¿Qué puede deducir acerca del orden de $2x^2 + 15x + 4$?

17. a. Demuestre que para cualquier número real x,

$$\text{si } x > 1 \text{ entonces } |x^4| \leq |23x^4 + 8x^2 + 4x|.$$

b. Demuestre que para cualquier número real x,

$$\text{si } x > 1 \text{ entonces } |23x^4 + 8x^2 + 4x| \leq 35|x^4|.$$

c. Use las notaciones Ω y O para expresar los resultados de los incisos *a*) y *b*).

d. ¿Qué puede deducir acerca del orden de $23x^4 + 8x^2 + 4x$?

18. Utilice la definición de la notación Θ para demostrar que

$$5x^3 + 65x + 30 \text{ es } \Theta(x^3).$$

19. Aplique la definición de la notación Θ para demostrar que

$$x^2 + 100x + 88 \text{ es } \Theta(x^2).$$

20. a. Demuestre que para cualquier número real x, si $x > 1$ entonces $|x^2| \leq |\lceil x^2 \rceil|$.

b. Demuestre que para cualquier número real x, si $x > 1$ entonces $\frac{1}{2}|\lceil x^2 \rceil| \leq |x^2|$.

c. Use las notaciones Ω y O para expresar los resultados de los incisos *a*) y *b*).

d. ¿Qué puede deducir sobre el orden de $[x^2]$?

21. a. Demuestre que para cualquier número real x, si $x > 1$ entonces $|\lfloor \sqrt{x} \rfloor| \leq |\sqrt{x}|$.

b. Demuestre que para cualquier número real x, si $x > 1$ entonces $\frac{1}{2}|\sqrt{x}| \leq |\lfloor x \rfloor|$.

c. Utilice las notaciones Ω y O para expresar los resultados de los incisos *a*) y *b*).

d. ¿Qué puede deducir acerca del orden de $\lfloor \sqrt{x} \rfloor$?

22. a. Demuestre que para cualquier número real x, si $x > 1$ entonces $|7x^4 - 95x^3 + 3| \leq 105|x^4|$.

b. Use la notación O para expresar el resultado del inciso *a*).

23. a. Demuestre que para cualquier número real x, si $x > 1$ entonces $|\frac{1}{5}x^2 - 42x - 8| \leq 51|x^2|$.

b. Aplique la notación O para expresar el resultado del inciso *a*).

24. a. Demuestre que para cualquier número real x, si $x > 1$ entonces $|\frac{1}{4}x^5 - 50x^3 + 3x + 12| \leq 66|x^5|$.

b. Utilice la notación O para expresar el resultado del inciso *a*).

H 25. Demuestre que x^5 no es $O(x^2)$.

26. Suponga que $a_0, a_1, a_2, \ldots, a_n$ son números reales con $a_n \neq 0$. Use la generalización de la desigualdad del triángulo para n enteros (ejercicio 43, sección 5.5) para demostrar que

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \text{ es } O(x^n).$$

27. Suponga que $a_0, a_1, a_2, \ldots, a_n$ son números reales con $a_n \neq 0$. Demuestre que $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ es $\Omega(x^n)$, haciendo

$$d = 2\left(\frac{|a_0| + |a_1| + |a_2| + \cdots + |a_{n-1}|}{|a_n|}\right).$$

y haciendo $a = \text{máx}(d, 1)$.

En los ejercicios del 28 al 30: *a*) Sea d el número obtenido sumando los valores absolutos de los coeficientes de los términos de bajo orden del polinomio dado, dividido entre el valor absoluto del término de más alto orden y multiplicando el resultado por 2. Sea a el número máximo de 1 y d y hagamos que A sea la mitad del coeficiente del valor absoluto del término de más alto orden del polinomio. *b*) Demuestre que si $x > a$, el valor absoluto del polinomio será mayor que el producto de A y el valor absoluto de x^n, en donde n es el grado del polinomio. *c*) Deduzca el resultado dado en el ejercicio.

28. $7x^4 - 95x^3 + 3$ es $\Omega(x^4)$.

29. $\frac{1}{5}x^2 - 42x - 8$ es $\Omega(x^2)$.

30. $\frac{1}{4}x^5 - 50x^3 + 3x + 12$ es $\Omega(x^5)$.

31. Consulte los resultados de los ejercicios 22 y 28 para encontrar un orden para $7x^4 - 95x^3 + 3$ apoyándose en el conjunto de funciones potencia.

32. Con los resultados de los ejercicios 23 y 29 encuentre un orden para $\frac{1}{5}x^2 - 42x - 8$ utilizando el conjunto de funciones potencia.

33. Vea los resultados de los ejercicios 24 y 30 para obtener un orden para $\frac{1}{4}x^5 - 50x^3 + 3x + 12$ empleando el conjunto de funciones potencia.

Use el teorema de órdenes de polinomios para demostrar cada uno de los enunciados en los ejercicios del 34 al 39.

34. $\dfrac{(x+1)(x-2)}{4}$ es $\Theta(x^2)$.

35. $\dfrac{x}{3}(4x^2 - 1)$ es $\Theta(x^3)$.

36. $\dfrac{x(x-1)}{2} + 3x$ es $\Theta(x^2)$.

37. $\dfrac{n(n+1)(2n+1)}{6}$ es $\Theta(n^3)$.

38. $\left[\dfrac{n(n+1)}{2}\right]^2$ is $\Theta(n^4)$.

39. $2(n-1)+\dfrac{n(n+1)}{2}+4\left(\dfrac{n(n-1)}{2}\right)$ is $\Theta(n^2)$.

Demuestre cada uno de los enunciados en los ejercicios del 40 al 47, suponiendo que n es una variable que toma valores enteros positivos. (Use las fórmulas del conjunto de ejercicios de la sección 5.2 y el teorema de órdenes de polinomios, como sea apropiado.)

40. $1^2+2^2+3^2+\cdots+n^2$ es $\Theta(n^3)$.

41. $1^3+2^3+3^3+\cdots+n^3$ es $\Theta(n^4)$.

42. $2+4+6+\cdots+2n$ es $\Theta(n^2)$.

43. $5+10+15+20+25+\cdots+5n$ es $\Theta(n^2)$.

44. $\displaystyle\sum_{i=1}^{n}(4i-9)$ es $\Theta(n^2)$.

45. $\displaystyle\sum_{k=1}^{n}(k+3)$ es $\Theta(n^2)$.

H 46. $\displaystyle\sum_{i=1}^{n} i(i+1)$ is $\Theta(n^3)$.

47. $\displaystyle\sum_{k=3}^{n}(k^2-2k)$ es $\Theta(n^3)$.

H 48. (Requiere el concepto de límite de cálculo)

a. Sean $a_0, a_1, a_2, \ldots, a_n$ números reales con $a_n \neq 0$. Demuestre que:

$$\lim_{x\to\infty}\left|\frac{a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0}{a_nx^n}\right|=1.$$

b. Use el resultado del inciso *a*) y la definición de límite para demostrar que

$$a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0 \text{ es } \Theta(x^n).$$

49. Otro método para demostrar parte del teorema de órdenes de polinomios, utiliza propiedades de la notación O.

a. Demuestre que si f, g y h son funciones de $\mathbf{R}$ a $\mathbf{R}$ y $f(x)$ es $O(h(x))$ y $g(x)$ es $O(h(x))$, entonces $f(x)+g(x)$ es $O(h(x))$.

b. ¿Cómo se deduce del inciso *a*) y del teorema 11.2.1(3) que x^4+x^2 es $O(x^4)$?

c. El resultado del ejercicio 11 establece que si f es una función de $\mathbf{R}$ a $\mathbf{R}$, $f(x)$ es $O(g(x))$ y c es cualquier número real distinto de cero, entonces $cf(x)$ es $O(g(x))$. ¿Cómo se obtiene de este resultado y del inciso *a*) que $12x^5-34x^2+7$ es $O(x^5)$?

d. Use los resultados del inciso *a*) y del ejercicio 11 para demostrar que si n es cualquier entero positivo y $a_1, a_2, \ldots, a_n$ son números reales, entonces

$$a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0 \text{ es } O(x^n).$$

50. a. Sea x cualquier número real positivo. Utilice inducción matemática para demostrar que para todos los enteros $n \geq 1$, si $x \leq 1$ entonces $x^n \leq 1$.

b. Explique cómo se deduce, del inciso *a*), que si x es cualquier número real positivo, entonces para todos los enteros $n \geq 1$, si $x^n > 1$ entonces $x > 1$.

c. Indique cómo, se deduce del inciso *b*), que si x es cualquier número real positivo, entonces para todos los enteros $n \geq 1$, si $x > 1$ entonces $x^{1/n} > 1$.

H d. Sean p, q y s enteros positivos, r un entero no-negativo y suponga que $p/q > r/s$. Use el inciso *c*) y el resultado del ejercicio 15 para demostrar la propiedad (11.2.1). En otras palabras, demuestre que para cualquier número real x, si $x > 1$ entonces $x^{p/q} > x^{r/s}$.

Explique cómo cada enunciado en los ejercicios 51 y 52 se deduce de los ejercicios 13 y 50 y de los incisos *a*) y *c*) del ejercicio 49.

51. $4x^{4/3}-15x+7$ es $O(x^{4/3})$.

52. $\sqrt{x}(38x^5+9)$ es $O(x^{11/2})$.

H 53. Demuestre que si r y s son números racionales con $r > s$, entonces x^r no es $O(x^s)$.

En los ejercicios del 54 al 56, use el teorema 11.2.4 para encontrar un orden para cada una de las funciones dadas, apoyándose en el conjunto de funciones potencia racionales.

54. $f(x)=\dfrac{\sqrt{x}(3x+5)}{2x+1}$

55. $f(x)=\dfrac{(2x^{7/2}+1)(x-1)}{(x^{1/2}+1)(x+1)}$

56. $f(x)=\dfrac{(5x^2+1)\left(\sqrt{x}-1\right)}{4x^{3/2}-2x}$

✶ 57. **a.** Utilice la inducción matemática para demostrar que

$$\sqrt{1}+\sqrt{2}+\sqrt{3}+\cdots+\sqrt{n} \leq n^{3/2}$$

para todos los enteros $n \geq 1$.

H b. Aplique inducción matemática para demostrar que

$$\frac{1}{2}n^{3/2} \leq \sqrt{1}+\sqrt{2}+\sqrt{3}+\cdots+\sqrt{n}.$$

c. ¿Qué se puede concluir de los incisos *a*) y *b*) sobre el orden de $\sqrt{1}+\sqrt{2}+\sqrt{3}+\cdots+\sqrt{n}$?

✶ 58. a. Use inducción matemática para comprobar que

$1^{1/3}+2^{1/3}+\cdots+n^{1/3} \leq n^{4/3}$, para todos los enteros $n \geq 1$.

b. Implemente inducción matemática para demostrar que

$$\frac{1}{2}n^{4/3} \leq 1^{1/3}+2^{1/3}+3^{1/3}+\cdots+n^{1/3}.$$

c. ¿Qué puede concluir de los incisos *a*) y *b*) acerca del orden de $1^{1/3}+2^{1/3}+3^{1/3}+\cdots+n^{1/3}$?

Los ejercicios del 59 al 61 utilizan la siguiente definición, la que requiere el concepto de límite del cálculo.

> **Definición:** Si f y g son funciones valuadas en los reales, de una variable real y $\lim x \to \infty\ g(x) \neq 0$, entonces
>
> $$f(x) \text{ es } o(g(x)) \quad \Leftrightarrow \quad \lim_{x\to\infty}\frac{f(x)}{g(x)}=0.$$
>
> La notación $f(x)$ es $o(g(x))$ se lee "$f(x)$ es o pequeña de $g(x)$".

59. Demuestre que si $f(x)$ es $o(g(x))$, entonces $f(x)$ es $O(g(x))$.

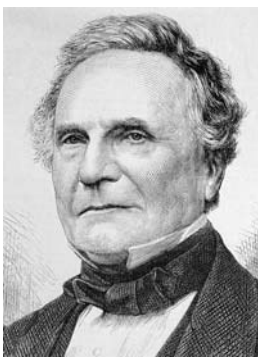
60. Demuestre que si $f(x)$ y $g(x)$ son $o(h(x))$, entonces para todos los números reales a y b, $af(x) + bg(x)$ es $o(h(x))$.

61. Compruebe que para cualesquiera números reales positivos a y b, si $a < b$ entonces x^a es $o(x^b)$.

Respuestas del autoexamen

1. $f(x)$ es $\Omega(g(x))$ 2. $f(x)$ es $O(g(x))$ 3. $f(x)$ es $\Theta(g(x))$ 4. $>$; $>$ 5. el grado de $p(x)$ 6. n^2.

11.3 Aplicación: análisis de la eficiencia del algoritmo I



Bettmann/CORBIS

Charles Babbage (1792-1871)

Tan pronto como exista una máquina analítica, será necesario guiar el futuro curso de la ciencia. Siempre que se le solicite ayuda para lograr un resultado, entonces surgirá la pregunta: ¿mediante qué ruta de cálculo la máquina podrá obtener los resultados en el tiempo más corto?
—Charles Babbage, 1864

La máquina analítica de Charles Babbage fue similar, en concepto, a una moderna computadora y la cita anterior sugiere que él se anticipó cien años a la importancia de analizar las eficiencias de algoritmos computacionales. Al final de 1940, diversos matemáticos y científicos en computación contribuyeron al desarrollo del análisis de algoritmos. Alan Turing puede haber sido el primero en sugerir una forma concreta de hacer esto. En un artículo de 1948 él escribió: "Es conveniente tener una medida de la cantidad de trabajo implicado en procesos de cómputo, aunque sea en una forma muy cruda . . . Podríamos, por ejemplo, contar el número de sumas, restas, multiplicaciones, divisiones, registro de números . . .".* Al inicio de 1960, Donald Knuth inició la redacción de *El Arte de programar una computadora,* una obra de varios volúmenes, la que da una base sólida y extensa sobre el tema, elegante y con rigor matemático.†

El algoritmo de la búsqueda sucesiva

Nota Para conocer más acerca del trabajo de Alan Turing, vea las secciones 6.4 y 12.2.

La finalidad de un algoritmo de búsqueda es indagar en un arreglo de datos para localizar un objeto particular x. En una búsqueda sucesiva, se compara a x con el primer objeto en el arreglo, luego con el segundo, después con el tercero y así sucesivamente. La indagación se detiene si se encuentra un igual en cualquier etapa. Por otro lado, si todo el arreglo se procesa sin encontrar el igual, entonces x no está en el arreglo. En la figura 11.3.1 se muestra esquemáticamente un ejemplo de búsqueda sucesiva.

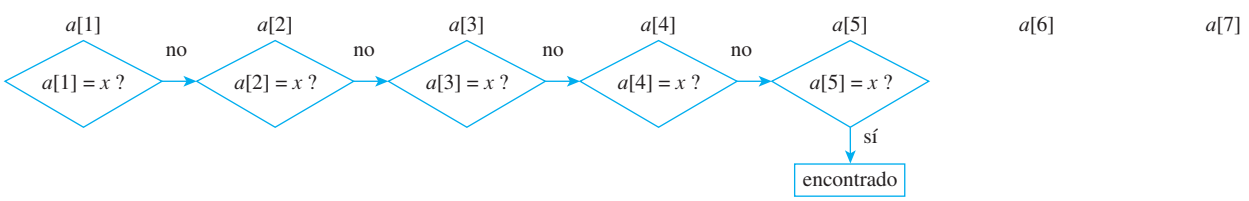


Figura 11.3.1 **Búsqueda sucesiva de $a[1], a[2], \ldots, a[7]$ para x en donde $x = a[5]$**

**Quarterly Journal of Mechanics and Applied Mathematics,* vol. 1 (1949), pp. 287-308.
†Donald E. Knuth, *The Art of Computer Programming*, vol. 1: *Fundamental Algorithms*, 3a. ed. (1997); vol. 2: *Seminumerical Algorithms*, 3a. ed. (1997); vol. 3: *Searching and Sorting*, 2a. ed. (1998) (Reading, MA: Addison-Wesley).

Ejemplo 11.3.4 Órdenes del mejor y el peor caso para una búsqueda sucesiva

En un algoritmo de búsqueda sucesiva y apoyándose en el conjunto de funciones potencia, encuentre los órdenes del mejor y el peor caso.

Solución Suponga que el algoritmo de búsqueda sucesiva se aplica a un arreglo de entrada $a[1], a[2], \ldots, a[n]$ para encontrar un objeto x. En el mejor caso, el algoritmo sólo requiere una comparación entre x y los objetos en $a[1], a[2], \ldots, a[n]$. Esto ocurre cuando x es el primer elemento en el arreglo. Así en el mejor caso, el algoritmo de búsqueda sucesiva es $\Theta(1)$. (Observe que $\Theta(1) = \Theta(n^0)$.) En el peor caso, sin embargo, el algoritmo requiere n comparaciones. Esto sucede cuando $x = a[n]$ o cuando x no aparece en el arreglo. Entonces en el peor caso, el algoritmo de búsqueda sucesiva es $\Theta(n)$. ■

El algoritmo de ordenamiento por inserción

El ordenamiento por inserción es un algoritmo para colocar los objetos en un arreglo en orden ascendente. Inicialmente, el segundo objeto se compara con el primero. Si el segundo elemento es menor que el primero, sus valores son intercambiados y como resultado los primeros dos objetos del arreglo están en orden ascendente. La idea del algoritmo es ir aumentando gradualmente la sección del arreglo que va quedando en orden ascendente, esto mediante la inserción de cada objeto en su posición correcta con respecto a los elementos previos. Cuando el último objeto ha sido colocado, entonces el arreglo completo está en orden ascendente.

La figura 11.3.2 muestra la acción del paso k de ordenamiento por inserción sobre un arreglo $a[1], a[2], a[3], \ldots, a[n]$.

Cortesía de Donald Knuth

Donald Knuth
(nacido en 1938)

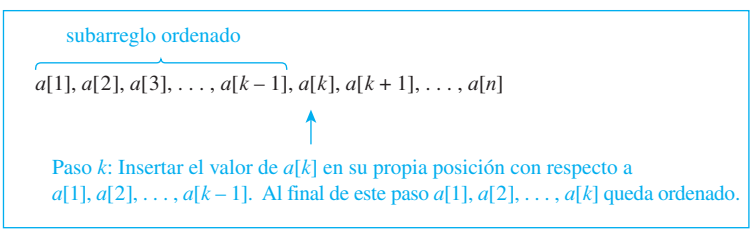


Figura 11.3.2 Paso k de ordenamiento por inserción

El entender las eficiencias relativas de los algoritmos diseñados para realizar el mismo trabajo, es más que un simple interés académico. En asuntos industriales y científicos la elección de un programa eficiente, en lugar de uno ineficiente, puede resultar en ahorros de miles de dólares o puede significar el lograr o no la realización de un proyecto.

Respecto a la eficiencia de un algoritmo, son importantes dos aspectos: la cantidad de tiempo requerida para ejecutar el algoritmo y la cantidad de memoria necesitada para ejecutarlo. En este capítulo introducimos técnicas básicas para calcular la eficiencia en tiempo de máquina (eficiencia temporal). Existen técnicas similares para calcular la eficiencia en memoria de almacenamiento (eficiencia espacial). Ocasionalmente, un algoritmo puede ser eficiente en el uso del tiempo pero menos eficiente (en relación a otros algoritmos) en cuestiones de memoria, forzando al usuario a negociar entre eficiencias temporal y espacial según sus necesidades.

Eficiencia temporal de un algoritmo

¿Cómo puede calcularse la eficiencia temporal de un algoritmo? La respuesta depende de varios factores. Uno es el tamaño del conjunto de datos que constituye la entrada al algoritmo; por ejemplo, a un algoritmo le toma más tiempo procesar 1 000 000 elementos que 100 elementos. En consecuencia, el tiempo de ejecución de un algoritmo generalmente se expresa como una función del tamaño de los datos de entrada.

Otro factor que puede afectar el tiempo de ejecución de un algoritmo es la naturaleza de los datos de entrada. Por ejemplo, un programa que busca sucesivamente a través de una lista de longitud n para encontrar un elemento requiere solamente un paso si éste es el primero en la lista, pero el programa realizará n pasos si el elemento es el último en dicha lista.

Así, frecuentemente los algoritmos son analizados en términos del desempeño de su "mejor caso", de su "peor caso" y de su "caso promedio" para una entrada de tamaño n.

Burdamente hablando, el análisis de la eficiencia temporal de un algoritmo empieza por contar el número de operaciones elementales que deben efectuarse cuando el algoritmo es ejecutado con una entrada de tamaño n (en los casos mejor, peor o promedio). Lo clasificado como una "operación elemental" puede variar dependiendo de la naturaleza del problema para cuya solución fueron diseñados los algoritmos (bajo comparación). Por ejemplo, para comparar dos algoritmos que evalúan polinomios, el asunto crucial es el número de restas y multiplicaciones necesitadas, mientras que para comparar dos algoritmos de búsqueda para encontrar en una lista un elemento particular, la distinción importante es el número de comparaciones requeridas. Como es común, las siguientes serán clasificadas como **operaciones elementales**: suma, resta, multiplicación, división y comparaciones que se indican explícitamente en un enunciado si emplean uno de los símbolos relacionales $<$, $\leq$, $>$, $\geq$, $=$ o $\neq$.

Cuando se implementan los algoritmos en un particular lenguaje de programación y se ejecutan en una determinada computadora, entonces algunas operaciones se efectúan más rápido que otras y, de hecho, de una máquina a otra hay diferencias en los tiempos de ejecución. En ciertas situaciones prácticas esos factores se toman en cuenta al decidir qué algoritmo o que máquina emplear para resolver un problema específico. Sin embargo, en otros casos la máquina es dada y todo lo que necesitamos son burdas estimaciones para determinar la clara superioridad de un algoritmo sobre otro. Como cada operación elemental se ejecuta en un tiempo no mucho mayor que la más lenta, entonces la eficiencia temporal de un algoritmo es aproximadamente proporcional al número de operaciones elementales requerido para ejecutar el algoritmo.

Considere el ejemplo de dos algoritmos, A y B, diseñados para realizar cierto trabajo. Suponga que para una entrada de tamaño n, el número de operaciones elementales que se necesitan para realizar el algoritmo A está entre $10n$ y $20n$ (al menos para n grandes) y que el número de operaciones elementales requeridas para ejecutar el algoritmo B está entre $2n^2$ y $4n^2$. Observe que $20n < 2n^2$ siempre que $n > 10$, lo que significa que el número máximo de operaciones necesitadas para ejecutar A es menor que el número *mínimo* de operaciones requeridas para implementar B siempre que $n > 10$. En efecto, $20n$ es mucho menor que $2n^2$ cuando n es grande. Por ejemplo, si $n = 1\,000$, entonces $20n = 20\,000$, mientras que $2n^2 = 2\,000\,000$. Decimos que en el peor caso, el algoritmo A es $\Theta(n)$ (o que tiene un peor caso de orden n) y que en el peor caso el algoritmo B es $\Theta(n^2)$(o que tiene un peor caso de orden n^2).

• Definición

Sea A un algoritmo.

1. Suponga que el número de operaciones elementales efectuadas cuando se ejecuta A para una entrada de tamaño n depende únicamente de n y no de la naturaleza de los datos de entrada; digamos que es igual a $f(n)$. Si $f(n)$ es $\Theta(g(n))$, decimos que ***A* es $\Theta(g(n))$** o que ***A* es de orden $g(n)$.**
2. Suponga que el número de operaciones elementales realizadas cuando se ejecuta A para una entrada de tamaño n depende de éste y de la naturaleza de los datos de entrada.
   a. Sea $b(n)$ el mínimo número de operaciones elementales requeridas para ejecutar A para todos los posibles conjuntos de entrada de tamaño n. Si $b(n)$ es $\Theta(g(n))$, decimos que **en el mejor caso, *A* es $\Theta(g(n))$** o que ***A* tiene un mejor caso de orden $g(n)$.**
   b. Sea $w(n)$ el número máximo de operaciones elementales necesitadas para ejecutar A para todos los posibles conjuntos de entrada de tamaño n. Si $w(n)$ es $\Theta(g(n))$, decimos que **en el peor caso, *A* es $\Theta(g(n))$** o que ***A* tiene un peor caso de orden $g(n)$.**

En la tabla 11.3.1 se muestran algunos de los órdenes más comúnmente empleados para describir eficiencias de algoritmos. Ahí se ve que son más que astronómicas las diferencias entre los órdenes de varios tipos de algoritmos. Un algoritmo de orden 2^n para operar un conjunto de datos de tamaño 100 000 requiere un tiempo de aproximadamente $10^{30,076}$ veces la edad del universo (15 billones de años de acuerdo a determinada teoría cosmológica). Por otro lado, un algoritmo de orden $\log_2 n$ necesita a lo más una fracción de segundo para procesar el mismo conjunto de datos.

Tabla 11.3.1 Comparaciones en tiempo de algunos órdenes de algoritmos

Tiempo aproximado para ejecutar $f(n)$ operaciones suponiendo una operación por nanosegundo*				
$f(n)$	$n = 10$	$n = 1\,000$	$n = 100\,000$	$n = 10\,000\,000$
$\log_2 n$	3.3×10^{-9} seg	10^{-8} seg	1.7×10^{-8} seg	2.3×10^{-8} seg
n	10^{-8} seg	10^{-6} seg	0.0001 seg	0.01 seg
$n \log_2 n$	$3(3 \times 10^{-8}$ seg	10^{-5} seg	0.0017 seg	0.23 seg
n^2	10^{-7} seg	0.001 seg	10 seg	27.8 min
n^3	10^{-6} seg	1 seg	11.6 días	31,688 años
2^n	10^{-6} seg	3.4×10^{284} años	3.1×10^{30086} años	2.9×10^{3010283} años

*un nanosegundo $= 10^{-9}$ segundo

Ejemplo 11.3.1 Cálculo del orden de un segmento de algoritmo

Suponga que n es un entero positivo y considere el siguiente segmento de algoritmo:

$p := 0, x := 2$
for $i := 2$ **to** n
  $p := (p + i) \cdot x$
next i

a. Calcule el número real de sumas y multiplicaciones que se deben efectuar cuando se ejecute este segmento de algoritmo.

b. Use el teorema de órdenes de polinomios para encontrar un orden para este segmento de algoritmo.

Solución

a. Hay una multiplicación y una suma por cada iteración del bucle, así hay el doble de multiplicaciones y sumas que de iteraciones del bucle. Ahora el número de iteraciones para el bucle **for-next** es igual al índice superior del bucle menos el índice inferior más 1; es decir, $n - 2 + 1 = n - 1$. Por tanto hay $2(n - 1) = 2n - 2$ multiplicaciones y sumas.

b. Por el teorema de órdenes de polinomios,

$$2n - 2 \text{ es } \Theta(n),$$

y así este segmento de algoritmo es $\Theta(n)$. ■

El siguiente ejemplo se refiere a un segmento de algoritmo que contiene un bucle anidado.

Ejemplo 11.3.2 Un orden para un algoritmo con un bucle anidado

Suponga que n es un entero positivo y considere el siguiente segmento de algoritmo:

$s := 0$
for $i := 1$ **to** n
  for $j := 1$ **to** i
    $s := s + j \cdot (i - j + 1)$
  next j
next i

a. Calcule el número real de sumas, restas y multiplicaciones que deben realizarse cuando se ejecuta este segmento de algoritmo.

b. Use el teorema de órdenes polinomiales para encontrar un orden para este segmento de algoritmo.

Solución

a. Hay dos sumas, una multiplicación y una resta para cada iteración del bucle interno, así el número total de sumas, multiplicaciones y restas es cuatro veces el número de iteraciones del bucle interior. Ahora el bucle interno es iterado

una vez cuando $i = 1$,
dos veces cuando $i = 2$,
tres veces cuando $i = 3$,
$\vdots$
n veces cuando $i = n$.

Esto lo puede ver fácilmente si construye una tabla que muestre los valores de i y j para los que se ejecuten los enunciados en el bucle interior. Existe una iteración para cada columna en la tabla.

i	1	2		3			4				$\cdots$	n				
j	1	1	2	1	2	3	1	2	3	4	$\cdots$	1	2	3	$\cdots$	n
	1	2		3			4					n				

Así que el número total de iteraciones del bucle interno es

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2} \quad \text{por el teorema 5.2.2,}$$

y así el número de sumas, restas y multiplicaciones es

$$4 \cdot \frac{n(n+1)}{2} = 2n(n+1).$$

Un método alternativo para calcular el número de columnas de la tabla utiliza un enfoque analizado en el ejemplo 9.6.3. Observe que el número de columnas en la tabla es igual que el número de maneras de colocar dos $\times$'s en n categorías, 1, 2,..., n, en donde la localización de las $\times$'s indica los valores de i y j con $j \leq i$. Por el teorema 9.6.1, este número es

$$\binom{n-1+2}{2} = \binom{n+1}{2} = \frac{(n+1)!}{2!((n+1)-2)!} = \frac{(n+1)n(n-1)!}{2(n-1)!} = \frac{n(n+1)}{2}.$$

No obstante, para este ejemplo, el método alternativo es más complicado que el anterior, pero es más simple cuando el número de bucles anidados excede de dos. (Vea el ejercicio 19.)

b. Por el teorema de órdenes de polinomios, $2n(n + 1) = 2n^2 + 2n$ es $\Theta(n^2)$ y así este segmento de algoritmo es $\Theta(n^2)$. ■

Ejemplo 11.3.3 Cuando el número de iteraciones depende de la función piso

Suponga que n es un entero positivo y considere el siguiente segmento de algoritmo:

```
for i := ⌊n/2⌋ to n
    a := n − i
next i
```

a. Calcule el número real de restas que se deben efectuar cuando se ejecuta este segmento de algoritmo.

b. Use el teorema de órdenes de polinomios para encontrar un orden para este segmento de algoritmo.

Solución

a. Existe una resta por cada iteración del bucle y el bucle es iterado $n - \left\lfloor \frac{n}{2} \right\rfloor + 1$ veces. Si n es par, entonces $\left\lfloor \frac{n}{2} \right\rfloor = \frac{n}{2}$ y así el número de restas es

$$n - \left\lfloor \frac{n}{2} \right\rfloor + 1 = n - \frac{n}{2} + 1 = \frac{n+2}{2}.$$

Si n es impar, entonces $\left\lfloor \frac{n}{2} \right\rfloor = \frac{n-1}{2}$ y el número de diferencias es

$$n - \left\lfloor \frac{n}{2} \right\rfloor + 1 = n - \frac{n-1}{2} + 1 = \frac{2n - (n-1) + 2}{2} = \frac{n+3}{2}.$$

b. Por el teorema de órdenes de polinomios,

$$\frac{n+2}{2} \text{ es } \Theta(n) \quad \text{y} \quad \frac{n+3}{2} \text{ es } \Theta(n)$$

también. Por tanto, para n par e impar, este segmento de algoritmo es $\Theta(n)$. ■

El siguiente es un algoritmo formal para ordenamiento por inserción.

Algoritmo 11.3.1 Ordenamiento por inserción

[La finalidad de este algoritmo es hacer un arreglo a[1], a[2], a[3], . . . , a[n], en donde n ≥ 1 y lo reordene. El arreglo de salida también se denota por a[1], a[2], a[3], . . . , a[n], que tiene los mismos valores que el arreglo de entrada, pero en orden ascendente. En el k-ésimo paso, a[1], a[2], a[3], . . . , a[k − 1] está en orden ascendente y a[k] se inserta en la posición correcta con respecto a éste.]

Entrada: *n [un entero positivo], a[1], a[2], a[3], . . . , a[n] [un arreglo de objetos de datos capaces de ordenarse].*

Cuerpo del algoritmo:

for $k := 2$ **to** n

[Compare $a[k]$ con los objetos previos en el arreglo $a[1], a[2], a[3], \ldots, a[k-1]$, empezando desde el más grande y moviéndose hacia abajo. Siempre que $a[k]$ sea menor que un objeto del arreglo precedente, incremente el índice del objeto precedente para moverlo una posición a la derecha. Tan pronto como $a[k]$ sea más grande que o igual a un elemento del arreglo, inserte el valor de $a[k]$ a la derecha de ese elemento. Si $a[k]$ es mayor o igual que $a[k-1]$, entonces deje inalterado el valor de $a[k]$.]

$x := a[k]$
$j := k - 1$
while $(j \neq 0)$
if $x < a[j]$ **then**
$a[j+1] := a[j]$
$j := j - 1$
end if
end while
$a[j+1] := x$

next k

Salida: $a[1], a[2], a[3], \ldots, a[n]$ *[en orden ascendente]*

La figura 11.3.3 muestra el resultado de cada paso cuando se aplica el ordenamiento por inserción al arreglo particular.

$$a[1] = 6, \quad a[2] = 3, \quad a[3] = 5, \quad a[4] = 7, \quad a[5] = 2.$$

	$a[1]$	$a[2]$	$a[3]$	$a[4]$	$a[5]$
Inicial	6	3	5	7	2
Resultado del paso 1	3	6	5	7	2
Resultado del paso 2	3	5	6	7	2
Resultado del paso 3	3	5	6	7	2
Resultado del paso 4	2	3	5	6	7

El renglón superior de la tabla muestra los valores iniciales del arreglo y el renglón de abajo indica los valores finales. El resultado de cada paso se muestra en una fila por separado. En cada paso, se sombrea la sección ordenada del arreglo.

Figura 11.3.3 **Acción del ordenamiento por inserción sobre un arreglo**

El ejemplo 11.3.5 desarrolla una tabla de seguimiento para mostrar la acción del ordenamiento por inserción en un arreglo particular.

Ejemplo 11.3.5 Una tabla de seguimiento para el ordenamiento por inserción

Construya una tabla de seguimiento que muestre la acción del ordenamiento por inserción sobre el arreglo:

$$a[1] = 6, a[2] = 3, a[3] = 5, a[4] = 7, a[5] = 2.$$

Solución

La primera columna, en la siguiente página, indica el estado de las variables antes de la primera iteración de **for-next** en el bucle. Cuando se itera primero el bucle **for-next**, a k se le asigna el valor 2; a x el valor $a[2]$, que es 3; y a j el valor $k - 1$, que es 1. Como $j \neq 0$, se introduce el bucle **while** y se prueba la condición para el enunciado **if-then-else**. Como $a[1] > x$, entonces a $a[2]$ se le asigna el valor de $a[1]$, que es 6, a j se le da el valor de $j - 1$, que es 0 y $a[1]$ toma el valor de x, que es 3. La condición gobernada por el bucle **while** se prueba otra vez, pero como $j = 0$, entonces no se satisface y así no entra el bucle **while**. Así el valor de k se incrementa por 1 (entonces es igual a 3) y se introduce el bucle **for-next** por segunda vez.

Este proceso continúa hasta que el valor de k se ha incrementado a 6. Como 6 es mayor que el valor superior en el bucle **for-next**, entonces se detiene la ejecución del algoritmo y los objetos del arreglo quedan en orden ascendente.

n	5													
***a*[1]**	6		3										2	
***a*[2]**	3	6				5							3		
***a*[3]**	5				6							5			
***a*[4]**	7							7			6				
***a*[5]**	2									7					
k	2			3			4		5						6
x	3			5			7		2						
j	1	0		2	1		3		4	3	2	1	0		

■

Ejemplo 11.3.6 Encontrando el orden para el peor caso en el ordenamiento por inserción

a. ¿Cuál es el máximo número de comparaciones que se realizan cuando el ordenamiento por inserción se aplica al arreglo $a[1], a[2], a[3], \ldots, a[n]$?

b. Use el teorema de órdenes de polinomios para encontrar el orden del peor caso para ordenamiento por inserción.

Solución

a. En cada iteración del bucle **while**, se hacen dos comparaciones explícitas: una para demostrar si $j \neq 0$ y la otra para demostrar si $a[j] > x$. Durante el tiempo en que $a[k]$ es puesta en posición con respecto a $a[1], a[2], \ldots, a[k-1]$, el máximo número de iteraciones realizadas del bucle **while** es k. Esto pasa cuando $a[k]$ es menor que cada uno de $a[1], a[2], \ldots, a[k-1]$; en la k-ésima iteración, la condición del bucle **while** no se satisface porque $j = 0$. Así el máximo número de comparaciones para un valor dado de k es $2k$. Como k va de 2 a n, se tiene que el máximo del número total de comparaciones ocurre cuando los objetos en el arreglo están en orden inverso y es igual a

$$\begin{aligned} 2\cdot 2 + 2\cdot 3 + \cdots + 2\cdot n &= 2(2 + 3 + \cdots + n) && \text{factorizando el 2} \\ &= 2[(1 + 2 + 3 + \cdots + n) - 1] && \text{sumando y restando 1} \\ &= 2\left(\frac{n(n+1)}{2} - 1\right) && \text{por el teorema 5.2.2} \\ &= n(n+1) - 2 \\ &= n^2 + n - 2 && \text{por álgebra.} \end{aligned}$$

b. Por el teorema de órdenes polinomiales, $n^2 + n - 2$ es $\Theta(n^2)$ y así el algoritmo de ordenamiento por inserción tiene un peor caso de orden $\Theta(n^2)$. ■

La definición de valor esperado que fue introducida en la sección 9.8 puede ser usada para encontrar un orden del caso promedio de un ordenamiento por inserción.

Ejemplo 11.3.7 Determinación de un orden del caso promedio de un ordenamiento por inserción

a. ¿Cuál es el número promedio de comparaciones que son realizadas cuando el ordenamiento por inserción se aplica al arreglo $a[1], a[2], a[3], \ldots, a[n]$?

b. Use el teorema de órdenes de polinomios para encontrar un orden del caso promedio para ordenamiento por inserción.

Solución

a. Sea E_n el número promedio, o esperado, de comparaciones empleadas para ordenar por inserción a $a[1], a[2], \ldots, a[n]$. Observe que para cada entero $k = 2, 3, \ldots, n$,

$$\begin{bmatrix}\text{número esperado de}\\ \text{comparaciones empleadas para}\\ \text{ordenar } a\ [1], a[2], \ldots, a[k]\end{bmatrix}$$
$$= \begin{bmatrix}\text{número esperado de}\\ \text{comparaciones efectuadas para}\\ \text{ordenar } a[1], a[2], \ldots, a[k-1]\end{bmatrix} + \begin{bmatrix}\text{número esperado de comparaciones}\\ \text{realizadas para colocar } a[k] \text{ en posición}\\ \text{con respecto a } a[1], a[2], \ldots, a[k-1]\end{bmatrix}$$

Así

$$E_k = E_{k-1} + \begin{bmatrix}\text{número esperado de comparaciones}\\ \text{usadas para colocar } a[k] \text{ en posición}\\ \text{con respecto a } a[1], a[2], \ldots, a[k-1]\end{bmatrix}.$$

También, $E_1 = 0$ porque cuando sólo existe un objeto en el arreglo, entonces $n = 1$ y no se efectúan iteraciones del bucle externo.

Ahora bien, en el momento en que $a[k]$ se coloca en posición con respecto a $a[1]$, $a[2], \ldots, a[k-1]$, una suposición razonable es que a ésta le es igualmente posible pertenecer a cualesquiera de las primeras k posiciones. Así, la probabilidad de que pertenezca a cualquier posición particular es $1/k$. Si realmente pertenece a la posición j, entonces serán empleadas $2(k-j+1)$ comparaciones para moverlo, porque existirán $k-j+1$ iteraciones del bucle **while** y hay 2 comparaciones por cada iteración.

De acuerdo a la definición de valor esperado dado en la sección 9.8, el número esperado de comparaciones empleadas para colocar $a[k]$ con respecto a $a[1]$, $a[2], \ldots, a[k-1]$ es por tanto

$$\begin{aligned}\sum_{j=1}^{k} \frac{1}{k} 2(k-j+1) &= \frac{2}{k}[k + (k-1) + \cdots + 3 + 2 + 1] && \text{escribiendo la suma en forma desarrollada,}\\ &= \frac{2}{k}\left(\frac{k(k+1)}{2}\right) && \text{por el teorema 5.2.2,}\\ &= k + 1 && \text{por álgebra.}\end{aligned}$$

Por tanto

$$E_k = E_{k-1} + k + 1 \quad \text{para cada entero} \quad k \geq 2 \quad \text{y}$$
$$E_1 = 0.$$

El ejercicio 27, al final de la sección, le pide resolver esta relación de recurrencia para demostrar que

$$E_n = \frac{n^2 + 3n - 4}{2} \quad \text{para cada entero } n \geq 1.$$

b. Por el teorema de órdenes de polinomios, $\dfrac{n^2 + 3n - 4}{2} = \dfrac{1}{2}n^2 + \dfrac{3}{2}n - 2$ es $\Theta(n^2)$ y entonces el orden del caso promedio de ordenamiento por inserción también es $\Theta(n^2)$. ■

Autoexamen

1. Cuando un segmento de algoritmo contiene un bucle anidado **for-next,** puede encontrar el número de veces que el bucle se iterará construyendo una tabla en la cual cada columna representa _____.
2. En el peor caso para un arreglo de entrada de longitud n, el algoritmo de búsqueda sucesiva tiene que ver a través de _____ elementos del arreglo antes de que se detenga.
3. El orden del peor caso para el algoritmo de ordenamiento por inserción es _____ y el orden de su caso promedio es _____.

Conjunto de ejercicios 11.3

1. Suponga que una computadora tarda un nanosegundo ($= 10^{-9}$ segundo) al ejecutar cada operación. Aproximadamente, ¿qué tiempo tardará la máquina en realizar las siguientes operaciones? Convierta sus respuestas a segundos, minutos, horas, días, semanas, o años, según sea apropiado. Por ejemplo, en lugar de 250 nanosegundos, escriba 13 días.

   a. $\log_2 200$ b. 200 c. $200 \log_2 200$
   d. 200^2 **e.** 200^8 f. 2^{200}

2. Suponga que un algoritmo requiere cn^2 operaciones cuando se aplica a una entrada de tamaño n (en donde c es una constante).
   a. ¿Cuántas operaciones serán requeridas cuando el tamaño de la entrada se incremente de m a $2m$ (en donde m es un entero positivo)?
   b. ¿Por qué factor se incrementará el número de operaciones cuando se duplique el tamaño de entrada?
   c. ¿Por qué factor se incrementará el número de operaciones cuando el tamaño de entrada se multiplique por un factor de diez?

3. Suponga que un algoritmo requiere cn^3 operaciones cuando se aplica a una entrada de tamaño n (en donde c es una constante).
   a. ¿Cuántas operaciones se requerirán cuando el tamaño de la entrada se incremente de m a $2m$ (en donde m es un entero positivo)?
   b. ¿Por qué factor se incrementará el número de operaciones cuando se duplique el tamaño de entrada?
   c. ¿Por qué factor aumentará el número de operaciones cuando el tamaño de entrada se incremente por un factor de diez?

Los ejercicios 4 y 5 exploran el hecho de que para relativamente pequeños valores de n, los algoritmos con órdenes grandes pueden ser más eficientes que los algoritmos con órdenes muy pequeños.

4. Suponga que el algoritmo A, al aplicarse a una entrada de tamaño n, requiere $2n^2$ operaciones, mientras que el algoritmo B necesita $80n^{3/2}$ operaciones.
   a. ¿Cuáles son los órdenes de los algoritmos A y B en términos de funciones potencia?
   b. ¿Para qué valores de n el algoritmo A es más eficiente que el algoritmo B?
   c. ¿Para qué valores de n el algoritmo B es al menos 100 veces más eficiente que el algoritmo A?

5. Acepte que el algoritmo A, al ejecutarse sobre una entrada de tamaño n, requiere de 10^6n^2 operaciones, mientras que el algoritmo B necesita n^3 operaciones.
   a. ¿Cuáles son los órdenes de los algoritmos A y B en términos de funciones potencia?
   b. ¿Para qué valores de n el algoritmo A es más eficiente que el algoritmo B?
   c. ¿Para qué valores de n el algoritmo B es al menos 100 veces más eficiente que el algoritmo A?

Para cada uno de los segmentos de algoritmo en los ejercicios del 6 al 19, suponga que n es un entero positivo. *a*) Calcule el número real de sumas, restas, multiplicaciones, divisiones y comparaciones que se deben efectuar cuando se ejecuta el segmento de algoritmo. Sin embargo, por simplicidad, sólo cuente las comparaciones que ocurran dentro de los enunciados **if-then**; ignore aquellas implicadas por los bucles **for-next**. *b*) Utilice el teorema de órdenes de polinomios para encontrar un orden para cada segmento de algoritmo.

6. **for** $i := 3$ **to** $n - 1$
   $a := 3 \cdot n + 2 \cdot i - 1$
   next i

7. $max := a[1]$
   for $i := 2$ **to** n
   if $max < a[i]$ **then** $max := a[i]$
   next i

8. **for** $i := 1$ **to** $\lfloor n/2 \rfloor$
   $a := n - i$
   next i

9. **for** $i := 1$ **to** n
   for $j := 1$ **to** $2n$
   $a := 2 \cdot n + i \cdot j$
   next j
   next i

10. **for** $k := 2$ **to** n
    for $j := 1$ **to** $3n$
    $x := a[k] - b[j]$
    next j
    next k

11. **for** $k := 1$ **to** $n - 1$
    for $j := 1$ **to** $k + 1$
    $x := a[k] + b[j]$
    next j
    next k

12. **for** $k := 1$ **to** $n - 1$
    $max := a[k]$
    for $i := k + 1$ **to** n
    if $max < a[i]$ **then** $max := a[i]$
    next i
    $a[k] := max$
    next k

13. **for** $i := 1$ **to** $n - 1$
    for $j := i$ **to** n
    if $a[j] > a[i]$ **then do**
    $temp := a[i]$
    $a[i] := a[j]$
    $a[j] := temp$
    end do
    next j
    next i

14.
```
t := 0
for i := 1 to n
    s := 0
    for j := 1 to i
        s := s + a[j]
    next j
    t := t + s^2
next i
```

15.
```
r := 0
for i := 1 to n − 1
    p := 1
    q := 1
    for j := i + 1 to n
        p := p · c[j]
        q := q · (c[j])^2
    next j
    r := p + q
next i
```

16.
```
t := 0
for i := 1 to n
    s := 0
    for j := 1 to i − 1
        s := s + j · (i − j + 1)
    next j
    r := s^2
next i
```

17.
```
for i := 1 to n
    for j := 1 to ⌊(i + 1)/2⌋
        a := (n − i) · (n − j)
    next j
next i
```

18.
```
for i := 1 to n
    for j := ⌊(i + 1)/2⌋ to n
        x := i · j
    next j
next i
```

H ∗ 19.
```
for i := 1 to n
    for j := 1 to i
        for k := 1 to j
            x := i · j · k
        next k
    next j
next i
```

20. Construya una tabla que muestre el resultado de cada paso cuando se aplica el ordenamiento por inserción al arreglo $a[1] = 6$, $a[2] = 2$, $a[3] = 1$, $a[4] = 8$ y $a[5] = 4$.

21. Elabore una tabla que indique el resultado de cada paso cuando se aplica el ordenamiento por inserción al arreglo $a[1] = 7$, $a[2] = 3$, $a[3] = 6$, $a[4] = 9$ y $a[5] = 5$.

22. Construya una tabla de seguimiento que indique la acción del ordenamiento por inserción sobre el arreglo del ejercicio 20.

23. Elabore una tabla de seguimiento que muestre la acción del ordenamiento por inserción sobre el arreglo del ejercicio 21.

24. ¿Cuántas comparaciones entre los valores de $a[j]$ y x realmente ocurrirán cuando el ordenamiento por inserción sea aplicado al arreglo del ejercicio 20?

25. ¿Cuántas comparaciones entre los valores de $a[j]$ y x sucederán cuando el ordenamiento por inserción se aplique al arreglo del ejercicio 21?

26. De acuerdo con el ejemplo 11.3.6, el máximo número de comparaciones que se necesitan para efectuar ordenamiento por inserción en un arreglo de longitud cinco es $5^2 - 5 + 2 = 22$. Encuentre un arreglo de longitud cinco que requiera el máximo número de comparaciones cuando se le aplique ordenamiento por inserción.

***H* 27.** Considere la relación de recurrencia que surgió en el ejemplo 11.3.7: $E_1 = 0$ y $E_k = E_{k-1} + k + 1$, para todos los enteros $k \geq 2$.

a. Use iteración para encontrar una fórmula explícita para la secuencia.

b. Utilice inducción matemática para checar la validez de dicha fórmula.

Los ejercicios del 28 al 35 se refieren a *ordenamiento por selección*, que es otro algoritmo para ordenar en orden ascendente a los elementos de un arreglo.

Algoritmo 11.3.2 Ordenamiento por selección

[Partiendo de un arreglo a[1], a[2], a[3], . . . , a[n], este algoritmo se ordena seleccionando el objeto correcto para colocarlo en cada posición moviéndose secuencialmente a través de los elementos del arreglo. En general, para cada k = 1 a n − 1, el k-ésimo paso del algoritmo encuentra el índice del objeto del arreglo, con un valor mínimo, de entre los elementos a[k + 1], a[k + 2], a[k + 3], . . . , a[n]. Una vez que se encuentra este índice, el valor del correspondiente elemento del arreglo se intercambia con el valor de a[k]. Al final de la ejecución los elementos del arreglo están en orden ascendente.]

Input: *n [un entero positivo], a[1], a[2], a[3], . . . , a[n] [un arreglo de elementos datos susceptibles de ser ordenados]*

Cuerpo del algoritmo:

```
for k := 1 to n − 1
    IndexOfMin := k
    for i := k + 1 to n
      if (a[i] < a[IndexOfMin])
      then IndexOfMin := i
    next i
    if IndexOfMin ≠ k then
      Temp := a[k]
      a[k] := a[IndexOfMin]
      a[IndexOfMin] := Temp
next k
```

Output: *a[1], a[2], a[3],. . . , a[n] [en orden ascendente]*

La acción de ordenamiento por selección se puede representar pictóricamente de la siguiente manera:

$$a[1]\,a[2]\cdots\boxed{a[k]}\,a[k+1]\cdots a[n]$$

↑

k-ésimo paso: se encuentra el índice del elemento del arreglo con valor mínimo, seleccionado entre los elementos $a[k+1], \ldots, a[n]$ y se intercambia su valor con el valor de $a[k]$.

28. Construya una tabla que muestre los intercambios que ocurren cuando el ordenamiento por selección se aplica al arreglo $a[1] = 5$, $a[2] = 3$, $a[3] = 4$, $a[4] = 6$ y $a[5] = 2$.

29. Elabore una tabla que exhiba los intercambios que suceden cuando se aplica el ordenamiento por selección al arreglo $a[1] = 6$, $a[2] = 4$, $a[3] = 5$, $a[4] = 8$ y $a[5] = 1$.

30. Construya una tabla de seguimiento para mostrar la acción del ordenamiento por selección sobre el arreglo del ejercicio 28.

31. Elabore una tabla de seguimiento para exhibir la acción del ordenamiento por selección en el arreglo del ejercicio 29.

32. Cuando el ordenamiento por selección se aplica al arreglo del ejercicio 28, ¿cuántas veces se efectúan las comparaciones en el enunciado **if-then**?

33. Cuando el ordenamiento por selección actúa sobre el arreglo del ejercicio 29, ¿cuántas veces se realizan las comparaciones en el enunciado **if-then**?

34. Cuando el ordenamiento por selección se aplica a un arreglo $a[1]$, $a[2]$, $a[3]$, $a[4]$, ¿cuántas veces se realiza la comparación en el enunciado **if-then**?

35. Considere el ordenamiento por selección actuando sobre el arreglo $a[1]$, $a[2]$, $a[3]$,. . . , $a[n]$.
   a. ¿Cuántas veces se efectúa la comparación en el enunciado **if-then** cuando $a[1]$ se compara con cada uno de los elementos $a[2], a[3], \ldots, a[n]$?
   b. ¿Cuántas veces se realiza la comparación en el enunciado **if-then** cuando $a[2]$ se compara con cada uno de los elementos $a[3], a[4], \ldots, a[n]$?
   c. ¿Cuántas veces se hace la comparación en el enunciado **if-then** cuando $a[k]$ se compara con cada uno de los elementos $a[k-1], a[k+2], \ldots, a[n]$?

H **d.** Utilizando el número de veces que se efectúa la comparación en el enunciado **if-then**, como una medida de la eficiencia temporal del ordenamiento por selección, encuentre un orden para éste. Aplique el teorema de órdenes de polinomios.

Los ejercicios del 36 al 39 se refieren al siguiente algoritmo para calcular el valor de un polinomio real.

Algoritmo 11.3.3 Evaluación polinomial término a término

[Este algoritmo determina el valor del polinomio real $a[n]x^n + a[n-1]x^{n-1} + \cdots + a[2]x^2 + a[1]x + a[0]$ *mediante el cálculo por separado de cada término, empezando con* $a[0]$ *y sumándolo a una suma acumulativa.]*

Input: *n [un entero no-negativo], a*[0], *a*[1], *a*[2], . . . , *a*[*n*] *[un arreglo de números reales], x [un número real].*

Cuerpo del algoritmo:

polyval := *a*[0]
for *i* := 1 **to** *n*
  term := *a*[*i*]
  for *j* := 1 **to** *i*
    term := *term* · *x*
  next *j*
  polyval := *polyval* + *term*
next *i*
[En este punto
$valorpolinomio = a[n]x^n + a[n-1]x^{n-1} + \cdots + a[2]x^2 + a[1]x + a[0]$*].*

Output: *valorpolinomio [un número real]*

36. Represente el algoritmo 11.3.3 para la entrada $n = 3$, $a[0] = 2$, $a[1] = 1$, $a[2] = -1$, $a[3] = 3$ y $x = 2$.

37. Represente el algoritmo 11.3.3 para la entrada $n = 2$, $a[0] = 5$, $a[1] = -1$, $a[2] = 2$ y $x = 3$.

38. Sea s_n = número de sumas y multiplicaciones que se deben efectuar cuando se ejecuta el algoritmo 11.3.3 para un polinomio de grado n. Exprese s_n como una función de n.

39. Use el teorema de órdenes de polinomios para encontrar un orden para el algoritmo 11.3.3.

Los ejercicios del 40 al 43 se refieren a otro algoritmo, conocido como regla de Horner, para encontrar el valor de un polinomio real.

Algoritmo 11.3.4 Regla de Horner

[Este algoritmo calcula el valor del polinomio real $a[n]x^n + a[n-1]x^{n-1} + \cdots + a[2]x^2 + a[1]x + a[0]$ *por anidadas sucesivas sumas y multiplicaciones como indicado en el siguiente paréntesis:*

$$((\cdots((a[n]x + a[n-1])x + a[n-2])x + \cdots + a[2])x + a[1])x + a[0].$$

En cada etapa, iniciando con a[*n*]*, el valor presente de valorpolinomio se multiplica por x y se suma el próximo coeficiente más bajo del polinomio.]*

Input: *n [un entero no-negativo], a*[0], *a*[1], *a*[2], . . . , *a*[*n*] *[un arreglo de números reales], x [un número real]*

Cuerpo del algoritmo:

polyval := *a*[*n*]
for *i* := 1 a *n*
  polyval := *polyval* · *x* + *a*[*n* − *i*]
next *i*
[En este punto
$valorpolinomio = a[n]x^n = a[n-1]x^{n-1} + \cdots + a[2]x^2 + a[1]x + a[0].]$

Salida: *valorpolinomio [un número real]*

40. Represente el algoritmo 11.3.4 para la entrada $n = 3$, $a[0] = 2$, $a[1] = 1$, $a[2] = -1$, $a[3] = 3$ y $x = 2$.

41. Represente el algoritmo 11.3.4 para la entrada $n = 2$, $a[0] = 5$, $a[1] = -1$, $a[2] = 2$ y $x = 3$.

H 42. Sea t_n = número de sumas y multiplicaciones que se deben efectuar cuando se ejecuta el algoritmo 11.3.4 para un polinomio de grado n. Exprese t_n como una función de n.

43. Use el teorema de órdenes de polinomios para encontrar un orden para el algoritmo 11.3.4. ¿Cómo se compara este orden con el del algoritmo 11.3.3?

Respuestas del autoexamen

1. Una iteración del bucle más interno 2. n 3. n^2; n^2

11.4 Funciones exponenciales y logarítmicas: gráficas y órdenes

Nunca deberíamos permitir ser persuadidos de la verdad de cualquier cosa a menos que se tenga la evidencia de nuestra propia razón. —René Descartes, 1596-1650

Las funciones exponencial y logarítmica son de gran importancia en matemáticas en general y en particular en ciencia computacional. Varios importantes algoritmos para computadora tienen tiempos de ejecución que implican funciones logarítmicas del tamaño de los datos de entrada (lo que significa que son relativamente eficientes para grandes conjuntos de datos) y algunos tiempos de ejecución que son funciones exponenciales del tamaño de los datos de entrada (lo que implica que son completamente ineficientes para grandes conjuntos de datos). Además, como las funciones exponencial y logarítmica surgen naturalmente en la descripción de muchos procesos de crecimiento, decaimiento y en el cálculo de muchos tipos de probabilidades, esas funciones se emplean en el análisis de sistemas que operan con computadoras, en la teoría de colas y en la teoría de la información.

Gráficas de funciones exponenciales

Como se define en la sección 7.2, la función exponencial con base $b > 0$ es la función que envía a cada número real x a b^x. En la figura 11.4.1 se muestra la gráfica de la función exponencial de base 2 (junto con una tabla parcial de sus valores). Observe que los valores de esta función incrementan con extraordinaria rapidez. Si intentamos continuar dibujando la gráfica usando la escala que se indica en la figura 11.4.1, tendríamos que dibujar el punto $(10, 2^{10})$ más de 21 pies sobre el eje horizontal. Y el punto $(30, 2^{30})$ estaría localizado a más de 610 080 millas sobre el eje horizontal, ¡más allá de la Luna!

x	2^x
0	$2^0 = 1$
1	$2^1 = 2$
2	$2^2 = 4$
3	$2^3 = 8$
–1	$2^{-1} = 0.5$
–2	$2^{-2} = 0.25$
–3	$2^{-3} = 0.125$
0.5	$2^{0.5} \cong 1.414$
–0.5	$2^{-0.5} \cong 0.707$

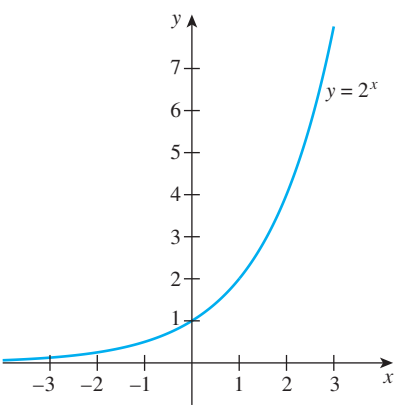
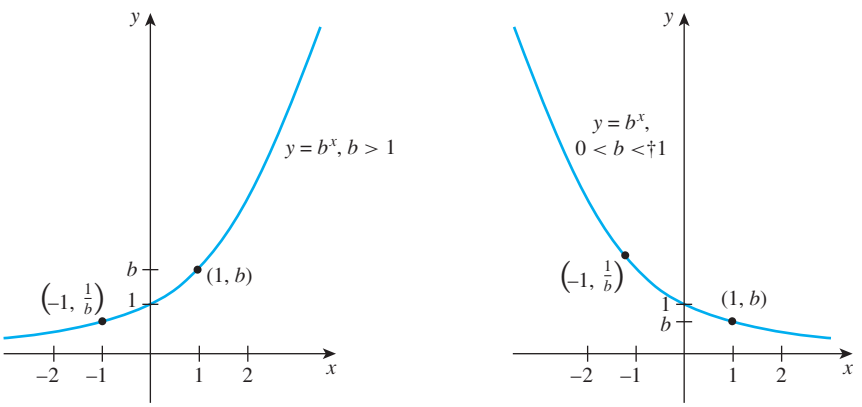


Figura 11.4.1 **La función exponencial de base 2**

La gráfica de cualquier función exponencial de base $b > 1$ tiene una forma que es similar a la gráfica de la función exponencial de base 2. Si $0 < b < 1$, entonces $1/b > 0$ y la gráfica de la función exponencial de base b es la reflexión, respecto al eje vertical, de la función exponencial de base $1/b$. En la figura 11.4.2 se muestran estos hechos.



Gráfica de la función exponencial de base $b > 1$

a)

Gráfica de la función exponencial de base b en donde $0 < b < 1$

b)

Figura 11.4.2 **Gráficas de funciones exponenciales**

Gráficas de funciones logarítmicas

Bettmann/CORBIS

John Naiper (1550-1617)

Los logaritmos se introdujeron por primera vez por el escocés John Napier. Los astrónomos y navegantes los encontraron muy útiles para reducir el tiempo necesario para multiplicar y dividir, así que rápidamente ganaron amplia aceptación y desempeñaron un papel crucial en el notable desarrollo de esas áreas en el siglo XVIII. Sin embargo, actualmente están disponibles en las computadoras y calculadoras electrónicas para realizar operaciones de manera rápida y confiable y así los logaritmos y las funciones logarítmicas se emplean principalmente como herramientas conceptuales.

Recordemos la definición de función logarítmica de base b dada en la sección 7.1. A continuación la establecemos formalmente

• Definición

Si b es un número real positivo no igual a 1, entonces la **función logarítmica de base** b, $\log_b$: $\mathbf{R}^+ \rightarrow \mathbf{R}$, es la función que envía a cada número real positivo x al número $\log_b x$, que es el exponente al que debemos elevar b para obtener x.

La función logarítmica de base b es, en efecto, la inversa de la función exponencial de base b. (Vea el ejercicio 10 al final de esta sección.) Se tiene de las gráficas de las dos funciones que son simétricas con respecto a la recta $y = x$. La gráfica de la función logarítmica de base $b > 1$ se muestra en la figura 11.4.3 de la siguiente página.

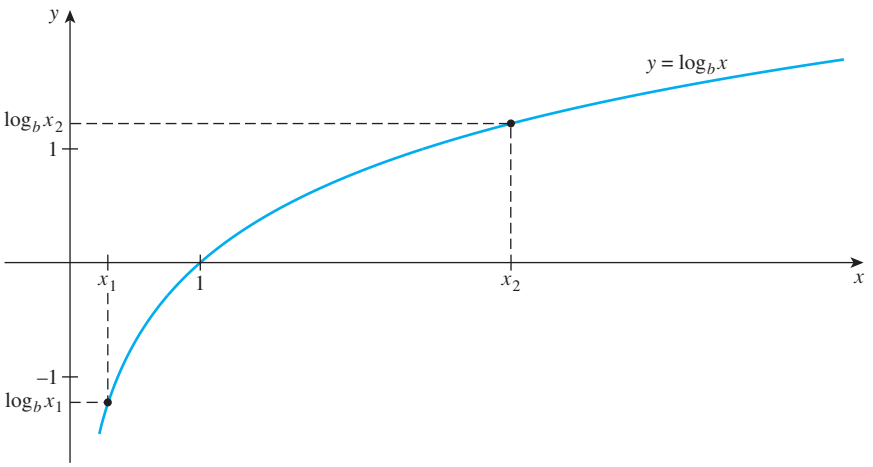


Figura 11.4.3 **La gráfica de la función logarítmica de base $b > 1$**

Si su base b es mayor que 1, entonces la función logarítmica es creciente. Analíticamente, esto significa que

si $b > 1$, entonces para todos los números positivos x_1 y x_2,

$$\text{si } x_1 < x_2 \text{ entonces } \log_b(x_1) < \log_b(x_2) \qquad 11.4.1$$

Nota Como ejemplos, $\log_2(1\,024)$ es sólo 10 y $\log_2(1\,048\,576)$ es exactamente 20.

La función exponencial tiene un rápido crecimiento, sin embargo, la función logarítmica es de muy lento crecimiento. Así que tiene que irse muy a la derecha sobre el eje horizontal para encontrar logaritmos de gran valor.

El siguiente ejemplo muestra cómo hacer uso de la naturaleza creciente de la función logarítmica de base 2 para deducir una propiedad notablemente útil.

Ejemplo 11.4.1 Logaritmos de base 2 de números entre dos potencias consecutivas de 2

Demuestre la siguiente propiedad:

a. Si k es un entero y x es un número real con

$$2^k \le x < 2^{k+1}, \text{ entonces } [\log_2 x] = k. \qquad 11.4.2$$

b. Describa la propiedad (11.4.2) en palabras y dé una interpretación gráfica de la propiedad para $x > 1$.

Solución

a. Suponga que k es un entero y que x es un número real con

$$2^k \le x < 2^{k+1}.$$

La función logarítmica de base 2 es creciente, lo cual implica que

$$\log_2(2^k) \le \log_2 x < \log_2(2^{k+1}).$$

Pero $\log_2(2^k) = k$ *[el exponente al que se debe elevar 2 para obtener 2^k es k]* y $\log_2(2^{k+1}) = k + 1$ *[por una razón similar]*. Así

$$k \le \log_2 x < k + 1.$$

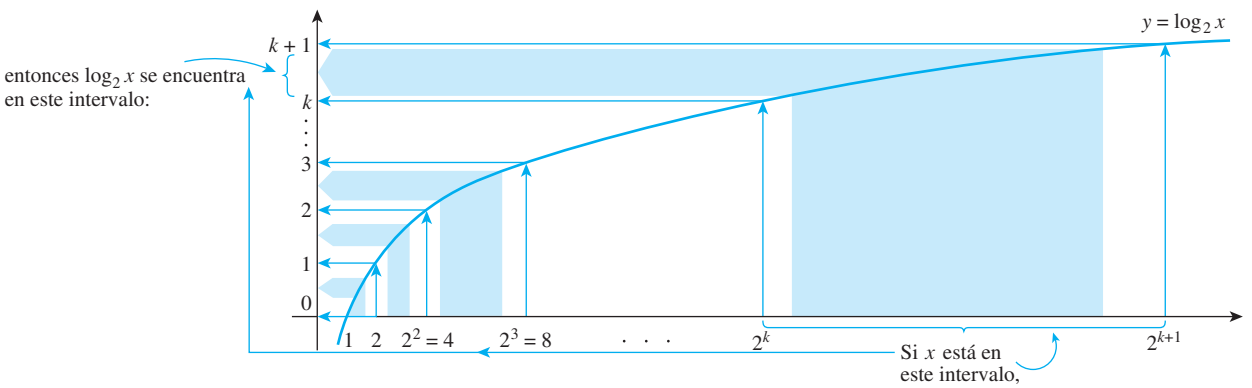
Por la definición de la función piso, entonces

$$\lfloor \log_2 x \rfloor = k.$$

b. Recuerde que el piso de un número positivo es su parte entera. Por ejemplo $\lfloor 2.82 \rfloor = 2$. Así la propiedad (11.4.2) se puede describir con palabras de la forma siguiente:

> Si x es un número positivo que descansa entre dos potencias enteras consecutivas de 2, entonces el piso del logaritmo en base 2 de x es el exponente de la potencia más pequeña de 2.

A continuación se presenta una representación gráfica:



Una consecuencia de la propiedad (11.4.2) que no parece particularmente importante en su propio derecho pero que se necesita con frecuencia puede ser descrita como un paso en el análisis de la eficiencia de un algoritmo.

Ejemplo 11.4.2 Cuando $\lfloor \log_2 (n-1) \rfloor = \lfloor \log_2 n \rfloor$

Demuestre la siguiente propiedad 11.4.3:

> Para cualquier entero impar $n > 1$, $\lfloor \log_2(n-1) \rfloor = \lfloor \log_2 n \rfloor$. 11.4.3

Solución Si n es un entero impar que es mayor que 1, entonces n se encuentra estrictamente entre dos potencias sucesivas de 2:

$$2^k < n < 2^{k+1} \quad \text{para algún entero } k > 0. \qquad 11.4.4$$

Se tiene que $2^k \leq n-1$ porque $2^k < n$ y 2^k y n son enteros. En consecuencia:

$$2^k \leq n-1 < 2^{k+1}. \qquad 11.4.5$$

Aplicando la propiedad (11.4.2) tanto a (11.4.4) como a (11.4.5) se obtiene

$$\lfloor \log_2 n \rfloor = k \quad \text{y también} \quad \lfloor \log_2(n-1) \rfloor = k.$$

Por tanto $\lfloor \log_2 n \rfloor = \lfloor \log_2(n-1) \rfloor$.

Aplicación: número de bits necesarios para representar a un entero en notación binaria

Dado un entero positivo n, ¿cuántos dígitos binarios se necesitan para representar a n? Para responder a esta pregunta, recordemos de la sección 5.4 que cualquier entero positivo n se puede escribir, de manera única, en la forma:

$$n = 2^k + c_{k-1}\cdot 2^{k-1} + \cdots + c_2\cdot 2^2 + c_1\cdot 2 + c_0,$$

donde k es un entero no-negativo y las cantidades $c_0, c_1, c_2, \ldots, c_{k-1}$ valen 0 o 1. Entonces la representación binaria de n es

$$1c_{k-1}c_{k-2}\cdots c_2c_1c_0,$$

y así el número de dígitos binarios necesarios para representar a n es $k + 1$.

¿Cómo se expresa a $k+1$ como una función de n? Observe que para toda i se tiene $c_i \le 1$, entonces

$$n = 2^k + c_{k-1}\cdot 2^{k-1} + \cdots + c_2\cdot 2^2 + c_1\cdot 2 + c_0 \le 2^k + 2^{k-1} + \cdots + 2^2 + 2 + 1.$$

Pero por la fórmula para la suma de una sucesión geométrica (teorema 5.2.3),

$$2^k + 2^{k-1} + \cdots + 2^2 + 2 + 1 = \frac{2^{k+1} - 1}{2 - 1} = 2^{k+1} - 1.$$

Así que, por transitividad de orden,

$$n \le 2^{k+1} - 1 < 2^{k+1} \qquad 11.4.6$$

En suma, para cada i se tiene que $c_i \ge 0$,

$$2^k \le 2^k + c_{k-1}\cdot 2^{k-1} + \cdots + c_2\cdot 2^2 + c_1\cdot 2 + c_0 = n. \qquad 11.4.7$$

Al juntar las desigualdades (11.4.6) y (11.4.7) se obtiene la doble desigualdad

$$2^k \le n < 2^{k+1}.$$

Pero entonces, por la propiedad (11.4.2),

$$k = \lfloor \log_2 n \rfloor.$$

Por tanto, el número de dígitos binarios necesarios para representar a n es $\lfloor \log_2 n \rfloor + 1$.

Ejemplo 11.4.3 Número de bits en una representación binaria

¿Cuántos dígitos binarios se requieren para representar a 52 837 en notación binaria?

Solución Si calcula el logaritmo en base 2 empleando la fórmula del teorema 7.2.1*a*) y una calculadora le da los valores aproximados de logaritmos de base 10, encuentra que

$$\log_2(52\ 837) \cong \frac{\log_{10}(52\ 837)}{\log_{10}(2)} \cong \frac{4.722938151}{0.3010299957} \cong 15.7.$$

Así la representación binaria de 52 837 tiene $\lfloor 15.7 \rfloor + 1 = 15 + 1 = 16$ dígitos binarios. ■

Aplicación: uso de logaritmos para resolver relaciones de recurrencia

En el capítulo 5 analizamos métodos para resolver relaciones de recurrencia. Una clase de relaciones de recurrencia que es muy importante en ciencia computacional tiene soluciones

que se pueden expresar en términos de logaritmos. En el siguiente ejemplo se estudia una relación de recurrencia de ese tipo.

Ejemplo 11.4.4 Relación de recurrencia con solución logarítmica

Se define, en forma recursiva, una sucesión $a_1, a_2, a_3, \ldots$ como sigue:

$$a_1 = 1,$$
$$a_k = 2a_{\lfloor k/2 \rfloor} \quad \text{para todos los enteros } k \geq 2.$$

a. Use iteración para suponer una fórmula explícita para esta sucesión.

b. Aplique inducción matemática fuerte para confirmar la validez de la fórmula que se obtuvo en el inciso *a*).

Solución

a. Se inicia la iteración para así encontrar los valores de los pocos primeros términos de la sucesión.

$$\begin{aligned}
a_1 &= 1 && 1 = 2^0\\
a_2 &= 2a_{\lfloor 2/2 \rfloor} = 2a_1 = 2\cdot 1 = 2 \Big\} && 2 = 2^1\\
a_3 &= 2a_{\lfloor 3/2 \rfloor} = 2a_1 = 2\cdot 1 = 2 \Big\}\\
a_4 &= 2a_{\lfloor 4/2 \rfloor} = 2a_2 = 2\cdot 2 = 4 \Big\} && 4 = 2^2\\
a_5 &= 2a_{\lfloor 5/2 \rfloor} = 2a_2 = 2\cdot 2 = 4 \Big\}\\
a_6 &= 2a_{\lfloor 6/2 \rfloor} = 2a_3 = 2\cdot 2 = 4 \Big\}\\
a_7 &= 2a_{\lfloor 7/2 \rfloor} = 2a_3 = 2\cdot 2 = 4 \Big\}\\
a_8 &= 2a_{\lfloor 8/2 \rfloor} = 2a_4 = 2\cdot 4 = 8 \Big\} && 8 = 2^3\\
a_9 &= 2a_{\lfloor 9/2 \rfloor} = 2a_4 = 2\cdot 4 = 8 \Big\}\\
&\vdots \qquad\qquad\qquad\qquad \vdots \Big\}\\
a_{15} &= 2a_{\lfloor 15/2 \rfloor} = 2a_7 = 2\cdot 4 = 8 \Big\}\\
a_{16} &= 2a_{\lfloor 16/2 \rfloor} = 2a_8 = 2\cdot 8 = 16 \Big\} && 16 = 2^4\\
&\vdots \qquad\qquad\qquad\qquad \vdots \Big\}
\end{aligned}$$

Observe que en cada caso cuando el subíndice n está entre dos potencias de 2, entonces a_n es igual a la potencia más pequeña de 2. Más precisamente:

$$\text{Si } 2^i \leq n < 2^{i+1}\text{, entonces } a_n = 2^i. \qquad 11.4.8$$

Pero n satisface la desigualdad

$$2^i \leq n < 2^{i+1},$$

entonces (por la propiedad 11.4.2)

$$i = \lfloor \log_2 n \rfloor.$$

Y sustituyendo en el enunciado (11.4.8) resulta

$$a_n = 2^{\lfloor \log 2\ n \rfloor}.$$

b. La siguiente demostración muestra que si $a_1, a_2, a_3, \ldots$ es una sucesión de números que satisfacen que

$$a_1 = 1, \text{ y } a_k = 2a_{\lfloor k/2 \rfloor} \quad \text{para todos los enteros } k \geq 2,$$

entonces la sucesión satisface la fórmula

$$a_n = 2^{\lfloor \log_2\ n \rfloor} \quad \text{para todos los enteros } n \geq 1.$$

Demostración:
Sea $a_1, a_2, a_3, \ldots$ la sucesión definida al especificar que $a_1 = 1$ y $a_k = 2a_{\lfloor k/2 \rfloor}$ para todos los enteros $k \geq 2$ y sea la propiedad $P(n)$ de la ecuación

$$a_n = 2^{\lfloor \log_2 n \rfloor}. \qquad \leftarrow P(n)$$

Usaremos inducción matemática fuerte para demostrar que $P(n)$ es verdadera para todos los enteros $n \geq 1$.

Demostración de que P* (1) *es verdadera: Por definición de $a_1, a_2, a_3, \ldots$, tenemos que $a_1 = 1$. Pero también tenemos el caso de que $2^{\lfloor \log_2 1 \rfloor} = 2^0 = 1$. Así $a_1 = 2^{\lfloor \log_2 1 \rfloor}$ y $P(1)$ es verdadera.

Demostración de que para todos los enteros k ≥ 1, si P(i) es verdadera para todos los enteros i de 1 a k, entonces P(k + 1) también es verdadera: Sea k cualquier entero con $k \geq 1$ y suponga que

$$a_i = 2^{\lfloor \log_2 i \rfloor} \text{ para todos los enteros } i \text{ con } 1 \leq i \leq k. \qquad \leftarrow \text{hipótesis de inducción}$$

Debe demostrar que

$$a_{k+1} = 2^{\lfloor \log_2 (k+1) \rfloor} \qquad \leftarrow P(k+1)$$

Considere los dos casos: k es par y k es impar.

Caso 1 (k es par): En este caso, $k + 1$ es impar y

$$\begin{aligned}
a_{k+1} &= 2a_{\lfloor (k+1)/2 \rfloor} && \text{por definición de } a_1, a_2, a_3, \ldots, \\
&= 2a_{k/2} && \text{porque } \lfloor (k+1)/2 \rfloor = k/2 \text{ ya que k + 1 es impar,} \\
&= 2 \cdot 2^{\lfloor \log_2 (k/2) \rfloor} && \text{por hipótesis de inducción ya que } k \text{ es par, } k \geq 2 \\
& && \text{y así } k/2 \geq 1, \\
&= 2^{\lfloor \log_2 (k/2) \rfloor + 1} && \text{por las leyes de los exponentes del álgebra (7.2.1),} \\
&= 2^{\lfloor \log_2 k - \log_2 2 \rfloor + 1} && \text{por la identidad } \log_b (x/y) = \log_b x - \log_b y, \text{ del} \\
& && \text{teorema 7.2.1,} \\
&= 2^{\lfloor \log_2 k - 1 \rfloor + 1} && \text{ya que } \log_2 2 = 1, \\
&= 2^{\lfloor \log_2 k \rfloor - 1 + 1} && \text{sustituyendo } x = \log_2 k \text{ en la identidad } \lfloor x - 1 \rfloor = \lfloor x \rfloor - 1 \\
& && \text{deducida en el ejercicio 15 de la sección 4.5,} \\
&= 2^{\lfloor \log_2 k \rfloor} && \\
&= 2^{\lfloor \log_2 (k+1) \rfloor} && \text{por la propiedad (11.4.3)}
\end{aligned}$$

Caso 2 (k es impar): El análisis de este caso es muy similar al realizado en el caso 1 y se deja como ejercicio 56 al final de la sección.

Entonces, en cualquier caso, $a_n = 2^{\lfloor \log_2 (k+1) \rfloor}$, que era lo que se quería demostrar. ■

Órdenes exponenciales y logarítmicas

Ahora consideremos la pregunta ¿cómo se comparan las gráficas de las funciones exponencial y logarítmica con las gráficas de funciones potencia? Resulta que para valores de x suficientemente grandes, la gráfica de la función logarítmica de cualquier base $b > 1$ está *abajo* de la gráfica de cualquier función potencia positiva y la gráfica de la función exponencial de cualquier base $b > 1$ está *arriba* de la gráfica de cualquier función potencia positiva. En términos analíticos, esto dice lo siguiente:

Para todos los números reales b y r con $b > 1$ y $r > 0$,

$\log_b x \leq x^r$ para todos los números reales x suficientemente grandes. 11.4.9

y $x^r \leq b^x$ para todos los números reales x suficientemente grandes. 11.4.10

Estos enunciados tienen las siguientes implicaciones para la notación O.

Para todos los números reales b y r con $b > 1$ y $r > 0$,

$$\log_b x \quad \text{es} \quad O(x^r) \tag{11.4.11}$$

y

$$x^r \quad \text{es} \quad O(b^x) \tag{11.4.12}$$

Otra importante función en el análisis de algoritmos es la función f definida por la fórmula

$$f(x) = x \log_b x \quad \text{para todos los números reales } x > 0.$$

Para grandes valores de x, la gráfica de esta función queda entre la gráfica de la función identidad y la gráfica de la función cuadrática. Más precisamente:

Para todos los números reales b con $b > 1$ y para todos los números reales x suficientemente grandes,

$$x \leq x \log_b x \leq x^2. \tag{11.4.13}$$

En la notación O estos hechos se expresan como:

Para todos los números reales $b > 1$,

$$x \text{ es } O(x \log_b x) \quad \text{y} \quad x \log_b x \text{ es } O(x^2) \tag{11.4.14}$$

No obstante que las demostraciones de algunos de esos hechos requiere cálculo, las demostraciones de algunos casos se pueden realizar utilizando el álgebra de desigualdades. (Vea los ejercicios al final de esta sección.) La figura 11.4.4 muestra las relaciones entre algunas funciones potencia, la función logarítmica de base 2, la función exponencial de base 2 y la función definida por la fórmula $x \to x \log_2 x$. Observe que se emplean diferentes escalas sobre los ejes horizontal y vertical.

El ejemplo 11.4.5 indica cómo utilizar desigualdades tales como (11.4.9), (11.4.10) y (11.4.13) para deducir órdenes adicionales implicando a la función logarítmica.

Ejemplo 11.4.5 Deducción de un orden a partir de desigualdades logarítmicas

Demuestre que $x + x \log_2 x$ es $\Theta(x \log_2 x)$.

Solución Primero observe que $x + x \log_2 x$ es $\Omega(x \log_2 x)$ ya que para todos los números reales $x > 1$,

$$x \log_2 x \quad \leq \quad x + x \log_2 x,$$

y como todas las cantidades son positivas,

$$|x \log_2 x| \quad \leq \quad |x + x \log_2 x|.$$

Sean $A = 1$ y $a = 1$. Entonces

$$A\,|x \log_2 x| \quad \leq \quad |x + x \log_2 x| \quad \text{para todas las } x > a.$$

Así, por definición de notación Ω,

$$x + x \log_2 x \quad \text{es} \quad \Omega(x \log_2 x).$$

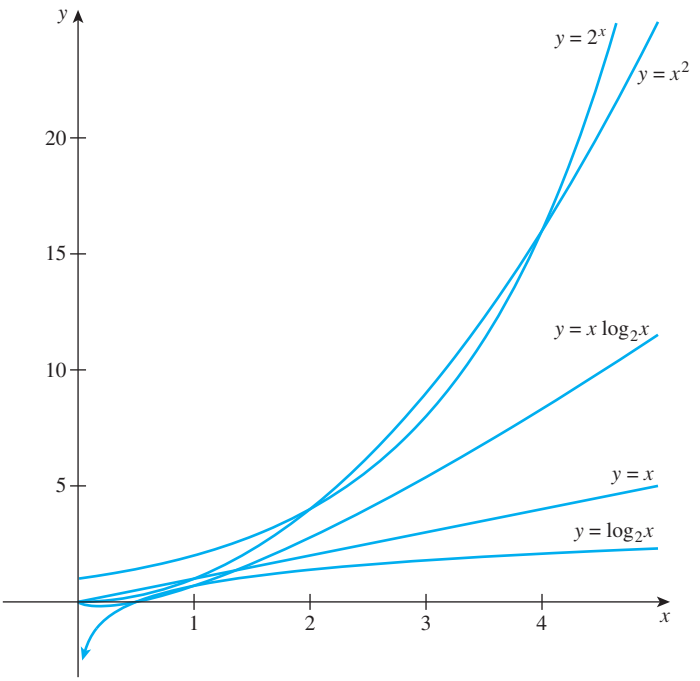


Figura 11.4.4 **Gráficas de algunas funciones logarítmicas, exponenciales y potencia**

Para demostrar que $x + x \log_2 x$ es $O(x \log_2 x)$, observe que de acuerdo a la propiedad (11.4.13) con $b = 2$, existe un número b tal que para toda $x > b$,

$$x < x \log_2 x$$
$$\Rightarrow \quad x + x \log_2 x < 2x \log_2 x \quad \text{sumando } x \log_2 x \text{ en ambos lados}$$

Así, si b se toma más grande que 2, entonces

$$|x + x \log_2 x| < 2|x \log_2 x| \quad \begin{array}{l}\text{porque cuando } x > 2, x \log_2 x > 0 \\ \text{y en consecuencia } |x + x \log_2 x| = x + x \log_2 x \text{ y} \\ \log_2 x = |x \log_2 x|.\end{array}$$

Sea $B = 2$. Entonces

$$|x + x \log_2 x| \leq B|x \log_2 x| \quad \text{para toda } x > b.$$

Por tanto, por definición de la notación O:

$$x + x \log_2 x \quad \text{es} \quad O(x \log_2 x).$$

Por tanto, como $x + x \log_2 x$ es $\Omega(x \log_2 x)$ y $x + x \log_2 x$ es $O(x \log_2 x)$, entonces por el teorema 11.2.1,

$$x + x \log_2 x \quad \text{es} \quad \Theta(x \log_2 x).$$ ■

El ejemplo 11.4.5 muestra un caso especial de un útil hecho general acerca de la notación O: *Si una función "domina" a otra (en el sentido de ser mayor para valores grandes de la variable), entonces la suma de las dos es O de la función dominante*. (Vea el ejercicio 49a, de la sección 11.2.)

El ejemplo 11.4.6 muestra que cualesquiera dos funciones logarítmicas de bases mayores que 1 tienen el mismo orden.

Ejemplo 11.4.6 Logaritmo de base b es Θ de logaritmo de base c

Demuestre que si b y c son números reales tales que $b > 1$ y $c > 1$, entonces $\log_b x$ es $\Theta(\log_c x)$.

Solución Suponga que b y c son números reales con $b > 1$ y $c > 1$. Para demostrar que $\log_b x$ es $\Theta(\log_c x)$, se deben encontrar números reales positivos A, B y k tales que

$$A|\log_c x| \le |\log_b x| \le B|\log_c x| \quad \text{para todos los números reales } x > k.$$

Por el inciso d) del teorema 7.2.1,

$$\log_b x = \frac{\log_c x}{\log_c b} = \left(\frac{1}{\log_c b}\right)\log_c x. \qquad (*)$$

Como $b > 1$ y la función logarítmica de base c es estrictamente creciente, entonces $\log_c b > \log_c 1 = 0$ y así también $\dfrac{1}{\log_c b} > 0$. Además, si $x > 1$, entonces $\log_b x > 0$ y $\log_c x > 0$. Por tanto, de la ecuación $(*)$ se tiene que

$$\left(\frac{1}{\log_c b}\right)\log_c x \le \log_b x \le \left(\frac{1}{\log_c b}\right)\log_c x \qquad (**)$$

para todos los números reales $x > 1$. Sean $A = \dfrac{1}{\log_c b}$, $B = \dfrac{1}{\log_c b}$ y $k = 1$. Entonces, debido a que todas las cantidades en $(**)$ son positivas,

$$A|\log_c x| \le |\log_b x| \le B|\log_c x| \quad \text{para todos los números reales } x > k.$$

Así, por definición de notación Θ,

$$\log_b x \quad \text{es} \quad \Theta(\log_c x). \qquad \blacksquare$$

El ejemplo 11.4.7 muestra cómo un orden logarítmico puede originarse en la determinación de un cierto tipo de suma, que requiere del siguiente hecho del cálculo:

El área bajo la gráfica de $y = 1/x$ entre $x = 1$ y $x = n$ es igual a $\ln n$, en donde $\ln n = \log_e n$. La figura 11.4.5 muestra este hecho.

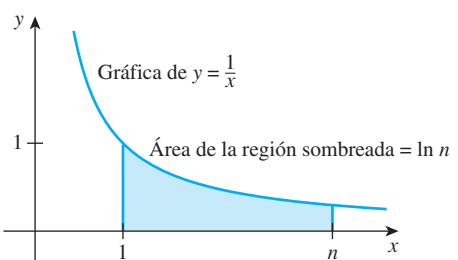


Figura 11.4.5 Área bajo la gráfica de $y = \dfrac{1}{x}$ entre $x = 1$ y $x = n$

Ejemplo 11.4.7 Orden de una suma armónica

Sumas de la forma $1 + \dfrac{1}{2} + \cdots + \dfrac{1}{n}$ se conocen como *sumas armónicas*. Las que ocurren en el análisis de varios algoritmos computacionales de ordenamiento rápido. Demuestre que $1 + \dfrac{1}{2} + \dfrac{1}{3} + \cdots + \dfrac{1}{n}$ es $\Omega(\ln n)$ realizando los pasos de la siguiente página:

a. Interprete la figura 11.4.6 para demostrar que

$$\frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} \leq \ln n.$$

y

$$\ln n \leq 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}.$$

b. Demuestre que si n es un entero que al menos es 3, entonces $1 \leq \ln n$.

c. De *a*) y *b*) deduzca que si el entero n es mayor o igual que 3, entonces

$$\ln n \leq 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} \leq 2 \ln n.$$

d. De *c*) deduzca que

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} \text{ es } \Theta(\ln n).$$

Solución

a. La figura 11.4.6 *a*) muestra rectángulos cuyas bases son los intervalos entre cada par de enteros de 1 a n y cuyas alturas son las alturas de la gráfica de $y = 1/x$ arriba de los puntos extremos de los intervalos de la derecha. La figura 11.4.6 *b*) muestra rectángulos con las mismas bases, pero cuyas alturas son las alturas de la gráfica sobre los puntos extremos de los intervalos de la izquierda.

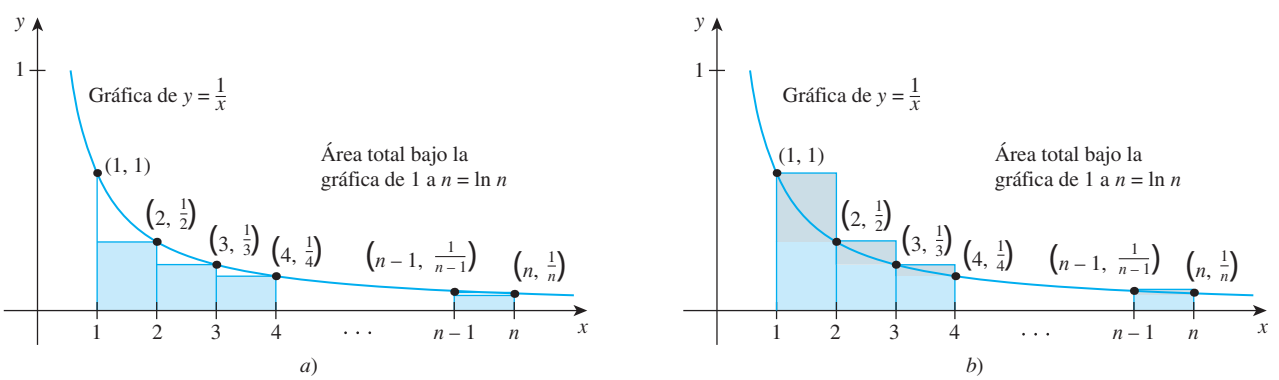


Figura 11.4.6

Ahora el área de cada rectángulo es su base por su altura. Como todos los rectángulos tienen base 1, el área de cada rectángulo es igual a su altura. Así en la figura 11.4.6 *a*),

el área del rectángulo de 1 a 2 es $\frac{1}{2}$;

el área del rectángulo de 2 a 3 es $\frac{1}{3}$;

$\vdots$

el área del rectángulo de $n - 1$ a n es $\frac{1}{n}$.

Así la suma de las áreas de todos los rectángulos es $\frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$. De la figura es claro que esta suma es menor que el área bajo la gráfica de f entre $x = 1$ y $x = n$, que es igual a $\ln n$. Es decir,

$$\frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} \leq \ln n.$$

Un análisis similar de las áreas de los rectángulos combinados azul y gris en la figura 11.4.6*b*), muestra que

$$\ln n \leq 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}.$$

b. Suponga que n es un entero con $n \geq 3$. Como $e \cong 2.718$, entonces $n \geq e$. La función logarítmica de base e es estrictamente creciente. Puesto que $e \leq n$, entonces $1 = \ln e \leq \ln n$.

c. Por el inciso *a*),

$$\frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} \leq \ln n,$$

y por el inciso *b*),

$$1 \leq \ln n.$$

Sumando estas dos desigualdades se obtiene

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} \leq 2 \ln n \quad \text{para cualquier entero } n \geq 3.$$

d. Juntando los resultados de los incisos *a*) y *c*) se llega a la conclusión de que para todos los enteros $n \geq 3$,

$$\ln n \leq 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} \leq 2 \ln n.$$

Y como todas las cantidades son positivas para $n \geq 3$,

$$|\ln n| \leq \left|1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}\right| \leq 2|\ln n|.$$

Sean $A = 1$, $B = 2$ y $k = 3$. Entonces

$$A|\ln n| \leq \left|1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}\right| \leq B|\ln n| \quad \text{para todo } n > k.$$

Así que por definición de notación Θ,

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} \quad \text{es} \quad \Theta(\ln n).$$

■

Autoexamen

1. El dominio de cualquier función exponencial es _____ y su rango es _____.
2. El dominio de cualquier función logarítmica es _____ y su rango es _____.
3. Si k es un entero y $2^k \leq x < 2^{k+1}$, entonces $\lfloor \log_2 x \rfloor =$ _____.
4. Si b es un número real con $b > 1$ y si x es un número real suficientemente grande, entonces cuando las cantidades x, x^2, $\log_b x$ y $x \log_b x$ son arregladas en orden creciente, el resultado es _____.
5. Si n es un entero positivo, entonces $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$ tiene orden _____.

Conjunto de ejercicios 11.4

Trace la gráfica de cada función definida en los ejercicios del 1 al 8.

1. $f(x) = 3^x$ para todos los números reales x.
2. $g(x) = \left(\frac{1}{3}\right)^x$ para todos los números reales x.
3. $h(x) = \log_{10} x$ para todos los números reales positivos x.
4. $k(x) = \log_2 x$ para todos los números reales positivos x.
5. $F(x) = \lfloor \log_2 x \rfloor$ para todos los números reales positivos x.

6. $G(x) = \lceil \log_2 x \rceil$ para todos los números reales positivos x.

7. $H(x) = x \log_2 x$ para todos los números reales positivos x.

8. $K(x) = x \log_{10} x$ para todos los números reales positivos x.

9. La escala de la gráfica que se muestra en la figura 11.4.1 es un cuarto de pulgada por cada unidad. Si se marca el punto $(2, 2^{64})$ sobre la gráfica de $y = 2^x$, ¿a cuántas millas estará sobre el eje horizontal? ¿Cuál es la razón de la altura del punto a la distancia tierra-sol? (Hay 12 pulgadas por pie y 5 280 pies por milla. En promedio, la tierra está aproximadamente a 93 000 000 millas del sol.)

($\frac{1}{4}$ pulgada $\cong$ 0.635 cm, 1 milla $\cong$ 0.62 km)

10. a. Use la definición de logaritmo para demostrar que $\log_b b^x = x$ para todos los números reales x.
b. Utilice la definición de logaritmo para demostrar que $b^{\log_b x} = x$ para todos los números reales positivos x.
c. Por el resultado del ejercicio 25 de la sección 7.3, si $f: X \to Y$ y $g: Y \to X$ son funciones y $g \circ f = I_X$ y $f \circ g = I_Y$, entonces f y g son funciones inversas. Use este resultado para demostrar que $\log_b$ y $\exp_b$ (la función exponencial de base b) son funciones inversas.

11. Sea $b > 1$.
a. Aplique el hecho de que $u = \log_b v \Leftrightarrow v = b^u$ para demostrar que un punto (u, v) está sobre la gráfica de la función logarítmica de base b si y sólo si (v, u), está sobre la gráfica de la función exponencial de base b.
b. Dibuje varios pares de puntos de la forma (u, v) y (v, u) sobre un sistema coordenado. Describa la relación geométrica entre las ubicaciones de los puntos en cada par.
c. Dibuje las gráficas de $y = \log_2 x$ y $y = 2^x$. Describa la relación geométrica entre esas gráficas.

12. Dé una interpretación gráfica de la propiedad (11.4.2) del ejemplo 11.4.1*a*) para $0 < x < 1$.

***H* 13.** Suponga que un número real positivo x satisface la desigualdad $10^m \leq x < 10^{m+1}$ en donde m es un entero. ¿Qué se puede inferir sobre $\lfloor \log_{10} x \rfloor$? Justifique su respuesta.

14. a. Demuestre que si x es un número real positivo y k es un entero no-negativo tal que $2^{k-1} < x \leq 2^k$, entonces $\lceil \log_2 x \rceil = k$.
b. Describa con palabras el enunciado que se demostró en el inciso *a*).

15. Si n es un entero impar y $n > 1$, es ¿$\lceil \log_2 (n-1) \rceil = \lceil \log_2 (n) \rceil$? Justifique su respuesta.

***H* 16.** Si n es un entero impar y $n > 1$, es ¿$\lceil \log_2 (n+1) \rceil = \lceil \log_2 (n) \rceil$? Justifique su respuesta.

17. Si n es un entero impar y $n > 1$, es ¿$\lfloor \log_2 (n+1) \rfloor = \lfloor \log_2 (n) \rfloor$? Justifique su respuesta.

En los ejercicios 18 y 19 indique cuántos dígitos binarios son necesarios para representar los números dados en notación binaria. Use el método que se muestra en el ejemplo 11.4.3.

18. 148 206 19. 5 067 329

20. En el libro se demostró que el número de dígitos binarios necesarios para representar un entero positivo n es $\lfloor \log_2 n \rfloor + 1$. ¿Esto también se puede dar como $\lceil \log_2 n \rceil$? ¿Por qué sí o por qué no?

En cada uno de los ejercicios 21 y 22, se especifica una sucesión por una relación de recurrencia y condiciones iniciales. En cada caso: *a*) use iteración para conjeturar una fórmula explícita para la sucesión; *b*) utilice inducción matemática fuerte para confirmar la validez de la fórmula que haya obtenido en el inciso *a*).

21. $a_k = a_{\lfloor k/2 \rfloor} + 2$, para todos los enteros $k \geq 2$
$a_1 = 1$.

22. $b_k = b_{\lceil k/2 \rceil} + 1$, para todos los enteros $k \geq 2$
$b_1 = 1$.

***H* 23.** Se define una sucesión $c_1, c_2, c_3, \ldots$, recursivamente como sigue:

$$c_1 = 0,$$
$$c_k = 2c_{\lfloor k/2 \rfloor} + k, \quad \text{para todos los enteros } k \geq 2.$$

Use inducción matemática fuerte para demostrar que $c_n \leq n^2$ para todos los enteros $n \geq 1$.

*** *H* 24.** Utilice inducción matemática fuerte para demostrar que para la sucesión del ejercicio 23, $c_n \leq n \log_2 n$, para todos los enteros $n \geq 4$.

Los ejercicios del 25 al 28 se refieren a las propiedades 11.4.9 y 11.4.10. Resuélvalos, ¡piense en grande!

25. Encuentre un número real $x > 3$ tal que $\log_2 x < x^{1/10}$.

26. Determine un número real $x > 1$ tal que $x^{50} < 2^x$.

27. Obtenga un número real $x > 2$ tal que $x < 1.0001^x$.

28. Use una graficadora o un programa de cómputo para encontrar dos distintos valores aproximados de x tal que $x = 1.0001^x$. ¿En qué intervalos aproximados es $x > 1.0001^x$? ¿En qué intervalos aproximados es $x < 1.0001^x$?

29. Utilice la notación Θ para expresar el siguiente enunciado:

$$|x^2| \leq |7x^2 + 3x \log_2 x| \leq 10|x^2|,$$

para todos los números reales $x > 2$.

Deduzca cada enunciado en los ejercicios del 30 al 33.

30. $2x + \log_2 x$ es $\Theta(x)$.

31. $x^2 + 5x \log_2 x$ es $\Theta(x^2)$.

32. $n^2 + 2^n$ es $\Theta(2^n)$.

***H* 33.** 2^{n+1} es $\Theta(2^n)$.

***H* 34.** Demuestre que 4^n no es $O(2^n)$.

Demuestre cada uno de los enunciados en los ejercicios del 35 al 40, suponiendo que n es una variable entera que toma valores enteros positivos. Utilice identidades de la sección 5.2 conforme se vayan necesitando.

35. $1 + 2 + 2^2 + 2^3 + \cdots + 2^n$ es $\Theta(2^n)$.

***H* 36.** $4 + 4^2 + 4^3 + \cdots + 4^n$ es $\Theta(4^n)$.

37. $2 + 2 \cdot 3^2 + 2 \cdot 3^4 + \cdots + 2 \cdot 3^{2n}$ es $\Theta(3^{2n})$.

38. $\dfrac{1}{5} + \dfrac{4}{5^2} + \dfrac{4^2}{5^3} + \cdots + \dfrac{4^n}{5^{n+1}}$ es $\Theta(1)$.

39. $n + \dfrac{n}{2} + \dfrac{n}{4} + \cdots + \dfrac{n}{2^n}$ es $\Theta(n)$.

40. $\dfrac{2n}{3} + \dfrac{2n}{3^2} + \dfrac{2n}{3^3} + \cdots + \dfrac{2n}{3^n}$ es $\Theta(n)$.

41. Cantidades de la forma

$$kn + kn \log_2 n \quad \text{para enteros positivos } k_1 \cdot k_2 \text{ y } n,$$

se presentan en ciencia computacional en el análisis del algoritmo de ordenamiento. Demuestre que para cualquier entero positivo k,

$$k_1 n + k_2 n \log_2 n \quad \text{es} \quad \Theta(n \log_2 n).$$

42. Calcule los valores de las sumas armónicas

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} \quad \text{para } n = 2, 3, 4 \text{ y } 5$$

43. Use el inciso *d*) del ejemplo 11.4.7 para demostrar que

$$n + \frac{n}{2} + \frac{n}{3} + \cdots + \frac{n}{n} \quad \text{es} \quad \Theta(n \ln n)$$

44. Utilice el hecho de que $\log_2 x = \left(\dfrac{1}{\log_e 2}\right) \log_e x$ y que $\log_e x = \ln x$, para todos los números positivos y el inciso *c*) del ejemplo 11.4.7 para demostrar que

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} \quad \text{es} \quad \Theta(\log_2 n)$$

45. a. Demuestre que $\lfloor \log_2 n \rfloor$ es $\Theta(\log_2 n)$.
b. Demuestre que $\lfloor \log_2 n \rfloor + 1$ es $\Theta(\log_2 n)$

46. Demuestre por inducción matemática que $n \leq 10^n$ para todos los enteros $n \geq 1$.

H 47. Demuestre por inducción matemática que $\log_2 n \leq n$ para todos los enteros $n \geq 1$.

H 48. Demuestre que si n es una variable que toma valores enteros positivos, entonces 2^n es $O(n!)$.

49. Sea n una variable que toma valores enteros positivos.
a. Demuestre que $n!$ es $O(n^n)$.
b. Use el inciso *a*) para demostrar que $\log_2(n!)$ es $O(n \log_2 n)$.
H c. Demuestre que $n^n \leq (n!)^2$ para todos los enteros $n \geq 2$.
d. Utilice el inciso *c*) para demostrar que $\log_2(n!)$ es $\Omega(n \log_2 n)$.
e. Aplique los incisos *b*) y *d*) para encontrar un orden para $\log_2 n!$

✶ 50. a. Para todos los números reales positivos u, $\log_2 u < u$. Use este hecho para demostrar que para cualquier entero positivo n, $\log_2 x < n\, x^{1/n}$ para todos los números reales $x > 0$.
b. Interprete el enunciado del inciso *a*) utilizando la notación O.

51. a. Para todos los números reales x, $x < 2^x$. Use este hecho para demostrar que para cualquier entero positivo n, $x^n < n^n 2^x$ para todos los números reales $x > 0$.
b. Interprete el enunciado del inciso *a*) empleando la notación O.

✶ 52. Para todos los números reales positivos u, $\log_2 u < u$. Aplique este hecho y el resultado del ejercicio 21, sección 11.1, para demostrar lo siguiente: Para todos los enteros $n \geq 1$, $\log_2 x < x^{1/n}$ para todos los números reales $x > (2n)^{2n}$.

53. Use el resultado del ejercicio 52 anterior para demostrar lo siguiente: Para todos los enteros $n \geq 1$, $x^n < 2^x$ para todos los números reales $x > (2n)^{2n}$.

En los ejercicios 54 y 55 se necesita la regla de L'Hôpital del cálculo.

54. a. Sea b cualquier número real mayor que 1. Aplique la regla de L'Hôpital e inducción matemática para demostrar que para todos los enteros $n \geq 1$,

$$\lim_{x \to \infty} \frac{x^n}{b^x} = 0.$$

b. Use el resultado del inciso *a*) y las definiciones de límite y de la notación O para demostrar que x^n es $O(b^x)$ para cualquier entero $n \geq 1$.

55. a. Sea b cualquier número real mayor que 1. Utilice la regla de L'Hôpital para demostrar que para todos los enteros $n \geq 1$,

$$\lim_{x \to \infty} \frac{\log_b x}{x^{1/n}} = 0.$$

b. Use el resultado del inciso *a*) y las definiciones de límite y de la notación O para demostrar que $\log_b x$ es $O(x^{1/n})$ para cualquier entero $n \geq 1$.

56. Complete la demostración en el ejemplo 11.4.4.

Respuestas del autoexamen

1. el conjunto de todos los números reales; el conjunto de todos los números reales positivos 2. el conjunto de todos los números reales positivos; el conjunto de todos los números reales, 3. k 4. $\log_b x < x < x \log_b x < x^2$ 5. $\ln x$ (o, equivalentemente, $\log_2 x$)

11.5 Aplicación: análisis de la eficiencia de un algoritmo II

Elige un número, cualquier número. —Donal O'Shea, 2007

¿Ha participado en el juego "adivina mi número"? Una persona piensa un número entre otros dos números, por ejemplo, entre 1 y 10 o 1 y 100 y usted trata de conocer qué número es empleando la mínima cantidad de intentos. Cada vez que propone un número, la persona le dice si está en lo correcto, muy abajo o demasiado arriba.

Si ha participado en este juego, probablemente haya descubierto la estrategia más eficiente: Al inicio sugerir un número muy cercano a la mitad entre los dos números dados. Si su propuesta fue alta, entonces el número está entre su primera sugerencia y el número dado más pequeño. Si su propuesta inicial fue baja, entonces el número está entre el primer número que dio y el número dado más grande. En cualquier caso, en su segunda propuesta elige un número tan cercano como sea posible a la mitad del nuevo rango en donde ya sabe que está el número buscado. Este proceso lo repite tantas veces como sea necesario para encontrar el número de la persona.

La técnica descrita previamente es un ejemplo de una estrategia general llamada **divide y vencerás**, la que funciona como sigue: Para resolver un problema, hay que reducirlo a un determinado número de problemas más pequeños del mismo tipo, los que a su vez se pueden reducir al mismo número dado de problemas más pequeños del mismo tipo y así sucesivamente hasta que se obtengan problemas más fácilmente solubles. En este caso, el problema de encontrar un número particular en un rango dado de números, se reduce en cada etapa a la búsqueda de un número particular en un rango de números aproximadamente la mitad del rango anterior.

Resulta que los algoritmos que emplean la estrategia de divide-y-vencerás, en general son muy eficientes y casi siempre tienen órdenes que implican funciones logarítmicas. En esta sección definimos el algoritmo de la *búsqueda binaria*, que es la formalización del juego "adivina mi número" previamente descrito y comparamos la eficiencia de búsqueda binaria con la búsqueda sucesiva analizada en la sección 11.3. Entonces desarrollamos un algoritmo divide-y-vencerás para ordenar, *ordenamiento por mezcla* y comparar su eficiencia con los ordenamientos por inserción y por selección, que fueron tratados en la sección 11.3.

Búsqueda binaria

Mientras que una búsqueda sucesiva se puede efectuar en un arreglo cuyos elementos están en cualquier orden, una búsqueda binaria sólo se puede realizar en un arreglo cuyos elementos están colocados en orden ascendente (o descendente). Dado un arreglo $a[1]$, $a[2], \ldots, a[n]$ de distintos elementos colocados en orden ascendente, considere el problema de intentar encontrar un elemento particular x en el arreglo.

Para usar búsqueda binaria, primero compare x con el "elemento medio" del arreglo. Si los dos son iguales, entonces la búsqueda fue exitosa. Si no coinciden, entonces como los elementos del arreglo están en orden ascendente, compare los valores de x y el elemento medio del subarreglo inferior (que consiste de todos los elementos del arreglo bajo el elemento medio inicial) o del superior (que consiste de todos los elementos del arreglo arriba del elemento medio inicial).

La búsqueda continúa mediante repetición de este proceso básico en subarreglos más y más pequeños. Y termina cuando ocurre una igualdad o cuando el subarreglo, al cual se le está aplicando la búsqueda ya no contiene elementos. La eficiencia del algoritmo es resultado del hecho de que en cada paso, la longitud del subarreglo a ser investigado es prácticamente la mitad de la longitud del subarreglo anterior. La figura 11.5.1 muestra este proceso.

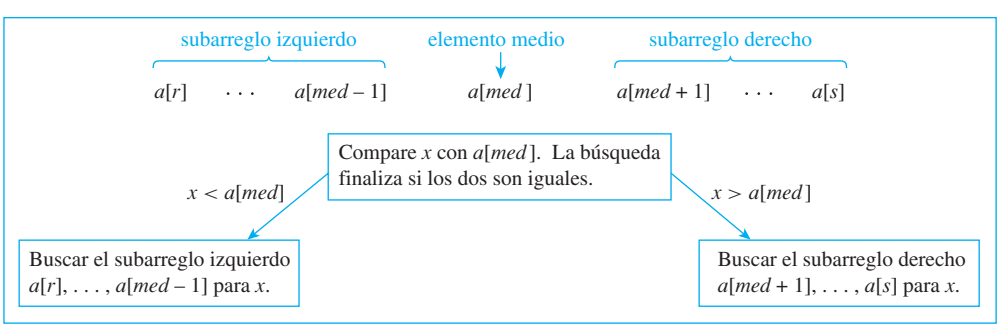


Figura 11.5.1 Una iteración del proceso de búsqueda binaria

Para escribir un algoritmo formal de búsqueda binaria, introducimos una variable *índice* cuyo valor final nos dirá si x está o no en el arreglo y si es así, indicará la ubicación de x. Como el arreglo va de $a[1]$ a $a[n]$, entonces *índice* queda inicializada en 0. Si se encuentra x, se cambia el valor de *índice* al subíndice del elemento del arreglo que coincide con x. Si *índice* mantiene el valor 0 cuando el algoritmo finaliza, entonces x no está en el arreglo. La figura 11.5.2 muestra la acción de una búsqueda binaria particular.

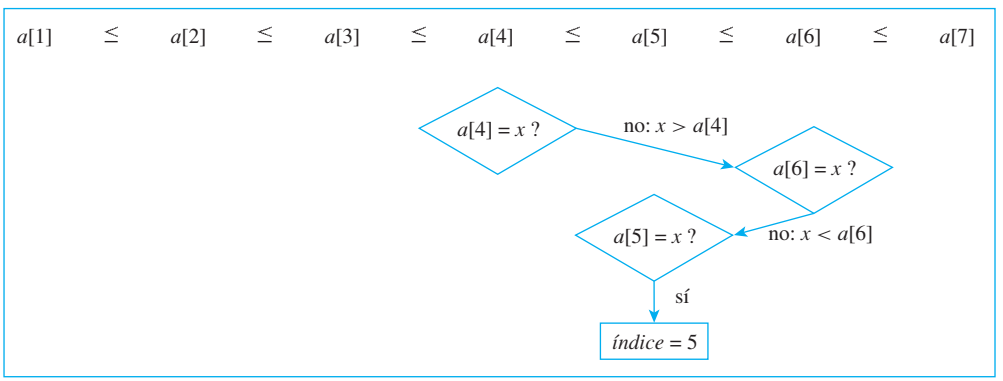


Figura 11.5.2 **Búsqueda binaria de x en $a[1], a[2], \ldots, a[7]$ en donde $x = a[5]$**

El formalizar un algoritmo de búsqueda binaria también requiere que seamos más precisos sobre el significado del "elemento medio" de un arreglo. (En la figura 11.5.2 este asunto fue dejado de lado al seleccionar n cuidadosamente). Si el arreglo consiste de un número par de elementos, hay dos elementos en la parte media. Por ejemplo, $a[6]$ y $a[7]$ están por igual en la parte media del siguiente arreglo.

$$\underbrace{a[3]\quad a[4]\quad a[5]}_{\text{tres elementos}}\quad \underbrace{a[6]\quad a[7]}_{\text{dos elementos medios}}\quad \underbrace{a[8]\quad a[9]\quad a[10]}_{\text{tres elementos}}$$

En un caso como este, el algoritmo debe elegir cuál tomar de los dos elementos medios, el más pequeño o el más grande. La opción es arbitraria, cualquiera que sea. Escribiremos el algoritmo para elegir el más pequeño. El índice del más pequeño de los dos elementos medios es el piso del promedio de los índices superior e inferior del arreglo. Es decir, si

$$inf = \text{el índice inferior del arreglo,}$$
$$sup = \text{el índice superior del arreglo} \quad \text{y}$$
$$med = \text{el menor de los dos índices medios del arreglo,}$$

entonces

$$med = \left\lfloor \frac{inf + sup}{2} \right\rfloor$$

En este caso, $inf = 3$ y $sup = 10$, así el índice del "elemento medio" es

$$med = \left\lfloor \frac{3 + 10}{2} \right\rfloor = \left\lfloor \frac{13}{2} \right\rfloor = \lfloor 6.5 \rfloor = 6.$$

El siguiente es un algoritmo formal para una búsqueda binaria.

Algoritmo 11.5.1 Búsqueda binaria

[El objetivo de este algoritmo es buscar un elemento x en un arreglo ascendente de elementos a[1], a[2], . . . , a[n]. Si se encuentra x, la variable índice es igual al índice del elemento del arreglo en donde x fue localizado. Si x no se encuentra, la variable índice continúa con su valor inicial, que es 0. Las variables inf y sup denotan los índices inferior y superior del arreglo bajo análisis].

Entrada: *n [un entero positivo], a[1], a[2], . . . , a[n] [un arreglo de datos dados en orden ascendente], x [un dato del mismo tipo de datos como los elementos del arreglo]*

Cuerpo del algoritmo

índice := 0, *inf* := 1, *sup* := *n*

[Calcule el índice medio del arreglo, med. Compare x con a[med]. Si los dos coinciden, la búsqueda ha sido exitosa. Si no, repita el proceso para el subarreglo inferior o superior ya sea dando a sup el nuevo valor med − 1 o dando a inf el nuevo valor med + 1. Cada iteración del bucle disminuye el valor de sup o incrementa el valor de inf. Así, si las iteraciones no son detenidas por el éxito en el proceso de búsqueda, eventualmente el valor de sup será menor que el valor de inf. Este hecho detiene el proceso iterativo e indica que x no es un elemento del arreglo.]

while (*sup* ≥ *inf* e *índice* = 0)

$$med := \left\lfloor \frac{inf + sup}{2} \right\rfloor$$

if *a*[*med*] = *x* **then** *índice* := *med*

if *a*[*med*] > *x*

then *sup* := *med* − 1

else *inf* := *med* + 1

end while

[Si índice tiene el valor 0 en este punto, entonces x no está en el arreglo. De otra forma, índice da el índice del elemento del arreglo en donde se localiza x.]

Salida: *índice [un entero no-negativo]*

Ejemplo 11.5.1 Seguimiento del algoritmo de búsqueda binaria

Siga la acción del algoritmo 11.5.1 sobre las variables *índice*, *inf*, *sup*, *med* y los valores de *x* dados en *a*) y *b*) para el arreglo de entrada

$$a[1] = \text{Ann}, a[2] = \text{Dawn}, a[3] = \text{Erik}, a[4] = \text{Gail}, a[5] = \text{Juan},$$
$$a[6] = \text{Matt}, a[7] = \text{Max}, a[8] = \text{Rita}, a[9] = \text{Tsuji}, a[10] = \text{Yuen}$$

donde se utiliza el ordenamiento alfabético para comparar elementos del arreglo.

a. $x = \text{Max}$ b. $x = \text{Sara}$

Solución

a.

índice	0				7
inf	1	6		7	
sup	10		7		
med		5	8	6	7

b.

índice	0			
inf	1	6	9	
sup	10			8
med		5	8	9

Eficiencia del algoritmo de búsqueda binaria

No es difícil la idea de deducir la eficiencia del algoritmo de búsqueda binaria. Aquí se presenta brevemente. En cada etapa del proceso de búsqueda binaria, la longitud del nuevo subarreglo por investigar es aproximadamente la mitad del anterior y en el peor caso, cada subarreglo se reduce a un subarreglo con un solo elemento, a buscar. En consecuencia, en el peor caso, el número máximo de iteraciones del bucle **while** en el algoritmo de búsqueda binaria es 1 más que el número de veces en que el arreglo original puede subdividirse aproximadamente a la mitad. Si la longitud n de este arreglo es una potencia de 2 ($n = 2^k$) para algún entero k), entonces n se puede subdividir exactamente $k = \log_2 n = \lfloor \log_2 n \rfloor$ veces antes de alcanzar un arreglo de longitud 1. Si n no es una potencia de 2, entonces $n = 2^k + m$ para algún entero k (en donde $m < 2^k$) y así n se puede subdividir aproximadamente k veces. Así en este caso, $k = \lfloor \log_2 n \rfloor$. Entonces en el peor caso, el número de iteraciones del bucle **while** en el algoritmo de búsqueda binaria, que es proporcional al número de comparaciones requeridas para ejecutarlo, es $\lfloor \log_2 n \rfloor + 1$. La deducción se concluye haciendo notar que $\lfloor \log_2 n \rfloor + 1$ es $O(\log_2 n)$.

Los detalles de la deducción son desarrollados en los ejemplos del 11.5.2 al 11.5.6. A través de la deducción, para cada entero $n \geq 1$, sea

w_n = número de iteraciones del bucle **while** en una ejecución del *peor caso* del algoritmo de búsqueda binaria para un arreglo de entrada de longitud n.

El primer punto a considerar es éste. Si se conoce la longitud del arreglo de entrada para una iteración del bucle **while**, entonces, ¿cuál es la longitud más grande posible del arreglo de entrada a la siguiente iteración?

Ejemplo 11.5.2 La longitud del arreglo de entrada a la siguiente iteración del bucle

Demuestre que si se introduce un arreglo de longitud k al bucle **while** del algoritmo de búsqueda binaria, entonces después de una iteración no exitosa del bucle, la entrada a la siguiente iteración es un arreglo de longitud a lo más $\lfloor k/2 \rfloor$.

Solución Considere qué ocurre cuando se introduce un arreglo de longitud k al bucle **while** en el caso en donde $x \neq a[med]$:

$$\underbrace{a[\text{inf}], a[\text{inf}+1], \ldots, a[\text{med}-1]}_{\text{nueva entrada al bucle while si } x < a[\text{med}]}, \quad \underbrace{a[\text{med}]}_{\text{elemento medio}}, \quad \underbrace{a[\text{med}+1], \ldots, a[\text{sup}-1], a[\text{sup.}]}_{\text{nueva entrada al bucle while si } x > a[\text{med}]}$$

Como el arreglo de entrada tiene longitud k, el valor de *med* depende de si k es impar o par. En ambos casos, acoplamos los elementos del arreglo con los enteros de 1 a k y analizamos las longitudes de los subarreglos izquierdo y derecho. En el caso de k impar, los subarreglos izquierdo y derecho tienen longitud $\lfloor k/2 \rfloor$. En el caso k par, el subarreglo izquierdo tiene longitud $\lfloor k/2 \rfloor - 1$ y el derecho tiene longitud $\lfloor k/2 \rfloor$. En la figura 11.5.3 se muestra el razonamiento implicado en estos resultados.

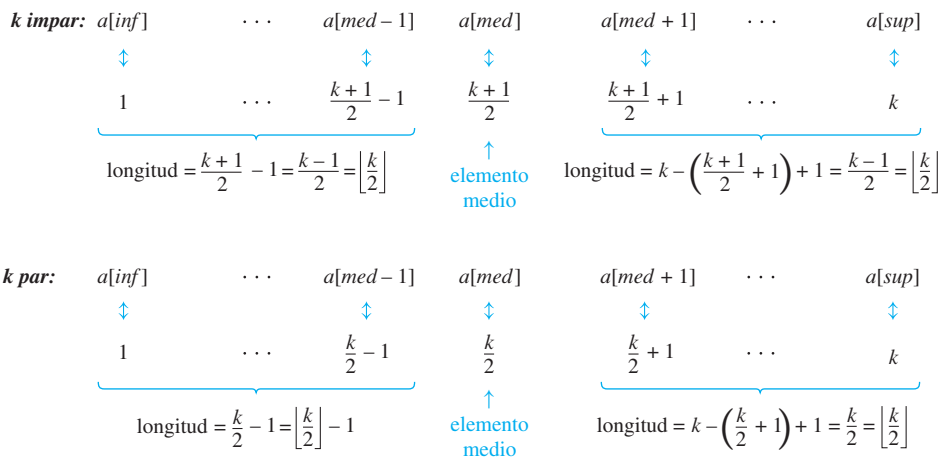


Figura 11.5.3 **Longitudes de los subarreglos izquierdo y derecho**

Como el máximo de los números $\lfloor k/2 \rfloor$ y $\lfloor k/2 \rfloor - 1$ es $\lfloor k/2 \rfloor$, en el peor caso ésta será la longitud del arreglo de entrada a la siguiente iteración del bucle. ■

Para encontrar el orden del algoritmo, se necesita una fórmula para $w_1, w_2, w_3, \ldots$. En el siguiente ejemplo se obtiene una relación de recurrencia para la sucesión.

Ejemplo 11.5.3 Una relación de recurrencia para $w_1, w_2, w_3, \ldots$

Demuestre que la sucesión $w_1, w_2, \ldots, w_n, \ldots$ satisface la relación de recurrencia y la condición inicial

$$w_1 = 1,$$
$$w_k = 1 + w_{\lfloor k/2 \rfloor} \text{ para todos los enteros } k > 1.$$

Solución El ejemplo 11.5.2 demostró que dado un arreglo de entrada de longitud k, al bucle **while**, lo peor que puede pasar es que la siguiente iteración del bucle tendrá que buscar un arreglo de longitud $\lfloor k/2 \rfloor$. Así el máximo número de iteraciones del bucle es 1 más que el máximo número necesario para ejecutar un arreglo de entrada de longitud $\lfloor k/2 \rfloor$. En símbolos

$$w_k = 1 + w_{\lfloor k/2 \rfloor}.$$

También
$$w_1 = 1$$

Porque para cada arreglo de entrada de longitud 1 ($inf = sup$), el bucle **while** itera sólo una vez. ■

Ahora que se ha encontrado una relación de recurrencia para $w_1, w_2, w_3, \ldots$, se puede emplear la iteración para sugerir una fórmula explícita.

Ejemplo 11.5.4 Una fórmula explícita para $w_1, w_2, w_3, \ldots$

Aplique iteración a la relación de recurrencia encontrada en el ejemplo 11.5.3 para inferir una fórmula explícita para $w_1, w_2, w_3, \ldots$.

Solución Inicie iterando para encontrar los valores de algunos primeros términos de la sucesión.

$$
\begin{aligned}
w_{①} &= ① && && 1 = 2^0;\ 1 = 0 + 1\\
w_{②} &= 1 + w_{\lfloor 2/2 \rfloor} = 1 + w_1 = 1 + 1 = ② && && 2 = 2^1;\ 2 = 1 + 1\\
w_3 &= 1 + w_{\lfloor 3/2 \rfloor} = 1 + w_1 = 1 + 1 = 2 && &&\\
w_{④} &= 1 + w_{\lfloor 4/2 \rfloor} = 1 + w_2 = 1 + 2 = ③ && && 4 = 2^2;\ 3 = 2 + 1\\
w_5 &= 1 + w_{\lfloor 5/2 \rfloor} = 1 + w_2 = 1 + 2 = 3 && &&\\
w_6 &= 1 + w_{\lfloor 6/2 \rfloor} = 1 + w_3 = 1 + 2 = 3 && &&\\
w_7 &= 1 + w_{\lfloor 7/2 \rfloor} = 1 + w_3 = 1 + 2 = 3 && &&\\
w_{⑧} &= 1 + w_{\lfloor 8/2 \rfloor} = 1 + w_4 = 1 + 3 = ④ && && 8 = 2^3;\ 4 = 3 + 1\\
w_9 &= 1 + w_{\lfloor 9/2 \rfloor} = 1 + w_4 = 1 + 3 = 4 && &&\\
&\vdots && \vdots &&\\
w_{15} &= 1 + w_{\lfloor 15/2 \rfloor} = 1 + w_7 = 1 + 3 = 4 && &&\\
w_{⑯} &= 1 + w_{\lfloor 16/2 \rfloor} = 1 + w_8 = 1 + 4 = ⑤ && && 16 = 2^4;\ 5 = 4 + 1\\
&\vdots && \vdots &&
\end{aligned}
$$

Observe que en cada caso cuando el subíndice n está entre dos potencias de 2, w_n es 1 más que el exponente de la menor potencia de 2. En otras palabras:

$$\text{Si } 2^i \le n < 2^{i+1}, \text{ entonces } w_n = i + 1 \qquad 11.5.1$$

Pero si $$2^i \le n < 2^{i+1},$$

entonces *[por la propiedad (11.4.2) del ejemplo 11.4.1]*

$$i = \lfloor \log_2 n \rfloor.$$

Sustituyendo en el enunciado (11.5.1) se infiere que

$$w_n = \lfloor \log_2 n \rfloor + 1. \qquad \blacksquare$$

Ahora puede emplearse inducción matemática para demostrar la validez de la fórmula encontrada en el ejemplo 11.5.4.

Ejemplo 11.5.5 Verificando la validez de la fórmula

Use inducción matemática fuerte para demostrar que si $w_1, w_2, w_3, \ldots$ es una sucesión de números que satisface la relación de recurrencia y la condición inicial

$$w_1 = 1 \quad \text{y} \quad w_k = 1 + w_{\lfloor k/2 \rfloor} \quad \text{para todos los enteros } k > 1,$$

entonces $w_1, w_2, w_3, \ldots$ satisface la fórmula

$$w_n = \lfloor \log_2 n \rfloor + 1 \quad \text{para todos los enteros } n \ge 1.$$

Solución Sea $w_1, w_2, w_3, \ldots$ la sucesión definida al especificar que $w_1 = 1$ y $w_k = 1 + w_{\lfloor k/2 \rfloor}$ para todos los enteros $k \ge 2$ y aceptemos que la propiedad $P(n)$ sea la ecuación

$$w_n = \lfloor \log_2 n \rfloor + 1. \qquad \leftarrow P(n)$$

Usaremos inducción matemática para demostrar que para todos los enteros $n \ge 1$, $P(n)$ es verdadera.

Demostración de que P(1) es verdadera: Por definición de $w_1, w_2, w_3,...$, tenemos que $w_1 = 1$. Pero este también es el caso para $\lfloor \log_2 1 \rfloor + 1 = 0 + 1 = 1$. Así $w_1 = \lfloor \log_2 1 \rfloor + 1$ y $P(1)$ es verdadera.

Demostración de que para todos los enteros $k \geq 1$, si $P(i)$ es verdadera para todos los enteros i de 1 a k, entonces $P(k+1)$ también es verdadera: Sea k cualquier entero con $k \geq 1$ y supongamos que

$$w_i = \lfloor \log_2 i \rfloor + 1 \quad \text{para todos los enteros } i \text{ con } 1 \leq i \leq k. \qquad \leftarrow \text{hipótesis de inducción}$$

Debemos demostrar que

$$w_{k+1} = \lfloor \log_2 (k+1) \rfloor + 1 \qquad \leftarrow P(k+1)$$

Consideremos los dos casos: k es par y k es impar.

Caso 1 (k es par): En este caso, $k+1$ es impar y

$$\begin{aligned}
w_{k+1} &= 1 + w_{\lfloor (k+1)/2 \rfloor} && \text{por definición de } w_1, w_2, w_3, \ldots, \\
&= 1 + w_{\lfloor k/2 \rfloor} && \text{porque } \lfloor (k+1)/2 \rfloor = k/2 \text{ ya que } k+1 \text{ es impar,} \\
&= 1 + \left(\lfloor \log_2 (k/2) \rfloor + 1 \right) && \text{por hipótesis de inducción porque ya que } k \text{ es par, } k \geq 2 \text{ y así } 1 \leq \lfloor k/2 \rfloor \leq k/2 < k \\
&= \lfloor \log_2 (k) - \log_2 2 \rfloor + 2 && \text{sustituyendo en la identidad } \log_b (x/y) = \log_b x - \log_b y \text{ y del teorema 7.2.1,} \\
&= \lfloor \log_2 (k) - 1 \rfloor + 2 && \text{porque } \log_2 2 = 1, \\
&= (\lfloor \log_2 (k) \rfloor - 1) + 2 && \text{sustituyendo } x = \log_2 (k) \text{ en la identidad } \lfloor x - 1 \rfloor = \lfloor x \rfloor - 1 \text{ deducida en el ejercicio 15, sección 4.5,} \\
&= \lfloor \log_2 (k+1) \rfloor + 1 && \text{por la propiedad (11.4.3) del ejemplo 11.4.2.>}
\end{aligned}$$

Caso 2(k es impar): En este caso, se puede demostrar que $w_k = \lfloor \log_2 k \rfloor + 1$. El análisis es muy similar al caso 1 y se deja como ejercicio 16 al final de la sección.

Así, sin importar si k es par o k es impar,

$$w_{k+1} = \lfloor \log_2 (k+1) \rfloor + 1,$$

que es lo que se quería demostrar. *[Como los pasos básico e inductivo se han probado, entonces queda completa la demostración por inducción matemática fuerte.]* ■

El ejemplo final muestra cómo usar la fórmula para $w_1, w_2, w_3, \ldots$ para encontrar un orden para el algoritmo, en el peor caso.

Ejemplo 11.5.6 El algoritmo de búsqueda binaria es logarítmico

Dado que por el ejemplo 11.5.5, para todos los enteros positivos n,

$$w_n = \lfloor \log_2 n \rfloor + 1,$$

demuestre que en el peor caso, el algoritmo de búsqueda binaria es $\Theta(\log_2 n)$.

Solución Para cualquier entero $n > 2$,

$$\begin{aligned}
& w_n = \lfloor \log_2 n \rfloor + 1 && \text{por el ejemplo 11.5.5,} \\
\Rightarrow \quad & \log_2 n \leq w_n \leq \log_2 n + 1 && \text{porque } x < \lfloor x \rfloor + 1 \text{ y } \lfloor x \rfloor \leq x \text{ para todos los números reales } x, \\
\Rightarrow \quad & \log_2 n \leq w_n \leq \log_2 n + \log_2 n && \text{puesto que el logaritmo en base 2 es creciente, si } 2 < n, \text{ entonces } 1 = \log_2 2 < \log_2 n. \\
\Rightarrow \quad & \log_2 n \leq w_n \leq 2 \log_2 n.
\end{aligned}$$

Tanto w_n como $\log_2 n$ son positivos para $n > 2$. Por tanto,

$$|\log_2 n| \leq |w_n| \leq 2|\log_2 n| \quad \text{para todos los enteros } n > 2.$$

Sean $A = 1$, $B = 2$ y $k = 2$. Entonces

$$A|\log_2 n| \leq |w_n| \leq B|\log_2 n| \quad \text{para todos los enteros } n > k.$$

Así que por definición de notación Θ,

$$w_n \text{ es } \Theta(\log_2 n).$$

Pero w_n, el número de iteraciones del bucle **while**, es proporcional al número de comparaciones efectuadas al ejecutar el algoritmo de búsqueda binaria. Entonces el algoritmo de búsqueda binaria es $\Theta(\log_2 n)$. ■

Los ejemplos del 11.5.2 al 11.5.6 muestran que en el peor caso, el algoritmo de búsqueda binaria tiene orden $\log_2 n$. Como se observó en la sección 11.3, en el peor caso el algoritmo de búsqueda sucesiva tiene orden n. Esta diferencia en eficiencia crece de manera importante conforme n aumenta. Suponiendo que una iteración del bucle se realiza cada nanosegundo, entonces al efectuar n iteraciones para $n = 100\,000\,000$ requiere 0.1 segundos, mientras que el hacer $\log_2 n$ iteraciones requiere 0.000000027 segundos. Para $n = 100\,000\,000\,000$ los tiempos son 1.67 minutos y 0.000000037 segundos, respectivamente. Y para $n = 100\,000\,000\,000\,000$, los respectivos tiempos son 27.78 horas y 0.000000047 segundos.

Ordenamiento por mezcla

Observe que es mucho más fácil escribir un algoritmo detallado para búsqueda sucesiva que para búsqueda binaria. Pero ésta es mucho más eficiente que la búsqueda sucesiva. Dicha situación ocurre frecuentemente en ciencia de la computación. Comúnmente, la solución "obvia" a un problema es menos eficiente que una inteligente solución que es más complicada en su descripción.

En el texto y en los ejercicios de la sección 11.3, dimos dos métodos para ordenamiento, por inserción y por selección, los cuales son formalizaciones de métodos que los seres humanos utilizan frecuentemente en situaciones ordinarias. ¿El enfoque de divide y vencerás puede emplearse para encontrar un método de ordenamiento más eficiente que esos? Resulta que la respuesta es un enfático "sí". En efecto, en algunas de las décadas pasadas, los científicos computacionales han desarrollado varios métodos de ordenamiento basados en divide y vencerás, los cuales son más complejos de describir pero son significativamente más eficientes que el de inserción o que el de selección.

Uno de esos métodos, **ordenamiento por mezcla**, se obtiene al pensar recursivamente. Imagine que ya se conoce una manera eficiente de ordenar arreglos de longitud menor que k. ¿Cómo se puede emplear dicho conocimiento para ordenar un arreglo de longitud k? Una manera es suponer que el arreglo de longitud k se divide en dos partes burdamente iguales y que cada parte es ordenada utilizando el método ya conocido. ¿Existe una manera eficiente de combinar las partes en un arreglo ordenado? Seguro. Sólo "mézclalos".

La figura 11.5.4 muestra cómo trabaja un mezcla. Imagine que los elementos de dos subarreglos ordenados, 2, 5, 6, 8 y 3, 6, 7, 9, están escritos en tarjetas de papel (para así moverlos con fácilmente). En un tablero coloque en dos columnas las tarjetas para cada subarreglo, una a la izquierda y una a la derecha. En el fondo del tablero, pone ocho posiciones en las que puedan moverse las tarjetas. Entonces, una a una, bajando las tarjetas al fondo de cada columna. En esa etapa compare los números de tarjetas sobre el fondo de las columnas y mueva la tarjeta con el número más pequeño a la próxima posición en el arreglo como un todo. Si en alguna etapa los dos números son iguales, tome, digamos, la tarjeta a la izquierda y muévala a la siguiente posición. Y si una de las columnas queda vacía en alguna etapa, sólo mueva en orden las tarjetas de la otra columna en posición una por una.

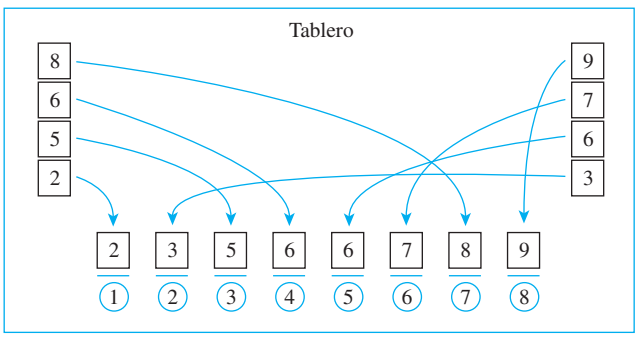


Figura 11.5.4 **Mezcla de dos subarreglos ordenados para obtener un arreglo ordenado**

Una observación importante acerca del algoritmo por mezcla previamente descrito: requiere memoria para mover los elementos del arreglo. Se necesita un segundo conjunto de posiciones del arreglo junto con el arreglo original, para así colocar en orden a los elementos de los dos subarreglos. En la figura 11.5.4 este segundo conjunto de posiciones se representa por las posiciones al fondo del tablero. De hecho, uno de los elementos del arreglo original se han colocado en este nuevo arreglo, se pueden mover de regreso, en orden, hacia las posiciones del arreglo original.

Sin embargo, en términos de tiempo, la mezcla es eficiente porque el número total de comparaciones necesario para mezclar dos subarreglos en un arreglo de longitud k es exactamente $k - 1$. Puede ver el porqué al analizar la figura 11.5.4. Observe que en cada etapa, la decisión sobre qué tarjeta mover se hace comparando los números sobre las tarjetas de los fondos de las dos columnas, excepto cuando una de las columnas está vacía, en cuyo caso no se realizan comparaciones. Así, en el peor caso habrá una comparación para cada una de las k posiciones en el arreglo final excepto el último (porque cuando se coloca la última tarjeta en posición, la otra columna seguramente estará vacía) o un total de $k - 1$ comparaciones.

El algoritmo de ordenamiento por mezcla es recursivo: sus enunciados de definición incluyen referencias a sí mismo. Sin embargo, el algoritmo está bien definido porque en cada etapa la longitud del arreglo que es introducida al algoritmo es más corta que en la etapa previa, así, finalmente, el algoritmo tiene que ocuparse sólo con arreglos de longitud 1, que ya están ordenados. Específicamente, el ordenamiento por mezcla funciona como sigue.

Dado un arreglo de elementos susceptibles de poder ser ordenados, si el arreglo consiste de un solo elemento, déjelo como está. Ya está ordenado. En casos diferentes:

1. Divida el arreglo en dos subarreglos de aproximadamente la misma longitud.
2. Use el ordenamiento por mezcla para ordenar cada subarreglo.
3. Mezcle entre sí a los dos subarreglos.

La figura 11.5.5 muestra un ordenamiento por mezcla en un caso particular.

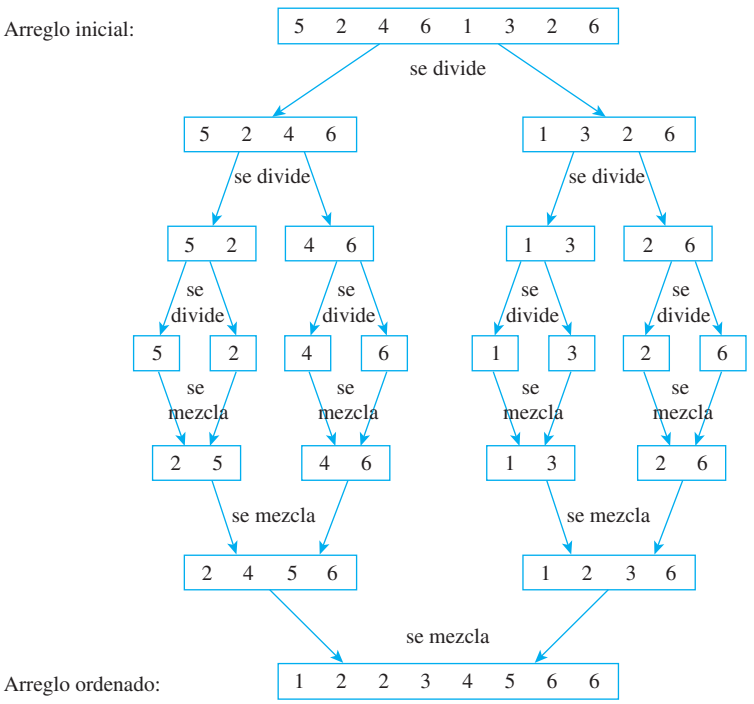


Figura 11.5.5 **Aplicando ordenamiento por mezcla al arreglo 5, 2, 4, 6, 1, 3, 2, 6**

Como en el caso del algoritmo de búsqueda binaria, con el fin de formalizar al ordenamiento por mezcla debemos decidir en exactamente qué punto dividir cada arreglo. Dado un arreglo que se denota por $a[inf], a[inf + 1], \ldots, a[sup]$ y sea $med = [(inf + sup)/2]$. Tome el subrreglo de la izquierda como $a[inf], a[inf + 1], \ldots, a[med]$ y el subarreglo de la derecha como $a[med + 1], a[med + 2], \ldots, a[sup]$. Lo siguiente es una versión formal de ordenamiento por mezcla.

Algoritmo 11.5.2 Ordenamiento por mezcla

[El objetivo de este algoritmo es tomar un arreglo de elementos $a[r], a[r + 1], \ldots, a[s]$(en donde $r \leq s$) para ordenarlo. El arreglo de salida se denota por $a[r], a[r + 1], \ldots, a[s]$, que tiene los mismos valores que el arreglo de entrada, pero en orden ascendente. El arreglo de entrada se divide en dos subarreglos de aproximadamente la misma longitud, cada uno de los cuales es ordenado usando ordenamiento por mezcla. Entonces los dos subarreglos son mezcla entre sí.]

Entrada: *r* y *s [enteros positivos con $r < s$] $a[r], a[r + 1], \ldots, a[s]$ [un arreglo de objetos datos que se pueden ordenar]*

Cuerpo del algoritmo:

$inf := r$, $sup := s$
while $(inf < sup)$
$med := \left\lfloor \frac{inf + sup}{2} \right\rfloor$
llame a **ordenamiento por mezcla** con entrada *inf*, *med* y $a[inf], a[inf + 1], \ldots, a[med]$
llame a **ordenamiento por mezcla** con entrada $med + 1$, *sup* y $a[med + 1], a[med + 2], \ldots, a[sup]$

[Después de que se han completado estos pasos, los arreglos a[inf], a[inf + 1], . . . , a[med] y a[med + 1], a[med + 2], . . . , a[sup] quedan ordenados.]
mezclar $a[inf], a[inf + 1], \ldots, a[med]$ y
$a[med + 1], a[med + 2], \ldots, a[sup]$
[Este paso se puede hacer con una llamada a un algoritmo de mezcla. Para poner el arreglo final en orden ascendente, el algoritmo de mezcla se debe escribir para tomar dos arreglos en orden ascendente y mezclarlos en un arreglo en orden ascendente].
end while
Salida: $a[r], a[r + 1], \ldots, a[s]$ *[un arreglo con los mismos elementos como el arreglo de entrada pero en orden ascendente]*

Para deducir la eficiencia de ordenamiento por mezcla, sea

$m_n =$ máximo número de comparaciones empleadas cuando se aplica ordenamiento por mezcla a un arreglo de longitud n.

Entonces $m_1 = 0$ porque ninguna comparación se emplea cuando se aplica el ordenamiento por mezcla a un arreglo de longitud 1. También, para cualquier entero $k > 1$, considere un arreglo $a[inf], a[inf + 1], \ldots, a[sup]$ de longitud k que se divide en dos subarreglos, $a[inf], a[inf + 1], \ldots, a[med]$ y $a[med + 1], a[med + 2], \ldots, a[sup]$, en donde $med = \lfloor (inf + sup)/2 \rfloor$. En el ejercicio 24 se le pide demostrar que el subarreglo derecho tiene longitud $\lfloor k/2 \rfloor$ y el arreglo izquierdo tiene longitud $\lceil k/2 \rceil$. Del análisis anterior del proceso de mezclado, se sabe que para mezclar dos subarreglos en un arreglo de longitud k, a lo más se necesitan $k - 1$ comparaciones.

En consecuencia,

$$\begin{bmatrix}\text{número de comparaciones cuando}\\ \text{se aplica el ordenamiento por}\\ \text{mezcla a un arreglo de longitud } k\end{bmatrix} = \begin{bmatrix}\text{número de comparaciones cuando}\\ \text{se aplica ordenamiento por mezcla}\\ \text{a un arreglo de longitud } \lfloor k/2 \rfloor\end{bmatrix} + \begin{bmatrix}\text{número de comparaciones cuando}\\ \text{se aplica ordenamiento por mezcla}\\ \text{a un arreglo de longitud } \lceil k/2 \rceil\end{bmatrix} + \begin{bmatrix}\text{número de comparaciones usadas}\\ \text{para mezclar dos subarreglos en}\\ \text{un arreglo de longitud } k\end{bmatrix}.$$

O, en otras palabras,

$$m_k = m_{\lfloor k/2 \rfloor} + m_{\lceil k/2 \rceil} + (k - 1) \quad \text{para todos los enteros } k > 1.$$

En el ejercicio 25 se le pide usar esta relación de recurrencia para demostrar que

$$\frac{1}{2} n \log_2 n \leq m_n \leq 2n \log_2 n \quad \text{para todos los enteros } n \geq 1.$$

Se tiene que por el ordenamiento por mezcla es $\Theta(n \log_2 n)$.

En el texto y en los ejercicios de la sección 11.3, probamos que el ordenamiento por inserción y por selección son $\Theta(n^2)$. ¿Qué tanta diferencia puede haber por el hecho de que el ordenamiento por mezcla es $\Theta(n \log_2 n)$? Si $n = 100\,000\,000$ y se utiliza una computadora para efectuar una operación cada nanosegundo, entonces el tiempo necesario para realizar $n \log_2 n$ operaciones es de alrededor de 2.7 segundos, mientras que el tiempo requerido para ejecutar n^2 operaciones es casi 115 días.

Problemas manejables e inmanejables

En un extremo opuesto de un algoritmo como la búsqueda binaria, que tiene orden logarítmico, está un algoritmo con orden exponencial. Por ejemplo, considere un algoritmo para

dirigir el movimiento de cada uno de los 64 discos en la Torre de Hanoi, conforme son transferidos uno por uno de un polo a otro. En la sección 5.7 probamos que tal transferencia requiere $2^{64} - 1$ pasos. Si a una computadora le toma un nanosegundo calcular cada paso de transferencia, entonces el tiempo total para calcular todos los pasos sería

$$(2^{64} - 1) \cdot \left(\frac{1}{10^9}\right) \cdot \left(\frac{1}{60}\right) \cdot \left(\frac{1}{60}\right) \cdot \left(\frac{1}{24}\right) \cdot \left(\frac{1}{365(25}\right) \cong 584 \text{ años.}$$

número de movimientos; movimientos por segundo; segundos por minuto; minutos por hora; horas por día; días por año

Problemas cuyas soluciones se pueden encontrar con algoritmos cuyo orden del peor caso con respecto al tiempo es un polinomio, se dice que son de **clase P**. Se les llama **algoritmos de tiempo polinomial** y se dice que son **manejables**. Problemas que no se pueden resolver en tiempo polinomial son llamados **inmanejables**. Para ciertos problemas, es posible comprobar la validez de una solución propuesta con un algoritmo de tiempo polinomial, pero no es posible encontrar una solución en tiempo polinomial. Se dice que tales problemas son de **clase NP**.* En ciencia de la computación teórica, la pregunta abierta más grande es si cada problema tipo NP pertenece a la clase P. Esta se conoce como el problema **P vs. NP**. El Instituto Clay, en Cambridge, Massachusetts, ha ofrecido un premio de $1 000 000 a quien demuestre o refute que P = NP.

En los años recientes, los científicos computacionales han definido un amplio conjunto de problemas, llamado **NP-completo**, perteneciente a la clase NP pero se piensa que no pertenece a la clase P. Lo que sí se sabe es que si uno de esos problemas es resuelto en tiempo polinomial, entonces así será con los todos los demás problemas. Uno de los problemas NP-completos, comúnmente conocido como el *problema del agente viajero*, fue analizado en la sección 10.2.

Una observación final acerca de la eficiencia de un algoritmo

Esta sección y la atención acerca de la eficiencia de un algoritmo han ofrecido solamente una vista parcial de los que está implicado al analizar un algoritmo computacional. Por ejemplo, se supone que las búsquedas y los ordenamientos ocurren en la memoria del ordenador. Búsquedas y ordenamientos basados en discos requieren diferentes algoritmos, no obstante que son similares los métodos para su análisis. Por otro lado, como mencionamos al inicio de la sección 11.3, la eficiencia en tiempo no es el único factor que importa al decidir qué algoritmo seleccionar. La cantidad de memoria requerida también es importante y hay técnicas matemáticas para estimar eficiencia espacial en forma similar a como se estima la eficiencia en tiempo. Además, conforme predomina el procesamiento en paralelo de los datos, se hace necesario modificar y ampliar los actuales métodos de análisis de algoritmos, para así aplicarlos a algoritmos diseñados para las nuevas tecnologías.

Autoexamen

1. Para resolver un problema empleando el algoritmo divide y vencerás, lo reduce a un determinado número de problemas más pequeños del mismo tipo, los cuales en sí mismos pueden ser _____ y así hasta _____.
2. Para analizar un arreglo utilizando en cada paso el algoritmo de búsqueda binaria, compare un elemento medio del arreglo con _____. Si el elemento medio es menor que _____, usted _____ y si el elemento medio es mayor que _____, usted _____.
3. El orden del peor caso del algoritmo de búsqueda binaria es _____.
4. Para ordenar un arreglo aplicando el algoritmo de ordenamiento por mezcla, en cada paso hasta el final divide el arreglo en dos secciones aproximadamente iguales y ordena cada sección empleando _____. Entonces usted _____ las dos secciones ordenadas.
5. El orden del peor caso del algoritmo de ordenamiento por mezcla es _____.

*Técnicamente hablando, un problema cuya solución se puede comprobar en una computadora ordinaria (o *máquina sucesiva determinista*) con un algoritmo de tiempo polinomial, se puede resolver en una *máquina sucesiva no-determinista* con un algoritmo de tiempo polinomial. Dichos problemas son llamados NP, lo que denota al *algoritmo de tiempo polinomial no-determinista*.

Conjunto de ejercicios 11.5

1. Aplique que $\log_2 10 \cong 3.32$ y que para todos los números reales a, $\log_2(10^a) = a \log_2 10$ para encontrar $\log_2 (1\,000)$, $\log_2 (1\,000\,000)$ y $\log_2 (1\,000\,000\,000\,000)$.

2. Suponga que un algoritmo requiere $c\lfloor \log_2 n \rfloor$ operaciones cuando se ejecuta con una entrada de tamaño n (en donde c es una constante).
   a. ¿En qué factor se incrementará el número de operaciones cuando el tamaño de entrada se aumenta de m a m^2 (en donde m es una potencia entera positiva de 2)?
   b. ¿En qué factor se incrementará el número de operaciones cuando el tamaño de entrada se aumenta de m a m^{10} (en donde m es una potencia positiva de 2)?
   c. Cuando n aumenta de 128 $(= 2^7)$ a 268 435 456 $(= 2^{28})$, ¿En qué factor se incrementa $c\lfloor \log_2 n \rfloor$?

Los ejercicios 3 y 4 muestran que para valores de n relativamente pequeños, los algoritmos con órdenes grandes pueden ser más eficientes que los algoritmos con órdenes pequeñas. Use una computadora o una graficadora para responder las preguntas.

3. ¿Para qué valores de n es un algoritmo, que requiere n operaciones, más eficiente que un algoritmo que necesita $\lfloor 50 \log_2 n \rfloor$ operaciones?

4. ¿Para qué valores de n es un algoritmo, que necesita $\lfloor n^2/10 \rfloor$ operaciones, más eficiente que un algoritmo que requiere $\lfloor n \log_2 n \rfloor$ operaciones?

En 5 y 6, indique la acción del algoritmo de búsqueda binaria (algoritmo 11.5.1) sobre las variables *índice*, *inf*, *sup*, *med* y los valores dados de x para el arreglo de entrada $a[1]$ = Chia, $a[2]$ = Doug, $a[3]$ = Jan, $a[4]$ = Jim, $a[5]$ = José, $a[6]$ = Mary, $a[7]$ = Rob, $a[8]$ = Roy, $a[9]$ = Sue, $a[10]$ = Usha, en donde el ordenamiento alfabético se emplea para comparar elementos del arreglo.

5. a. x = Chia b. x = Max

6. a. x = Amanda b. x = Roy

7. Suponga que *inf* y *sup* son enteros positivos con $inf \leq sup$. Considere el arreglo

$$a[inf],\ a\ [inf + 1], \ldots, a[sup].$$

   a. ¿Cuántos elementos hay en este arreglo?
   b. Demuestre que si el número de elementos en el arreglo es impar, entonces la cantidad $inf + sup$ es par.
   c. Demuestre que si el número de elementos en el arreglo es par, entonces la cantidad $inf + sup$ es impar.

Los ejercicios del 8 al 11 se refieren al siguiente segmento de algoritmo. Para cada entero positivo n, sea a_n el número de iteraciones del bucle **while.**

```
while (n > 0)
    n := n div 2
end while
```

8. Represente la acción de este segmento de algoritmo sobre n cuando el valor inicial de n es 27.

9. Encuentre una relación de recurrencia para a_n.

10. Obtenga una fórmula explícita para a_n.

11. Determine un orden para este segmento de algoritmo.

Los ejercicios del 12 al 15 están relacionados con el siguiente segmento de algoritmo. Para cada entero positivo n, sea b_n el número de iteraciones del bucle **while.**

```
while (n > 0)
    n := n div 3
end while
```

12. Siga la acción sobre n de este segmento de algoritmo cuando el valor inicial de n es 424.

13. Encuentre una relación de recurrencia para b_n.

***H* 14.** a. Use iteración para sugerir una fórmula explícita para b_n.
   b. Demuestre que si k es un entero y x es un número real con $3^k \leq x < 3^k$, entonces $\lfloor \log_3 x \rfloor = k$.
   c. Demuestre que para todos los enteros $m \geq 1$,

$$\lfloor \log_3(3m) \rfloor = \lfloor \log_3(3m + 1) \rfloor = \lfloor \log_3(3m + 2) \rfloor.$$

   d. Compruebe la validez de la fórmula que encontró en el inciso *a*).

15. Encuentre un orden para el segmento de algoritmo.

16. Complete la demostración del caso 2 del argumento de inducción fuerte del ejemplo 11.5.5. En otras palabras, demuestre que si k es un entero impar y $w_i = \lfloor \log_2 i \rfloor + 1$ para todos los enteros i con $1 \leq i \leq k$, entonces $w_{k+i} = \lfloor \log_2 k + 1 \rfloor + 1$.

Para los ejercicios del 17 al 19, modifique el algoritmo de búsqueda binaria (algoritmo 11.5.1) para tomar el mayor de los dos elementos medios del arreglo en caso de que el arreglo de entrada tenga longitud par. En otras palabras, en el algoritmo 11.5.1 reemplace

$$med := \left\lfloor \frac{inf + sup}{2} \right\rfloor \text{ con } med := \left\lceil \frac{inf + sup}{2} \right\rceil.$$

17. Indique el algoritmo de búsqueda binaria modificado para la misma entrada utilizada en el ejemplo 11.5.1.

18. Suponga que se introduce un arreglo de longitud k para el bucle **while** del algoritmo de búsqueda binaria modificado. Demuestre que después de una iteración del bucle, si $a[med] \neq x$, la entrada a la siguiente iteración es un arreglo de longitud a lo más $\lfloor k/2 \rfloor$.

19. Sea w_n el número de iteraciones del bucle **while** en una ejecución del peor caso del algoritmo de búsqueda binaria modificado para un arreglo de entrada de longitud n. Demuestre que $w_k = 1 + w_{\lfloor k/2 \rfloor}$ para $k \geq 2$.

En los ejercicios 20 y 21, dibuje un diagrama semejante al de la figura 11.5.4 para mostrar cómo mezclar los subarreglos dados en un solo arreglo en orden ascendente.

20. 3, 5, 6, 9, 12 y 2, 4, 7, 9, 11

21. F, K, L, R, U y C, E, L, P, W (orden alfabético)

En los ejercicios 22 y 23, dibuje un diagrama similar al de la figura 11.5.5 para mostrar cómo funciona el ordenamiento por mezcla para los arreglos de entrada dados.

22. R, G, B, U, C, F, H, G (orden alfabético)

23. 5, 2, 3, 9, 7, 4, 3, 2

24. Demuestre que dado un arreglo $a[inf], a[inf+1], \ldots, a[sup]$ de longitud k, si $med = \lfloor (inf + sup)/2 \rfloor$ entonces
    a. el subarreglo $a[med+1], a[med+2], \ldots, a[sup]$ tiene longitud $\lfloor k/2 \rfloor$.
    b. el subarreglo $a[inf], a[inf+1], \ldots, a[med]$ tiene longitud $\lceil k/2 \rceil$.

***H* 25.** La relación de recurrencia para $m_1, m_2, m_3, \ldots$, que surge en el cálculo de la eficiencia de ordenamiento por mezcla, es

$$m_1 = 0$$
$$m_k = m_{\lfloor k/2 \rfloor} + m_{\lceil k/2 \rceil} + k - 1.$$

Demuestre que para todos los enteros $n \geq 1$,

a. $\frac{1}{2} n \log_2 n \leq m_n$ b. $m_n \leq 2n \log_2 n$

26. Podría pensar que se necesitan $n - 1$ multiplicaciones para calcular x^n, puesto que

$$x^n = \underbrace{x \cdot x \cdots x}_{n-1 \text{ multiplicaciones}}.$$

Pero observe que, por ejemplo, como $6 = 4 + 2$,

$$x^6 = x^4 x^2 = (x^2)^2 x^2.$$

Así x^6 puede calcularse empleando tres multiplicaciones: una para obtener x^2, una para determinar $(x^2)^2$ y una más para multiplicar x^2 veces a $(x^2)^2$. Similarmente, como $11 = 8 + 2 + 1$,

$$x^{11} = x^8 x^2 x^1 = ((x^2)^2)^2 x^2 x$$

y así x^{11} se puede calcular usando cinco multiplicaciones: una para obtener x^2, una para determinar $(x^2)^2$, una para calcular $((x^2)^2)^2$, una para multiplicar $((x^2)^2)^2$ veces por x^2 y una para multiplicar ese producto por x.

a. Escriba un algoritmo para tomar un número real x y un entero positivo n y que calcule x^n:
   (i) llamando al algoritmo 5.1.1 para encontrar la representación binaria de n:

   $$(r[k]r[k-1] \cdots r[0])_2,$$

   en donde cada $r[i]$ es 0 o 1;
   (ii) calculando $x^2, x^{2^2}, x^{2^3}, \ldots, x^{2^k}$ elevando al cuadrado, después elevando al cuadrado otra vez y así sucesivamente,
   (iii) calculando x^n empleando el hecho de que

   $$x^n = x^{r[k]2^k + \cdots + r[2]2^2 + r[1]2^1 + r[0]2^0}$$
   $$= x^{r[k]2^k} \cdots x^{r[2]2^2} \cdot x^{r[1]2^1} \cdot x^{r[0]2^0}$$

b. Demuestre que el número de multiplicaciones efectuadas por el algoritmo del inciso *a*) es menor o igual que $2\lfloor \log_2 n \rfloor$.

Respuestas del autoexamen

1. reducido al mismo número finito de problemas más pequeños del mismo tipo; obtener problemas fácilmente solubles 2. el elemento que está buscando; el elemento que está buscando; aplique el algoritmo de búsqueda binaria a la mitad inferior del arreglo; el elemento que está buscando; aplique el algoritmo de búsqueda binaria a la mitad superior del arreglo 3. $\log_2 n$, en donde n es la longitud del arreglo 4. ordenamiento por mezcla; mezcla 5. $n \log_2 n$

CAPÍTULO 12

EXPRESIONES REGULARES Y AUTÓMATAS DE ESTADO-FINITO

Los fundamentos teóricos de la ciencia computacional provienen de varias disciplinas: lógica (fundamentos de las matemáticas), ingeniería eléctrica (el diseño de circuitos), investigación cerebral (modelos de neuronas) y lingüística (especificación formal de lenguajes).

Como se analizó brevemente en las secciones 6.4 y 7.4, la década de los 1930 vio el desarrollo de tratamientos matemáticos para cuestiones básicas concernientes a lo que se puede demostrar en matemáticas y a lo que se puede calcular mediante una sucesión finita de operaciones mecanizadas. No obstante que las primeras computadoras digitales fueron construidas hasta inicios de 1940, Alan Turing desarrolló, 10 años antes, un simple modelo abstracto de una máquina, ahora llamada máquina de Turing, con la cual él definió lo que significa que una función sea computable.

Por la misma época, se desarrollaron modelos de computación similares por americanos expertos en lógica, a saber, Alonzo Church, Stephen C. Kleene y Emil Post (nació en Polonia pero desde muy pequeño emigró a EUA), pero Church y otros mostraron que todos estos modelos eran equivalentes. Como un resultado, Church formuló una conjetura, ahora conocida como **tesis de Church-Turing**, asegurando que la máquina de Turing es universal en el sentido de que cualquier cosa que se pueda calcular en una máquina también es calculable con una máquina de Turing. Si esta tesis es correcta —y se cree que sí lo es— entonces todas las computadoras que se han fabricado o las que serán construidas son teóricamente equivalentes en lo que ellas pueden hacer, no obstante que puedan diferir ampliamente en velocidad y capacidad de almacenamiento. Por ejemplo, las computadoras cuánticas pueden tener la capacidad de calcular ciertas cantidades de manera enormemente más rápida que las computadoras clásicas. Pero la tesis de Church implica que la teoría de la computación es muy factible de permanecer fundamentalmente igual, no obstante que la tecnología esté sujeta a un cambio constante.

En los inicios de 1940, Warren S. McCulloch y Walter Pitts, trabajando en el Instituto tecnológico de Massachusetts (M.I.T)., desarrollaron un modelo de cómo podrían funcionar las neuronas en el cerebro y estudiaron cómo se podrían combinar los modelos de neuronas para hacer "circuitos" o "autómatas" capaces de cálculos más complicados. Hasta cierto punto, fueron influenciados por los resultados de Claude Shannon, quien también laboró en el M.I.T. y que en la década de los años 30 había desarrollado los fundamentos de una teoría que utilizaba funciones Booleanas como interruptores circuitales. En los años 50, Kleene analizó el trabajo de McCulloch y de Pitts y lo conectó con versiones de los modelos de máquinas introducidos por Turing y otros.

Otro desarrollo de los años 50 fue la introducción de lenguajes computacionales de alto nivel. Durante los mismos años, los intentos del lingüista Noam Chomsky por entender los principios subyacentes por medio de los cuales los seres humanos generan palabras lo llevó a desarrollar una teoría de lenguajes formales, que definió empleando conjuntos de reglas

abstractas, llamadas *gramáticas,* de diversos niveles de complejidad. Pronto se captó la gran utilidad de la teoría de Chomsky en el análisis y construcción de los lenguajes computacionales. Para la ciencia de la computación, las más útiles de las clasificaciones de lenguajes de Chomsky también son las más simples: los *regulares* y los *libres de contexto*.

Los lenguajes regulares, que se definen por *expresiones regulares*, se emplean extensamente para igualar patrones dentro de un texto (como en un procesador de palabras o en búsquedas por internet) y para el análisis léxico en compiladores de lenguajes computacionales. Ellos son parte de sofisticados editores de texto y un cierto número de utilerías en UNIX* y también se emplean en transformación de documentos XML†.

A través del uso de la notación Backus-Naur (introducida en la sección 10.5), los lenguajes libres de contexto permiten describir muchos de los más complejos aspectos de los modernos lenguajes computacionales de alto nivel y forman la base de la parte principal de los compiladores, que traducen programas escritos en un lenguaje de alto nivel en un código de máquina que sea conveniente para su ejecución.

Un hecho notable es que todos los temas previamente comentados están relacionados. Cada gramática libre de contexto resulta ser equivalente a un tipo de autómata llamado *autómata de empuje hacia abajo y* cada expresión regular resulta equivalente a un tipo de autómata llamado *autómata de estado-finito*. En este capítulo, nos enfocamos en el estudio de lenguajes regulares y autómatas de estado-finito, dejando el tópico de gramáticas libres de contexto y sus autómatas equivalentes para un curso posterior sobre construcción de compiladores o teoría de autómatas.

12.1 Lenguajes formales y expresiones regulares

La mente tiene medios finitos pero hace uso ilimitado de ellos, en maneras específicas y organizadas. Es decir, el problema central del lenguaje que ésta hizo posible encarar [mediados del siglo XX]. —Noam Chomsky, 1998

Fotografía de Norman Lenburg, 1979. Cortesía University of Wisconsin-Madison Archives.

Noam Chomsky (nacido en 1928)

Una frase en inglés se puede considerar como una cadena de palabras y una palabra en inglés se puede considerar como una cadena de letras. No toda la cadena de letras es una palabra legítima y no toda cadena de palabras es una frase gramatical. Podríamos decir que una palabra es legítima si se puede encontrar en un diccionario completo de inglés y que una frase es gramatical si satisface las reglas en un libro común de gramática inglesa.

Los lenguajes computacionales son similares al inglés en que ciertas cadenas de caracteres son palabras legítimas del lenguaje y ciertas cadenas de palabras pueden juntarse de acuerdo a determinadas reglas para formar programas sintáxicamente correctos. Un compilador para un lenguaje computacional analiza el flujo de caracteres en un programa primero para reconocer las palabras individuales y las unidades de la frase (a esta parte del compilador se le llama escáner léxico), después analiza la sintaxis o gramática, de las frases (a esta parte se le llama analizador sintáxico) y finalmente para traducir las frases en código de máquina (esta parte se le llama generador de códigos).

En ciencia computacional se probó que es útil ver a los lenguajes desde un punto de vista muy abstracto como cadenas de ciertas unidades fundamentales, permitiendo que cualquier conjunto finito de símbolos se pueda emplear como un alfabeto. Es común denotar a un alfabeto por la letra griega sigma mayúscula Σ. (Es decir, el mismo símbolo utilizado para representar una suma, pero ambos conceptos no tienen otra conexión.)

La definición de una *cadena de caracteres de un alfabeto* Σ (o una cadena sobre Σ) es una generalización de la definición de cadena previamente analizada. Un *lenguaje formal en un alfabeto* es cualquier conjunto de caracteres del alfabeto. Esas definiciones se presentan formalmente en la siguiente página.

*UNIX es un sistema operativo que se desarrolló en 1969 por Kenneth Thompson en los laboratorios Bell. Posteriormente fue reescrito en el lenguaje de Dennis Ritchie, que también fue desarrollado en dichos laboratorios.

†XML es una norma para lenguajes utilizados en aplicaciones de internet.

Alfabeto Σ:	un conjunto finito de caracteres.
Cadena sobre Σ:	1) una sucesión finita de elementos (llamados **caracteres**) de Σ o 2) la cadena nula ϵ.
Longitud de una cadena sobre Σ:	El número de caracteres que forman la cadena, con la cuerda nula teniendo longitud 0.
Lenguaje formal sobre Σ:	un conjunto de cadenas sobre el alfabeto.

Observe que el conjunto vacío satisface el criterio para ser un lenguaje formal. En ciertas situaciones técnicas resulta conveniente permitir que el conjunto vacío sea un lenguaje formal.

Ejemplo 12.1.1 Ejemplos de lenguajes formales

Sea el alfabeto $\Sigma = \{a, b\}$.

a. Defina un lenguaje L_1 sobre Σ: es el conjunto de todas las cadenas que empiezan con el carácter a y como longitud tienen a lo más tres caracteres. Encuentre L_1.

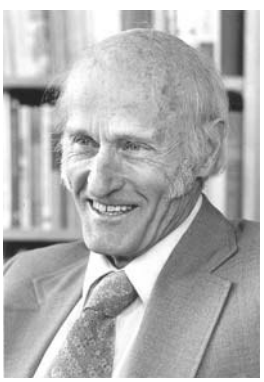
b. Un **palíndromo** es una cadena que parece la misma si se invierte el orden de sus caracteres. Por ejemplo, *aba* y *baab* son palíndromos. Defina un lenguaje L_2 sobre Σ: es el conjunto de todos los palíndromos obtenidos empleando los caracteres de Σ. Escriba diez elementos de L_2.

Solución

a. $L_1 = \{a, aa, ab, aaa, aab, aba, abb\}$.

b. L_2 contiene las siguientes diez cadenas (entre una infinidad de opciones):

$$\epsilon, a, b, aa, bb, aaa, bab, abba, babaabab, abaabbbbbaaba$$ ■



University of Wisconsin

Stephen C. Kleene (1909-1994)

• Notación

Sea Σ un alfabeto. Para cada entero no-negativo n, sean

Σ^n = conjunto de todas las cadenas sobre Σ que tienen longitud n,

Σ^+ = conjunto de todas las cadenas sobre Σ que al menos tienen longitud 1 y

Σ^* = conjunto de todas las cadenas sobre Σ.

Observe que Σ^n es esencialmente el producto cartesiano de n copias de Σ. El lenguaje Σ^* se llama **cerradura de Kleene de Σ,** en honor de Stephen C. Kleene. Σ^+ es el conjunto de todas las cadenas sobre Σ excepto por ϵ y se llama **cerradura positiva de Σ**.

Ejemplo 12.1.2 Los lenguajes Σ^n, Σ^+ y Σ^*

Sea $\Sigma = \{a, b\}$.

a. Encuentre Σ^0, Σ^1, Σ^2 y Σ^3.

b. Sean $A = \Sigma^0 \cup \Sigma^1$ y $B = \Sigma^2 \cup \Sigma^3$. Con palabras describa A, B y $A \cup B$.

c. Describa una manera sistemática de escribir los elementos de Σ^+. ¿Qué cambios son necesarios para obtener los elementos de Σ^*?

Solución

a. $\Sigma^0 = \{\epsilon\}$, $\Sigma^1 = \{a, b\}$, $\Sigma^2 = \{aa, ab, ba, bb\}$ y $\Sigma^3 = \{aaa, aab, aba, abb, baa, bab, bba, bbb\}$.

b. A es el conjunto de todas las cadenas sobre Σ de longitud a lo más 1.
B es el conjunto de todas las cadenas sobre Σ de longitud 2 o 3.
$A \cup B$ es el conjunto de todas las cadenas sobre Σ de longitud a lo más 3.

c. Los elementos de Σ^+ se pueden escribir sistemáticamente escribiendo todas las cadenas de longitud 1, después todas las cadenas de longitud 2 y así sucesivamente.

$$\Sigma^+: a, b, aa, ab, ba, bb, aaa, aab, aba, abb, baa, bab, bba, bbb, aaaa,\ldots$$

De hecho, el proceso de escribir las cadenas en Σ^+ continuaría indefinidamente ya que Σ^+ es un conjunto infinito. El único cambio que se necesita hacer para obtener Σ^* es colocar la cadena nula al inicio de la lista. ■

Ejemplo 12.1.3 Notación polaca: un lenguaje que consiste de expresiones posfijas

Una expresión tal como $a + b$, en la cual un operador binario como $+$ se coloca entre las dos cantidades sobre las que actúa, se dice que está escrita en **notación interfija.** Notaciones alternativas se llaman **notación prefija** (en la que el operador binario precede a las cantidades sobre las que actúa) y **notación posfija** (en la que el operador binario sigue a las cantidades sobre las que actúa). En notación prefija, $a + b$ se escribe como $+ ab$. En notación posfija, $a + b$ se escribe como $ab +$.

Notaciones prefijas y posfijas fueron introducidas en 1920 por el matemático polaco Jan Łukasiewicz. En su honor —y porque alguna gente tenía problemas para pronunciar su nombre— frecuentemente se llamaban como **notación polaca** y **notación polaca invertida**, respectivamente. Una gran ventaja de esas notaciones es que eliminan la necesidad de paréntesis al escribir expresiones aritméticas. Por ejemplo, en la notación posfija (o polaca invertida), la expresión 8 4 + 6 / se evalúa de izquierda a derecha como sigue: se suman 8 y 4 se obtiene 12 y después se divide 12 por 6 para obtener 2. Como otro ejemplo, si la expresión $(a + b) \cdot c$ en notación interfija se convierte a notación posfija, el resultado es $ab + c \cdot$.

a. Si la expresión $ab \cdot cd \cdot +$ en notación posfija se convierte a notación interfija, ¿qué resulta?

b. Sean $\Sigma = \{4, 1, +, -\}$ y $L =$ conjunto de todas las cadenas sobre Σ que se obtienen escribiendo primero un 1 o un 4, después un 4 o un 1 y finalmente un $+$ o un $-$. Enumere todos los elementos de L entre paréntesis y evalúe las expresiones resultantes.

Solución

a. $a \cdot b + c \cdot d$

b. $L = \{4\,1\,+,\ 4\,1\,-,\ 1\,4\,+,\ 1\,4\,-,\ 4\,4\,+,\ 4\,4\,-,\ 1\,1\,+,\ 1\,1\,-\}$

$$4\,1\,+ = 4 + 1 = 5, \quad 4\,1\,- = 4 - 1 = 3, \quad 1\,4\,+ = 1 + 4 = 5,$$

$$1\,4\,- = 1 - 4 = -3, \quad 4\,4\,+ = 4 + 4 = 8, \quad 4\,4\,- = 4 - 4 = 0,$$

$$1\,1\,+ = 1 + 1 = 2, \quad 1\,1\,- = 1 - 1 = 0$$ ■

La siguiente definición describe maneras en las que se pueden combinar los lenguajes para formar nuevos lenguajes.

• Definición

Sea Σ un alfabeto. Dadas cualesquiera cadenas x y y sobre Σ, la **concatenación de x y y** es la cadena que se obtiene al escribir todos los caracteres de x seguidos de todos los caracteres de y. Para lenguajes arbitrarios L y L' sobre Σ, se pueden definir tres nuevos lenguajes como sigue:

La **concatenación de L y L'**, que se denota con LL', es

$$LL' = \{xy \mid x \in L \text{ y } y \in L'\}.$$

La **unión de L y L'**, que se denota por $L \cup L'$, es

$$L \cup L' = \{x \mid x \in L \text{ o } x \in L'\}.$$

La **cerradura de Kleene de L**, que se denota L^*, es

$L^* = \{x \mid x$ es una concatenación de cualquier número finito de cadenas en $L\}$.

Observe que ϵ está en L^* porque se considera como una concatenación de cadenas de ceros en L.

Ejemplo 12.1.4 Nuevos lenguajes a partir de lenguajes viejos

Sean L_1 el conjunto de todas las cadenas que consisten de un número par de a (a saber, ε, aa, $aaaa$, $aaaaaa$,…) y $L_2 = \{b, bb, bbb\}$. Encuentre L_1L_2, $L_1 \cup L_2$ y $(L_1 \cup L_2)^*$. Observe que la cadena nula está en L_1 porque 0 es un número par.

Solución

$L_1 L_2 =$ conjunto de todas las cadenas que consisten de un número par de a seguidas por b o bb o por bbb.

$L_1 \cup L_2 =$ conjunto que incluye las cadenas b, bb, bbb y cadenas arbitrarias que consisten de un número par de a.

$(L_1 \cup L_2)^* =$ conjunto de todas las cadenas de a y b en las cuales cada ocurrencia de a está en un bloque que consiste de un número par de a. ■

El lenguaje definido por una expresión regular

Una de las maneras más útiles de definir un lenguaje es por medio de una *expresión regular*, concepto introducido por Kleene. Damos una definición recursiva para generar el conjunto de todas las expresiones regulares sobre un alfabeto.

• Definición

Dado un alfabeto Σ, las siguientes son **expresiones regulares sobre Σ:**

I. BASE: $\emptyset$, ϵ y cada símbolo individual en Σ son expresiones regulares sobre Σ.

II. RECURSIÓN: Si r y s son expresiones regulares sobre Σ, entonces las siguientes también son expresiones regulares sobre Σ:

(i) (rs) (ii) $(r \mid s)$ (iii) (r^*)

donde rs denota la concentración de r y s, r^* representa la concatenación de r consigo mismo de cualquier número finito (incluyendo cero) de veces y $r \mid s$ denota a una de las cadenas r o s. La expresión regular r^* se llama **cerradura de Kleene** de r.

III. RESTRICCIÓN: Nada es una expresión regular sobre Σ excepto los objetos que se han definido en (I) y (II).

Como un ejemplo, una expresión regular sobre $\Sigma = \{a, b, c\}$ es

$$a \mid (b \mid c)^* \mid (ab)^*.$$

Si el alfabeto Σ incluye símbolos, tales como $(\ \mid\ )^*$, entonces deben tomarse precauciones especiales para eliminar ambigüedad. Un *caracter de escape,* usualmente una diagonal hacia la izquierda, se coloca antes del símbolo potencialmente ambiguo. Por ejemplo, un paréntesis izquierdo se escribiría como \ (y la barra inversa misma se escribiría como \\).

Para eliminar el paréntesis, se ha definido un orden de precedencia para las operaciones empleadas en la definición de expresiones regulares. La más alta es *, concatenación es la siguiente y $\mid$ es la más baja. También se acostumbra eliminar el conjunto externo de paréntesis en una expresión regular, porque hacerlo no produce ambigüedad. Así

$$(a((bc)^*)) = a(bc)^* \quad \text{y} \quad (a \mid (bc)) = a \mid bc.$$

Ejemplo 12.1.5 Orden de precedencia para las operaciones en una expresión regular

a. En la siguiente expresión utilice paréntesis para hacer claro el orden de precedencia: $ab^* \mid b^*a$.

b. Use la convención sobre orden de precedencia para eliminar paréntesis en la siguiente expresión: $((a \mid ((b^*)c))(a^*))$.

Solución

a. $((a(b^*)) \mid ((b^*)a))$ b. $(a \mid b^*c)a^*$ ■

Dado un alfabeto finito, cada expresión regular r sobre el alfabeto define un lenguaje formal $L(r)$. La función L está definida recursivamente.

• Definición

Para cualquier alfabeto finito Σ, la función L que asocia a un lenguaje con cada expresión regular sobre Σ se define por (I) y (II) como se indica a continuación. Para cada expresión regular r, $L(r)$ se llama el **lenguaje definido por *r***.

I. BASE: $L(\emptyset) = \emptyset$, $L(\epsilon) = \{\epsilon\}$, $L(a) = \{a\}$ para cada a en Σ.

II. RECURSIÓN: Si $L(r)$ y $L(r')$ son los lenguajes definidos por las expresiones regulares r y r' sobre Σ, entonces

(i) $L(rr') = L(r)L(r')$ (ii)$L(r|r') = L(r) \cup L(r')$ (iii) $L(r^*) = (L(r))^*$

Observe que cualquier lenguaje finito se puede definir por una expresión regular. Por ejemplo, el lenguaje {gato, perro, pájaro} está definido por la expresión regular (gato | perro | pájaro). El siguiente es un ejemplo importante:

Ejemplo 12.1.6 Uso de la notación de conjuntos para describir el lenguaje definido por una expresión regular

Sea $\Sigma = \{a, b\}$ y considere el lenguaje definido por la expresión regular $(a \mid b)^*$. Utilice notación de conjuntos para encontrar este lenguaje y descríbalo con sus palabras.

Solución El lenguaje definido por $(a \mid b)^*$ es

$$\begin{aligned} L((a \mid b)^*) &= (L(a \mid b))^* \\ &= (L(a) \cup L(b))^* \\ &= (\{a\} \cup \{b\})^* \\ &= \{a, b\}^* && \text{por definición de operaciones sobre lenguajes} \\ &= \text{conjunto de todas las cadenas de } a \text{ y } b. \\ &= \Sigma^*. \end{aligned}$$

■

Observe que concatenar cadenas y tomar uniones de conjuntos son operaciones asociativas. Así para las expresiones regulares arbitrarias r, s y t,

$$L((rs)t) = L(r(st)).$$

Además,

$$\begin{aligned} L\ ((r \mid s) \mid t) &= (L(r \mid s)) \cup L(t) && \text{por definición de } \mid \\ &= (L(r) \cup L(s)) \cup L(t) && \text{por definición de } \mid \\ &= L(r) \cup (L(s) \cup L(t)) && \text{por la asociatividad de la unión de conjuntos} \\ &= L(r) \cup (L(s \mid t)) && \text{por definición de } \mid \\ &= L(r \mid (s \mid t)) && \text{por definición de } \mid \end{aligned}$$

Debido a estas relaciones, se acostumbra eliminar el paréntesis en situaciones "asociativas" y escribir

$$rst = (rs)t = r(st)$$

y

$$r \mid s \mid t = (r \mid s) \mid t = r \mid (s \mid t).$$

Cuando acostumbre trabajar con expresiones regulares, encontrará que no se necesita usar deducciones formales para determinar el lenguaje definido por una expresión.

Ejemplo 12.1.7 El lenguaje definido por una expresión regular

Sea $\Sigma = \{0, 1\}$. Utilice sus palabras para describir los lenguajes definidos por las siguientes expresiones regulares sobre Σ.

a. $0^*1^* \mid 1^*0^*$ b. $0(0 \mid 1)^*$

Solución

a. Las cadenas en este lenguaje consisten de una cadena de 0 seguidos por una cadena de 1 o una cadena de 1 seguidos por una cadena de 0. Sin embargo, en cualquier caso las cadenas podrían ser vacías, lo que significa que ε está también en el lenguaje.

b. En este lenguaje las cadenas tienen que iniciar con un 0. El 0 puede ser seguido por cualquier número finito (incluyendo cero) de 0 y 1 en orden arbitrario. Así el lenguaje es el conjunto de todas las cadenas de 0 y 1 que empiezan con un 0. ■

Ejemplo 12.1.8 Cadenas individuales en el lenguaje definido por una expresión regular

En *a*) y *b*), sea $\Sigma = \{a, b\}$ y considere el lenguaje L sobre Σ definido por las expresiones regulares dadas.

a. La expresión regular es $a^*b(a \mid b)^*$. Escriba cinco cadenas que pertenezcan a L.

b. La expresión regular es $a^* \mid (ab)^*$. Indique cuál de las siguientes cadenas pertenecen a L:

$$a \quad b \quad aaaa \quad abba \quad ababab$$

Solución

a. Las cadenas b, ab, $abbb$, $abaaa$ y $ababba$ son cinco cadenas de una infinidad que existen en L.

b. Las siguientes cadenas son las únicas que pertenecen a L: a, $aaaa$ y $ababab$. La cadena b no pertenece a L porque no es una cadena de a ni es posiblemente una cadena de repetidas ab. La cadena $abba$ no está en L porque dos b arbitrarias que podrían ocurrir en una cadena de L están separadas por una a. ■

Ejemplo 12.1.9 Una expresión regular que define un lenguaje

Sea $\Sigma = \{0, 1\}$. Encuentre expresiones regulares sobre Σ que definen los siguientes lenguajes.

a. El lenguaje que consiste de todas las cadenas de 0 y 1 que tienen longitud par en las cuales se alternan los 0 y 1.

b. El lenguaje que consiste de todas las cadenas de 0 y 1 con un número par de 1. Se dice que tales cadenas tienen *paridad par*.

c. El lenguaje que consiste de todas las cadenas de 0 y 1 que no contienen dos 1 consecutivos.

Solución

a. Si una cadena en el lenguaje inicia con un 1, el patrón 10 debe continuar a lo largo de la cadena. Si empieza con 0, el patrón 01 debe mantenerse a lo largo de la cadena. También, la cadena nula satisface la condición por defecto. Así, una respuesta es:

$$(10)^* \mid (01)^*.$$

b. Las cadenas básicas con paridad par son ϵ, 0 y 10^*1. La concatenación de cadenas con paridad par también es par. Como tal cadena puede iniciar o terminar con una cadena de 0, una respuesta es

$$(0 \mid 10^*1)^*.$$

c. Observe que una cadena puede finalizar en un 1, pero cualquier otro 1 debe ser seguido inmediatamente por un 0. Así, es suficiente con enfatizar la regla de que un 1 debe ser seguido por un 0, a menos de que 1 sea el fin de la cadena. Una expresión regular que satisface esas condiciones es

$$(0 \mid 10)^*(\epsilon \mid 1).$$ ■

Observe que un lenguaje dado se puede definir con más de una expresión regular. Por ejemplo,

$$(a^* \mid b^*)^* \quad \text{y} \quad (a \mid b)^*$$

definen el lenguaje que consiste del conjunto de todas las cadenas de a y b.

Ejemplo 12.1.10 Decisión de si expresiones regulares definen el mismo lenguaje

En *a*) y *b*), determine si las expresiones regulares dadas definen el mismo lenguaje. Si es así, entonces describa el lenguaje. Si no es el caso, dé un ejemplo de una cadena que esté en uno de los lenguajes, pero no en el otro.

a. $(a \mid \epsilon)^*$ y a^* b. $0^* \mid 1^*$ y $(01)^*$

Solución

a. Observe que como la cadena nula ϵ no tiene caracteres, entonces cuando se concatena con cualquier otra cadena x, entonces el resultado es justamente x: para todas las cadenas x, $x\epsilon = \epsilon x = x$. Así $L((a \mid \epsilon)^*)$ es el conjunto de cadenas formadas empleando a y ϵ en cualquier orden y así, como $a\epsilon = \epsilon a = a$, esto coincide con el conjunto de cadenas que consiste de ceros o más a. Entonces $L((a \mid \epsilon)^*) = L(a^*)$.

b. Los dos lenguajes definidos por las expresiones regulares dadas no son los mismos: 0101 está en el segundo lenguaje, pero no en el primero. ■

Usos prácticos de expresiones regulares

Muchas aplicaciones de las computadoras implican la ejecución de operaciones en pedazos de texto. Por ejemplo, los programas para procesar palabras y textos nos permiten encontrar ciertas palabras o frases en un documento y posiblemente reemplazarlas con otras. Un compilador para un lenguaje computacional analiza un flujo de entrada de caracteres para localizar agrupamientos que representen aspectos del lenguaje computacional tales como palabras clave, constantes, identificadores y operadores. Y en bioinformática, el igualar patrones y las técnicas de búsquedas flexibles se emplean extensamente para analizar las largas sucesiones de los caracteres A, C, G y T que ocurren en el ADN.

A través de su conexión con autómatas de estado-finito, que serán analizados en la siguiente sección, las expresiones regulares proporcionan una forma extremadamente útil para describir un patrón para identificar una cadena o una colección de cadenas dentro de un pedazo de texto. Las expresiones regulares hacen posible reemplazar un complicado conjunto de enunciados si-entonces-de otra manera, con un código que es fácil de producir y de entender. Por ser muy convenientes, las expresiones regulares se introdujeron en numerosos accesorios de UNIX, tales como *grep* (forma abreviada para la frase "***g***lobally ***s***earch for ***r***egular ***e***xpression y ***p***rint") y *egrep* (*grep extendido*), en editores de texto, tales como *QED* (para ***Q***uick ***ED***itor, el primer editor de textos en usar expresiones regulares), *vi* (para ***v***isual ***i***nterface), *sed* (para ***s***tream ***ed***itor y originalmente desarrollado para UNIX pero ahora empleado por muchos sistemas) y *Emacs* (para ***E***ditor ***mac***ros) y también en el componente de escáner léxico de un compilador. El lenguaje computacional Perl tiene una implementación particularmente poderosa para expresiones regulares, que se ha convertido en un estándar. Son similares las implementaciones utilizadas en Java y en .NET

En procesamiento de textos, para facilitar el trabajo con expresiones regulares se ha desarrollado un cierto número de notaciones abreviadas. Cuando los caracteres en un alfabeto o en una parte de un alfabeto ocurren en un orden estándar, es común emplear la notación *[carácter inicial-carácter final]* para representar la expresión regular que consiste de un solo carácter en el rango del inicio al carácter final. A esto se le llama **clase de carácter**. Así

$$[A - C] \quad \text{significa} \quad (A|B|C)$$

y

$$[0 - 9] \quad \text{denota} \quad (0 \mid 1 \mid 2 \mid 3 \mid 4 \mid 5 \mid 6 \mid 7 \mid 8 \mid 9).$$

En las clases de caracteres también se permite incluir más de un rango de caracteres. Por ejemplo,

$$[A - C\, x - z] \quad \text{que representa} \quad (A \mid B \mid C \mid x \mid y \mid z).$$

Como un ejemplo, considere el lenguaje definido por la expresión regular

$$[A - Z\, a - z]([A - Z\, a - z] \mid [0 - 9])^*.$$

Las siguientes son algunas cadenas en el lenguaje:

$$\textit{Numero de cuenta}, \quad z23, \quad \textit{jsmith}109, \quad \textit{bosquejo2rev}$$

En general, el lenguaje es el conjunto de todas las cadenas que inician con una letra seguida por una sucesión de dígitos o letras. Este conjunto es igual al conjunto de identificador permitidos en diversos lenguajes computacionales.

Otras abreviaciones comúnmente usadas son

$$[ABC] \text{ para } (A \mid B \mid C)$$

y un solo punto

. para denotar un carácter arbitrario.

Así, por ejemplo, si $\Sigma = \{A, B, C\}$, entonces

$$A.C \quad \text{representa} \quad (AAC \mid ABC \mid ACC).$$

Cuando se coloca el símbolo ^ al inicio de una clase de caracteres, indica que un carácter del mismo tipo como aquellos en el rango de la clase ocurre en ese punto de la cadena, excepto para uno de los caracteres específicos indicados después del signo ^. Por ejemplo,

$$[\hat{}D - Z][0 - 9][0 - 9]^*$$

para cualquier cadena iniciando con una letra del alfabeto diferente de D a Z, seguida por cualquier número positivo con dígitos de 0 a 9. Ejemplos son $B3097$, $C0046$ y así sucesivamente. Si r es una expresión regular, la notación $r+$ denota la concatenación de r consigo misma cualquier número positivo finito de veces. En símbolos,

$$r + = r\, r^*.$$

Por ejemplo, $[A - Z]+$

representa cualquier cadena no vacía de letras mayúsculas. Si r es una expresión regular, entonces

$$r? = (\epsilon \mid r).$$

Es decir, $r?$ denota cero ocurrencias o exactamente una ocurrencia de r. Finalmente, si m y n son enteros positivos con $m \leq n$,

$r\{n\}$ representa la concatenación de r consigo misma exactamente n veces,

y

$r\{m, n\}$ indica la concatenación de r consigo misma de m a n veces.

Así, una comprobación para ayudar a determinar si una cadena dada es un número telefónico local en Estados Unidos consiste en ver si tiene la forma

$$[0 - 9][0 - 9][0 - 9] \text{ - } [0 - 9][0 - 9][0 - 9][0 - 9],$$

o, equivalentemente, si la cadena tiene la forma

$$[0 - 9]\{3\} \text{ - } [0 - 9]\{4\}.$$

Ejemplo 12.1.11 Una expresión regular para una fecha

Las personas frecuentemente escriben fechas en una variedad de formatos. Por ejemplo, en Estados Unidos el 5 Febrero del 2050 puede representarse de varias maneras:

2/5/2050 2-5-2050 02/05/2050 02-05-2050

Nota En la mayor parte del resto del mundo estas expresiones representan el dos de mayo de 2050.

Escriba una expresión regular que ayude a comprobar si una cadena dada podría ser una fecha válida escrita en una de esas formas.

Solución El lenguaje definido por la siguiente expresión regular consiste de todas las cadenas que inician con uno o dos dígitos seguidos por un guión − o por una barra diagonal /, después por uno o dos dígitos, luego por un guión − o una barra diagonal /, seguidos por cuatro dígitos.

$$[0-9]\{1,2\}[-/][0-9]\{1,2\}[0-9]\{4\}$$

Todas las fechas válidas del formato dado son elementos del lenguaje definido por esta expresión, pero el lenguaje también incluye cadenas que no son fechas válidas. Por ejemplo, 09/54/1978 está en el lenguaje, pero no es una fecha válida porque septiembre no tiene 54 días y 38/12/2184 no es válida porque no existe el mes número 38. Es posible escribir una de la validez de una fecha (véase el ejercicio 40 al final de la sección), no obstante, es útil el tipo más simple de expresión dada renglones arriba. Por ejemplo, nos da una forma fácil de notificar al usuario de un programa interactivo, que fue hecho un cierto tipo de error y que la información debería ser ingresada nuevamente. ■

Autoexamen

Las respuestas a las preguntas del autoexamen se localizan al final de cada sección.

1. Si x y y son cadenas, la concatenación de x y y es _____.
2. Si L y L' son lenguajes, la concatenación de L y L' es _____.
3. Si L y L' son lenguajes, la unión de L y L' es _____.
4. Si L es un lenguaje, la cerradura de Kleene de L es _____.
5. El conjunto de expresiones regulares sobre un alfabeto Σ está definido recursivamente. La BASE para la definición es el enunciado de que ____. La RECURSIÓN para la definición específica que si r y s son expresiones regulares arbitrarias sobre Σ, entonces las siguientes también son expresiones regulares en el conjunto: _____, _____ y _____.
6. La función que asocia un lenguaje con cada expresión regular sobre un alfabeto Σ está definida recursivamente. La BASE para la definición es el enunciado de que $L(\emptyset) =$ _____, $L(\epsilon) =$ _____ y $L(a) =$ _____ para cada a en Σ. La RECURSIÓN para la definición especifica que si $L(r)$ y $L(r')$ son los lenguajes definidos por las expresiones regulares r y r' sobre Σ, entonces $L(rr') =$ _____, $L(r \mid r') =$ _____ y $L(r^*) =$ _____.
7. La notación [A - C] es un ejemplo de una _____ y denota la expresión regular _____.
8. El uso de un punto único en una expresión regular representa _____.
9. El símbolo ^, colocado al inicio de una clase de carácter, indica _____.
10. Si r es una expresión regular, la notación $r+$ denota _____.
11. Si r es una expresión regular, la notación $r?$ denota _____.
12. Si r es una expresión regular, la notación $r\{n\}$ representa _____ y la notación $r\{m, n\}$ significa _____.

Conjunto de ejercicios 12.1*

En 1 y 2 sea $\Sigma = \{x, y\}$ un alfabeto.

1. a. Sea L_1 el lenguaje que consiste de todas las cadenas sobre Σ que son palíndromos y tienen longitud ≤ 4. Enumere, entre llaves, a los elementos de L_1.

b. Sea L_2 el lenguaje que consiste de todas las cadenas sobre Σ que inician con una x y tienen longitud ≤ 3. Enumere los elementos de L_2.

2. a. Sea L_3 el lenguaje que consiste de todas las cadenas sobre Σ de longitud ≤ 3 en las cuales todas las x aparecen a la izquierda de todas las y. Enumere los elementos de L_3 entre llaves.

b. Enumere entre llaves los elementos de Σ^4, el conjunto de cadenas de longitud 4 sobre Σ.

c. Sean $A = \Sigma^1 \cup \Sigma^2$ y $B = \Sigma^3 \cup \Sigma^4$. Con sus palabras describa A, B y $A \cup B$.

***H* 3.** a. Si la expresión $ab + cd + \cdot$ en notación posfija se convierte a notación interfija, ¿qué resulta?

b. Sean $\Sigma = \{1, 2, *, /\}$ y L el conjunto de todas las cadenas sobre Σ que se obtiene al escribir primero un número (1 o 2), entonces un segundo número (1 o 2), que puede ser igual al primero y finalmente una operación (* o / en donde * indica multiplicación y / significa división). Entonces L es un conjunto de expresiones posfijas o en notación polaca invertida. Entre paréntesis enumere todos los elementos de L y evalúe las expresiones resultantes.

*Para los ejercicios con números o letras azules, las soluciones están dadas en el apéndice B. El símbolo ***H*** indica que sólo se da una sugerencia o una solución parcial. El símbolo ✶ indica que el ejercicio es más difícil de lo normal.

En los ejercicios del 4 al 6, describa $L_1\,L_2$, $L_1 \cup L_2$ y $(L_1 \cup L_2)^*$ para los lenguajes dados L_1 y L_2.

4. L_1 es el conjunto de todas las cadenas de a y b que inician con una a y sólo contiene a esa a; L_2 es el conjunto de todas las cadenas de a y b que contienen un número par de a.

5. L_1 es el conjunto de todas las cadenas de a, b y c que no contienen c pero tienen el mismo número de a y b; L_2 es el conjunto de todas las cadenas de a, b y c que no contienen a ni b.

6. L_1 es el conjunto de todas las cadenas de 0 y 1 que inician con un 0 y L_2 es el conjunto de todas las cadenas de 0 y 1 que terminan con un 0.

En los ejercicios del 7 al 9, introduzca paréntesis para hacer claro el orden de precedencia en las expresiones dadas.

7. $(a \mid b^*b)(a^* \mid ab)$ 8. $0^*1 \mid 0(0^*1)^*$

9. $(x \mid yz^*)^*(yx \mid (yz)^*z)$

En los ejercicios del 10 al 12 use la convención sobre el orden de precedencia para eliminar los paréntesis en la expresión regular dada.

10. $((a(b^*)) \mid (c(b^*)))\ ((ac) \mid (bc))$

11. $(1(1^*)) \mid ((1(0^*)) \mid ((1^*)1))$

12. $(xy)(((x^*)y)^*) \mid (((yx) \mid y)(y^*))$

En los ejercicios del 13 al 15 utilice la notación de conjuntos para deducir el lenguaje definido por la expresión regular dada. Suponga que $\Sigma = \{a, b, c\}$.

13. $\epsilon \mid ab$ 14. $\emptyset \mid \epsilon$ 15. $(a \mid b)c$

En los ejercicios del 16 al 18 escriba cinco cadenas que pertenezcan al lenguaje definido por la expresión regular dada.

16. $0^*1(0^*1^*)^*$ 17. $b^* \mid b^*ab^*$ 18. $x^*(yxxy \mid x)^*$

En los ejercicios del 19 al 21 use sus palabras para describir el lenguaje definido por la expresión regular dada.

19. $b^*ab^*ab^*a$ 20. $1(0 \mid 1)^*00$ 21. $(x \mid y)\ y\ (x \mid y)^*$

En los ejercicios del 22 al 24 indique si las cadenas dadas pertenecen al lenguaje definido por la expresión regular dada. En forma breve justifique sus respuestas.

22. Expresión: $(b \mid \epsilon)a(a \mid b)^*a(b \mid \epsilon)$, cadenas: *aaaba*, *baabb*

23. Expresión: $(x^*y \mid zy^*)^*$, cadenas: *zyyxz*, *zyyzy*

24. Expresión: $(01^*2)^*$, cadenas: 120, 01202

En los ejercicios 25 al 27 encuentre una expresión regular que defina al lenguaje dado.

25. El lenguaje que consiste de todas las cadenas de 0 y 1 con un número impar de 1. (Se dice que dicha cadena tiene *paridad impar*.)

26. El lenguaje que consiste de todas las cadenas de a y b en las cuales el tercer caracter del final es una b.

27. El lenguaje que consiste de cadenas de x y y en las que los elementos en cada par de x están separados por al menos una y.

Sean r, s y t expresiones regulares sobre $\Sigma = \{a, b\}$. En los ejercicios del 28 al 30 determine si las dos expresiones regulares definen el mismo lenguaje. Si así es, entonces describa el lenguaje. Si no, dé un ejemplo de una cadena que esté en un lenguaje pero no en el otro.

28. $(r \mid s)t$ y $rt \mid st$ 29. $(rs)^*$ y r^*s^*

30. $(rs)^*$ y $((rs)^*)^*$

En los ejercicios del 31 al 39 escriba una expresión regular para definir el conjunto dado de cadenas. Cuando sea conveniente use las notaciones abreviadas dadas en la sección. En la mayoría de los casos, su expresión describirá otras cadenas además de las dadas, pero intente que su respuesta iguale a las cadenas dadas tan cercanamente como sea posible dentro de razonables limitaciones de espacio.

31. Todas las palabras escritas en minúsculas y que inician con las letras *pre*, pero que no consisten de *pre* en sí misma.

32. Todas las palabras escritas en mayúsculas y que contienen las letras *BIO* (como una unidad) o *INFO* (como una unidad).

33. Todas las palabras escritas en minúsculas, en inglés, que finalizan en *ly* y que contienen al menos cinco letras.

34. Todas las palabras escritas en minúsculas y que contienen al menos una de las vocales a, e, i, o, u.

35. Todas las palabras escritas en minúsculas y conteniendo exactamente una de las vocales a, e, i, o, u.

36. Todas las palabras que están escritas en mayúsculas y que no inician con una de las vocales A, E, I, O, U, pero que contienen exactamente dos de esas vocales próximas una a la otra.

37. Todos los números de seguridad social de Estados Unidos (los cuales consisten de tres dígitos, un guión, dos dígitos, otro guión y finalmente cuatro dígitos más), en donde los cuatro dígitos finales inician con un 3 y terminan con un 6.

38. Todos los números telefónicos que tienen tres dígitos, luego un guión, después tres dígitos más, otra vez un guión y después cuatro dígitos, en donde los primeros tres dígitos son 800 o 888 y los últimos cuatro dígitos inician y finalizan con un 2.

39. Todos los números con o sin signo, con o sin un punto decimal. Un número con signo tiene uno de los prefijos $+$ o $-$ y un número careciendo de signo no tiene un prefijo. Represente el punto decimal como \. para distinguirlo del símbolo de punto único para un carácter arbitrario.

***H* 40.** Escriba una expresión regular para efectuar un completo chequeo para determinar si una cadena dada representa una fecha válida de 1980 a 2079, escrita en alguno de los formatos del ejemplo 12.1.11. (Durante este periodo, ocurren años bisiestos cada cuatro años iniciando en 1980.)

✶ 41. Escriba una expresión regular para definir el conjunto de cadenas de 0 y 1 con un número par de 0 y un número par de 1.

Respuestas del autoexamen

1. la cadena que se obtiene al escribir todos los caracteres de x seguidos por todos los caracteres de y 2. $\{xy \mid x \in L \text{ y } y \in L'\}$ 3. $\{s \mid s \in L \text{ o } s \in L'\}$ 4. $\{t \mid t$ es una concatenación de cualquier número finito de cadenas en $L\}$ 5. $\emptyset$, ϵ y cada símbolo individual en Σ son expresiones regulares sobre Σ; (rs) : $(r \mid s)$; (r^*) 6. $\emptyset$; $\{\epsilon\}$; $\{a\}$; $L(r)L(r')$; $L(r) \cup L(r')$; $(L(r))^*$ 7. clase de caracter; $(A \mid B \mid C)$ 8. un caracter arbitrario 9. un caracter del mismo tipo que aquellos en el rango de la clase que se presentan en ese punto de la cadena, excepto por uno de los caracteres específicos indicados después del signo ^ 10. La concatenación de r consigo misma con cualquier número finito positivo de veces 11. $(\epsilon \mid r)$ 12. la concatenación de r consigo misma exactamente n veces; la concatenación de r consigo misma desde m hasta n veces.

12.2 Autómatas de estado-finito

El mundo del futuro será cada vez más una lucha contra las limitaciones de nuestra inteligencia, no una confortable hamaca en la cual podamos descansar y esperar ser levantados por nuestros robots esclavizados. —Norbert Wiener, 1964

El tipo de circuito que se analiza en la sección 2.4 se llama *circuito combinacional*. Tal circuito está caracterizado por el hecho de que su salida está completamente determinada por su tabla de entrada/salida, o, en otras palabras, por una función booleana. Su salida no depende en ninguna forma de la historia de previas entradas al circuito. Por esta razón, se dice que un circuito combinacional no tiene memoria.

Los circuitos combinacionales son muy importantes en el diseño de computadoras, pero no son los únicos tipos de circuitos empleados. Los *circuitos sucesivos* son igualmente importantes. Para circuitos sucesivos no se puede predecir la salida correspondiente a una entrada particular, a menos que se conozca algo sobre la historia previa del circuito, o, más técnicamente, a menos que se sepa el estado del circuito antes de recibir la entrada. El comportamiento de un circuito sucesivo no sólo es función de la entrada al circuito sino también del estado de éste cuando se recibe la entrada. Un circuito de la memoria de la computadora es de tipo sucesivo.

Un **autómata de estado-finito** es una máquina idealizada que encarna la idea esencial de un circuito sucesivo. Cada parte de la entrada a un autómata de estado-finito conduce a un cambio en el estado del autómata, lo que a su vez afecta la manera en que se procesará el resto de la entrada. Imagine, por ejemplo, el acto de marcar un número telefónico. Marcando 1-800 pone al circuito telefónico en un estado de alerta para recibir los siete dígitos finales de una llamada gratis, mientras que marcando 328 lo conduce a un estado de espera para los cuatro dígitos finales de una llamada local. Las máquinas automáticas operan similarmente. Sólo conociendo que pone una peseta en una máquina automática no es suficiente para que pueda predecir qué comportamiento tendrá la máquina. También debe conocer en qué estado se encontraba la máquina cuando se insertó la peseta. Si antes se hubieran depositado 75¢, podría obtener una bebida o algún caramelo, pero no obtendría nada si la peseta fue la primera moneda depositada.

Ejemplo 12.2.1 Una máquina automática simple

Una máquina automática simple reparte botellas de jugo que cuestan $1 cada una. La máquina sólo acepta pesetas y medio dólar y no da cambio. Tan pronto como la cantidad depositada es igual o mayor que $1 la máquina da una botella de jugo. La siguiente moneda depositada inicia otra vez el proceso. La operación de la máquina está representada en el diagrama de la figura 12.2.1.

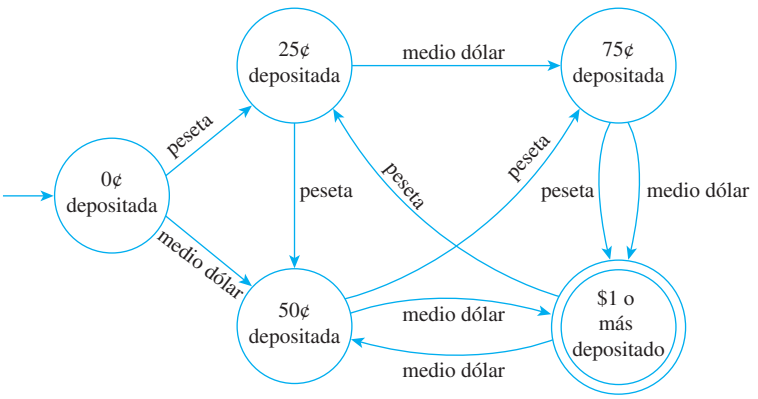


Figura 12.2.1 **Una máquina automática simple**

Cada círculo representa un estado de la máquina: el estado en la que se han depositado 0¢, 50¢, 75¢ y $1 o más. La flecha no etiquetada que apunta a "0¢ depositado" indica que este es el estado inicial de la máquina. El doble círculo alrededor de "$1 depositado o más" indica que una botella de jugo se libera cuando la máquina alcanza este estado. (Este último estado se conoce como *estado aceptable* de la máquina porque cuando se encuentra en él, ha aceptado la secuencia de entrada de monedas como pago para el jugo.) Las flechas que encadenan los estados indican qué pasa cuando una entrada particular se introduce a la máquina en cada uno de sus diversos estados. Por ejemplo, la flecha marcada "peseta" que va de "0¢ depositado" a "25¢ depositado" indica que cuando la máquina se encuentra en el estado "0¢ depositado" y se inserta una peseta, entonces la máquina va al estado "25¢ depositado". La flecha etiquetada con "medio dólar" que va de "75¢ depositado" a "$1 depositado o más" indica que cuando la máquina está en el estado "75¢ depositado" y se introduce un medio dólar, entonces la máquina va al estado "$1 depositado o más" y se entrega el jugo. (En este caso el comprador pagaría $1.25 por el jugo porque la máquina no regresa cambio.) La flecha marcada con "peseta" que va de "$1 depositado o más" a "25¢ depositado" señala que cuando la máquina se encuentra en el estado "$1 depositado o más" y se introduce una peseta, la máquina retorna al estado "25¢ depositado". (Esto corresponde al caso en que después de que la máquina ha dado una botella de jugo, inicia otra vez toda la operación.)

Equivalentemente, la operación de la máquina automática puede ser representada por una *tabla de siguiente estado* como se muestra en la tabla 12.2.1

Tabla 12.2.1 **Tabla del siguiente estado**

		Entrada	
		peseta	**medio dólar**
→	0¢ depositada	25¢ depositada	50¢ depositada
	25¢ depositada	50¢ depositada	75¢ depositada
Estado	50¢ depositada	75¢ depositada	$1 o más depositado
	75¢ depositada	$1 o más depositado	$1 o más depositado
◎	$1 o más depositado	25¢ depositada	50¢ depositada

La flecha, que apunta a "0¢ depositado" en la tabla, indica que la máquina inicia su operación en este estado. El doble círculo próximo a "$1 depositado o más" indica que se libera una botella de jugo cuando la máquina ha llegado a dicho estado. Las entradas en el cuerpo de la tabla se interpretan de manera obvia. Por ejemplo, la entrada en la tercera fila de la columna marcada con *Medio-Dólar* muestra que cuando la máquina se encuentra en el estado "50¢ depositado" y se deposita medio dólar, va hacia el estado "$1 depositado o más".

Observe que la tabla 12.2.1 tiene exactamente la misma información que el diagrama de la figura 12.2.1. Si se da el diagrama, entonces se puede construir la tabla y si se da la tabla, entonces se puede dibujar el diagrama. ■

David Eugene Smith Collection, Rare Book and Manuscript Library, Columbia University

David Hilbert (1862–1943)

Time & Life Pictures/Getty Images

Alan M. Turing (1912–1954)

Observe que podemos pensar que la máquina automática que se describe en el ejemplo 12.2.1 tiene una memoria primitiva: Ella "recuerda" cuánto dinero se ha depositado (dentro de ciertos límites) por referencia al estado en que se encuentra. Esta capacidad de almacenar información y actuar de acuerdo a ella, es lo que da al autómata de estado-finito su tremendo poder.

Las computadoras digitales son los más importantes autómatas de estado-finito. Cada computadora consiste de varios subsistemas: dispositivos de entrada, un procesador y dispositivos de salida. Un procesador típico consiste de una unidad central de procesamiento y un número finito de sectores de memoria. En cualquier momento, el estado del procesador está determinado por los sectores y valores de todos los bits almacenados en su memoria. Una computadora que tiene n distintos sectores para almacenar un solo bit, puede existir en 2^n estados diferentes. Para una computadora moderna, n es del orden de miles de millones o aún de millones de millones, así que es enorme el número total de estados. Pero ese número *es* finito. Por lo tanto, a pesar de la complejidad de una computadora, es posible predecir (como ocurrió en la máquina automática) el siguiente estado dado el conocimiento del estado presente y de la entrada. En efecto, esencialmente esto es lo que los programadores intentan hacer cada vez que escriben un programa. Afortunadamente, los lenguajes computacionales modernos de alto nivel son de gran ayuda.

La teoría básica de autómatas fue desarrollada para contestar cuestiones teóricas sobre los fundamentos de las matemáticas, las cuales fueron propuestas en 1900 por el gran matemático alemán David Hilbert. El trabajo pionero sobre autómatas fue realizado, a mediados de 1930, por el matemático y lógico inglés Alan M. Turing. En las décadas de 1940 y 1950, el trabajo de Turing desempeñó un papel fundamental en el desarrollo de las computadoras automáticas del mundo real.

Definición de un autómata de estado-finito

Un *autómata de estado-finito* general está descrito completamente por un conjunto dado de estados, junto con una indicación sobre cuál es el estado inicial y cuáles son los estados aceptables (cuando suceda algo especial), una lista de todos los elementos de entrada y especificación para una *función de siguiente estado* que defina cuál estado se produce por cada entrada en cada estado. Esto es formalizado en la siguiente definición:

• Definición

Un **autómata de estado-finito** A consiste de cinco objetos:

1. Un conjunto finito $\boldsymbol{I}$, llamado el **alfabeto de entrada**, de símbolos de entrada;
2. Un conjunto finito $\boldsymbol{S}$ de **estados** en los que puede estar el autómata;
3. Un estado se denota por $\boldsymbol{s_0}$ llamado el **estado inicial**;
4. Un determinado conjunto de estados llamado de **estados aceptables**;
5. Una **función de estado próximo** $\boldsymbol{N}$: $\boldsymbol{S \times I \rightarrow S}$ que asocia un "estado siguiente" a cada par ordenado que consiste de un "estado presente" y una "entrada presente". Para cada estado s en S y un símbolo de entrada m en I, $N(s, m)$ es el estado al que va A si m es entrada para A cuando éste se encuentra en el estado s.

El funcionamiento de un autómata de estado-finito es comúnmente descrito por un diagrama llamado un **diagrama de transición de estados,** similar al que se muestra en la figura 12.2.1. Se le llama *diagrama de transición* porque muestra las transiciones de la máquina de un estado a otro en respuesta a diversas entradas. En un diagrama de transición, los estados se representan con círculos y los dobles círculos denotan a los estados aceptables. Existe una flecha que apunta al estado inicial y otras flechas que se marcan con

símbolos de entrada y que apuntan de cada estado a otros estados para indicar la acción de la función del siguiente estado. Específicamente, una flecha (marcada con m) del estado s al estado t significa que $N(s, m) = t$.

La **tabla de siguiente estado** para un autómata muestra los valores de la función de siguiente estado N para todos los posibles estados s y símbolos de entrada i. En la **tabla de siguiente estado**, el estado inicial se indica por una flecha y los estados aceptables se marcan con círculos dobles.

Ejemplo 12.2.2 Un autómata de estado-finito dado por un diagrama de transición

Considere el autómata de estado-finito A definido por el diagrama de transición que se muestra en la figura 12.2.2.

a. ¿Cuáles son los estados de A?

b. ¿Cuáles son los símbolos de entrada de A?

c. ¿Cuál es el estado inicial de A?

d. ¿Cuáles son los estados aceptables de A?

e. Determine $N(s_1, 1)$.

f. Construya la tabla de siguiente estado para A.

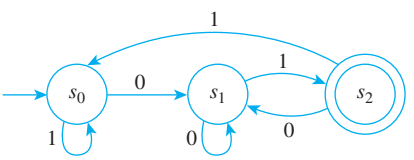


Figura 12.2.2

Solución

a. Los estados de A son s_0, s_1 y s_2 *[ya que esas son las marcas de los círculos]*.

b. Los símbolos de entrada de A son 0 y 1 *[porque esas son las etiquetas de las flechas]*.

c. El estado inicial de A es s_0 *[porque la flecha no marcada apunta hacia s_0]*.

d. El único estado aceptable de A es s_2 *[porque ese es el único estado marcado por un doble círculo]*.

e. $N(s_1, 1) = s_2$ *[porque existe una flecha, marcada 1, de s_1 a s_2]*.

f.

		Entrada: 0	Entrada: 1
Estado →	s_0	s_1	s_0
	s_1	s_1	s_2
Estado ◎	s_2	s_1	s_0

■

Ejemplo 12.2.3 Un autómata de estado-finito dado por una tabla de siguiente estado

Considere el autómata de estado-finito A definido por la siguiente tabla de siguiente estado:

a. ¿Cuáles son los estados de A?

b. ¿Cuáles son los símbolos de entrada de A?

c. ¿Cuál es el estado inicial de A?

d. ¿Cuáles son los estados aceptables de A?

e. Encuentre $N(U, c)$.

f. Dibuje el diagrama de transición para A.

		Entrada: a	Entrada: b	Entrada: c
Estado →	U	Z	Y	Y
Estado ◎	V	V	V	V
Estado	Y	Z	V	Y
Estado ◎	Z	Z	Z	Z

Solución

a. Los estados de A son U, V, Y y Z.

b. Los símbolos de entrada de A son a, b y c.

c. El estado inicial de A es U *[porque la flecha apunta a U]*.

d. Los estados aceptables de A son V y Z *[porque ellos están marcados con círculos dobles]*.

e. $N(U, c) = Y$ *[porque Y es la entrada en la fila marcada U y la columna etiquetada c en la tabla de siguiente estado]*.

f. El diagrama de transición para A se muestra en la figura 12.2.3. Y puede dibujarse más compactamente con flechas marcadas con múltiples símbolos de entrada en donde sea apropiado. Esto se ilustra en la figura 12.2.4.

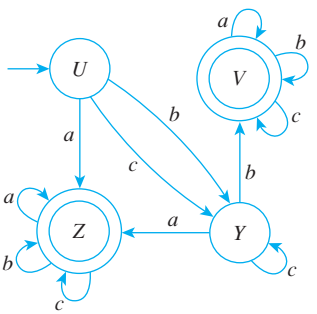


Figura 12.2.3

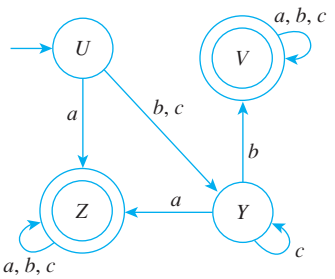


Figura 12.2.4

El lenguaje aceptado por un autómata

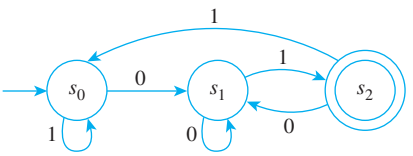
Ahora supongamos que una cadena de símbolos de entrada es alimentada en un autómata de estado-finito en sucesión. Al final del proceso, después de que cada símbolo de entrada sucesivo ha cambiado el estado del autómata, éste termina en un cierto estado, el cual puede o no ser un estado aceptable. De esta manera, la acción de un autómata de estado-finito separa al conjunto de todas las cadenas de símbolos de entrada en dos subconjuntos: aquellos que mandan al autómata a un estado aceptable y aquellos que no lo hacen. Se dice que las cadenas son *aceptadas* por el autómata si éste es enviado a un estado aceptable por dichas cadenas.

• Definición

Sea A un autómata de estado-finito con el conjunto de símbolos de entrada I. Sean I^* el conjunto de todas las cadenas sobre I y w una cadena en I^*. Entonces **w es aceptada por A** si y sólo si, A va a un estado aceptable cuando los símbolos de w son entrada para A en sucesión de izquierda a derecha, empezando cuando A esté en su estado inicial. El **lenguaje aceptado por A**, que se denota por $L(A)$, es el conjunto de todas las cadenas que son aceptadas por A.

Ejemplo 12.2.4 Determinación del lenguaje aceptado por un autómata

Considere el autómata de estado-finito A definido en el ejemplo 12.2.2 y que se muestra otra vez a continuación:



a. ¿A qué estados va A si los símbolos de las siguientes cadenas son entrada para A en sucesión, empezando por el estado inicial?

(i) 01 (ii) 0011 (iii) 0101100 (iv) 10101

b. ¿Qué cadenas del inciso *a*) envían A a un estado aceptable?

c. ¿Cuál es el lenguaje aceptado por A?

d. ¿Existe una expresión regular que define el mismo lenguaje?

Solución

a. (i) s_2 (ii) s_0 (iii) s_1 (iv) s_2

b. Las cadenas 01 y 10101 envían A a un estado aceptable.

c. Observe que si w es cualquier cadena que termina en 01, entonces w es aceptada por A. Porque si w es cualquier cadena de longitud $n \geq 2$, entonces después de que los primeros $n - 2$ símbolos de w han sido introducidos, A está en uno de sus tres estados: s_0, s_1, o s_2. Pero en cualquiera de esos tres estados, la entrada de los símbolos 01 en sucesión envía A primero a s_1 y después al estado aceptable s_2. Así que cualquier cadena que termine en 01 es aceptada por A.

También observe que las únicas cadenas aceptadas por A son aquellas que finalizan en 01. (Es decir, ningunas otras cadenas son aceptadas por A, excepto las terminadas en 01.) La razón de esto es que el único estado aceptado de A es s_2 y la única flecha que apunta a s_2 proviene de s_1 y está marcada con 1. Así, para que una cadena de entrada w de longitud n mande A a un estado aceptable, el último símbolo de w debe ser un 1 y los primeros $n - 1$ símbolos de w deben enviar A al estado s_1. Ahora tres flechas apuntan a s_1, uno de cada uno de los tres estados de A y todas ellas marcadas con 0. Así, el último de los primeros $n - 1$ símbolos de w debe ser 0, o, en otras palabras, el siguiente al último símbolo de w debe ser 0. Entonces los últimos dos símbolos de w deben ser 01 y así sucesivamente.

$L(A) =$ conjunto de todas las cadenas de 0 y 1 que terminan en 01.

d. Sí. Una expresión regular que define $L(A)$ es $(0 \mid 1)^*01$. ■

Un autómata de estado-finito con múltiples estados aceptables puede tener dispositivos de salida anexados a cada uno de ellos, tal que el autómata pueda clasificar cadenas de entrada en una variedad de diferentes categorías, una para cada estado aceptable. Así es como los autómatas de estado-finito son empleados en el componente escáner léxico de un compilador para agrupar, los símbolos de un flujo de caracteres de entrada, en identificadores, palabras clave y así sucesivamente.

La función de estado-eventual

Ahora suponga que un autómata de estado-finito está en uno de sus estados (no necesariamente el estado inicial) y se alimenta en sucesión de una cadena de símbolos de entrada. ¿Eventualmente a qué estado irá el autómata? La función que responde a esta pregunta para cada posible combinación de cadenas de entrada y estados del autómata, se llama la *función de estado-eventual*.

• Definición

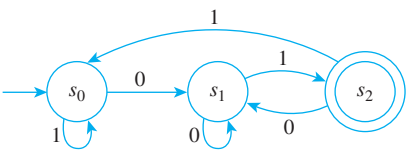
Sea A un autómata de estado-finito con un conjunto de símbolos de entrada I, conjunto de estados S y función de estado siguiente N: $S \times I \to$ S. Sea I^* el conjunto de todas las cadenas sobre I y defina la **función de estado-eventual** N^*: $S \times I^* \to S$ como sigue:

Para cualquier estado s y arbitraria cadena de entrada w,

$$N^*(s, w) = \begin{bmatrix} \text{estado al que se envía } A \text{ si los símbolos de } w \\ \text{se introducen en } A \text{ en sucesión, iniciando} \\ \text{cuando } A \text{ se encuentra en el estado } s \end{bmatrix}.$$

Ejemplo 12.2.5 Cálculo de los valores de la función de estado-eventual

Considere otra vez el autómata de estado-finito del ejemplo 12.2.2 que se muestra a continuación por conveniencia. Encuentre $N^*(s_1, 10110)$.



Solución Por definición de la función estado-eventual,

$$N^*(s_1, 10110) = \begin{bmatrix} \text{estado al cual va } A \text{ si los símbolos de } 10110 \\ \text{se introducen en } A \text{ en sucesión, iniciando} \\ \text{cuando } A \text{ se encuentra en el estado } s_1 \end{bmatrix}.$$

En referencia al diagrama de transición de A, puede ver que iniciando en s_1, cuando se introduce un 1, A se envía a s_2; entonces cuando se introduce un 0, A retorna a s_1; después de eso, cuando se introduce un 1, A se manda a s_2; de ahí, cuando se introduce un 1, A se manda a s_0 y finalmente, cuando se introduce un 0, A retorna a s_1. Esta sucesión de transiciones de estado puede ser escrita como sigue:

$$s_1 \xrightarrow{1} s_2 \xrightarrow{0} s_1 \xrightarrow{1} s_2 \xrightarrow{1} s_0 \xrightarrow{0} s_1.$$

Así, después de que se han introducido en sucesión todos los símbolos de 10110, el estado eventual de A es s_1, entonces

$$N^*(s_1, 10110) = s_1.$$ ■

Las definiciones de cadena y de lenguaje aceptados por un autómata se pueden reescribir simbólicamente empleando la función de estado-eventual. Suponga que A es un autómata de estado-finito al que se introducen un conjunto de símbolos I y la función de siguiente estado N y suponga que I^* es el conjunto de todas las cadenas sobre I y que w es una cadena en I^*.

$$w \text{ es aceptada por } A \iff N^*(s_0, w) \text{ es un estado aceptable de } A.$$

$$L(A) = \{w \in I^* \mid N^*(s_0, w) \text{ es un estado aceptable de } A\}$$

Diseño de un autómata de estado-finito

Ahora consideremos el problema de iniciar con la descripción de un lenguaje y diseñar un autómata que acepte exactamente ese lenguaje.

Ejemplo 12.2.6 Un autómata de estado-finito que acepta el conjunto de cadenas de 0 y 1 para el cual la cantidad de 1 es divisible por 3

a. Diseñe un autómata de estado-finito A que acepte el conjunto de todas las cadenas de 0 y 1 tales que la cantidad de 1's en la cadena es divisible por 3.

b. ¿Existe una expresión regular que defina a este conjunto?

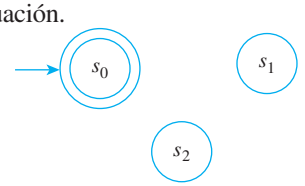
Solución

a. Sean s_0 el estado inicial de A, s_1 su estado después de que se ha introducido un 1 y s_2 su estado después se han introducido dos 1's. Observe que s_0 es el estado de A después de la introducción de cero 1 y como cero es divisible por 3 ($0 = 0 \cdot 3$), s_0 debe ser un estado aceptable. Los estados s_0, s_1 y s_2 deben ser diferentes entre sí porque desde el estado s_0 se necesitan tres 1's para alcanzar un nuevo total divisible por 3, mientras que del estado s_1 son necesarios dos 1's y desde el estado s_2 sólo se requiere un 1.

Ahora el estado de A después de la introducción de tres 1's también se puede tomar como s_0 ya que después de la entrada de tres 1's, se necesitan tres más para alcanzar un nuevo total divisible por 3. Más generalmente, si se han introducido $3k$ 1's en A, en donde k es cualquier entero no-negativo, entonces se necesitan tres más para que otra vez el total sea divisible por 3 (ya que $3k + 3 = 3(k + 1)$). Así que el estado en el cual se han introducido $3k$ 1's, para k entero arbitrario no-negativo, se puede tomar como el estado inicial s_0.

Por un razonamiento similar, los estados en los cuales se han introducido $(3k + 1)$ 1's y $(3k + 2)$ 1's, en donde k es un entero no-negativo, se pueden seleccionar como s_1 y s_2, respectivamente.

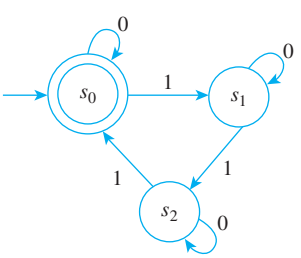
Ahora cada entero no-negativo se puede escribir en una de las tres formas $3k$, $3k + 1$ o $3k + 2$ (véase la sección 4.4), así los tres estados s_0, s_1 y s_2 son todo lo que se requiere para crear A. Entonces los estados de A se pueden dibujar y etiquetar como se muestra a continuación.



Considere las posibles entradas en A en cada uno de sus estados. No importa en qué estado se encuentre A, si se introduce un 0 entonces el número total de 1's en la cadena de entrada permanece inalterado. Por tanto, existe un bucle con cada estado marcado 0.

Ahora suponga que se introduce un 1 en A cuando éste se encuentra en el estado s_0. Entonces A va al estado s_1 (ya que el número total de 1's en la cadena de entrada ha cambiado de $3k$ a $3k + 1$). Similarmente, si se introduce un 1 en A cuando éste está en el estado s_1, entonces A va al estado s_2 (porque el número total de 1's en la cadena de entrada ha cambiado de $3k + 1$ a $3k + 2$). Finalmente, si se introduce un 1 en A cuando éste se encuentra en el estado s_2, entonces va al estado s_0 (ya que el número total de 1's en la cadena de entrada será $(3k + 2) + 1 = 3k + 3 = 3(k + 1)$, que es un múltiplo de 3).

Se sigue que el diagrama de transición para A tiene el aspecto que se muestra a continuación.



Este autómata acepta el conjunto de cadenas de 0 y 1 para las cuales el número de 1 es divisible por 3.

b. Una expresión regular que define al conjunto dado es $0^* \mid (0^*10^*10^*10^*)^*$. ■

Ejemplo 12.2.7 Un autómata de estado-finito que acepta al conjunto de todas las cadenas de 0 y 1 que contienen exactamente un 1

a. Diseñe un autómata de estado-finito A que acepte al conjunto de todas las cadenas de 0 y 1 que contienen exactamente un 1.

b. ¿Existe una expresión regular que defina a este conjunto?

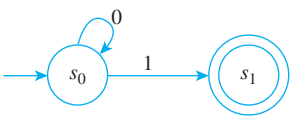
Solución

a. El autómata A debe tener al menos dos estados distintos:

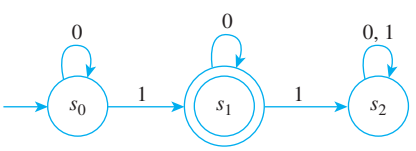
s_0: estado inicial;

s_1: estado al cual A se mueve cuando la cadena de entrada contiene exactamente un 1.

Si A está en el estado s_0 y se introduce un 0, entonces A puede ya sea permanecer en el estado s_0 (porque necesita esperar un 1 para moverse al estado s_1), pero tan pronto como se introduce un 1, A se mueve al estado s_1. A continuación se muestra un dibujo parcial del diagrama de transición.



Ahora consideremos qué pasa cuando A se encuentra en el estado s_1. Si se introduce un 0, entonces la cadena de entrada continúa teniendo un solo 1, así que A permanece en el estado s_1. Pero si se introduce un 1, entonces la cadena de entrada contiene más de un 1, por lo que A debe dejar s_1 (ya que ninguna cadena con más de un 1 es aceptada por A). No puede retornar al estado s_0 porque no hay forma de ir de s_0 a s_1 y después de la entrada del segundo 1, A nunca puede retornar al estado s_1. Por tanto, A debe ir a un tercer estado, s_2, del cual no hay retorno a s_1. Así ya que en s_2 cada entrada puede muy bien dejar A en el estado s_2. Se tiene que el diagrama de transición completo para A tiene la apariencia que se muestra a continuación.

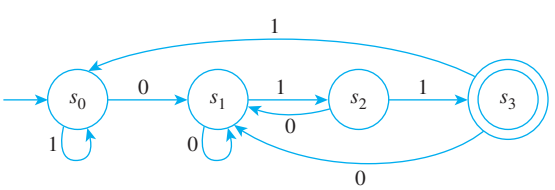


Este autómata acepta al conjunto de cadenas de 0 y 1, con exactamente un 1.

b. Una expresión regular que define al conjunto dado es 0^*10^*. ■

Simulación de un autómata de estado-finito utilizando software

Suponga que se han codificado ciertos objetos con cadenas de 0 y 1. Se debe escribir un programa para controlar el procesamiento de los objetos codificados mediante cadenas que finalizan en 011; se ignoraran los objetos codificados de otra manera. Esta situación se puede modelar por el autómata de estado-finito que se muestra en la figura 12.2.5.



Este autómata reconoce cadenas que terminan en 011.

Figura 12.2.5

Los símbolos del código del objeto se alimentan en sucesión en este autómata y cada cadena de símbolos en un código dado envía al autómata a uno de los cuatro estados s_0, s_1, s_2, o s_3. Si se alcanza el estado s_3, el objeto se procesa; en caso contrario, el objeto se ignora.

La acción de este autómata de estado-finito se puede simular con un algoritmo computacional como el dado en el algoritmo 12.2.1.

Algoritmo 12.2.1 Un autómata de estado-finito

[Este algoritmo simula la acción del autómata de estado-finito de la figura 12.2.5, por mimetización del funcionamiento del diagrama de transición. Los estados se denotan por 0, 1, 2 *y* 3.*]*

Entrada: *cadena [cadena de* 0 *y* 1 *más un marcador final e]*

Cuerpo del algoritmo:

```
estado := 0
símbolo := primer símbolo en la cadena de entrada
while (símbolo ≠ e)
      if estado = 0 then if símbolo = 0
                         then estado := 1
                         else estado := 0
  else if estado = 1 then if símbolo = 0
                         then estado := 1
                         else estado := 2
  else if estado = 2 then if símbolo = 0
                         then estado := 1
                         else estado := 3
  else if estado = 3 then if símbolo = 0
                         then estado := 1
                         else estado := 0
  símbolo := próximo símbolo en la cadena de entrada
end while
```

[Después de la ejecución del bucle ***while****, el valor del estado es* 3 *si y sólo si, la cadena de entrada finaliza con* 011*e.]*

Salida: *estado*

Observe cómo el uso del autómata de estado-finito permite al creador del algoritmo enfocarse sobre cada etapa del análisis de la cadena de entrada independientemente de las otras etapas.

Una forma alternativa de programar este autómata es introducir directamente los valores de la función siguiente estado como un arreglo bidimensional. Esto se hace en el algoritmo 12.2.2.

Algoritmo 12.2.2 Un autómata de estado-finito

[Este algoritmo simula la acción del autómata de estado-finito de la figura 12.2.5 mediante repetida aplicación de la función siguiente estado. Los estados se denotan 0, 1, 2 *y* 3.*]*

Entrada: *cadena [cadena de* 0 *y* 1 *más un marcador final e]*

Cuerpo del algoritmo:

$N(0, 0) := 1, N(0, 1) := 0, N(1, 0) := 1, N(1, 1) := 2,$
$N(2, 0) := 1, N(2, 1) := 3, N(3, 0) := 1, N(3, 1) := 0$
estado := 0
símbolo := primer símbolo en la cadena de entrada
while (*símbolo* $\neq e$)
    estado := N (*estado*, *símbolo*)
    símbolo := próximo símbolo en la cadena de entrada
end while
[Después de la ejecución del bucle ***while****, el valor del estado es 3 si y sólo si, la cadena de entrada termina en 011e.]*

Salida: *estado*

Autómatas de estado-finito y expresiones regulares

En las secciones previas, cada vez que consideramos un lenguaje aceptado por un autómata de estado-finito, encontramos una expresión regular que define el mismo lenguaje. Stephen Kleene demostró que nuestra habilidad para esto no es pura coincidencia. Él probó que cualquier lenguaje aceptado por un autómata de estado-finito se puede definir por una expresión regular y que, inversamente, cualquier lenguaje definido por una expresión regular es aceptado por un autómata de estado-finito. Así para las muchas aplicaciones de expresiones regulares analizadas en la sección 12.1, teóricamente es posible encontrar un autómata de estado-finito correspondiente, el cual se puede entonces simular empleando los tipos de algoritmos computacionales descritos en la subsección previa.

En la práctica, es de frecuente interés retener solamente pedazos de los patrones solicitados. Por ejemplo, para obtener una referencia en un documento HTML, se especificaría una expresión regular definiendo la completa etiqueta HTML, <a href= "la deseada URL">, pero se estaría interesado en recuperar solamente la cadena entre las marcas indicadas. Debido a ese tipo de consideraciones, las implementaciones actuales de autómatas de estado-finito incluyen características adicionales.*

El enunciado del teorema de Kleene lo separamos en dos partes.

Teorema de Kleene, Parte 1

Dado cualquier lenguaje aceptado por un autómata de estado-finito, existe una expresión regular que define el mismo lenguaje.

Demostración:

Suponga que A es un autómata de estado-finito con un conjunto I de símbolos de entrada, un conjunto S de n estados y una función de siguiente estado N: $S \times I \rightarrow S$. Sea que I^* denote el conjunto de todas las cadenas sobre I. Numere los estados s_1, s_2, s_3, … s_n, empleando s_1 para representar el estado inicial y para cada entero $k = 1, 2, 3, \ldots, n$, sean

$$L_{i,j}^{k} = \left\{ x \in I^* \;\middle|\; \begin{array}{l} \text{cuando los símbolos de } x \text{ se introducen en sucesión} \\ \text{en } A, \text{ éste va del estado } s_i \text{ al estado } s_j \text{ sin pasar a través} \\ \text{de un estado intermedio } s_h \text{ para el que } h > k \end{array} \right\}.$$

continúa en la página 802

*Para mayor información, vea *Dominando Expresiones Regulares*, 3a. ed., Jeffrey E. F. Friedl, (Sebastopol, CA: O'Reilly & Associates, 2006)

Observe que cada índice i o j en $L^k_{i,j}$ podría ser mayor que k; la única restricción es que los símbolos de una cadena en $L^k_{i,j}$ no pueden hacer que A entre o salga de un estado intermedio con índice mayor que k.

Si s_j es un estado aceptable y si $k = n$ e $i = 1$, entonces $L^n_{1,j}$ es el conjunto de todas las cadenas que envían A a s_j cuando los símbolos de la cadena se introducen en sucesión en A iniciando de s_1. Así

$$L^n_{1,j} \subseteq L(A).$$

Además, como la sucesión de símbolos en cada cadena en $L(A)$ manda A hacia *algún* estado aceptable s_j, entonces

$L(A)$ es la unión de todos los conjuntos $L^k_{i,j}$, en donde s_j es un estado aceptable.

Usemos una versión de inducción matemática para construir un conjunto de expresiones regulares sobre I. Aceptemos que la propiedad $P(m)$ es la frase:

Para cualquier par de enteros i y j con $1 \leq i, j \leq n$,
existe una expresión regular $r^m_{i,j}$ que define a $L^m_{i,j}$. ← *P(m)*

Demostración de que P(0) es verdadera: Para cada par de enteros i y j con $1 \leq i, j \leq n$, $L^0_{i,j}$ es el conjunto de todas las cadenas que envían A de s_i a s_j sin mandarlo a través del estado intermedio s_h tal que $h > 0$. Como el subíndice de cada estado en A es mayor que cero, las cadenas en $L^0_{i,j}$ no envían A a cualquier estado intermedio y así cada uno es un solo símbolo de entrada de I. En otras palabras, para todos los enteros i y j con $1 \leq i, j \leq n$,

$$L^0_{i,j} = \{a \in I \mid N(s_i, a) = s_j\}.$$

Así $L^0_{i,j}$ es un subconjunto de I, entonces (porque I es finito) podemos denotar a los elementos de $L^0_{i,j}$ como sigue:

$$L^0_{i,j} = \{a_1, a_2, a_3, \ldots, a_M\} \subseteq I.$$

Ahora, por definición de expresión regular, cada símbolo de entrada de I es una expresión regular sobre I; así cada elemento de $L^0_{i,j}$ es una expresión regular sobre I. El resultado es que para todos los enteros i y j con $1 \leq i, j \leq n$, la siguiente expresión regular define a $L^0_{i,j}$:

$$a_1 \mid a_2 \mid a_3 \ldots \mid a_M$$

Demostración de que para todos los enteros k con $0 \leq k < n$, si P(k) es verdadera entonces P(k + 1) es verdadera: Sea k cualquier entero con $1 \leq k < n$ y suponga que

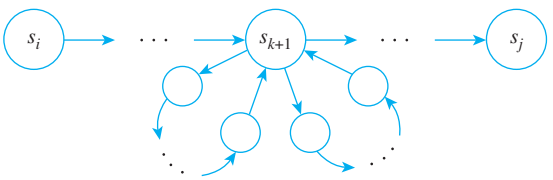
Para cada par de enteros p y q con $1 \leq p, q \leq n$, ← *P(k)*
existe una expresión regular $r^k_{p,q}$ que define a $L^k_{p,q}$. Hipótesis de inducción.

Demostraremos que:

Para cada par de enteros i y j con $1 \leq i, j \leq n$,
existe una expresión regular $r^{k+1}_{i,j}$ que define a $L^{k+1}_{i,j}$. ← *P(k + 1)*

Así supongamos que i y j son cualquier par de enteros con $1 \leq i, j \leq n$ y observemos que cualquier cadena en $L^{k+1}_{i,j}$ envía A de s_i a s_j, por una ruta que hace pasar A por s_{k+1} o por una ruta en la que A no pasa por s_{k+1}. Ahora cada cadena que manda A de s_i a s_j y hace pasar A por s_{k+1} una o más veces se puede separar en dos segmentos.

Los símbolos en el primer segmento envían A de s_i a s_{k+1} sin hacer pasar a A por s_{k+1}; aquellos en los que cada uno de los segmentos intermedios mandan a s_{k+1} a sí mismo sin que A pase por s_{k+1} y los del segmento final envían A de s_{k+1} a s_j sin que A pase por s_{k+1}. (El segmento intermedio podría ser la cadena nula.) A continuación se ilustra una trayectoria típica que muestra dos segmentos intermedios.



Observe que cada segmento intermedio de la cadena está en $L^k_{k+1,k+1}$, y por suposición la expresión regular $r^k_{k+1,k+1}$ define este conjunto. Por el mismo razonamiento, $r^k_{i,k+1}$ define al conjunto de todos los posibles primeros segmentos de la cadena y $r^k_{k+1,j}$ define al conjunto de todos los posibles segmentos finales de la cadena. Además, $r^k_{i,j}$ define al conjunto de todas las cadenas que envían A de s_i a s_j sin que A pase por un estado s_m con $m > k$. Así podemos definir la expresión regular $r^{k+1}_{i,j}$ como sigue:

$$r^{k+1}_{i,j} = r^k_{i,j} \mid r^k_{i,k+1} \left(r^k_{k+1,k+1}\right)^* r^k_{k+1,j}.$$

Entonces $r^{k+1}_{1,j}$ define al conjunto de todas las cadenas que envían A de s_1 a s_j sin que A pase por los estados s_m con $m > k + 1$ y entonces $r^{k+1}_{1,j}$ define a $L^{k+1}_{1,j}$ *[que era lo que se quería demostrar]*.

Para completar la demostración, sean S_{j1}, S_{j2},..., S_{jk} los estados aceptables de A. Como $L(A)$ es la unión de todos los $L^n_{1,j}$ en donde s_j es un estado aceptable, entonces tenemos

$$\begin{aligned} L(A) &= L\left(r^n_{1,j_1}\right) \cup L\left(r^n_{1,j_2} \cup \cdots \cup L\left(r^n_{1,j_n}\right)\right. \\ &= L\left(r^n_{1,j_1} \mid r^n_{1,j_2} \mid \cdots \mid r^n_{1,j_n}\right) \end{aligned}$$

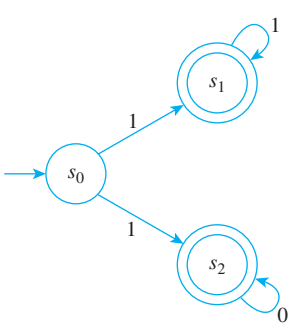
por la definición recursiva para el lenguaje definido por una expresión regular.

Así, si hacemos $r = r^n_{1,j_1} \left| r^n_{1,j_2} \right| \cdots \left| r^n_{1,j_n} \right.$, , tenemos que $L(A) = L(r)$. En otras palabras, hemos construido una expresión regular r que define el lenguaje aceptado por A.

Teorema de Kleene, Parte 2

Dado cualquier lenguaje definido por una expresión regular, existe un autómata de estado-finito que acepta el mismo lenguaje.

La manera más común de demostrar la parte 2 del teorema de Kleene consiste en introducir una nueva categoría de autómatas, llamados *autómatas de estado-finito no-deterministas*. Son similares a los autómatas de estado-finito (deterministas) que hemos analizado, excepto que para cualquier estado y símbolo de entrada dados, el siguiente estado es un subconjunto del conjunto de estados del autómata, que podría ser el conjunto vacío. Así el siguiente estado del autómata no está unívocamente determinado por la combinación de un estado presente y un símbolo de entrada. Una cadena es aceptada por un autómata de estado-finito no-determinista si y sólo si, cuando los símbolos en la cadena se introducen en sucesión al autómata, a partir de un estado inicial, existe *alguna* sucesión de estados próximos a través de los cuales el autómata podría viajar para enviarlo a un estado aceptable. Por ejemplo, el diagrama de transición a la izquierda es un ejemplo de un autómata de estado-finito no-determinista muy simple que acepta al conjunto de todas las cadenas empezando con un 1. Observe que $N(s_0, 1) = \{s_1, s_2\}$ y $N(s_0, 0) = \emptyset$.



Dado un lenguaje definido por cualquier expresión regular, existe un algoritmo recursivo rutinario para encontrar un autómata de estado-finito no-determinista que define el mismo lenguaje. La demostración del teorema de Kleene queda completa al demostrar que para cualquier autómata de estado-finito no-determinista de este tipo, existe un autómata de estado-finito (determinista) que define el mismo lenguaje. Los detalles de la demostración se dejan para un curso en teoría de autómatas.

Lenguajes regulares

De acuerdo al teorema de Kleene, el conjunto de lenguajes definidos por expresiones regulares es idéntico al conjunto de lenguajes aceptados por autómatas de estado-finito. Cualquiera de estos lenguajes se llama un **lenguaje regular**. Las breves alusiones que hicimos a lenguajes libres de contexto y a la clasificación de Chomsky sugieren que no todo lenguaje es regular. Probaremos esto dando un ejemplo de un lenguaje no-regular.

Para construir el ejemplo, observe que como un autómata de estado-finito sólo puede asumir un número finito de estados y puesto que hay una cantidad infinita de sucesiones de entrada, por el principio de las casillas debe existir al menos un estado al cual el autómata retorna una y otra vez. Este es el aspecto esencial de un autómata que hace posible encontrar un lenguaje no-regular.

Ejemplo 12.2.8 Demostración de que un lenguaje es no regular

Sea el lenguaje L que consiste de todas las cadenas de la forma $a^k b^k$, en donde k es un entero positivo. Simbólicamente, L es el lenguaje sobre el alfabeto $\Sigma = \{a, b\}$ definido por

$$L = \{s \in \Sigma^* \mid s = a^k b^k, \text{ donde } k \text{ es un entero positivo}\}$$

Use el principio de las casillas para demostrar que L es no regular. En otras palabras, demuestre que no existe un autómata de estado-finito que acepta a L.

Solución *[Use una demostración por contradicción.]* Suponga que no. Es decir, acepte que existe un autómata de estado-finito A que acepta a L. *[Se obtendrá una contradicción.]* Como A sólo tiene un número finito de estados, éstos se pueden denotar por $s_1, s_2, s_3, \ldots, s_n$, en donde n es un entero positivo. Considere todas las cadenas de entrada que consisten enteramente de a: $a, a^2, a^3, a^4, \ldots$. Ahora existe una infinidad de tales cadenas y solamente una cantidad finita de estados. Así, por el principio de las casillas, deben existir un estado s_m y dos cadenas de entrada a^p y a^q con $p \neq q$ tales que cuando a^p o a^q sean entradas de A, éste vaya al estado s_m. (Vea la figura 12.2.6.) *[Las palomas son las cadenas de a, las casillas son los estados y la correspondencia asocia cada cadena con el estado al cual A va cuando se introduce la cadena.]*

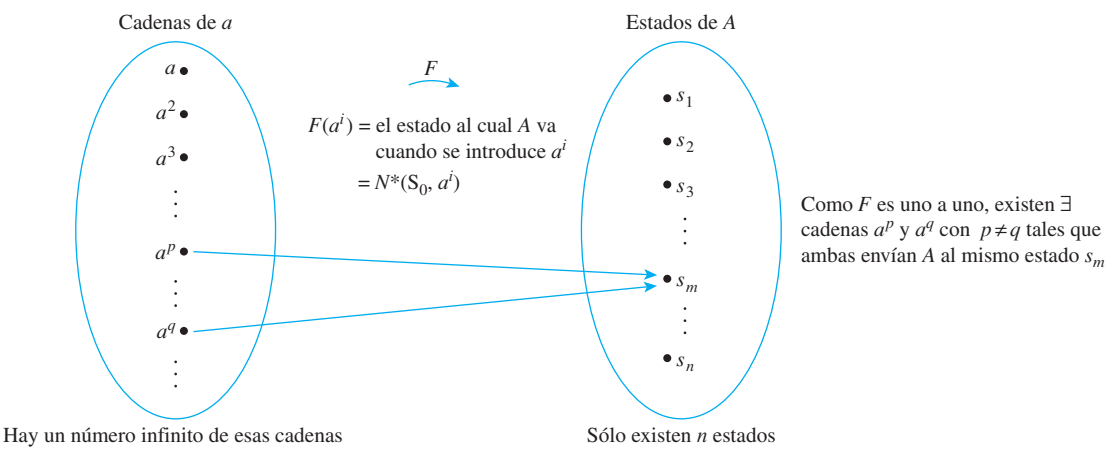


Figura 12.2.6

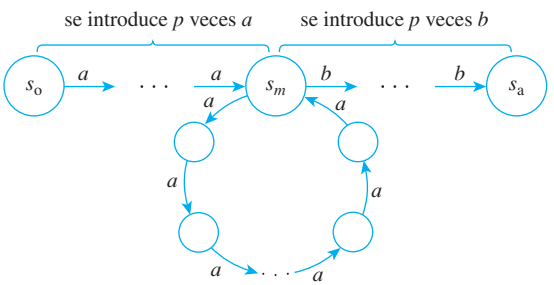
Ahora, por suposición, A acepta L. Así A acepta la cadena

$$a^p b^p.$$

Esto significa que después de que se ha introducido a p veces, entonces A se encuentra en el estado s_m y de que se ha introducido p veces b se envía a A al estado aceptable s_a. Pero eso implica que:

$$a^q b^p$$

también envía A al estado aceptable s_a y así $a^q b^p$ es aceptada por A. La razón es que después de la introducción de q veces a, A también va al estado s_m y a partir de ahí, la entrada de p veces b envía A al estado s_a, que es un estado aceptable. Pictóricamente, si $p < q$, entonces



se introducen adicionalmente
$q - p$ veces a

Ahora, por suposición, L es el lenguaje aceptado por A. Así puesto que s es aceptado por A, entonces $s \in L$. Pero por definición de L, éste consiste sólo de cadenas con igual cantidad de a y b. Como $p \neq q$, entonces s no es elemento de L. Por tanto, $s \notin L$ y s no es elemento de L, lo que es una contradicción.

Se tiene que la suposición es falsa y así no existe un autómata de estado-finito que acepte a L. ■

Autoexamen

1. Los cinco objetos que forman un autómata de estado-finito son _____, _____, _____, _____ y _____.
2. La tabla de siguiente estado para un autómata muestra los valores de _____ .
3. En las anotaciones de la tabla de estado siguiente, el estado inicial se indica con un _____ y los estados aceptables están marcados por _____.
4. Una cadena w que consiste de símbolos de entrada es aceptada por un autómata de estado-finito A si y sólo si, _____.
5. El lenguaje aceptado por un autómata de estado-finito A es _____ .
6. Si N es la función de estado siguiente para un autómata de estado-finito A, la función de estado-eventual N^* está definida como sigue: Para cada estado s de A y para cada cadena w que consiste de símbolos de entrada de A, $N^*(s, w) =$ _____.
7. Una parte del teorema de Kleene dice que dado cualquier lenguaje que es aceptado por un autómata de estado-finito, existe _____.
8. La segunda parte del teorema de Kleene expresa que dado cualquier lenguaje definido por una expresión regular, existe _____.
9. Un lenguaje regular es _____.
10. Dado el lenguaje que consiste de todas las cadenas de la forma $a^k b^k$, en donde k es un entero positivo, el principio de las casillas se puede emplear para demostrar que el lenguaje es _____.

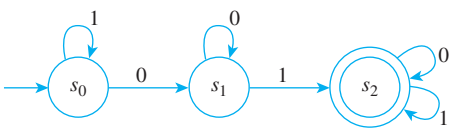
Conjunto de ejercicios 12.2

1. Encuentre el estado de la máquina automática del ejemplo 12.2.1, después de que se han introducido las siguientes sucesiones de monedas:
   a. Peseta, medio dólar, peseta
   b. Peseta, medio dólar, medio-dólar
   c. Medio dólar, peseta, peseta, peseta, medio dólar

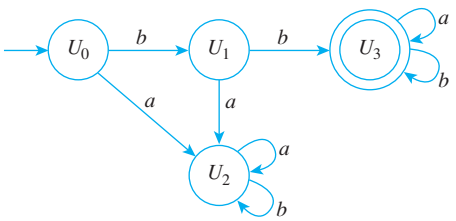
En los ejercicios del 2 al 7 se da un autómata de estado-finito con un diagrama de transición. Para cada autómata:

a. Encuentre sus estados.
b. Determine sus símbolos de entrada.
c. Obtenga su estado inicial.
d. Encuentre sus estados aceptables.
e. Escriba su tabla de siguiente estado.

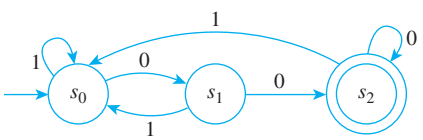
2.



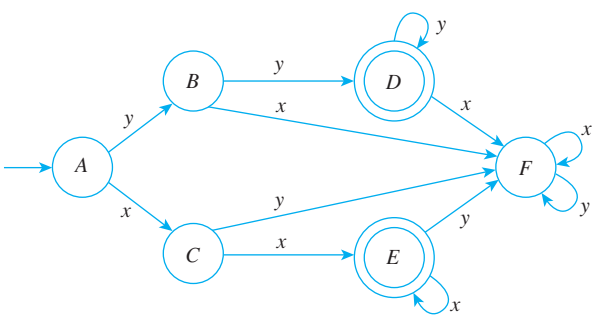
3.



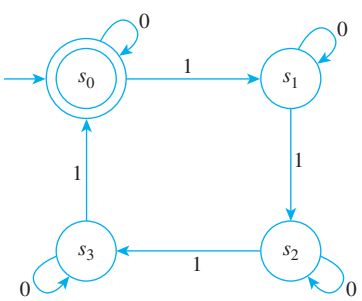
4.



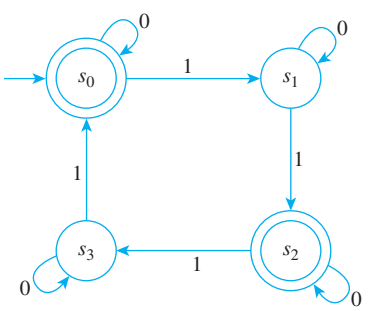
5.



6.



7.



En los ejercicios 8 y 9 se da un autómata de estado-finito con una tabla de siguiente estado. Para cada autómata:

a. Encuentre sus estados.
b. Determine sus símbolos de entrada.
c. Obtenga su estado inicial.
d. Encuentre sus estados aceptables.
e. Dibuje su diagrama de transición.

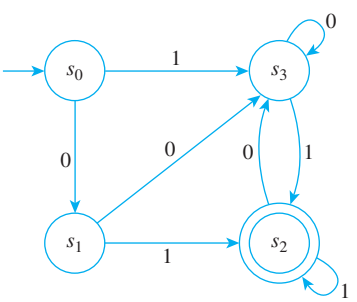
8. Tabla de estado siguiente.

	Estado	Entrada 0	Entrada 1
→	s_0	s_1	s_2
	s_1	s_1	s_2
◎	s_2	s_1	s_2

9. Tabla de estado siguiente.

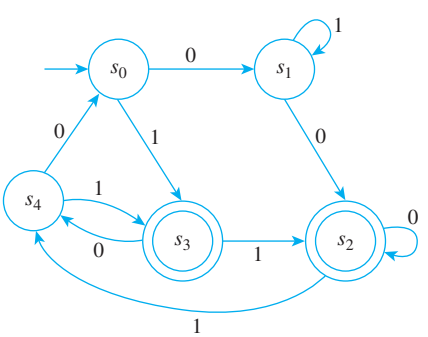
	Estado	Entrada 0	Entrada 1
→	s_0	s_0	s_1
◎	s_1	s_1	s_2
	s_2	s_2	s_3
	s_3	s_3	s_0

10. Un autómata de estado-finito A, dado por el diagrama de transición que se muestra a continuación, tiene la función de siguiente estado N y la función de estado-eventual N^*.



a. Encuentre $N(s_1, 1)$ y $N(s_0, 1)$.
b. Encuentre $N(s_2, 0)$ y $N(s_1, 0)$.
c. Encuentre $N^*(s_0, 10011)$ y $N^*(s_1, 01001)$.
d. Encuentre $N^*(s_2, 11010)$ y $N^*(s_0, 01000)$.

11. Un autómata de estado-finito A, dado por el diagrama de transición que se muestra a continuación, tiene la función de siguiente estado N y la función de estado-eventual N^*:



a. Encuentre $N(s_3, 0)$ y $N(s_2, 1)$.
b. Encuentre $N(s_0, 0)$ y $N(s_4, 1)$.
c. Encuentre $N^*(s_0, 010011)$ y $N^*(s_3, 01101)$.
d. Encuentre $N^*(s_0, 1111)$ y $N^*(s_2, 00111)$.

12. Considere de nuevo al autómata de estado-finito del ejercicio 2.
a. ¿A qué estado va el autómata cuando se introducen en sucesión los símbolos de las siguientes cadenas, empezando desde el estado inicial?
(i) 1110001 (ii) 0001000 (iii) 11110000
b. ¿Cuál de las cadenas del inciso *a*) envían al autómata a un estado aceptable?
c. ¿Cuál es el lenguaje aceptado por el autómata?
d. Encuentre una expresión regular que defina el lenguaje.

13. Considere de nuevo al autómata de estado-finito del ejercicio 3.
a. ¿A qué estado va el autómata cuando se introducen en sucesión los símbolos de las siguientes cadenas, partiendo del estado inicial?
(i) *bb* (ii) *aabbbaba* (iii) *babbbbbabaa* (iv) *bbaaaabaa*
b. ¿Cuál de las cadenas del inciso *a*) envían al autómata a un estado aceptable?
c. ¿Cuál es el lenguaje aceptado por el autómata?
d. Encuentre una expresión regular que defina el lenguaje.

En los ejercicios del 14 al 19, *a*) encuentre el lenguaje aceptado por el autómata en el ejercicio referenciado y *b*) determine una expresión regular que defina el mismo lenguaje.

14. Ejercicio 4 **15.** Ejercicio 5 16. Ejercicio 6
17. Ejercicio 7 **18.** Ejercicio 8 19. Ejercicio 9

En los ejercicios del 20 al 28, *a*) diseñe un autómata con el alfabeto de entrada dado que acepta el conjunto de cadenas dado y *b*) encuentre una expresión regular que defina el lenguaje aceptado por el autómata.

20. Alfabeto de entrada = {0, 1}; Acepta el conjunto de todas las cadenas para las cuales los tres símbolos de entrada finales son 1.

***H* 21.** Alfabeto de entrada = {*a*, *b*}; Acepta el conjunto de todas las cadenas de longitud al menos 2 para las cuales los dos símbolos de entrada finales son iguales.

22. Alfabeto de entrada = {0, 1}; Acepta el conjunto de todas las cadenas que inician con 01 o 10.

23. Alfabeto de entrada = {0, 1}; Acepta el conjunto de todas las cadenas que empiezan con 01.

24. Alfabeto de entrada = {0, 1}; Acepta el conjunto de todas las cadenas que inician con 101.

25. Alfabeto de entrada = {0, 1}; Acepta el conjunto de todas las cadenas que finalizan en 10.

26. Alfabeto de entrada = {*a*, *b*}; Acepta el conjunto de todas las cadenas que contienen exactamente dos *b*.

27. Alfabeto de entrada = {0, 1}; Acepta el conjunto de todas las cadenas que empiezan con 0 y contienen exactamente un 1.

28. Alfabeto de entrada = {0, 1}; Acepta el conjunto de todas las cadenas que contienen el patrón 010.

En los ejercicios del 29 al 47, diseñe un autómata de estado-finito que acepte el lenguaje definido por la expresión regular en el ejercicio referenciado de la sección 12.1.

29. Ejercicio 16 30. Ejercicio 17 **31.** Ejercicio 19
32. Ejercicio 19 **33.** Ejercicio 20 34. Ejercicio 21
35. Ejercicio 24 **36.** Ejercicio 25 37. Ejercicio 26
38. Ejercicio 27 **39.** Ejercicio 31 40. Ejercicio 32
41. Ejercicio 33 **42.** Ejercicio 34 43. Ejercicio 35
44. Ejercicio 36 **45.** Ejercicio 37 46. Ejercicio 38
47. Ejercicio 39

48. Un sistema interruptor telefónico simplificado permite las siguientes cadenas como números telefónicos legales:
a. Una cadena de siete dígitos con ninguno de los primeros dos dígitos *a* 0 o *a* 1 (*una cadena de llamada local*).
b. Un 1 seguido por una *cadena código de área* de tres dígitos (cualquier dígito excepto 0 o 1 seguido por un 0 o 1 seguido por cualquier dígito) seguido por una cadena de llamada local de siete dígitos.
c. Un 0 solo o seguido por una cadena código de área de tres dígitos más una cadena de llamada local de siete dígitos.

Diseñe un autómata de estado-finito para reconocer todos los números telefónicos legales en *a*), *b*) y *c*). Incluya un "estado de error" para invalidar los números telefónicos.

49. Escriba un algoritmo computacional que simule la acción del autómata de estado-finito del ejercicio 2, mimetizando la acción del diagrama de transición.

50. Escriba un algoritmo computacional que simule la acción del autómata de estado-finito del ejercicio 8, mediante repetida aplicación de la función siguiente estado.

***H* 51.** Sea L el lenguaje que consiste de todas las cadenas de la forma

$a^m b^n$, en donde m y n son enteros positivos con $m \geq n$.

Demuestre que no existe autómata de estado-finito que acepte a L.

52. Sea L el lenguaje que consiste de todas las cadenas de la forma

$a^m b^n$, en donde m y n son enteros positivos y $m \leq n$.

Demuestre que no existe autómata de estado-finito que acepte a L.

***H* 53.** Sea L el lenguaje que consiste de todas las cadenas de la forma

a^n, en donde $n = m^2$, para algún entero positivo m.

Demuestre que no existe autómata de estado-finito que acepte a L.

54. a. Sea A un autómata de estado-finito con alfabeto de entrada Σ y suponga que $L(A)$ es el lenguaje aceptado por A. El complemento de $L(A)$ es el conjunto de todas las cadenas sobre Σ que no están en $L(A)$. Demuestre que el complemento de un lenguaje regular es regular, demostrando lo siguiente: Si $L(A)$ es el lenguaje aceptado por un autómata de estado-finito

A, entonces existe un autómata de estado-finito A' que acepta el complemento de $L(A)$.

b. Demuestre que la intersección de cualesquiera dos lenguajes regulares es regular, como sigue: Primero pruebe que si $L(A_1)$ y $L(A_2)$ son lenguajes aceptados por los autómatas A_1 y A_2, respectivamente, entonces existe un autómata A que acepta $(L(A_1))^c \cup (L(A_2))^c$. Después use una de las leyes de De Morgan para conjuntos, la ley del doble complemento para conjuntos y el resultado del inciso *a*) para demostrar que existe un autómata que acepta $L(A_1) \cap L(A_2)$.

Respuestas del autoexamen

1. un conjunto finito de símbolos de entrada; un conjunto finito de estados; un estado inicial designado; un conjunto designado de estados aceptables; una función de estado siguiente que asocia un "estado siguiente" con cada estado y símbolo de entrada del autómata 2. la función siguiente estado para cada estado y símbolo de entrada del autómata 3. flecha; círculos dobles 4. cuando los símbolos en la cadena se introducen (de izquierda a derecha) en sucesión al autómata, empezando desde un estado inicial, el autómata finaliza en un estado aceptable 5. el conjunto de cadenas que son aceptadas por A 6. el estado al que A se mueve si está en el estado s y los caracteres de w se introducen en sucesión 7. una expresión regular que define el mismo lenguaje 8. un autómata de estado-finito que acepta el mismo lenguaje 9. un lenguaje definido por una expresión regular (*O*: un lenguaje aceptado por un autómata de estado-finito) 10. no regular.

12.3 Simplificando autómatas de estado-finito

Nuestra vida es desperdiciada por detalles… Simplifica, simplifica.
—Henry David Thoreau, *Walden*, 1854

Cualquier cadena que se introduce a un autómata de estado-finito lo envía o no a un estado aceptable y el conjunto de todas las cadenas aceptadas por un autómata es el lenguaje aceptado por él. Con frecuencia ocurre que cuando se crea un autómata para realizar cierto trabajo (como en la construcción de un compilador, por ejemplo), el autómata que emerge "naturalmente" del desarrollo del proceso es innecesariamente complicado; es decir, puede existir un autómata con muy pocos estados que acepte exactamente el mismo lenguaje. Es deseable encontrar tal autómata porque el espacio de memoria requerido para almacenar un autómata con n estados es aproximadamente proporcional a n^2. Así, 10 000 espacios de memoria se necesitan para almacenar un autómata de 100 estados, mientras que sólo se requieren 100 espacios de memoria para almacenar un autómata con 10 estados. Además, entre menos estados tenga un autómata, es más fácil escribir un algoritmo computacional basado en él y para ver que dos autómatas aceptan el mismo lenguaje, es más fácil simplificar a cada uno a un número mínimo de estados y comparar los autómatas simplificados. En esta sección mostramos cómo tomar un autómata dado y simplificarlo en el sentido de encontrar un autómata con muy pocos estados que acepte el mismo lenguaje.

Ejemplo 12.3.1 Un resumen general

Considere los autómatas de estado-finito A y A' de la figura 12.3.1. Un momento de reflexión debería convencerle de que A' acepta todas esas cadenas y sólo esas, que contienen un número par de 1. Pero A, no obstante que parece más complicado, acepta exactamente esas

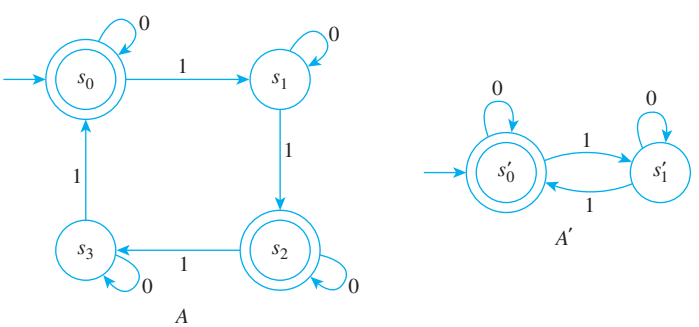


Figura 12.3.1 **Dos autómatas equivalentes**

mismas cadenas. Así, los dos autómatas son "equivalentes" en el sentido de que aceptan el mismo lenguaje, a pesar de que A' tiene mucho menos estados que A.

Burdamente hablando, la razón para la equivalencia de esos autómatas es que algunos de los estados de A se pueden combinar sin afectar la aceptación o no aceptación de cualquier cadena de entrada. Resulta así que s_2 puede ser combinado con el estado s_0 y que s_3 puede combinarse con el estado s_1. (En esta sección se explicará después cómo saber cuáles estados combinar.) El autómata con los estados combinados $\{s_0, s_2\}$ y $\{s_1, s_3\}$ se llama el *autómata cociente* de A y se denota por $\overline{A}$. Su diagrama de transición se obtiene al combinar los círculos para s_0 y s_2 y para s_1 y s_3; reemplazando cualquier flecha de un estado s a un estado t por una flecha del estado combinado que contiene a s al estado combinado que contiene t. Por ejemplo, en A hay una flecha marcada 1 de s_1 a s_2, en $\overline{A}$ existe una flecha etiquetada 1 de $\{s_1, s_2\}$ a $\{s_0, s_2\}$. En la figura 12.3.2 se muestra el diagrama de transición completo para $\overline{A}$. Como puede ver, excepto por las etiquetas de los estados, es idéntico al diagrama para A'.

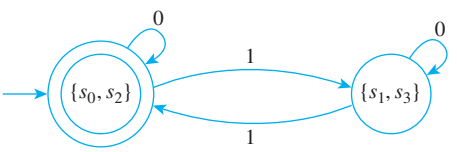


Figura 12.3.2

En general, la simplificación de un autómata de estado-finito implica identificar "estados equivalentes" que se pueden combinar sin afectar la acción del autómata sobre las cadenas de entradas. Matemáticamente hablando, esto significa definir una relación de equivalencia sobre el conjunto de estados del autómata y formar un nuevo autómata cuyos estados sean las clases de equivalencia de la relación. El resto de esta sección está dedicada al desarrollo de un algoritmo para realizar este proceso en una forma práctica.

∗-Equivalencia de Estados

Se dice que dos estados, de un autómata de estado-finito, son ∗-*equivalentes* ("estrella equivalentes") si cualquier cadena aceptada por el autómata cuando éste inicia de uno de los estados, es aceptada por el autómata cuando éste empieza desde el otro estado. Recuerde que el valor de la función estado-eventual, N^*, para un estado s y cadena de entrada w es el estado al que va el autómata si los caracteres de w se introducen en sucesión cuando el autómata se encuentra en el estado s.

• Definición

Sea A un autómata de estado-finito con función de siguiente estado N y función de estado-eventual N^*. Defina una relación binaria sobre el conjunto de estados de A como sigue: Dados los estados arbitrarios s y t de A, decimos que ***s* y *t* son ∗-equivalentes** y se escribe $s \; R_* \; t$ si y sólo si, para todas las cadenas de entrada w,

$N^*(s, w)$ y $N^*(t, w)$ ambos son estados aceptables o ambos son estados no-aceptables.

En otras palabras, los estados s y t son ∗-equivalentes si y sólo si, para todas las cadenas de entrada w,

$$N^*(s, w) \text{ es un estado aceptable} \quad \Leftrightarrow \quad N^*(t, w) \text{ es un estado aceptable.}$$

O, simplemente, para todas las cadenas de entrada w,

$$\left[\begin{array}{l}A \text{ va a un estado aceptable si } w\\ \text{se introduce cuando } A \text{ se encuentra}\\ \text{en el estado } s,\end{array}\right] \Leftrightarrow \left[\begin{array}{l}A \text{ se mueve a un estado aceptable}\\ \text{si } w \text{ se introduce cuando } A \text{ está en}\\ \text{el estado } t\end{array}\right].$$

Por sustitución en la definición, se sigue inmediatamente que:

R_* es una relación de equivalencia sobre S, el conjunto de estados de A. 12.3.1

En los ejercicios del final de esta sección se le pide demostrar esto de manera formal.

k-Equivalencia de estados

Desde un punto de vista operacional, mediante la definición directa es difícil determinar la $*$-equivalencia de dos estados. De acuerdo a la definición, debemos conocer la acción del autómata iniciando en estados s y t sobre *todas* las cadenas de entrada, esto con el fin de saber si s y t son equivalentes. Pero como la mayoría de los lenguajes tienen una cantidad infinita de cadenas de entrada, no puede checar individualmente el efecto de cada cadena que se introduce a un autómata. Como un asunto práctico, puede decidir si dos estados s y t son o no son $*$-equivalentes, empleando un procedimiento iterativo basado en un tipo más simple de equivalencia de estados, llamada *k-equivalencia*. Dos estados son *k-equivalentes* si cualquier cadena de longitud menor o igual que k, que es aceptada por el autómata cuando éste inicia desde uno de los estados también es aceptada por el autómata cuando empieza del otro estado.

• Definición

Sea A un autómata de estado-finito con función de estado siguiente N y función de estado-eventual N^*. Se define una relación sobre el conjunto de estados de A como sigue: Dados los estados arbitrarios s y t de A y un entero $k \geq 0$, decimos que s es ***k*-equivalente** a t y escribimos $s \; R_k \; t$ si y sólo si, para todas las cadenas de entrada w *de longitud menor o igual que* k, $N^*(s, w)$ y $N^*(t, w)$ son estados aceptables o ambos no son estados aceptables.

De la definición de k-equivalencia se siguen rápidamente ciertos hechos muy útiles:

Para cada entero $k \geq 0$, k-equivalencia es una relación de equivalencia. 12.3.2

Para cada entero $k \geq 0$, las clases de k-equivalencias particionan al conjunto de todos los estados del autómata en una unión de subconjuntos mutuamente ajenos. 12.3.3

Para cada entero $k \geq 1$, si dos estados son k-equivalentes, entonces ellos también son $(k - 1)$ equivalentes. 12.3.4

Para cada entero $k \geq 1$, cada clase de k-equivalencia es un subconjunto de una $(k - 1)$equivalencia. 12.3.5

Si dos estados son k-equivalentes para todos los enteros $k \geq 0$, entonces son $*$-equivalentes. 12.3.6

Las demostraciones de estos hechos se dejan como ejercicios.

El siguiente teorema da una descripción recursiva de k-equivalencia de estados. Éste dice, primero, que dos estados arbitrarios son 0-equivalentes si y sólo si, ambos son estados

aceptables o ambos no son estados aceptables y, segundo, que cualesquiera dos estados son k-equivalentes (para $k \geq 1$) si y sólo si, ellos son $(k-1)$-equivalentes y para símbolos arbitrarios de entrada sus estados siguientes también son $(k-1)$-equivalentes.

Teorema 12.3.1

Sea A un autómata de estado-finito con función de siguiente estado N. Dados los estados arbitrarios s y t en A,

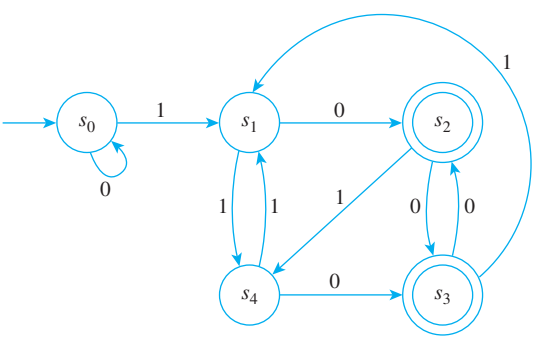
1. s es 0-equivalente a t $\Leftrightarrow$ [ambos s y t son estados aceptables o ambos no son estados aceptables]
2. para cada entero $k \geq 1$, s es k-equivalente a t $\Leftrightarrow$ [s y t son $(k-1)$-equivalentes y para cualquier símbolo de entrada m, $N(s, m)$ y $N(t, m)$ también son $(k-1)$-equivalentes].

La validez del teorema 12.3.1 se sigue del hecho de que al introducir una cadena w de longitud k tiene el mismo efecto que la introducción del primer símbolo de w y después los restantes $(k-1)$ símbolos de w. Es muy técnico dar una demostración detallada.

El teorema 12.3.1 implica que si conoce cuáles estados son $(k-1)$-equivalentes (en donde k es un entero positivo) y si también conoce la acción de la función de estado siguiente, entonces puede determinar cuáles estados son k-equivalentes. Específicamente, si s y t son estados $(k-1)$-equivalentes cuyos estados-próximos son $(k-1)$-equivalentes para cualquier símbolo de entrada m, entonces s y t son k-equivalentes. Así, las clases de k-equivalencia son las que obtienes subdividiendo las clases de $(k-1)$-equivalencia de acuerdo a la acción de la función de siguiente estado sobre los miembros de las clases. Un ejemplo debería hacer claro este procedimiento.

Ejemplo 12.3.2 Determinación de clases de *k*-equivalencia

Encuentre las clases de 0-equivalencia, las clases de 1-equivalencia y las clases de 2-equivalencia para los estados del autómata que se muestra a continuación.



Solución

1. ***Clases de 0-equivalencia:*** Por el teorema 12.3.1 dos estados son 0-equivalentes si y sólo si, ambos son estados aceptables o los dos son estados no-aceptables. Así que existen dos conjuntos de estados 0-equivalentes:

   $\{s_0, s_1, s_4\}$(los estados no-aceptables) y $\{s_2, s_3\}$(los estados aceptables),

y así

las clases de 0-equivalencia son $\{s_0, s_1, s_4\}$ y $\{s_2, s_3\}$.

2. ***Clases de 1-equivalencia:*** Por el teorema 12.3.1, dos estados son 1-equivalentes si y sólo si, ellos son 0-equivalentes y, después de introducir cualquier símbolo de entrada, sus próximos estados son 0-equivalentes. Así s_1 no es 1-equivalente a s_0 porque cuando un 0 entra al autómata en el estado s_1, éste va al estado s_2, mientras que cuando un 0 entra al autómata en el estado s_0, éste va al estado s_0, pero s_2 y s_0 no son 0-equivalentes. Por otro lado, s_1 *es* 1-equivalente a s_4 porque cuando un 0 entra al autómata en el estado s_1 o s_4 los estados-próximos son s_2 y s_3, los cuales son 0-equivalentes; y cuando un 1 entra al autómata en el estado s_1 o s_4 los estados siguientes son s_4 y s_1, los cuales son 0-equivalentes. Por un argumento similar, s_2 es 1-equivalente a s_3. Como los estados 1-equivalentes también deben ser 0-equivalentes [*por la propiedad* (12.3.4)], entonces no existen otros pares de estados que sean 1-equivalentes. Por lo tanto,

   las clases de 1-equivalencia son $\{s_0\}$,$\{s_1, s_4\}$ y $\{s_2, s_3\}$.

3. ***Clases de 2-equivalencia:*** Por el teorema 12.3.1, dos estados son 2-equivalentes si y sólo si, ellos son 1-equivalentes y, después de introducir cualquier símbolo de entrada, sus estados-próximos son 1-equivalentes. Ahora s_1 es 2-equivalente a s_4 porque ellos son 1-equivalentes y cuando un 1 entra al autómata en el estado s_1 o s_4 los estados-próximos son s_4 y s_1, los cuales son 1-equivalentes; y cuando un 0 entra al autómata en el estado s_1 o s_4 los estados próximos son s_2 y s_3, los cuales son 1-equivalentes. Similarmente, s_2 es 2-equivalente a s_3. Pero estados 2-equivalentes también deben ser 1-equivalentes [*por la propiedad* (12.3.4)], no existen otros pares de estados que sean 2-equivalentes. Así

   las clases de 2-equivalencia son $\{s_0\}$, $\{s_1, s_4\}$ y $\{s_2, s_3\}$.

   Observe que el conjunto de clases de 2-equivalencia es igual al conjunto de clases de 1-equivalencia. ■

Determinación de las clases de $*$-equivalencia

El ejemplo 12.3.2 ilustra la relativa facilidad con que se pueden encontrar los conjuntos de k-equivalencia. Pero para simplificar a un autómata de estado-finito necesita encontrar el conjunto de clases de $*$-equivalencia de estados. El próximo teorema expresa que para algún entero K, el conjunto de clases de $*$-equivalencia es igual al conjunto de clases de K-equivalencia.

Teorema 12.3.2

Si A es un autómata de estado-finito, entonces para algún entero, $K \geq 0$, el conjunto de clases de K-equivalencia de estados de A es igual al conjunto de clases de $(K + 1)$-equivalencia de estados de A y para tales K, ambos conjuntos son iguales al conjunto de clases de $*$-equivalencia de estados de A.

La demostración detallada del teorema 12.3.2 es algo técnica, pero no es difícil entender la idea de la demostración. El teorema 12.3.2 se sigue del hecho de que para cada entero positivo k, las clases de k-equivalencia se obtienen al subdividir las clases de $(k - 1)$-equivalencia de acuerdo a una cierta regla que es la misma para cada k. Como es finito el número de estados del autómata, entonces este proceso de subdivisión no puede continuar indefinidamente y así para algún entero $K \geq 0$, el conjunto de clases de K-equivalencia es igual al conjunto de clases de $(K + 1)$-equivalencia. Además, el conjunto de clases de m-equivalencia es igual al conjunto de clases de K-equivalencia para cada entero $m \geq K$. Pero esto implica que el conjunto de clases de $*$-equivalencia es igual al conjunto de clases de K-equivalencia.

Ejemplo 12.3.3 Determinación de las clases de $*$-equivalencia de R

Sea A el autómata de estado-finito definido en el ejemplo 12.3.2 Encuentre las clases de $*$-equivalencia de estados de A.

Solución De acuerdo al ejemplo 12.3.2, el conjunto de clases de 1-equivalencia para A es igual al conjunto de clases de 2-equivalencia. Por el teorema 12.3.2, entonces, el conjunto de clases de $*$-equivalencia también es igual al conjunto de clases de 1-equivalencia. Así que:

$$\text{las clases de } *\text{-equivalencia son } \{s_0\},\{s_1, s_4\} \text{ y } \{s_2, s_3\}.$$

En la notación de la sección 8.3, las clases de equivalencia se denotan por:

$$[s_0] = \{s_0\} \quad [s_1] = \{s_1, s_4\} = [s_4] \quad [s_2] = \{s_2, s_3\} = [s_3].$$ ■

El autómata cociente

Definamos el autómata cociente $\overline{A}$ de un autómata A. Sin embargo, para que todas las partes de la definición tengan sentido, debemos puntualizar dos hechos:

> Ninguna clase de $*$-equivalencia de estados de A puede tener tanto estados aceptables como no-aceptables. 12.3.7

La razón de que esto sea verdad es que las clases de 0-equivalencia dividen al conjunto de estados de A en estados aceptables y no-aceptables y las clases de $*$-equivalencia son subconjuntos de clases de 0-equivalencia.

> Si dos estados son $*$-equivalentes, entonces sus estados-próximos también son $*$-equivalentes para cualquier símbolo de entrada m. 12.3.8

Esto es verdadero por la siguiente razón. Suponga que los estados s y t son $*$-equivalentes. Entonces cualquier cadena de entrada que envía A a un estado aceptable cuando A está en el estado s, manda A a un estado aceptable cuando A se encuentra en el estado t. Ahora suponga que m es cualquier símbolo de entrada y considere los estados-próximos $N(s, m)$ y $N(t, m)$. Introduciendo en A una cadena de longitud k, cuando A está en el estado $N(s, m)$ o $N(t, m)$, produce el mismo efecto que al introducir en A una cierta cadena de longitud $(k + 1)$ cuando A se encuentra en el estado s o t (a saber, la concatenación de m con la cadena de longitud k). Así que cualquier cadena que envía A hacia un estado aceptable cuando A está en el estado $N(s, m)$ también manda A hacia un estado aceptable cuando A se encuentra en el estado $N(t, m)$. Se tiene que $N(s, m)$ y $N(t, m)$ son $*$-equivalentes. Las demostraciones completas de las propiedades (12.3.7) y (12.3.8) se dejan como ejercicios.

Ahora podemos definir el autómata cociente $\overline{A}$ de A. Él es el autómata de estado-finito cuyos estados son las clases de $*$-equivalencia de estados de A, tal que el estado inicial es la clase de $*$-equivalencia conteniendo el estado inicial de A, cuyos estados aceptables son de la forma $[s]$ en donde s es un estado aceptable de A y los símbolos de entrada son los mismos que los símbolos de entrada de A y su función de siguiente estado se deduce de la función de siguiente estado para A en la siguiente forma: Para encontrar el siguiente estado de $\overline{A}$ para un estado s y un símbolo de entrada m, elegir cualquier estado t en $[s]$ y ver a qué siguiente estado va A si m es entrada cuando A se encuentra en el estado t; la clase de equivalencia de este estado es el siguiente estado de $\overline{A}$.

• Definición

Sea A un autómata de estado-finito con conjunto de estados S, conjunto de símbolos de entrada I y función de siguiente estado N. El **autómata cociente** $\overline{A}$ se define como:

1. El conjunto de estados, $\overline{S}$ de $\overline{A}$ es el conjunto de clases de $*$-equivalencia de estados de A.
2. El conjunto de símbolos de entrada, $\overline{I}$, de $\overline{A}$ es igual a I.
3. El estado inicial de $\overline{A}$ es $[s_0]$, en donde s_0 es el estado inicial de A.
4. Los estados aceptables de $\overline{A}$ son los estados de la forma $[s]$, en donde s es un estado aceptable de A.
5. La función de siguiente estado $\overline{N}$: $\overline{S} \times I \to \overline{S}$ se define como sigue:

   Para todos los estados $[s]$ en $\overline{S}$ y símbolos de entrada m en I, $\overline{N}([s], m) = [N(s, m)]$.

   (Es decir, si m entra en $\overline{A}$ cuando éste se encuentra en el estado $[s]$, entonces $\overline{A}$ va al estado que es la clase $*$-equivalencia de $N(s, m)$.)

Observe que como los estados de $\overline{A}$ son *conjuntos* de estados de A, entonces en general $\overline{A}$ tiene mucho menos estados que A. (A y $\overline{A}$ tienen el mismo número de estados sólo en el caso en donde las clases de $*$-equivalencia de estados contienen sólo un elemento.) También, por la propiedad (12.3.7), cada estado aceptable de $\overline{A}$ consiste enteramente de estados aceptables de A. Aún más, la propiedad (12.3.8) garantiza que la función de estado siguiente $\overline{N}$ está bien definida.

Por construcción, un autómata cociente $\overline{A}$ acepta exactamente las mismas cadenas que A. Esto lo establecemos formalmente como el teorema 12.3.3. Los detalles los dejamos para un curso más avanzado sobre teoría de autómatas.

Teorema 12.3.3.

Si A es un autómata de estado-finito, entonces el autómata cociente $\overline{A}$ acepta exactamente los mismos lenguajes que A. En otras palabras, si $L(A)$ denota el lenguaje aceptado por A y $L(\overline{A})$ representa el lenguaje aceptado por $\overline{A}$, entonces

$$L(A) = L(\overline{A}).$$

Construcción del autómata cociente

Sea A un autómata de estado-finito con conjunto de estados S, función de siguiente estado N, relación R_* de $*$-equivalencia de estados y relación R_k de k-equivalencia de estados. Se sigue de los teoremas 12.3.2 y 12.3.3 y de la definición de autómata cociente que para encontrar el autómata cociente $\overline{A}$ de A, puede proceder como sigue:

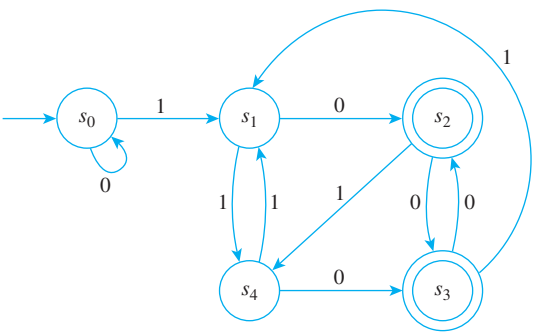
1. Encuentre el conjunto de clases de 0-equivalencia de S.
2. Para cada entero $k \geq 1$, subdivida las clases de $(k - 1)$-equivalencia de S (como se describió antes) para determinar las clases de k-equivalencia de S. Deje de subdividir cuando observe que para algún entero K el conjunto de clases de $(K + 1)$-equivalencias es igual al conjunto de clases de K-equivalencias. En este punto, concluya que el conjunto de clases de K-equivalencia es igual al conjunto de clases de $*$-equivalencias.
3. Construya el autómata cociente $\overline{A}$ cuyos estados son las clases de $*$-equivalencia de estados de A y cuya función de siguiente estado $\overline{N}$ está dada por

$\overline{N}([s], m) = [N(s, m)]$ para cualquier estado de $\overline{A}$ y cualquier símbolo de entrada m,

donde s es cualquier estado en $[s]$. *[Es decir, para ver hacia dónde se mueve* $\overline{A}$ *si m se introduce en* $\overline{A}$ *cuando se encuentra en el estado s, entonces observe hacia dónde va A si m entra en A cuando está en el estado s. La clase de* $*$*-equivalencia de ese estado es la respuesta.]*

Ejemplo 12.3.4 Construcción de un autómata cociente

Considere el autómata A de los ejemplos 12.3.2 y 12.3.3. Para referencia, a continuación se muestra otra vez este autómata. Encuentre el autómata cociente de A.



Solución De acuerdo al ejemplo 12.3.3 las clases de $*$-equivalencia de los estados de A son

$$\{s_0\} \quad \{s_1, s_4\} \quad \text{y} \quad \{s_2, s_3\}.$$

Así los estados del autómata cociente $\overline{A}$ son

$$[s_0] = \{s_0\}, \qquad [s_1] = \{s_1, s_4\} = [s_4], \qquad [s_2] = \{s_2, s_3\} = [s_3].$$

Los estados aceptables de A son s_2 y s_3, entonces el estado aceptable de $\overline{A}$ es $[s_2] = [s_3]$. La función de siguiente estado $\overline{N}$ de $\overline{A}$ está definida como sigue: para todos los estados $[s]$ y símbolos de entrada m de $\overline{A}$,

$$\overline{N}([s], m) = [N(s, m)] = \text{clase de } *\text{-equivalencia de } N(s, m).$$

Así,

$$\overline{N}([s_0], 0) = [N(s_0, 0)] = \text{clase de } *\text{-equivalencia de } N(s_0, 0).$$

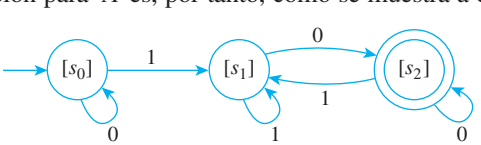
Pero $N(s_0, 0) = s_0$, entonces

$$\overline{N}([s_0], 0) = \text{clase de } *\text{-equivalencia de } s_0 = [s_0].$$

Similarmente,

$$\overline{N}([s_0], 1) = [N(s_0, 1)] = [s_1]$$
$$\overline{N}([s_1], 0) = [N(s_1, 0)] = [s_2]$$
$$\overline{N}([s_1], 1) = [N(s_1, 1)] = [s_4] = [s_1]$$
$$\overline{N}([s_2], 0) = [N(s_2, 0)] = [s_3] = [s_2]$$
$$\overline{N}([s_2], 1) = [N(s_2, 1)] = [s_4] = [s_1].$$

El diagrama de transición para $\overline{A}$ es, por tanto, como se muestra a continuación.



Por el teorema 12.3.3, este autómata acepta el mismo lenguaje que el autómata original. ■

Autómata equivalente

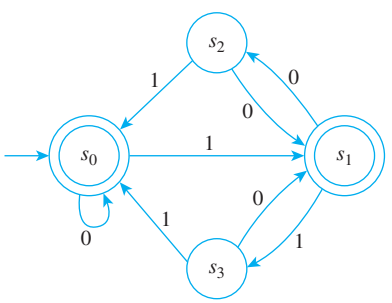
Los dispositivos de salida pueden ser anexados a los estados de autómatas de estado-finito para indicar si son o no estados aceptables. Por ejemplo, los estados aceptables podrían producir una salida de 1 y los no-aceptables una salida de 0. Entonces un autómata de estado-finito puede ser pensado como un dispositivo entrada/salida cuya entrada consiste de cadenas y cuya salida consiste de 0 y 1. Recuerde que un circuito puede pensarse como una caja negra que transforma combinaciones de señales de entrada a señales de salida. Dos circuitos que producen señales de salida idénticas para cada combinación de señales de entrada son llamados *equivalentes*. Similarmente, un autómata de estado-finito se puede considerar como una caja negra que procesa cadenas de entrada y produce señales de salida (indicando si las cadenas son o no aceptadas). Dos autómatas de estado-finito son llamados *equivalentes* si producen señales de salida idénticas para cada cadena de entrada. Pero esto significa que dos autómatas de estado-finito son equivalentes si y sólo si, ambos aceptan el mismo lenguaje.

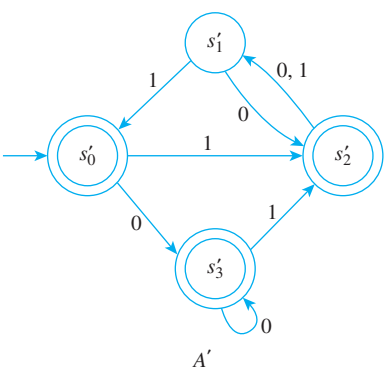
• Definición

Sean A y A' autómatas de estado-finito con el mismo conjunto de símbolos de entrada I. Sea que $L(A)$ denote el lenguaje aceptado por A y $L(A')$ el lenguaje aceptado por A'. Entonces se dice que A es **equivalente** a A' si y sólo si $L(A) = L(A')$.

Ejemplo 12.3.5 Demostración de que dos autómatas son equivalentes

Demuestre que los siguientes autómatas A y A' son equivalentes.





La etiqueta 0, 1 sobre una flecha de un diagrama de transición significa que para la entrada 0 o 1, el siguiente estado del autómata es el estado al cual apunta la flecha.

Solución

Para el autómata A: Las clases de 0-equivalencia son:

$$\{s_0, s_1\} \quad \text{y} \quad \{s_2, s_3\}$$

ya que s_0 y s_1 son estados aceptables y s_2 y s_3 son estados inaceptables.

Las clases de 1-equivalencia son:

$$\{s_0\}, \quad \{s_1\} \quad \text{y} \quad \{s_2, s_3\}$$

ya que s_0 y s_1 no son 1-equivalentes (ya que $N(s_0, 1) = s_1$, mientras que $N(s_1, 1) = s_3$ y s_1 no es 0-equivalente a s_3) pero s_2 y s_3 son 1-equivalentes.

Las clases de 2-equivalencia son:

$$\{s_0\}, \quad \{s_1\} \quad \text{y} \quad \{s_2, s_3\}$$

ya que s_2 y s_3 son 1-equivalentes.

Este análisis muestra que el conjunto de clases de 1-equivalencia es igual al conjunto de clases de 2-equivalencia, así por el teorema 12.3.2 esto es igual al conjunto de clases de $*$-equivalencia. Entonces las clases de $*$-equivalencia son

$$\{s_0\}, \quad \{s_1\} \quad \text{y} \quad \{s_2, s_3\}.$$

Para el autómata A′: Por un razonamiento similar al efectuado previamente, las clases de 0-equivalencia son:

$$\{s_0', s_2', s_3'\} \quad \text{y} \quad \{s_1'\}.$$

Las clases de 1-equivalencia son:

$$\{s_0', s_3'\}, \quad \{s_2'\} \quad \text{y} \quad \{s_1'\}.$$

Las clases de 2-equivalencias son las mismas que las clases de 1-equivalencias, las cuales son por lo tanto iguales a las clases de $*$-equivalencias. Así las clases de $*$-equivalencias son

$$\{s_0', s_3'\} \quad \{s_2'\} \quad \text{y} \quad \{s_1'\}.$$

Para calcular las funciones de estado siguiente para $\overline{A}$ y $\overline{A'}$, debes usar repetidamente el hecho de que en el autómata cociente, el estado siguiente de $[s]$ y m es la clase del siguiente estado de s y m. Por ejemplo,

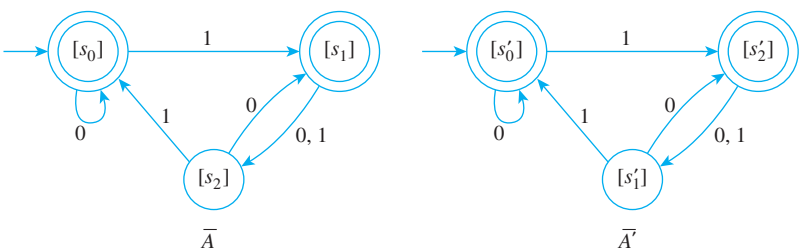
$$\overline{N}([s_1], 1) = [N(s_1, 1)] = [s_3] = [s_2]$$

y

$$\overline{N'}\left(\left[s_0'\right], 0\right) = \left[N'\left(s_0', 0\right)\right] = \left[s_3'\right] = \left[s_0'\right]$$

en donde N es la función siguiente estado para A y N' es la función de estado siguiente para A'.

Los diagramas de transición completos para los autómatas cociente $\overline{A}$ y $\overline{A'}$ se muestran a continuación.



$\overline{A}$ $\overline{A'}$

Como puede ver, excepto por el etiquetado de los nombres de los estados, $\overline{A}$ y $\overline{A'}$ son idénticos, así que aceptan el mismo lenguaje. Pero por el teorema 12.3.3, cada autómata original acepta el mismo lenguaje como su autómata cociente. Así A y A' aceptan el mismo lenguaje y así son equivalentes. ■

En matemáticas un objeto tal como un autómata de estado-finito se llama una *estructura*. En general, cuando dos estructuras matemáticas son las mismas en todos los aspectos, excepto por el etiquetado dado a sus elementos, se llaman **isomorfos**, lo que proviene de las palabras griegas *isos,* significando "lo mismo" o "igual" y *morphe*, significando "de". Puede demostrarse que, si los "estados inaccesibles" ya se han eliminado, dos autómatas son equivalentes si y sólo si, sus autómatas cocientes son isomorfos. (Los estados inaccesibles son aquellos que no se pueden alcanzar introduciendo al autómata cualquier cadena de símbolos cuando él se encuentra en su estado inicial.)

Autoexamen

1. Dado un autómata de estado-finito A con función de estado-eventual N^* y dados cualesquier estados s y t en A, decimos que s y t son $*$-equivalentes si y sólo si, _____.

2. Dado un autómata de estado-finito A con función de estado-eventual N^* y dados cualesquier estados s y t en A, decimos que s y t son k-equivalentes si y sólo si, _____.

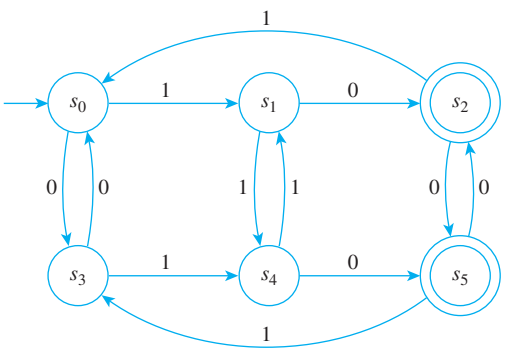
3. Dados los estados s y t en un autómata de estado-finito A, s es 0-equivalente a t si y sólo si, ambos s y t son _____ o ambos son _____. Además, para cada entero $k \geq 1$, s es k-equivalente a t si y sólo si, (1) s y t son (k-1)-equivalentes y (2) _____.

4. Si A es un autómata de estado-finito, entonces para algún entero $K \geq 0$, el conjunto de clases de K-equivalencias de estados de A es igual al conjunto de clases de _____ -equivalencia de A y para todos esos K ambos son iguales al conjunto de _____.

5. Dado un autómata de estado-finito A, el conjunto de estados del autómata cociente $\overline{A}$ es _____.

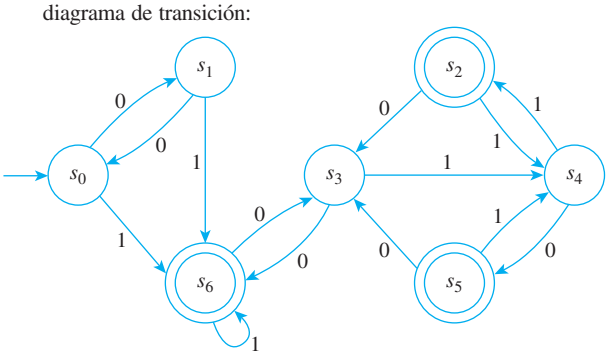
Conjunto de ejercicios 12.3

1. Considere el autómata de estado-finito A dado por el siguiente diagrama de transición:



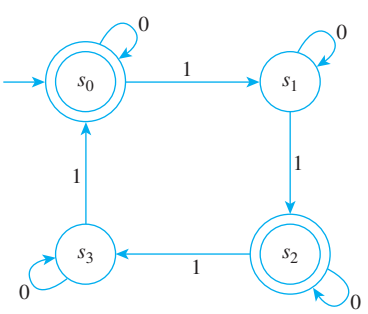
   a. Encuentre las clases de 0-, 1- y 2-equivalencias de estados de A.
   b. Dibuje el diagrama de transición para $\overline{A}$, el autómata cociente de A.

2. Considere el autómata de estado-finito A dado por el siguiente diagrama de transición:



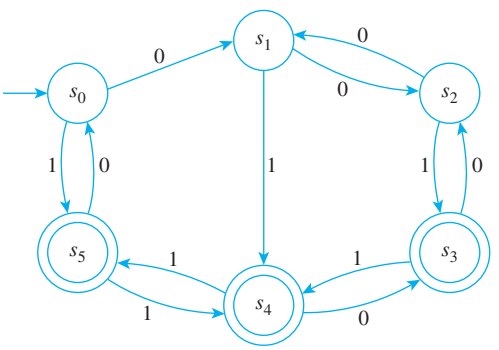
   a. Encuentre las clases de 0-, 1- y 2-equivalencias de estados de A.
   b. Dibuje el diagrama de transición para $\overline{A}$, el autómata cociente de A.

3. Considere el autómata de estado-finito A analizado en el ejemplo 12.3.1:



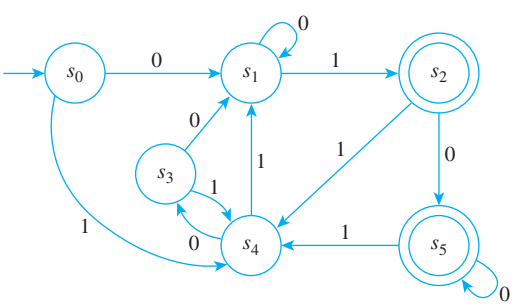
   a. Encuentre las clases de 0- y 1-equivalencia de estados de A.
   b. Dibuje el diagrama de transición de $\overline{A}$, el autómata cociente de A.

4. Considere el autómata de estado-finito dado por el siguiente diagrama de transición:



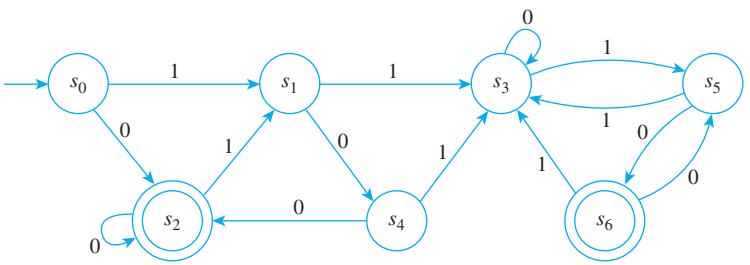
   a. Encuentre las clases de 0-, 1-, 2- y 3-equivalencia de estados de A.
   b. Dibuje el diagrama de transición para $\overline{A}$, el autómata cociente de A.

5. Considere el autómata de estado-finito dado por el siguiente diagrama de transición:



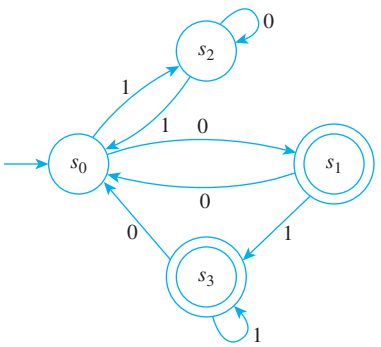
   a. Encuentre las clases de 0-, 1-, 2- y 3-equivalencias de estados de A.
   b. Dibuje el diagrama de transición para $\overline{A}$, el autómata cociente de A.

6. Considere el autómata de estado-finito dado por el siguiente diagrama de transición:

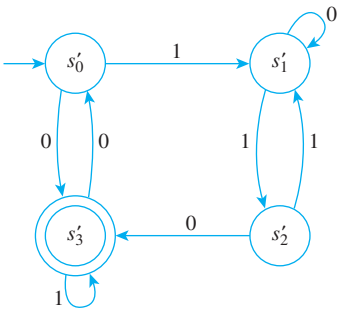


H a. Encuentre las clases de 0-, 1-, 2- y 3-equivalencias de estados de A.
b. Dibuje el diagrama de transición para $\overline{A}$, el autómata cociente de A.

7. ¿Son equivalentes los autómatas A y A' que se muestran a continuación?

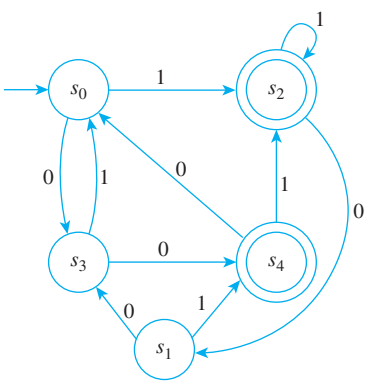


A

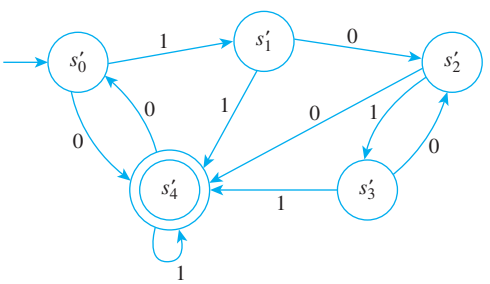


A'

8. ¿Son equivalentes los autómtas A y A' que se muestran a continuación?

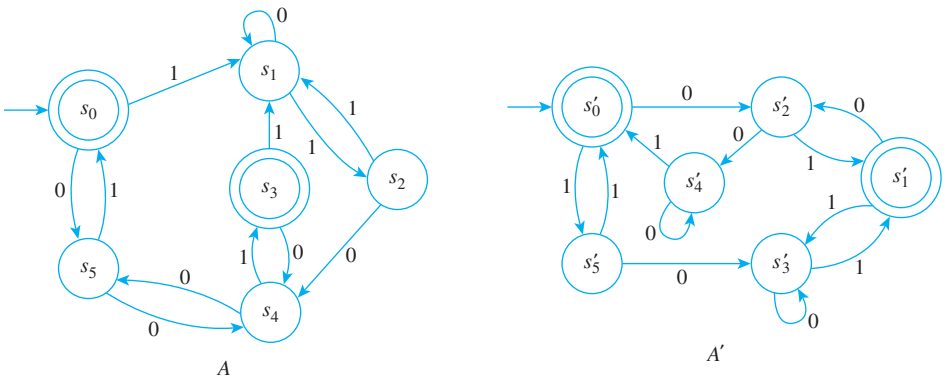


A

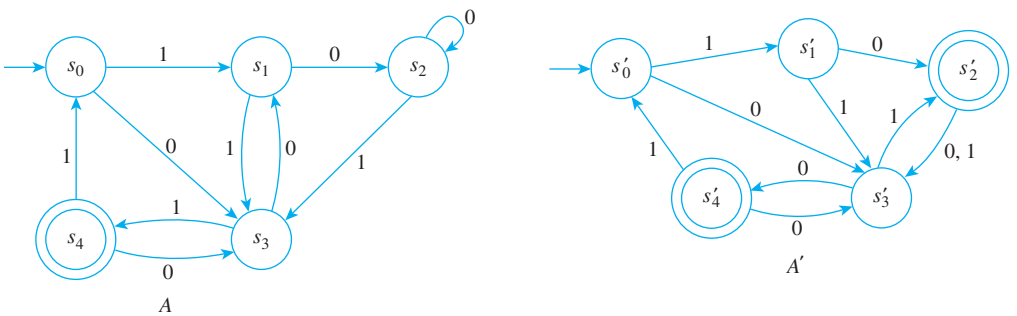


A'

9. ¿Son equivalentes los autómatas A y A' que se muestran a continuación?



10. ¿Son equivalentes los autómatas A y A' que se muestran a continuación?



***H* 11.** Demuestre la propiedad (12.3.1).

12. ¿Cómo se debería modificar la demostración de la propiedad (12.3.1) para demostrar la propiedad (12.3.2)?

13. Demuestre la propiedad (12.3.3).

14. Demuestre la propiedad (12.3.4).

***H* 15.** Demuestre la propiedad (12.3.5).

16. Demuestre la propiedad (12.3.6).

***H* 17.** Demuestre que si dos estados de un autómata de estado-finito son k-equivalentes para algún entero k, entonces esos estados son m-equivalentes para todos los enteros no negativos $m < k$.

18. Escriba una demostración completa de la propiedad (12.3.7).

***H* 19.** Escriba una demostración completa de la propiedad (12.3.8).

Respuestas del autoexamen

1. para todas las cadenas de entrada w ya sea $N^*(s, w)$ y $N^*(t, w)$ son ambos estados aceptables o ambos estados no aceptables 2. para todas las cadena w de longitud menor o igual a k ya sea $N^*(s, w)$ y $N^*(t, w)$ son ambos estados aceptables o ambos estados no aceptables 3. Estados aceptables; estados no aceptables; para cualquier símbolo de entrada m, $N(s, m)$ y $N(t, m)$ son también $(k - 1)$ equivalentes 4. $(K + 1)$; $*$-clases de equivalencias de los estados de A 5. El conjunto de $*$-clases de equivalencia de estados de A

APÉNDICE A

PROPIEDADES DE LOS NÚMEROS REALES*

En este libro tomamos los números reales y sus propiedades básicas, como nuestro punto de partida. Damos un conjunto base de propiedades, llamadas axiomas, aceptándose que son satisfechas por los números reales y establecemos algunas útiles propiedades que se pueden deducir de esos axiomas.

Suponemos que existen dos operaciones binarias definidas sobre el conjunto de números reales, llamadas **adición** y **multiplicación**, tales que si a y b son dos números reales cualesquiera, la **suma** de a y b, denotada $\boldsymbol{a + b}$ y el **producto** de a y b, denotado $\boldsymbol{a \cdot b}$ o $\boldsymbol{ab}$, también son números reales. Dichas operaciones satisfacen las propiedades de la F1 a la F6, llamadas **axiomas de campo**.

F1. *Leyes conmutativas*. Para todos los números reales a y b,

$$a + b = b + a \quad \text{y} \quad a\,b = b\,a.$$

F2. *Leyes asociativas*. Para todos los números reales a, b y c,

$$(a + b) + c = a + (b + c) \quad \text{y} \quad (ab)c = a(bc).$$

F3. *Leyes distributivas*. Para todos los números reales a, b y c,

$$a(b + c) = ab + ac \quad \text{y} \quad (b + c)a = ba + ca.$$

F4. *Existencia de los elementos identidad*. Existen dos números reales distintos, que se denotan por 0 y 1, tales que para cada número real a,

$$0 + a = a + 0 = a \quad \text{y} \quad 1\,a = a\,1 = a.$$

F5. *Existencia de inversos aditivos*. Para cada número real a, existe un número real, que se denota por $-a$ y se llama el **inverso aditivo** de a, tal que

$$a + (-a) = (-a) + a = 0.$$

F6. *Existencia de recíprocos*. Para cada número real $a \neq 0$, existe un número real, que se denota por $1/a$ o a^{-1}, llamado el **recíproco** de a, tal que

$$a \cdot \left(\frac{1}{a}\right) = \left(\frac{1}{a}\right) \cdot a = 1.$$

Todas las propiedades algebraicas usuales de los números reales que no implican orden, pueden deducirse de los axiomas de campo. A continuación, se presentan las más importantes que se establecen como los teoremas del T1 al T16. En todos esos teoremas los símbolos a, b, c y d representan números reales arbitrarios.

*Adaptado de Tom M. Apostol, *Calculus*, *Volume I* (Nueva York: Blaisdell,1961), pp. 13-19.

T1. *Ley de cancelación para la adición.* Si $a + b = a + c$, entonces $b = c$. (En particular, esto demuestra la unicidad del número 0 del axioma F4.)

T2. *Posibilidad de restar.* Dados a y b, existe exactamente una x tal que $a + x = b$. Esta x se denota por $b - a$. En particular, $0 - a$ es el inverso aditivo de a, $-a$.

T3. $b - a = b + (-a)$.

T4. $-(-a) = a$.

T5. $a(b - c) = ab - ac$.

T6. $0 \cdot a = a \cdot 0 = 0$.

T7. *Ley* de *cancelación para la multiplicación.* Si $ab = ac$ y $a \neq 0$, entonces $b = c$. (En particular, la unicidad del número 1 del axioma F4 es única.)

T8. *Posibilidad de dividir.* Dados a y b con $a \neq 0$, existe exactamente una x tal que $ax = b$. Esta x se denota por b/a y se llama el **cociente** de b y a. En particular, $1/a$ es el recíproco de a.

T9. Si $a \neq 0$, entonces $b/a = b \cdot a^{-1}$.

T10. Si $a \neq 0$, entonces $(a^{-1})^{-1} = a$.

T11. *Propiedad del producto cero.* Si $ab = 0$, entonces $a = 0$ o $b = 0$.

T12. *Regla para multiplicar con signos negativos.*

$$(-a)b = a(-b) = -(ab), \qquad (-a)(-b) = ab,$$

y

$$-\frac{a}{b} = \frac{-a}{b} = \frac{a}{-b}.$$

T13. *Propiedad de fracciones equivalentes.*

$$\frac{a}{b} = \frac{ac}{bc}, \quad \text{si } b \neq 0 \quad \text{y} \quad c \neq 0.$$

T14. *Regla para la adición de fracciones.*

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \quad \text{si } b \neq 0 \quad \text{y} \quad d \neq 0.$$

T15. *Regla para la multiplicación de fracciones.*

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}, \quad \text{si } b \neq 0 \quad \text{y} \quad d \neq 0.$$

T16. *Regla para división de fracciones.*

$$\frac{\dfrac{a}{b}}{\dfrac{c}{d}} = \frac{ad}{bc}, \quad \text{si } b \neq 0, c \neq 0, \quad \text{y} \quad d \neq 0.$$

Los números reales también satisfacen los siguientes axiomas, llamados **axiomas de orden**. Se supone que entre todos los números reales existen algunos, llamados **números reales positivos**, que satisfacen las propiedades Ord1-Ord3.

Ord1. Para cualesquiera números reales a y b, si a y b son positivos, entonces $a + b$ y ab también lo son.

Ord2. Para cada número real $a \neq 0$, a es positivo o $-a$ es positivo, pero no ambos.

Ord3. El número 0 no es positivo.

Los símbolos $<$, $>$, $\leq$ y $\geq$ y los números negativos se definen en términos de los números positivos.

• Definición

Dados los números reales a y b,

$a < b$ significa que $b + (-a)$ es positivo. $b > a$ significa $a < b$.

$a \leq b$ significa $a < b$ o $a = b$. $b \geq a$ significa $a \leq b$.

Si $a < 0$, decimos que a es **negativo**. Si $a \geq 0$, decimos que a es **no-negativo**.

De los axiomas de orden Ord1-Ord3 y de la definición anterior, se pueden deducir todas las reglas usuales para el cálculo con desigualdades. Las más importantes se exponen como los teoremas del T17 al T27. En todos esos teoremas los símbolos a, b, c y d representan números reales arbitrarios.

T17. *Ley de la tricotomía*. Para a y b números reales arbitrarios, se cumple exactamente una de las siguientes tres relaciones $a < b$, $b < a$ o $a = b$.

T18. *Ley de la transitividad*. Si $a < b$ y $b < c$, entonces $a < c$.

T19. Si $a < b$, entonces $a + c < b + c$.

T20. Si $a < b$ y $c > 0$, entonces $ac < bc$.

T21. Si $a \neq 0$, entonces $a^2 > 0$.

T22. $1 > 0$.

T23. Si $a < b$ y $c < 0$, entonces $ac > bc$.

T24. Si $a < b$, entonces $-a > -b$. En particular, $a < 0$ implica $-a > 0$

T25. Si $ab > 0$, entonces a y b son ambos positivos o ambos son negativos.

T26. Si $a < c$ y $b < d$, entonces $a + b < c + d$.

T27. Si $0 < a < c$ y $0 < b < d$, entonces $0 < ab < cd$.

Un axioma final distingue al conjunto de números reales del conjunto de números racionales, el cual es llamado el **axioma de mínima cota superior** [MCS].

MCS. Cualquier conjunto no vacío S de números reales, acotado por arriba, tiene una cota superior mínima. Es decir, si B es el conjunto de todos los números reales x tales que $x \geq s$, para todas las s en S y si B tiene al menos un elemento, entonces B tiene un elemento que es el más pequeño. Este elemento es llamado la **mínima cota superior de** S.

El axioma de la mínima cota superior es válido para el conjunto de los números reales, pero no para el conjunto de los números racionales. Por ejemplo, el conjunto de todos los números racionales que son menores que $\sqrt{2}$ tiene cotas superiores, pero ninguna mínima cota superior dentro del conjunto de los números racionales.

APÉNDICE B

SOLUCIONES Y SUGERENCIAS PARA LOS EJERCICIOS SELECCIONADOS

Sección 1.1

1. a. $x^2 = -1$ (O: el cuadrado de x es -1)

b. Un número real x

3. a. Entre a y b

b. Números reales a y b; existe un número real c

5. a. r es positivo

b. Positivo; el recíproco de r es positivo (O: es positivo; $1/r$ es positivo)

c. Es positivo; $1/r$ es positivo (O: es positivo; el recíproco de r es positivo)

7. a. Existen números reales cuya suma es menor que su diferencia.

Verdadero, por ejemplo, $1 + (-1) = 0$, $1 - (-1) = 1 + 1 = 2$ y $0 < 2$.

c. El cuadrado de cualquier entero positivo es más grande que el entero.

Verdadero. Si n es cualquier entero positivo, entonces $n \geq 1$. Al multiplicar ambos lados por el número positivo n no se altera la dirección de la desigualdad (vea el apéndice A, T20) y así $n^2 \geq n$.

8. a. Tiene cuatro lados

b. Tiene cuatro lados

c. Tiene cuatro lados

d. Es un cuadrado; J tiene cuatro lados

e. J tiene cuatro lados

10. a. Tiene un recíproco

b. Un recíproco

c. s recíproco de r

12. a. Número real; el producto de cada número deja inalterado al número

b. Con cada número no altera al número

c. $rs = s$

Sección 1.2

1. $A = C$ y $B = D$

2. a. El conjunto de todos los números reales positivos x tales que 0 es menor que x y x es menor que 1

c. El conjunto de todos los enteros n tales que n es un factor de 6

3. a. No, $\{4\}$ es un conjunto con un elemento, a saber 4, mientras que 4 es sólo un símbolo que representa al número 4

b. Tres: los elementos del conjunto son 3, 4 y 5

c. Tres: los elementos son el símbolo 1, el conjunto $\{1\}$ y el conjunto $\{1, \{1\}\}$

5. *Sugerencia:* $\mathbf{R}$ es el conjunto de todos los números reales, $\mathbf{Z}$ es el conjunto de todos los enteros y $\mathbf{Z}^+$ es el conjunto de todos los enteros positivos

6. *Sugerencia:* T_0 y T_1 no tienen el mismo número de elementos como T_2 y T_{-3}

7. a. $\{1, -1\}$

c. $\emptyset$ (el conjunto carece de elementos)

d. $\mathbf{Z}$ (cada entero está en el conjunto)

8. a. No, $B \not\subseteq A$, por tanto, $j \in B$ pero $j \notin A$.

d. Sí, C es un subconjunto propio de A. Ambos elementos de C están en A, pero A contiene elementos (a saber c y f) que no están en C.

9. a. Sí

b. No

f. No

i. Sí

10. a. No. Observe que $(-2)^2 = (-2)(-2) = 4$, mientras que $-2^2 = -(2^2) = -4$. Así $((-2)^2, -2^2) = (4, -4)$, $(-2^2, (-2)^2) = (-4, 4)$ y $(4, -4) \neq (-4, 4)$ porque $-4 \neq 4$.

c. Sí. Observe que $8 - 9 = -1$ y $\sqrt[3]{-1} = -1$ y así $(8 - 9, \sqrt[3]{-1} = (-1, -1)$.

11. a. $\{(w, a), (w, b), (x, a), (x, b), (y, a), (y, b), (z, a), (z, b)\}$

b. $\{(a, w), (b, w), (a, x), (b, x), (a, y), (b, y), (a, z), (b, z)\}$

c. $\{(w, w), (w, x), (w, y), (w, z), (x, w), (x, x), (x, y), (x, z), (y, w), (y, x), (y, y), (y, z), (z, w), (z, x), (z, y), (z, z)\}$

d. $\{(a, a), (a, b), (b, a), (b, b)\}$

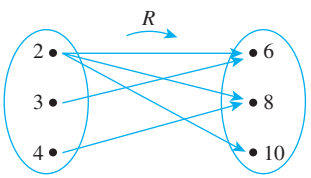
Sección 1.3

1. a. No. Sí. No. Sí.

b. $R = \{(2, 6), (2, 8), (2, 10), (3, 6), (4, 8)\}$

c. Dominio de $R = A = \{2, 3, 4\}$, codominio de $R = B = \{6, 8, 10\}$

d.



3. a. 3 T 0 porque $\frac{3-0}{3} = \frac{3}{3} = 1$, que es un entero

1 $\not T$ (-1) porque $\frac{1-(-1)}{3} = \frac{2}{3}$, que no es un entero

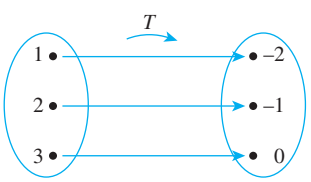
$(2, -1) \in T$ porque $\frac{2-(-1)}{3} = \frac{3}{3} = 1$, un entero

$(3, -2) \notin T$ porque $\frac{3-(-2)}{3} = \frac{5}{3}$, que no es un entero

b. $T = \{(1, -2), (2, -1), (3, 0)\}$

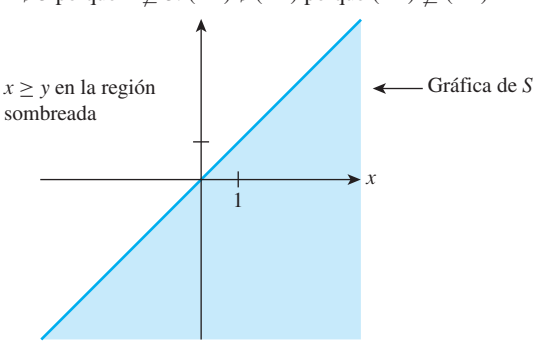
c. Dominio de $T = E = \{1, 2, 3\}$, codominio de $T = F = \{-2, -1, 0\}$

d.

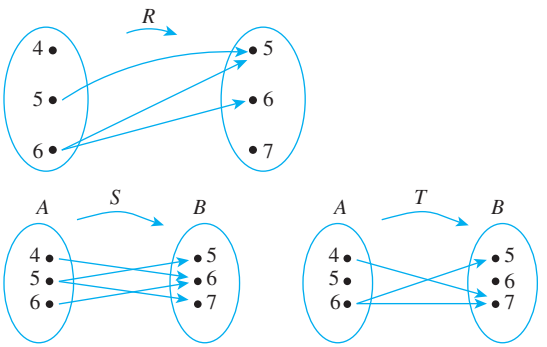


5. a. $(2, 1) \in S$ ya que $2 \geq 1$. $(2, 2) \in S$ porque $2 \geq 2$. $2 \$ 3$ porque $2 \not\geq 3$. $(-1) \$ (-2)$ porque $(-1) \not\geq (-2)$

b.



7. a.



b. R no es una función ya que no satisface ninguna de las propiedades (1) y (2) de la definición. Viola la propiedad (1) porque $(4, y) \notin$ de R, para cualquier y en B. No cumple la propiedad (2) ya que $(6, 5) \in$ y $(6, 6) \in R$ pero $5 \neq 6$

S no es una función porque $(5, 5) \in S$ y $(5, 7) \in S$ pero $5 \neq 7$. Así S no satisface la propiedad (2) de la definición de función

T no es función porque $(5, x) \notin T$ para cualquier x en B y también porque $(6, 5) \in T$ y $(6, 7) \in T$ y $5 \neq 7$. Así T no satisface la propiedad (1) ni la propiedad (2) de la definición de función

9. a. $\emptyset$, $\{(0, 1)\}$, $\{(1, 1)\}$, $\{(0, 1), (1, 1)\}$

b. $\{(0, 1), (1, 1)\}$

c. 1/4

11. No, P no es una función porque, por ejemplo, $(4, 2) \in P$ $(4, -2) \in P$ pero $2 \neq -2$

13. a. Dominio $= A = \{-1, 0, 1\}$, codominio $= B = \{t, u, v, w\}$.

b. $F(-1) = u$, $F(0) = w$, $F(1) = u$

15. a. Este diagrama no determina una función porque 2 está relacionado tanto con 2 como con 6

b. Este diagrama no determina una función porque 5 está en el dominio pero no está relacionado con cualquier elemento del codominio

16. $f(-1) = (-1)^2 = 1$, $f(0) = 0^2 = 0$, $f\left(\frac{1}{2}\right) = \left(\frac{1}{2}\right)^2 = \frac{1}{4}$

19. Para toda $x \in \mathbf{R}$, $g(x) = \frac{2x^3+2x}{x^2+1} = \frac{2x(x^2+1)}{x^2+1} = 2x = f(x)$. Por tanto, por definición de igualdad de funciones, $f = g$

Sección 2.1

1. Forma común**:** Si p entonces q

p.
Por tanto, q.

$(a + 2b)(a^2 - b)$ se puede escribir en notación de prefijo. Todas las expresiones algebraicas se pueden escribir en notación de prefijo

3. Forma común: $p \vee q$

$\sim p$.
Por tanto, q

Mi mente es brillante. La lógica es confusa

5. a. Es un enunciado porque es una frase verdadera. 1 024 es un cuadrado perfecto porque $1\,024 = 32^2$ y el siguiente cuadrado perfecto más pequeño es $31^2 = 961$, que tiene menos de cuatro dígitos

6. **a.** $s \wedge i$ **b.** $\sim s \wedge \sim i$

8. **a.** $(h \wedge w) \wedge \sim s$ **d.** $(\sim w \wedge \sim s) \wedge h$

10. **a.** $p \wedge q \wedge r$ **c.** $p \wedge (\sim q \vee \sim r)$

11. O inclusivo. Por ejemplo, un equipo podría ganar la final ganando en los juegos 1, 3 y 4 y perdiendo el partido 2. Tal resultado cumpliría con ambas condiciones

12.

p	q	$\sim p$	$\sim p \wedge q$
V	V	F	F
V	F	F	F
F	V	V	V
F	F	V	F

14.

p	q	r	$q \wedge r$	$p \wedge (q \wedge r)$
V	V	V	V	V
V	V	F	F	F
V	F	V	F	F
V	F	F	F	F
F	V	V	V	F
F	V	F	F	F
F	F	V	F	F
F	F	F	F	F

16.

p	q	$p \wedge q$	$p \vee (p \wedge q)$	p
V	V	V	V	V
V	F	F	V	V
F	V	F	F	F
F	F	F	F	F

$p \vee (p \wedge q)$ y p siempre tienen los mismos valores de verdad, así que son lógicamente equivalentes. (Esto prueba una de las leyes de absorción.)

18.

p	t	$p \vee$ t
V	V	V
F	V	V

$p \vee$ **t** y **t** siempre tienen los mismos valores de verdad, así que son lógicamente equivalentes. (Esto prueba una de las leyes universales acotadas.)

21.

p	q	r	$p \wedge q$	$q \wedge r$	$(p \wedge q) \wedge r$	$p \wedge (q \wedge r)$
V	V	V	V	V	V	V
V	V	F	V	F	F	F
V	F	V	F	F	F	F
V	F	F	F	F	F	F
F	V	V	F	V	F	F
F	V	F	F	F	F	F
F	F	V	F	F	F	F
F	F	F	F	F	F	F

$(p \wedge q) \wedge r$ y $p \wedge (q \wedge r)$ siempre tienen los mismos valores de verdad, entonces son lógicamente equivalentes. (Esto prueba la ley asociativa para $\wedge$.)

23.

p	q	r	$p \wedge q$	$q \vee r$	$(p \wedge q) \vee r$	$p \wedge (q \vee r)$
V	V	V	V	V	V	V
V	V	F	V	V	V	V
V	F	V	F	V	V	V
V	F	F	F	F	F	F
F	V	V	F	V	V	F
F	V	F	F	V	F	F
F	F	V	F	V	V	F
F	F	F	F	F	F	F

$(p \wedge q) \vee r$ y $p \wedge (q \vee r)$ tienen diferentes valores de verdad en el quinto y séptimo renglón, por lo que no son lógicamente equivalentes. (Esto prueba que los paréntesis son necesarios con $\wedge$ y $\vee$.)

25. Hal no estudia la licenciatura en matemáticas y la hermana de Hal no es estudiante de la licenciatura en ciencia computacional

27. El conector no está suelto y la máquina no está desconectada.

32. $-2 \geq x$ o $x \geq 7$

34. $2 \leq x \leq 5$

36. $1 \leq x$ o $x < -3$

38. La forma lógica de esta afirmación es $(p \wedge q) \vee r$, entonces su negación tiene la forma $\sim((p \wedge q) \vee r) \equiv \sim(p \wedge q) \wedge \sim r \equiv (\sim p \wedge \sim q) \wedge \sim r$. Así una negación para el enunciado es (*num_pedidos* $\leq$ 100 o *num_inexistencia* $>$ 500 y *num_inexistencia* $\geq$ 200.

40.

p	q	$\sim p$	$\sim q$	$p \wedge q$	$p \wedge \sim q$	$\sim p \vee (p \wedge \sim q)$	$(p \wedge q) \vee (\sim p \vee (p \wedge \sim q))$
V	V	F	F	V	F	F	V
V	F	F	V	F	V	V	V
F	V	V	F	F	F	V	V
F	F	V	V	F	F	V	V

↑

Todos sus valores de verdad son V, así $(p \wedge q) \vee (\sim p \vee (p \wedge \sim q))$ es una tautología.

41.

p	q	$\sim p$	$\sim q$	$p \wedge \sim q$	$\sim p \vee q$	$(p \wedge \sim q) \wedge (\sim p \vee q)$
V	V	F	F	F	V	F
V	F	F	V	V	F	F
F	V	V	F	F	V	F
F	F	V	V	F	V	F

↑

Todos sus valores de verdad son F, así $(p \wedge \sim q) \wedge (\sim p \vee q)$ es una contradicción.

44. Aceptemos que p sea "$x < 2$", q denote "$1 < x$" y que r sea "$x < 3$". Entonces los enunciados en *a*) y *b*) se simbolizan como $p \vee \sim(q \wedge r)$ y $\sim q \vee (p \vee \sim r)$, respectivamente.

p	q	r	$\sim q$	$\sim r$	$q \wedge r$	$\sim(q \wedge r)$	$p \vee \sim r$	$p \vee \sim(q \wedge r)$	$\sim q \vee (p \vee \sim r)$
V	V	V	F	F	V	F	V	V	V
V	V	F	F	V	F	V	V	V	V
V	F	V	V	F	F	V	V	V	V
V	F	F	V	V	F	V	V	V	V
F	V	V	F	F	V	F	F	F	F
F	V	F	F	V	F	V	V	V	V
F	F	V	V	F	F	V	F	V	V
F	F	F	V	V	F	V	V	V	V

↑ ↑

Las formas $p \vee \sim(q \wedge r)$ y $\sim q \vee (p \vee \sim r)$ siempre tienen los mismos valores de verdad, así son lógicamente equivalentes.

Por tanto, los enunciados en *a*) y *b*) son lógicamente equivalentes.

46. a. *Solución 1:* Construya una tabla de verdad para $p \oplus p$ utilizando los valores de verdad para *o excluyente*.

p	$p \oplus p$
V	F
F	F

porque un enunciado con *o excluyente* es falso cuando ambas componentes son verdaderas y cuando ambas componentes son falsas.

Puesto que todos sus valores de verdad son falsos, $p \oplus p =$ **c**, es una contradicción.

Solución 2: Reemplace q por p en la equivalencia lógica $p \oplus q \equiv (p \vee q) \wedge \sim(p \wedge q)$ y simplifique el resultado

$p \oplus p \equiv (p \vee q) \wedge \sim(p \wedge p)$ por definición de $\oplus$
$\equiv p \wedge \sim p$ por las leyes de identidad
$\equiv \mathbf{c}$ por la ley de negación para $\wedge$

47. Existe una famosa historia sobre un filósofo que dio una plática en donde él observó que, en inglés y en muchos otros lenguajes, una doble negación es equivalente a una positiva y que no existe lenguaje en que una doble positiva sea equivalente a una negativa. Entonces, otro filósofo, Sidney Morgenbesser, respondió sarcásticamente, "Sí, Sí".

[Estrictamente hablando, el sarcasmo funciona muy parecido a una negación. Al hablar sarcásticamente, las palabras "Sí, Sí" no es una verdadera doble positiva; exactamente significan "No".]

48. a. Ley distributiva.

b. Ley conmutativa para $\vee$

c. Ley de negación para $\vee$

d. Ley de identidad para $\wedge$

50. $(p \wedge \sim q) \vee p \equiv p \vee (p \wedge \sim q)$ por la ley conmutativa para $\vee$
$\equiv p$ por la ley de absorción (con $\sim q$ en lugar de q)

53. $\sim((\sim p \wedge q) \vee (\sim p \wedge \sim q)) \vee (p \wedge q)$
$\equiv \sim[\sim p \wedge (q \vee \sim q)] \vee (p \wedge q)$ por la ley distributiva
$\equiv \sim(\sim p \wedge \mathbf{t}) \vee (p \wedge q)$ por la ley de negación para $\vee$
$\equiv \sim(\sim p) \vee (p \wedge q)$ por la ley de identidad para $\wedge$
$\equiv p \vee (p \wedge q)$ por la ley de doble negación
$\equiv p$ por la ley de absorción

Sección 2.2

1. Si este bucle no contiene un **stop** o un **go to**, entonces se repetirá exactamente N veces.

3. Si no se detiene, entonces dispararé.

5.

			conclusión	hipótesis	
p	q	$\sim p$	$\sim q$	$\sim p \vee q$	$\sim p \vee q \rightarrow \sim q$
V	V	F	F	V	F
V	F	F	V	F	V
F	V	V	F	V	F
F	F	V	V	V	V

7.

			conclusión	hipótesis	
p	q	r	$\sim q$	$p \wedge \sim q$	$p \wedge \sim q \rightarrow r$
V	V	V	F	F	V
V	V	F	F	F	V
V	F	V	V	V	V
V	F	F	V	V	F
F	V	V	F	F	V
F	V	F	F	F	V
F	F	V	V	F	V
F	F	F	V	F	V

9.

p	q	r	$\sim r$	$p \wedge \sim r$	$q \vee r$	$p \wedge \sim r \leftrightarrow q \vee r$
V	V	V	F	F	V	F
V	V	F	V	V	V	V
V	F	V	F	F	V	F
V	F	F	V	V	F	F
F	V	V	F	F	V	F
F	V	F	V	F	V	F
F	F	V	F	F	V	F
F	F	F	V	F	F	V

12. Si $x > 2$ entonces $x^2 > 4$ y si $x < -2$ entonces $x^2 > 4$

13. a.

p	q	$\sim p$	$p \rightarrow q$	$\sim p \vee q$
V	V	F	V	V
V	F	F	F	F
F	V	V	V	V
F	F	V	V	V

$p \rightarrow q$ y $\sim p \vee q$ siempre tienen los mismos valores de verdad, así que son lógicamente equivalentes.

14. a. *Sugerencia:* $p \rightarrow q \vee r$ es verdadera en todos los casos excepto cuando p es verdadera y tanto q como r son falsas.

16. Sea que p represente "Paga el precio completo" y que q denote "No lo compraría en Crown Books". Así, "Si paga el precio completo, no lo compraría en Crown Books" tiene la forma $p \rightarrow q$. Y "No lo compraría en Crown Books o paga el precio completo" tiene la forma $q \vee p$.

p	q	$p \rightarrow q$	$q \vee p$
V	V	V	V
V	F	F	V
F	V	V	V
F	F	V	F

Esos dos enunciados no son lógicamente equivalentes porque sus formas tienen diferentes valores de verdad en los renglones 2 y 4.

(Una representación alternativa para las formas de los dos enunciados es $p \rightarrow \sim q$ y $\sim q \vee p$. En este caso, los valores de verdad difieren en los renglones 1 y 3).

19. Falso. La negación de un enunciado si-entonces no es un enunciado si-entonces. Es un enunciado y.

20. a. P es un cuadrado y P no es un rectángulo.

d. n es primo y tanto n no es impar como n no es 2.
O: n es primo y n no es impar ni 2.

f. Tom es el padre de Ann y Jim no es su tío o Sue no es su tía.

21. a. Porque $p \rightarrow q$ es falso, p es verdadera y q es falsa. Así $\sim p$ es falsa y entonces $\sim p \rightarrow q$ es verdadera.

22. a. Si P no es un rectángulo, entonces P no es un cuadrado.

d. Si n no es impar y n no es 2, entonces n no es primo.

f. Jim no es tío de Ann o Sue no es su tía, entonces Tom no es su padre.

23. a. *Conversa:* Si P es un rectángulo, entonces P es un cuadrado.
Inversa: Si P no es un cuadrado, entonces P no es un rectángulo.

d. *Conversa:* Si n es impar o n es 2, entonces n es primo.
Inversa: Si n no es primo, entonces n no es impar y n no es 2.

f. *Conversa:* Si Jim es tío de Ann y Sue es su tía, entonces Tom es su padre.
Inversa: Si Tom no es padre de Ann, entonces Jim no es su tío o Sue no es su tía.

24.

p	q	$p \rightarrow q$	$q \rightarrow p$
V	V	V	V
V	F	F	V
F	V	V	F
F	F	V	V

$p \rightarrow q$ y $q \rightarrow p$ tienen diferentes valores de verdad en el segundo y tercer renglón, así no son lógicamente equivalentes.

26.

p	q	$\sim q$	$\sim p$	$\sim q \rightarrow \sim p$	$p \rightarrow q$
V	V	F	F	V	V
V	F	V	F	F	F
F	V	F	V	V	V
F	F	V	V	V	V

$\sim q \rightarrow \sim p$ y $p \rightarrow q$ siempre tienen los mismos valores de verdad, así son lógicamente equivalentes.

28. *Sugerencia:* Una persona que dice "Expreso lo que digo" afirma hablar sinceramente. Una persona que dice "Digo lo que quiero expresar" afirma hablar con precisión.

29. $(p \rightarrow (q \vee r)) \leftrightarrow ((p \wedge \sim q) \rightarrow r)$

p	q	r	$\sim q$	$q \vee r$	$p \wedge \sim q$	$p \rightarrow (q \vee r)$	$p \wedge \sim q \rightarrow r$	$(p \rightarrow (q \vee r)) \leftrightarrow ((p \wedge \sim q) \rightarrow r)$
V	V	V	F	V	F	V	V	V
V	V	F	F	V	F	V	V	V
V	F	V	V	V	V	V	V	V
V	F	F	V	F	V	F	F	V
F	V	V	F	V	F	V	V	V
F	V	F	F	V	F	V	V	V
F	F	V	V	V	F	V	V	V
F	F	F	V	F	F	V	V	V

$(p \rightarrow (q \vee r)) \leftrightarrow ((p \wedge \sim q) \rightarrow r)$ es una tautología porque todos sus valores de verdad son V.

32. Si esta ecuación cuadrática tiene dos raíces reales distintas, entonces su discriminante es mayor que cero y si el discriminante de esta ecuación cuadrática es mayor que cero, entonces la ecuación tiene dos raíces reales.

34. Si los cachorros no triunfan en el juego de mañana, entonces no ganarán el banderín.

Si los cachorros ganan el banderín, entonces habrán triunfado en el partido de mañana.

37. Si una nueva audiencia no está garantizada, el pago se realizará en la quinta.

40. Si tomo el camión de las 8:05, entonces estoy a tiempo para mi trabajo.

42. Si este número no es divisible por 3, entonces no es divisible por 9.

Si este número es divisible por 9, entonces es divisible por 3.

44. Si el equipo de Jon triunfa en el resto de sus partidos, entonces ganará el campeonato.

46. a. Este enunciado es el converso del enunciado dado y así no necesariamente es verdadero. Por ejemplo, si el punto de ebullición real del compuesto X fuera 200 °C, entonces el enunciado dado sería verdadero, pero este enunciado sería falso.

b. Este enunciado debe ser verdadero. Es el contrapositivo del enunciado dado.

47. a. $p \wedge \sim q \rightarrow r \equiv \sim(p \wedge \sim q) \vee r$

b. Resultado de $a) \equiv \sim[\sim(\sim(p \wedge \sim q)) \wedge \sim r]$

una respuesta aceptable

$\equiv \sim[(p \wedge \sim q) \wedge \sim r]$

por la ley de doble negación (otra respuesta aceptable)

49. a. $(p \rightarrow r) \leftrightarrow (q \rightarrow r) \equiv (\sim p \vee r) \leftrightarrow (\sim q \vee r)$

$\equiv \sim(\sim p \vee r) \vee (\sim q \vee r)] \wedge [\sim(\sim q \vee r) \vee (\sim p \vee r)]$

una respuesta aceptable

$\equiv [(p \wedge \sim r) \vee (\sim q \vee r)] \wedge [(q \wedge \sim r) \vee (\sim p \vee r)]$

por la ley de De Morgan (otra respuesta aceptable)

b. Resultado de $a) \equiv \sim[\sim(p \wedge \sim r) \wedge \sim(\sim q \vee r)] \wedge \sim[\sim(q \wedge \sim r) \wedge \sim(\sim p \vee r)]$

por la ley de De Morgan

$\equiv \sim[\sim(p \wedge \sim r) \wedge (q \wedge \sim r)] \wedge \sim[\sim(q \wedge \sim r) \wedge (p \wedge \sim r)]$

por la ley de De Morgan

Sección 2.3

1. $\sqrt{2}$ no es racional.

3. La lógica no es fácil.

6.

		premisas		conclusión
p	q	$p \to q$	$q \to p$	$p \vee q$
V	V	V	V	V
V	F	F	V	
F	V	V	F	
F	F	V	V	F

Este renglón demuestra que para un argumento de esta forma es posible tener premisas verdaderas y una conclusión falsa. Entonces es inválida esta forma de argumento.

7.

			premisas				conclusión
p	q	r	$\sim q$	p	$p \to q$	$\sim q \vee r$	r
V	V	V	F	V	V	V	V
V	V	F	F	V	V	F	
V	F	V	V	V	F	V	
V	F	F	V	V	F	V	
F	V	V	F	F	V	V	
F	V	F	F	F	V	F	
F	F	V	V	F	V	V	
F	F	F	V	F	V	V	

Este renglón describe la única situación en donde todas las premisas son verdaderas. Como aquí también es verdadera la conclusión, entonces es válida esta forma de argumento.

8.

			premisas				conclusión
p	q	r	$\sim q$	$p \vee q$	$p \to \sim q$	$p \to r$	r
V	V	V	F	V	F	V	
V	V	F	F	V	F	F	
V	F	V	V	V	V	V	V
V	F	F	V	V	V	F	
F	V	V	F	V	V	V	V
F	V	F	F	V	V	V	F
F	F	V	V	F	V	V	
F	F	F	V	F	V	V	

Este renglón muestra que para un argumento de esta forma es posible tener premisas verdaderas y una falsa conclusión. Por tanto, es inválida esta forma de argumento.

12. a.

		premisas		conclusión
p	q	$p \to q$	q	p
V	V	V	V	V
V	F	F	F	
F	V	V	V	F
F	F	V	F	

Este renglón demuestra que para un argumento de esta forma es posible tener premisas verdaderas y una conclusión falsa. Así es inválida esta forma de argumento.

14.

		premisa	conclusión
p	q	p	$p \vee q$
V	V	V	V
V	F	V	V
F	V	F	
F	F	F	

Estos dos renglones muestran que en todas las situaciones donde la premisa es verdadera, entonces la conclusión también es verdadera. Así es válida esta forma de argumento.

18.

		premisas		conclusión
p	q	$p \vee q$	$\sim q$	p
V	V	V	F	
V	F	V	V	V
F	V	V	F	
F	F	F	V	

Este renglón representa la única situación en que ambas premisas son verdaderas. Como aquí la conclusión también es verdadera entonces la forma de argumento es válida.

22. Sea que p represente "Tom está en el equipo A" y q denote "Hua es del equipo B". Entonces el argumento tiene la forma

$$\sim p \to q$$
$$\sim q \to p$$
$$\therefore \sim p \vee \sim q$$

premisas — conclusión

p	q	$\sim p$	$\sim q$	$\sim p \rightarrow q$	$\sim q \rightarrow p$	$\sim p \vee \sim q$
V	V	F	F	V	V	F
V	F	F	V	V	V	V
F	V	V	F	V	V	V
F	F	V	V	F	F	

Este renglón demuestra que para un argumento de esta forma es posible tener premisas verdaderas y una falsa conclusión. Entonces es inválida esta forma de argumento.

24. $p \rightarrow q$
q
$\therefore p$ inválido: error converso

25. $p \vee q$
$\sim p$
$\therefore q$ válido: eliminación

26. $p \rightarrow q$
$q \rightarrow r$
$\therefore p \rightarrow r$ válido: transitividad

27. $p \rightarrow q$
$\sim p$
$\therefore \sim q$ inválido: error contrario

36. El programa contiene una variable no declarada.
Una explicación:
1. No falta ningún punto y coma ni tampoco está equivocado el nombre de la variable. *(por (c) y (d) y por la definición de $\wedge$)*
2. No es el caso de que falte ningún punto y coma o que el nombre incorrecto de la variable. *(por (1) y por las leyes de De Morgan)*
3. No existe un error de sintaxis en las primeras cinco líneas. *(por (b) y (2) y por modus tollens)*
4. Hay una variable no declarada. *(por (a) y (3) y por eliminación)*

37. El tesoro está enterrado bajo el asta.
Una explicación:
1. El tesoro no está en la cocina. *(por (a) y (c) y por modus ponens)*
2. El árbol en el patio de enfrente no es un olmo. *(por (b) y (1) y por modus tollens)*
3. El tesoro está enterrado bajo el asta. *(por (d) y (2) y por eliminación)*

38. a. *A* es un bribón y *B* es un caballero.
Una explicación:
1. Supongamos que *A* es un caballero.
2. $\therefore$ Lo que dice *A* es verdadero. *(por definición de caballero)*
3. $\therefore$ *B* también es un caballero. *(Eso es lo que A dice)*
4. $\therefore$ Lo que *B* dice es verdadero. *(por definición de caballero)*
5. $\therefore$ *A* es un bribón. *(Eso es lo que B dice)*
6. $\therefore$ Tenemos una contradicción: *A* es un caballero y un bribón. *(por (1) y (5))*
7. $\therefore$ Es falsa la suposición de que *A* es un caballero. *(por la regla de contradicción)*
8. $\therefore$ *A* es un bribón. *(negación de la suposición)*
9. $\therefore$ Lo que dice *B* es verdadero. *(B dice que A fue un bribón, que ahora sabemos que es verdadero).*
10. $\therefore$ *B* es un caballero. *(por definición de caballero)*

d. *Sugerencia: W* y *Y* son caballeros; el resto son bribones.

39. El chofer asesinó a Lord Hazelton.
Una explicación:
1. Supongamos que el cocinero estaba en la cocina en el momento del asesinato.
2. $\therefore$ El mayordomo mató a Lord Hazelton con estricnina. *(por (c) y (1) y modus ponens)*
3. $\therefore$ Tenemos una contradicción: Lord Hazelton fue asesinado con estricnina y un golpe en la cabeza. *(por (2) y (a))*
4. $\therefore$ Es falsa la suposición de que el cocinero estaba en la cocina. *(por la regla de contradicción)*
5. $\therefore$ El cocinero no se encontraba en la cocina en el momento del asesinato. *(negación de suposición)*
6. $\therefore$ Sara no estaba en el comedor cuando se cometió el asesinato. *(por (e) y (5) y modus ponens)*
7. $\therefore$ Lady Hazelton se encontraba en el comedor cuando ocurrió el asesinato. *(por (b) y (6) y eliminación)*
8. $\therefore$ El chofer mató a Lord Hazelton. *(por (d) y (7) y modus ponens)*

41.
(1)	$p \rightarrow t$	por premisa (d)
	$\sim t$	por premisa (c)
	$\therefore \sim p$	por *modus tollens*
(2)	$\sim p$	por (1)
	$\therefore \sim p \vee q$	por generalización
(3)	$\sim p \vee q \rightarrow r$	por premisa (a)
	$\sim p \vee q$	por (2)
	$\therefore r$	por *modus ponens*
(4)	$\sim p$	por (1)
	r	por (3)
	$\therefore \sim p \wedge r$	por conjunción
(5)	$\sim p \wedge r \rightarrow \sim s$	por premisa (e)
	$\sim p \wedge r$	por (4)
	$\therefore \sim s$	por *modus ponens*
(6)	$s \vee \sim q$	por premisa (b)
	$\sim s$	por (5)
	$\therefore \sim q$	por eliminación

43.
(1)	$\sim w$	por premisa (d)
	$u \vee w$	por premisa (e)
	$\therefore u$	por eliminación
(2)	$u \rightarrow \sim p$	por premisa (c)
	u	por (1)
	$\therefore \sim p$	por *modus ponens*
(3)	$\sim p \rightarrow r \wedge \sim s$	por premisa (a)
	$\sim p$	por (2)
	$\therefore r \wedge \sim s$	por *modus ponens*
(4)	$r \wedge \sim s$	por (3)
	$\therefore \sim s$	por especialización
(5)	$t \rightarrow s$	por premisa (b)
	$\sim s$	por (4)
	$\therefore \sim t$	por *modus tollens*

Sección 2.4

1. $R = 1$ **3.** $S = 1$

5.

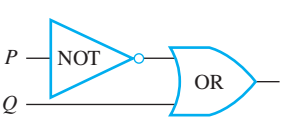
Entrada		Salida
P	***Q***	***R***
1	1	1
1	0	1
0	1	0
0	0	1

7.

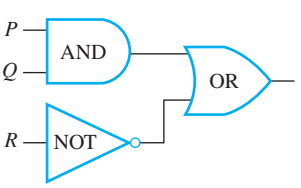
Entrada			Salida
P	***Q***	***R***	***S***
1	1	1	1
1	1	0	0
1	0	1	1
1	0	0	1
0	1	1	1
0	1	0	0
0	0	1	1
0	0	0	0

9. $P \vee \sim Q$ **11.** $(P \wedge \sim Q) \vee R$

13.

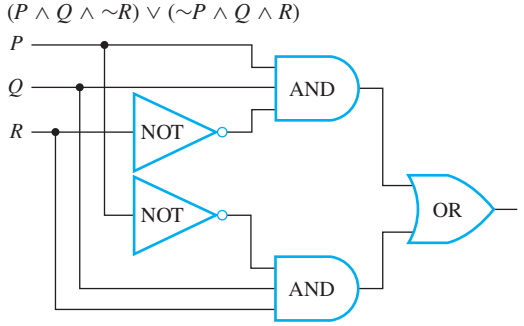


16.



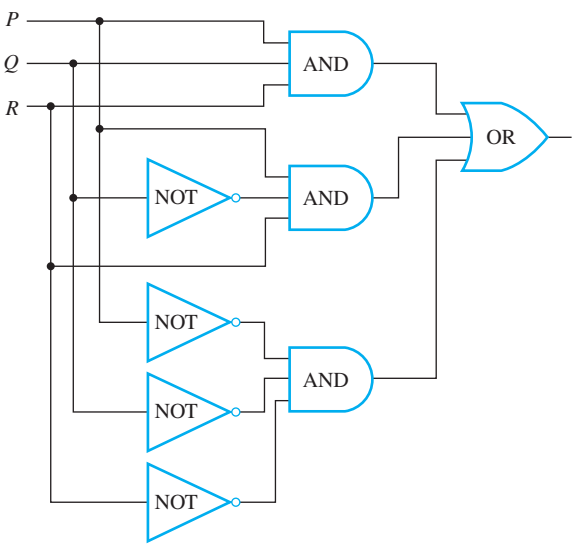
18. **a.** $(P \wedge Q \wedge \sim R) \vee (\sim P \wedge Q \wedge R)$

b.



20. **a.** $(P \wedge Q \wedge R) \vee (P \wedge \sim Q \wedge R) \vee (\sim P \wedge \sim Q \wedge \sim R)$

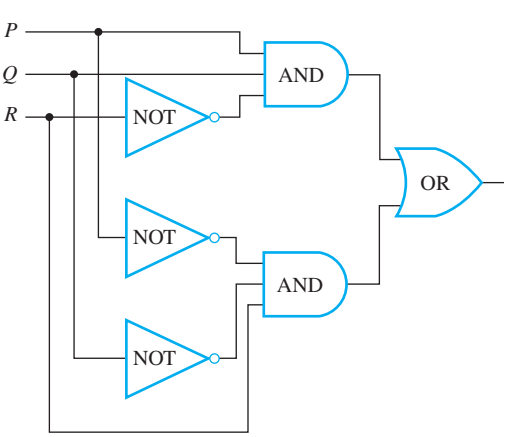
b.



22. La tabla de entrada/salida es

Entrada			Salida
P	***Q***	***R***	***S***
1	1	1	0
1	1	0	1
1	0	1	0
1	0	0	0
0	1	1	0
0	1	0	0
0	0	1	1
0	0	0	0

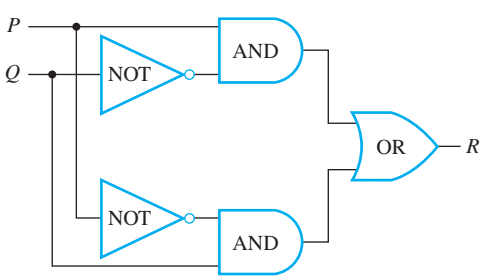
A continuación se muestra un bucle (entre muchos) que tiene esta tabla de entrada/salida



24. Sean P y Q las posiciones de los interruptores en el salón de clases, con 0 denotando "abajo" y 1 significando "arriba". Sea que R represente la condición de la luz, con 0 siendo "apagado" y 1 denotando "encendido". Inicialmente, $P = Q = 0$ y $R = 0$. Si P o Q (pero no ambos) se cambia a 1, se enciende la luz. Así cuando $P = 1$ y $Q = 0$, entonces $R = 1$ y cuando $P = 0$ y $Q = 1$, entonces $R = 1$. En consecuencia, la luz está encendida cuando un interruptor está arriba y el otro está abajo y entonces la luz se apaga al mover hacia arriba el interruptor que está abajo. Así cuando $P = 1$ y $Q = 1$, entonces $R = 0$. Se tiene que la tabla de entrada/salida tiene la siguiente apariencia:

Entrada		Salida
P	***Q***	***R***
1	1	0
1	0	1
0	1	1
0	0	0

El siguiente bucle (entre muchos) tiene esta tabla de entrada/salida:



26. La expresión booleana para *a*) es $(P \wedge Q) \vee Q$ y para *b*) es $(P \wedge Q) \wedge Q$. Debemos demostrar que si esas expresiones se consideran como formas de enunciado, entonces son lógicamente equivalentes. Pero

$(P \wedge Q) \vee Q$

$\equiv Q \vee (P \wedge Q)$ por la ley conmutativa para $\vee$

$\equiv (Q \vee P) \wedge (Q \vee Q)$ por la ley distributiva

$\equiv (Q \vee P) \wedge Q$ por la ley idempotente

$\equiv (P \vee Q) \wedge Q$ por la ley conmutativa para $\wedge$

Alternativamente, por las leyes de absorción, ambas formas de enunciado son lógicamente equivalentes a Q.

28. La expresión booleana para *a*) es

$$(P \wedge Q) \vee (P \wedge \sim Q) \vee (\sim P \wedge \sim Q)$$

y para *b*) es $P \vee \sim Q$. Debemos demostrar que si esas expresiones se consideran como formas de enunciado, entonces son lógicamente equivalentes. Pero

$(P \wedge Q) \vee (P \wedge \sim Q) \vee (\sim P \wedge \sim Q)$

$\equiv ((P \wedge Q) \vee (P \wedge \sim Q)) \vee (\sim P \wedge \sim Q)$
insertando paréntesis (que es legal por la ley asociativa)

$\equiv (P \wedge (Q \vee \sim Q)) \vee (\sim P \wedge \sim Q)$
por la ley distributiva

$\equiv (P \wedge \mathbf{t}) \vee (\sim P \wedge \sim Q)$ por la ley de negación para $\vee$

$\equiv P \vee (\sim P \wedge \sim Q)$ por la ley de identidad para $\wedge$

$\equiv (P \vee \sim P) \wedge (P \vee \sim Q)$ por la ley distributiva

$\equiv \mathbf{t} \wedge (P \vee \sim Q)$ por la ley de negación para $\vee$

$\equiv (P \vee \sim Q) \wedge \mathbf{t}$ por la ley conmutativa para $\wedge$

$\equiv P \vee \sim Q$ por la ley de identidad para $\wedge$

30. $(P \wedge Q) \vee (\sim P \wedge Q) \vee (\sim P \wedge \sim Q)$

$\equiv (P \wedge Q) \vee ((\sim P \wedge Q) \vee (\sim P \wedge \sim Q))$
insertando paréntesis (que es legal por la ley asociativa)

$\equiv (P \wedge Q) \vee (\sim P \wedge (Q \vee \sim Q))$
por la ley distributiva

$\equiv (P \wedge Q) \vee (\sim P \wedge \mathbf{t})$ por la ley de negación para $\vee$

$\equiv (P \wedge Q) \vee \sim P$ por la ley de identidad para $\wedge$

$\equiv \sim P \vee (P \wedge Q)$ por la ley conmutativa para $\vee$

$\equiv (\sim P \vee P) \wedge (\sim P \vee Q)$ por la ley distributiva

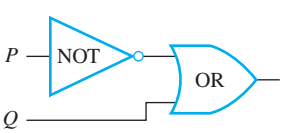
$\equiv (P \vee \sim P) \wedge (\sim P \vee Q)$
por la ley conmutativa para $\vee$

$\equiv \mathbf{t} \wedge (\sim P \vee Q)$ por la ley de negación para $\vee$

$\equiv (\sim P \vee Q) \wedge \mathbf{t}$ por la ley conmutativa para $\wedge$

$\equiv \sim P \vee Q$ por la ley de identidad para $\wedge$

Lo siguiente es, por tanto, un bucle con a lo más dos puertas lógicas que tiene la misma tabla de entrada/salida como el bucle correspondiente a la expresión dada.



34. b. $(P \downarrow Q) \downarrow (P \downarrow Q)$

$\equiv \sim(P \downarrow Q)$ por el inciso (a)

$\equiv \sim[\sim(P \vee Q)]$ por definición de $\downarrow$

$\equiv P \vee Q$ por la ley de doble negación

d. *Sugerencia:* Use los resultados del ejercicio 13 de la sección 2.2 y los incisos *a*) y *c*) de este ejercicio.

Sección 2.5

1. $19_{10} = 16 + 2 + 1 = 10011_2$

4. $458_{10} = 256 + 128 + 64 + 8 + 2 = 111001010_2$

7. $1110_2 = 8 + 4 + 2 = 14_{10}$

10. $1100101_2 = 64 + 32 + 4 + 1 = 101_{10}$

13.
$$\begin{array}{cccccc} & 1 & 1 & 1 & & \\ & 1 & 0 & 1 & 1_2 & \\ + & & 1 & 0 & 1_2 & \\ \hline 1 & 0 & 0 & 0 & 0_2 & \end{array}$$

15.
$$\begin{array}{ccccccc} & 1 & 1 & 1 & & 1 & \\ & 1 & 0 & 1 & 1 & 0 & 1_2 \\ + & & 1 & 1 & 1 & 0 & 1_2 \\ \hline 1 & 0 & 0 & 1 & 0 & 1 & 0_2 \end{array}$$

17.
$$\begin{array}{cccccc} & & & 1 & & \\ & 1 & 10 & \cancel{10} & 1 & \\ \cancel{1} & \cancel{0} & \cancel{1} & 0 & 0_2 & \\ - & 1 & 1 & 0 & 1_2 & \\ \hline & & 1 & 1 & 1_2 & \end{array}$$

19.
$$\begin{array}{cccccc} & & & 0 & \cancel{10} & \\ 1 & 0 & 1 & \cancel{1} & 0 & 1_2 \\ - & 1 & 0 & 0 & 1 & 1_2 \\ \hline & 1 & 1 & 0 & 1 & 0_2 \end{array}$$

21. a. $S = 0, T = 1$

23. $23_{10} = (16 + 4 + 2 + 1)_{10} = 00010111_2 \rightarrow 11101000 \rightarrow 11101001$. Así la respuesta es 11101001.

25. $4_{10} = 00000100_2 \rightarrow 11111011 \rightarrow 11111100$. Así la respuesta es 11111100.

27. Porque el bit principal es 1, esta es la representación 8-bit de un entero negativo. $11010011 \rightarrow 00101100 \rightarrow 00101101_2 \leftrightarrow -(32 + 8 + 4 + 1)_{10} = -45_{10}$. Así la respuesta es -45_{10}.

29. Porque el bit principal es 1, esta es la representación 8-bit de un entero negativo. $11110010 \rightarrow 00001101 \rightarrow 00001110_2 \leftrightarrow -(8 + 4 + 2)_{10} = -14_{10}$. Entonces la respuesta es -14_{10}.

31. $57_{10} = (32 + 16 + 8 + 1)_{10} = 111001_2 \rightarrow 00111001$
$-118_{10} = -(64 + 32 + 16 + 4 + 2)_{10} = -1110110 \rightarrow 01110110 \rightarrow 10001001 \rightarrow 10001010$. Así las representaciones de 57 y -118 son 00111001 y 10001010. La suma de estas representaciones 8-bit es

$$\begin{array}{r} \boxed{0}\boxed{0}\boxed{1}\boxed{1}\boxed{1}\boxed{0}\boxed{0}\boxed{1} \\ + \\ \boxed{1}\boxed{0}\boxed{0}\boxed{0}\boxed{1}\boxed{0}\boxed{1}\boxed{0} \\ \hline \boxed{1}\boxed{1}\boxed{0}\boxed{0}\boxed{0}\boxed{0}\boxed{1}\boxed{1} \end{array}$$

Ya que el bit principal de este número es un 1, entonces la respuesta es negativa. Convirtiendo de nuevo a la forma decimal se obtiene

$$11000011 \rightarrow 00111100 \rightarrow -00111101_2 = -(32 + 16 + 8 + 4 + 1)_{10} = -61_{10}.$$

Por tanto, la respuesta es -61.

32. $62_{10} = (32 + 16 + 8 + 4 + 2)_{10} = 111110_2 \rightarrow 00111110$
$-18_{10} = -(16 + 2)_{10} = -10010_2 \rightarrow 00010010 \rightarrow 11101101 \rightarrow 11101110$

Así las representaciones 8-bit de 62 y -18 son 00111110 y 11101110. La suma de las representaciones 8-bit es

$$\begin{array}{r} \boxed{0}\boxed{0}\boxed{1}\boxed{1}\boxed{1}\boxed{1}\boxed{1}\boxed{0} \\ + \\ \boxed{1}\boxed{1}\boxed{1}\boxed{0}\boxed{1}\boxed{1}\boxed{1}\boxed{0} \\ \hline 1\ \boxed{0}\boxed{0}\boxed{1}\boxed{0}\boxed{1}\boxed{1}\boxed{0}\boxed{0} \end{array}$$

Truncando el 1 en la posición 2^8 se obtiene 00101100. Ya que el bit principal de este número es un 0, la respuesta es positiva. Convirtiendo de nuevo a la forma decimal se obtiene

$$00101100 \rightarrow 101100_2 = (32 + 8 + 4)_{10} = 44_{10}.$$

Entonces la respuesta es 44.

33. $-6_{10} = -(4 + 2)_{10} = -110_2 \rightarrow 00000110 \rightarrow 11111001 \rightarrow 11111010$
$-73_{10} = -(64 + 8 + 1)_{10} = -1001001_2 \rightarrow 01001001 \rightarrow 10110110 \rightarrow 10110111$

Así las representaciones 8-bit de -6 y -73 son 11111010 y 10110111. Sumando las representaciones 8-bit se obtiene

$$\begin{array}{r} \boxed{0}\boxed{0}\boxed{1}\boxed{1}\boxed{1}\boxed{1}\boxed{1}\boxed{0} \\ + \\ \boxed{1}\boxed{1}\boxed{1}\boxed{0}\boxed{1}\boxed{1}\boxed{1}\boxed{0} \\ \hline 1\ \boxed{0}\boxed{0}\boxed{1}\boxed{0}\boxed{1}\boxed{1}\boxed{0}\boxed{0} \end{array}$$

Truncando el 1 en la posición 2^8 resulta 10110001. Como el bit principal de este número es un 1, la respuesta es negativa. Convirtiendo de regreso a la forma decimal se obtiene

$$10110001 \rightarrow 01001110 \rightarrow -01001111_2 = -(64 + 8 + 4 + 2 + 1)_{10} = -79_{10}.$$

Por tanto, la respuesta es -79.

38. $A2BC_{16} = 10 \cdot 16^3 + 2 \cdot 16^2 + 11 \cdot 16 + 12 = 41660_{10}$

41. $00011100000010101011110_2$

44. $2E_{16}$

47. a. $6 \cdot 8^4 + 1 \cdot 8^3 + 5 \cdot 8^2 + 0 \cdot 8 + 2 \cdot 1 = 25{,}410_{10}$

Sección 3.1

1. a. Falso **b.** Verdadero

2. a. El enunciado es verdadero. Los enteros corresponden a ciertos puntos en la recta numérica y los números reales corresponden a todos los puntos sobre la recta numérica.

b. El enunciado es falso; 0 no es positivo ni negativo.

c. El enunciado es falso. Por ejemplo, sea $r = -2$. Entonces $-r = -(-2) = 2$, que es positivo.

d. El enunciado es falso. Por ejemplo, el número $\frac{1}{2}$ es un número real, pero no es un entero.

3. a. $P(2)$ es "$2 > \frac{1}{2}$", que es verdadero.

$P\left(\frac{1}{2}\right)$ es "$\frac{1}{2} > \frac{1}{\frac{1}{2}}$." Esto es falso porque $\frac{1}{\frac{1}{2}} = 2$ y $\frac{1}{2} \not> 2$.

$P(-1)$ es "$-1 > \frac{1}{-1}$." Esto es falso porque $\frac{1}{-1} = -1$ y $-1 \not> -1$.

$P\left(-\frac{1}{2}\right)$ es "$-\frac{1}{2} > \frac{1}{-\frac{1}{2}}$." Esto es verdadero porque $\frac{1}{-\frac{1}{2}} = -2$ y $-\frac{1}{2} > -2$.

$P(-8)$ es "$-8 > \frac{1}{-8}$." Esto es falso porque $\frac{1}{-8} = -\frac{1}{8}$ y $-8 \not> -\frac{1}{8}$.

b. Si el dominio de $P(x)$ es el conjunto de todos los números reales, entonces su conjunto verdadero es el conjunto de todos los números reales x para los que $x > 1$ o $-1 < x < 0$.

c. Si el dominio de $P(x)$ es el conjunto de todos los números reales positivos, entonces su conjunto verdadero es el conjunto de todos los números reales x para que $x > 1$.

4. b. Si el dominio de $Q(n)$ es el conjunto de todos los enteros, entonces su conjunto verdadero es $\{-5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5\}$.

5. a. $Q(-2, 1)$ es el enunciado "Si $-2 < 1$ entonces $(-2)^2 < 1^2$". La hipótesis de este enunciado es $-2 < 1$, que es verdadera. La conclusión es $(-2)^2 < 1^2$, que es falsa porque $(-2)^2 = 4$ y $1^2 = 1$ y $4 \not< 1$. Así $Q(-2, 1)$ es un enunciado condicional con una hipótesis verdadera y una conclusión falsa. Entonces $Q(-2, 1)$ es falso.

c. $Q(3, 8)$ es el enunciado "Si $3 < 8$ entonces $3^2 < 8^2$". La hipótesis de este enunciado es $3 < 8$, que es verdadera. La conclusión es $3^2 < 8^2$, que también es verdadera porque $3^2 = 9$ y $8^2 = 64$ y $9 < 64$. Por tanto, $Q(3, 8)$ es un enunciado condicional con una hipótesis verdadera y una conclusión verdadera. Entonces $Q(3, 8)$ es verdadero.

7. a. El conjunto verdadero es el conjunto de todos los enteros d tales que $6/d$ sea un entero, así el conjunto verdadero es $\{-6, -3, -2, -1, 1, 2, 3, 6\}$.

c. El conjunto verdadero es el conjunto de todos los números reales x con la propiedad que $1 \leq x^2 \leq 4$, así el conjunto verdadero es $\{x \in \mathbf{R} \mid -2 \leq x \leq -1 \text{ o } 1 \leq x \leq 2\}$. En otras palabras, el conjunto verdadero es el conjunto de todos los números reales entre -2 y -1 inclusive junto con aquellos entre 1 y 2 inclusive.

8. a. $\{-9, -8, -7, -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

9. *Contraejemplo:* Sea $x = 1 : 1 \not> \frac{1}{1}$. (*Este es uno de tantos contraejemplos.*)

11. *Contraejemplo:* Sean $m = 1$ y $n = 1$. Entonces $m \cdot n = 1 \cdot 1 = 1$ y $m + n = 1 + 1 = 2$. Pero $1 \not\geq 2$ y así $m \cdot n \not\geq m + n$. (*Este es uno de tantos contraejemplos.*)

13. *a*), *e*), *f*) **14.** *b*), *c*), *e*), *f*)

15. a. *Respuesta parcial:* Cada rectángulo es un cuadrilátero.

b. *Respuesta parcial:* Al menos un conjunto tiene 16 subconjuntos.

16. a. $\forall$ dinosaurio x, x está extinto.

c. $\forall$ número irracional x, x no es un entero.

e. $\forall$ entero x, x^2 no es igual a 2, 147, 581, 953.

17. a. $\exists$ un ejercicio x tal que x tiene una respuesta.

18. a. $\exists s \in D$ tal que $E(s)$ y $M(s)$. (O: $\exists s \in D$ tal que $E(s) \wedge M(s)$.)

b. $\forall s \in D$, si $C(s)$ entonces $E(s)$. (O: $\forall s \in D$, $C(s) \rightarrow E(s)$.)

e. $(\exists s \in D \text{ tal que } C(s) \wedge E(s)) \wedge (\exists s \in D \text{ tal que } C(s) \wedge \sim E(s))$

19. *b*), *d*), *e*)

20. *Respuesta parcial:* La raíz cuadrada de un número real positivo es positiva.

21. a. El grado total de G es par, para cualquier gráfica G.

c. p es par, para algún número primo p.

22. a. $\forall x$, si x es un programa en Java, entonces x tiene al menos 5 líneas.

23. a. $\forall x$, si x es un triángulo equilátero, entonces x es isósceles.

24. a. Existe un sombrerero x tal que x está loco.

Existe x tal que x es un sombrerero y x está loco.

25. a. $\forall$ no fracciones x diferentes de cero, el recíproco de x es una fracción.

$\forall\ x$, si x no es una fracción distinta de cero, entonces el recíproco de x es una fracción.

c. $\forall$ triángulos x, la suma de los ángulos de x es 180°.

$\forall x$, si x es un triángulo, entonces la suma de los ángulos de x es 180°.

e. $\forall$ enteros pares x y y, la suma de x y y es par. $\forall\ x$ y y, si x y y son enteros pares, entonces la suma de x y y es par.

26. b. $\forall x(\text{Int}(x) \longrightarrow \text{Ratl}(x)) \wedge \exists x(\text{Ratl}(x) \wedge \sim \text{Int}(x))$

27. a. Falso. La figura b es un círculo que no es gris.

b. Verdadero. Todas las figuras grises son círculos.

28. b. *Una de tantas respuestas:* Si un número real es negativo, entonces cuando se calcula su opuesto, el resultado es un número real positivo.

Este enunciado es verdadero porque para todos los números reales x, $-(-|x|) = |x|$ (y cualquier número real negativo se puede representar como $-|x|$, para algún número real x).

d. *Una de tantas respuestas:* Existe un número real que no es un entero. Este enunciado es verdadero. Por ejemplo, $\frac{1}{2}$ es un número real que no es un entero.

30. b. *Una respuesta entre muchas:* Si un entero es primo, entonces él no es un cuadrado perfecto.

Este enunciado es verdadero porque un número primo es un entero mayor que 1 que no es el producto de dos enteros positivos más pequeños. Así un número primo no puede ser un cuadrado perfecto porque si lo fuera, entonces él sería un producto de dos enteros positivos más pequeños.

31. *Sugerencia:* Tu respuesta tendría la apariencia que se muestra en el siguiente ejemplo:
Enunciado: "Si una función es derivable, entonces es continua".
Versión formal: $\forall$ funciones f, si f es derivable, entonces f es continua.
Referencia: Calculus por D.R. Mathematician, Best Pub. Co., 2004, página 263.

32. a. Verdadero: Cualquier número real que es más grande que 2 es mayor que 1.

c. Falso: $(-3)^2 > 4$ pero $-3 \not> 2$.

33. a. Verdadero. Siempre que a y b sean positivos, entonces también lo es su producto.

b. Falso. Sea $a = -2$ y $b = -3$. Entonces $ab = 6$, que no es menor que cero.

Sección 3.2

1. *a*) y *e*) son negaciones.

3. a. Existe un pez x tal que x no tiene branquias.

c. $\forall$ película m, m es menor que o igual a 6 horas de duración. (*O:* $\forall$ película m, m es de no más de 6 horas de duración.)

En los ejercicios del 4 al 6 hay otras respuestas correctas además de las aquí que se muestran.

4. a. Algunos perros son poco amigables. (*O:* Al menos existe un perro no amigable.)

c. Todas las sospechas eran infundadas. (*O:* Ninguna sospecha era sustancial.)

5. a. Existe un argumento válido que no tiene una conclusión verdadera. (*O:* Al menos un argumento válido no tiene una conclusión verdadera.)

6. a. Los conjuntos A y B tienen al menos un punto en común.

7. El enunciado no es existencial.

Negación informal: Existe al menos un pedido del almacén A para el artículo B.

Versión formal del enunciado: $\forall$ pedidos x, si x es del almacén A, entonces x no es para el artículo B.

9. Existe un número real x tal que $x > 3$ y $x^2 \leq 9$.

11. No es correcta la negación propuesta. Considere el enunciado dado: "La suma de cualesquiera dos números irracionales es irracional". Que esto sea falso significa que es posible encontrar al menos un par de números irracionales cuya suma es racional. Por otro lado, la negación propuesta en el ejercicio ("La suma de cualesquiera dos números irracionales es racional") significa que dados cualesquiera dos números irracionales, su suma es racional. Esto es un enunciado mucho más fuerte que la negación real: La verdad de este enunciado implica la verdad de la negación (suponiendo que al menos existen dos números irracionales), pero la negación puede ser verdadera sin que sea verdadero este enunciado.

Negación correcta: Existen al menos dos números irracionales cuya suma es racional.

O: La suma de algunos dos números irracionales es racional.

13. No es correcta la negación propuesta. Hay dos errores: La negación de un enunciado "para todos" no es un enunciado "para todos" y la negación de un enunciado si-entonces no es un enunciado si-entonces.

Negación correcta: Existe un entero n tal que n^2 es par y n no es par.

15. a. Verdadero: Todos los números impares en D son positivos.

c. Falso: $x = 16$, $x = 26$, $x = 32$ y $x = 36$ son contraejemplos.

16. $\exists$ un número real x tal que $x^2 \geq 1$ y $x \not> 0$. En otras palabras, $\exists$ un número real x tal que $x^2 \geq 1$ y $x \leq 0$.

18. $\exists$ un número real x tal que $x(x + 1) > 0$ y tanto $x \leq 0$ como $x \geq -1$.

20. $\exists$ enteros a, b y c tales que $a - b$ es par, $b - c$ es par y $a - c$ no es par.

22. Hay un entero tal que el cuadrado de un entero es impar pero el entero no es impar. (*O:* Al menos un entero tiene un cuadrado impar pero él no es impar.)

24. a. Si una persona es un niño en la familia de Tom, entonces la persona es femenina.

Si una persona femenina pertenece a la familia de Tom, entonces la persona es un niño.

El segundo enunciado es converso del primero.

25. a. *Converso:* Si $n + 1$ es un entero par, entonces n es un número primo más grande que 2.

Contraejemplo: Sea $n = 15$. Entonces $n + 1$ es par pero n no es un número primo mayor que 2.

26. *Enunciado:* $\forall$ los números reales x, si $x^2 \geq 1$ entonces $x > 0$.

Contrapositivo: $\forall$ número real x, si $x \leq 0$ entonces $x^2 < 1$.

Converso: $\forall$ números reales x, si $x > 0$ entonces $x^2 \geq 1$.

Contraria: $\forall$ los números reales x, si $x^2 < 1$ entonces $x \leq 0$.

El enunciado y su contrapositivo son falsos. Como un contraejemplo, sea $x = -2$. Entonces $x^2 = (-2)^2 = 4$ y así $x^2 \geq 1$. Sin embargo, $x \not> 0$.

Los enunciados converso e inverso también son falsos. Como un contraejemplo, sea $x = 1/2$. Entonces $x^2 = 1/4$ y así $x > 0$ pero x^2 no es mayor o igual que 1.

28. *Enunciado:* $\forall\, x \in \mathbf{R}$, si $x(x + 1) > 0$ entonces $x > 0$ o $x < -1$.

Contrapositivo: $\forall$ x $\in \mathbf{R}$, si $x \leq 0$ y $x \geq -1$, entonces $x(x + 1) \leq 0$.

Converso: $\forall\, x \in \mathbf{R}$, si $x > 0$ o $x < -1$ entonces $x(x + 1) > 0$.

Contraria: $\forall\, x \in \mathbf{R}$, si $x(x + 1) \leq 0$ entonces $x \leq 0$ y $x \geq -1$.

Son verdaderos todos el enunciado, su contrapositivo, su converso y su contrario.

30. *Enunciado:* $\forall$ enteros a, b y c, si $a - b$ es par y $b - c$ es par, entonces $a - c$ es par.

Contrapositivo: $\forall$ enteros a, b y c, si $a - c$ no es par, entonces $a - b$ no es par o $b - c$ no es par.

Converso: $\forall$ enteros a, b y c, si $a - c$ es par, entonces $a - b$ es par y $b - c$ es par.

Contraria: $\forall$ enteros a, b y c, si $a - b$ no es par o $b - c$ no es par, entonces $a - c$ no es par.

El enunciado es verdadero, pero son falsos su contraria y converso. Como un contraejemplo, sean $a = 3$, $b = 2$ y $c = 1$. Entonces $a - c = 2$, que es par, pero $a - b = 1$ y $b - c = 1$, así no ocurre que ambos $a - b$ y $b - c$ sean pares.

32. *Enunciado:* Si el cuadrado de un entero es impar, entonces el entero es impar.

Contrapositivo: Si un entero no es impar, entonces el cuadrado del entero no es impar.

Converso: Si un entero es impar, entonces el cuadrado del entero es impar.

Inverso: Si el cuadrado de un entero no es impar, entonces el entero no es impar.

Son verdaderos el enunciado, su contrapositivo y su contraria y converso.

34. a. Si n es divisible por algún número primo estrictamente por 1 y $\sqrt{n}$, entonces n no es primo.

36. a. *Una posible respuesta:* Sea $P(x)$ sea "$2x \neq 1$". El enunciado "$\forall x \in \mathbf{Z}$, $2x \neq 1$" es verdadero, pero son falsos los enunciados "$\forall x \in \mathbf{Q}$, $2x \neq 1$" y "$\forall x \in \mathbf{R}$, $2x \neq 1$".

37. La afirmación es "$\forall x$, si $x = 1$ y x está en la secuencia 0204, entonces x está a la izquierda de todos los 0 de la secuencia". La negación es "$\exists x$ tal que $x = 1$ y x está en la secuencia 0204 y x no está a la izquierda de todos los 0 en la secuencia". La negación es falsa porque la secuencia no contiene el carácter 1. Así la afirmación es vacuamente verdadera (o verdadera por defecto).

39. Si una persona gana un grado de C^- en este curso, entonces el curso cuenta para la graduación.

41. Si una persona no está a tiempo cada día, entonces la persona no mantendrá su empleo.

43. No es el caso de que si un número es divisible por 4, entonces ese número es divisible por 8. En otras palabras, existe un número que es divisible por 4 y no es divisible por 8.

45. No es el caso de que si una persona tiene un gran ingreso, entonces esa persona sea feliz. En otras palabras, existe una persona con fuerte ingreso pero infeliz.

48. No. Interpretado formalmente, el enunciado dice, "Si los portadores no ofrecen la misma tarifa más baja, entonces tú puedes no seleccionar a ninguno de ellos", o, equivalentemente, "Si puede seleccionar entre los portadores, entonces ofrecen la misma tarifa más baja".

Sección 3.3

1. a. Verdadero: Tokio es la capital de Japón.

b. Falso: Atenas no es la capital de Egipto.

2. a. Verdadero: $2^2 > 3$ **b.** Falso: $1^2 \not> 1$.

3. a. $y = \frac{1}{2}$ **b.** $y = -1$

4. a. Sea $n = 16$. Entonces $n > x$ ya que $16 > 15.83$.

5. El enunciado dice que no importa qué círculo puedan darle, puede encontrar un cuadrado del mismo color. Esto es verdadero porque los únicos círculos son a, c y b y dado a o c, que son azules, el cuadrado j también es azul y dado b, que es gris, los cuadrados g y h también son grises.

7. Esto es verdadero porque el triángulo d está arriba de cada cuadrado.

9. a. Hay cinco elementos en D. Para cada elemento en E debe encontrar uno tal que la suma de los dos sea igual a cero. Así: si $x = -2$, tome $y = 2$; si $x = -1$, tome $y = 1$; si $x = 0$, tome $y = 0$; si $x = 1$, tome $y = -1$; si $x = 2$, tome $y = -2$.

Alternativamente, observe que para cada entero x en D, el entero $-x$ también está en D, incluyendo 0 (porque $-0 = 0$) y para todos los enteros x, $x + (-x) = 0$.

10. a. Verdadero. Cada estudiante elige al menos un postre: Uta elige un pay, Tom elige pay y pastel y Yuen elige pay.

c. Este enunciado dice que algún postre particular fue elegido por cada estudiante. Esto es verdadero: Cada estudiante eligió pay.

11. a. Existe un estudiante que vio *Casablanca*.

c. Cada estudiante ha visto al menos una película.

d. Existe una película que ha sido vista por cada estudiante. (Hay muchas otras formas aceptables de establecer esas respuestas.)

12. a. *Negación:* $\exists x$ en D tal que $\forall y$ en E, $x + y \neq 1$. La negación es verdadera. Cuando $x = -2$, el único número y con la propiedad que $x + y = 1$ es $y = 3$ y 3 no está en E.

b. *Negación:* $\forall x$ en D, $\exists y$ en E tal que $x + y \neq -y$. La negación es verdadera y el enunciado original es falso. Para ver que el enunciado original es falso, tome cualquier x en D y seleccione y como cualquier número en E con $y \neq -\frac{x}{2}$. Entonces $2y \neq -x$ y sumando x y restando y de ambos lados da $x + y \neq -y$.

En los ejercicios 13 al 19 hay otras respuestas correctas además de las que se muestran.

13. a. *Enunciado:* Para cada color, existe un animal de ese color.

Hay animales de cada color.

b. *Negación:* Existe un color C tal que $\forall$ los animales A, A no tiene el color C.

Para algún color, no hay algún animal de ese color.

14. *Enunciado:* Existe un libro que toda la gente ha leído.

Negación: No existe un libro que toda la gente haya leído. (*O:* $\forall$ los libros b, existe una persona p tal que p no ha leído b.)

15. a. *Enunciado:* Para cada entero impar n, existe un entero k tal que $n = 2k + 1$.

Dado cualquier entero impar, existe otro entero para el que el número dado es igual a dos veces el otro entero más 1. Dado cualquier entero impar n, podemos encontrar otro entero k tal que $n = 2k + 1$.

Un entero impar es igual al doble de otro entero más 1.

Cada entero impar tiene la forma $2k + 1$ para algún entero k.

b. *Negación:* Existe un entero impar n tal que $\forall$ los enteros k, $n \neq 2k + 1$.

Existe un entero impar que no es igual a $2k + 1$ para cualquier entero k.

Algún entero impar no tiene la forma $2k + 1$ para cualquier entero k.

18. a. *Enunciado:* Para cada número real x, existe un número real y tal que $x + y = 0$.

Dado cualquier número real x, existe un número real y tal que $x + y = 0$.

Dado cualquier número real, podemos encontrar otro número real (posiblemente él mismo) tal que la suma del número dado más el otro número sea igual a 0.

Cada número real se puede sumar a algún otro número real (posiblemente él mismo) para obtener 0.

b. *Negación:* Existe un número real x tal que $\forall$ los números reales y, $x + y \neq 0$.

Existe un número real x para el que no existe un número real y con $x + y = 0$.

Existe un número real x con la propiedad que $x + y \neq 0$ para cualquier número real y.

Algún número real tiene la propiedad de que su suma con cualquier otro número real no es cero.

20. El enunciado (1) dice que no importa qué cuadrado pueda tener, no puede encontrar un triángulo de color diferente. Esto es verdadero porque los únicos cuadrados son e, g, h y j y dados los cuadrados g y h, que son grises, podría tomar el triángulo d, que es negro; dado que el cuadrado e, es negro, podría tomar cualquiera de los triángulos f o i, que son grises y dado que el cuadrado j, es azul, podría tomar cualquiera de los triángulos f o h, que son grises o el triángulo d, que es negro.

21. a. (1) El enunciado "$\forall$ los números reales x, existe un número real y, $2x + y = 7$" es verdadero.

(2) El enunciado "Existe un número real x tal que $\forall$ los números reales y, $2x + y = 7$" es falso.

b. Ambos enunciados (1) "$\forall$ los números reales x, existe un número real y tal que $x + y = y + x$" y (2) "Existe un número real x tal que $\forall$ los números reales y, $x + y = y + x$" son verdaderos.

22. a. Dado cualquier número real, puede encontrar un número real tal que la suma de los dos sea cero. En otras palabras, cada número real tiene un inverso aditivo. Este enunciado es verdadero.

b. Existe un número real con la siguiente propiedad: No importa qué número se le sume, la suma de los dos será cero. En otras palabras, existe un número real particular cuya suma con cualquier número real es cero. El enunciado es falso; no habrá tal número que funcione para todos los números. Por ejemplo, si $x + 0 = 0$, entonces $x = 0$, pero en ese caso $x + 1 = 1 \neq 0$.

24. a. $\sim(\forall x \in D(\forall y \in E(P(x, y))))$

$$\equiv \exists x \in D(\sim(\forall y \in E(P(x, y))))$$
$$\equiv \exists x \in D(\exists y \in E(\sim P(x, y)))$$

25. Este enunciado dice que todos los círculos están arriba de todos los cuadrados. Este enunciado es verdadero porque los círculos son a, b y c y los cuadrados son e, g, h y j y todos estos a, b y c se encuentran arriba de todos estos e, g, h y j.

Negación: Existen un círculo x y un cuadrado y tales que x no está arriba de y. En otras palabras, al menos uno de los círculos no está arriba de al menos uno de los cuadrados.

27. El enunciado dice que existen un círculo y un cuadrado con la propiedad de que el círculo está arriba del cuadrado y tiene un color distinto al del cuadrado. Este enunciado es verdadero. Por ejemplo, el círculo a se encuentra arriba del cuadrado e y está coloreado diferente a éste. (Podrían ser dados otros ejemplos.)

29. a. *Versión con cuantificadores intercambiados:* Existe $x \in \mathbf{R}$ tal que $\forall\, y \in \mathbf{R}$, $x < y$.

b. El enunciado dado dice que para cualquier número real x, existe un número real y que es más grande que x. Esto es verdadero: Para cualquier número real x, sea $y = x + 1$. Entonces $x < y$. La versión con cuantificadores intercambiados dice que existe un número real que es menor que cualquier otro número real. Esto es falso.

31. $\forall$ gente x, $\exists$ una persona y tal que x es mayor que y.

32. Existe una persona x tal que $\forall$ gente y, x es mayor que y.

33. a. *Versión formal:* $\forall$ gente x, existe una persona y tal que x ama a y.

b. *Negación:* Existe una persona x tal que $\forall$ gente y, x no ama a y. En otras palabras, existe alguien que no ama a nadie.

34. a. *Versión formal:* Existe una persona x tal que $\forall$ gente y, x ama a y.

b. *Negación:* $\forall$ gente x, existe una persona y tal que x no ama a y. En otras palabras, todos tienen a alguien que no los ama.

37. a. *Enunciado:* $\forall$ entero par n, existe un entero k tal que $n = 2k$.

b. *Negación:* Existe un entero par n tal que $\forall$ entero k, n es $\neq 2k$.

Existe algún entero par que no es igual al doble de algún otro entero.

39. a. *Enunciado:* Existe un programa P tal que $\forall$ preguntas Q hechas a P, P da la respuesta correcta a Q.

b. *Negación:* $\forall$ programa P, existe una pregunta Q que puede ser hecha a P tal que P no da la respuesta correcta a Q.

40. a. $\forall$ minuto m, existe un incauto s tal que s nació en el minuto m.

41. a. El enunciado dice que dado cualquier entero positivo, existe un entero positivo tal que el primer entero es una unidad más que el segundo entero. Esto es falso. Dado el entero positivo $x = 1$, el único entero con la propiedad $x = y + 1$ es $y = 0$, pero 0 no es un entero positivo.

b. Este enunciado expresa que dado cualquier entero, existe un entero tal que el primer entero es una unidad más que el segundo entero. Esto es verdadero. Dado cualquier entero x, tome $y = x - 1$. Entonces y es un entero y $y + 1 = (x - 1) + 1 = x$.

e. Este enunciado dice que dado cualquier número real, existe un número real tal que el producto de los dos es igual a 1. Esto es falso porque $0 \cdot y = 0 \neq 1$ para cada número y. Así cuando $x = 0$, no existe número real y con la propiedad que $xy = 1$.

42. Existe $\varepsilon > 0$ tal que $\forall$ enteros N, existe un entero n tal que $n > N$ y ya sea $L - \varepsilon \geq a_n$ o $a_n \geq L + \varepsilon$. En otras palabras, existe un número positivo ε tal que para todos los enteros N, es posible encontrar un entero n que es mayor que N y con la propiedad de que a_n no está entre $L - \varepsilon$ y $L + \varepsilon$.

44. a. Este enunciado es verdadero. El único número real con la propiedad dada es 1. Observe que

$$1 \cdot y = y \quad \text{para todos los números reales } y,$$

y si x es cualquier número real tal que, por ejemplo, $x \cdot 2 = 2$, entonces dividiendo ambos lados entre 2 da $x = 2/2 = 1$.

46. a. Verdadero. Ambos triángulos a y c se encuentran sobre los cuadrados.

b. *Versión formal:* $\exists x(\text{Triángulo}(x) \wedge (\forall y(\text{Cuadrado}(y) \rightarrow \text{Arriba}(x, y))))$

c. *Negación formal:* $\forall x(\sim\text{Triángulo}(x) \vee (\exists y\ (\text{Cuadrado}\ (y) \wedge \sim\text{Arriba}(x, y))))$

48. a. Falso. No existe un cuadrado a la derecha del círculo k.

b. *Versión formal:* $\forall x(\text{Círculo}(x) \rightarrow (\exists y(\text{Cuadrado}(y) \wedge \sim\text{Derechade}(y, x))))$

c. *Negación formal:* $\exists x(\text{Círculo}(x) \wedge (\forall y(\sim\text{Cuadrado}(y) \vee \sim\text{Derechade}(y, x))))$

51. a. Falso. No existe ningún objeto que tenga un color diferente al de cada objeto

b. *Versión formal:* $\exists y\ (\forall x(x \neq y \rightarrow \sim\text{MismoColor}(x, y)))$

c. *Negación formal:* $\forall y(\exists\ x\ (x \neq y \wedge \text{MismoColor}(x, y)))$

53. a. Falso.

b. *Versión formal:* $\exists x(\text{Círculo}(x) \wedge (\exists y(\text{Cuadrado}(y) \wedge \text{MismoColor}(x, y))))$

c. *Negación formal:* $\forall x(\sim\text{Círculo}(x) \vee (\forall y(\sim\text{Cuadrado}(y) \vee \sim\text{MismoColor}(x, y))))$

55. No importa qué dominio es D o qué predicados sean $P(x)$ y $Q(x)$, los enunciados dados tienen el mismo valor de verdad. Si el enunciado "$\forall x$ en D, $(P(x) \wedge Q(x))$" es verdadero, entonces $P(x) \wedge Q(x)$ es verdadero para cada x en D, lo que implica que tanto $P(x)$ como $Q(x)$ son verdaderos para cada x en D. Pero entonces $P(x)$ es verdadero para cada x en D y también $Q(x)$ es verdadero para cada x en D. Así el enunciado "$(\forall x$ en D, $(P(x))$ $\wedge$ $(\forall x$ en D $(Q(x))$" es verdadero. Conversamente, si el enunciado "$(\forall x$ en D $(P(x)) \wedge (\forall x$ en D, $(Q(x))$" es verdadero, entonces $P(x)$ es verdadero para cada x en D y también $Q(x)$ es verdadero para cada x en D. Esto implica que tanto $P(x)$ como $Q(x)$ son verdaderos para cada x en D y así $P(x) \wedge Q(x)$ es verdadero para cada x en D. Entonces el enunciado "$\forall x$ en D, $(P(x) \wedge Q(x))$" es verdadero.

59. a. Sí. **b.** $X = w_1, X = w_2$ **c.** $X = b_2, X = w_2$

Sección 3.4

1. b. $(f_i + f_j)^2 = f_i^2 + 2f_i f_j + f_j^2$

c. $(3u + 5v)^2 = (3u)^2 + 2(3u)(5v) + (5v)^2$
$(= 9u^2 + 30uv + 25v^2)$

d. $(g(r) + g(s))^2 = (g(r))^2 + 2g(r)g(s) + (g(s))^2$

2. 0 es par.

3. $\frac{2}{3} + \frac{4}{5} = \frac{(2\cdot5+3\cdot4)}{(3\cdot5)} \left(= \frac{22}{15}\right)$

5. $\frac{1}{0}$ no es un número irracional

7. No válido; error converso

8. Válido por *modus ponens* universal (o instanciación universal)

9. No válido; error inverso

10. Válido por *modus tollens* universal

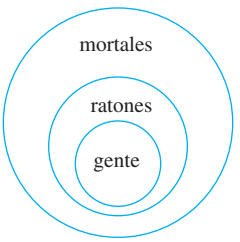
16. No válido; error converso

19. $\forall x$, si x es un buen auto, entonces x no es barato.

a. Válido, *modus ponens* universal (o instanciación universal)

b. No válido, error converso

21. Válido. (¡Un argumento válido puede tener falsas premisas y una conclusión verdadera!)

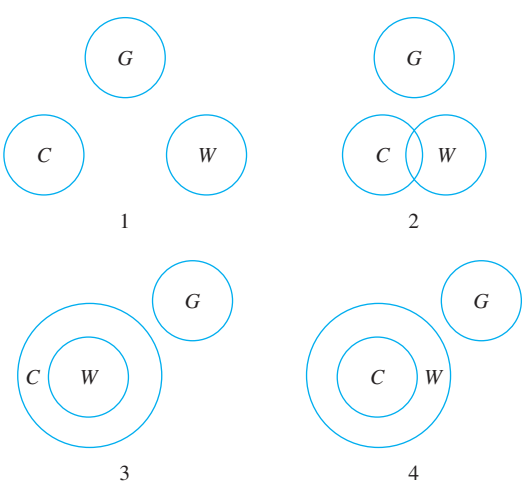


La principal premisa dice que el conjunto de personas está incluido en el conjunto de ratones. La premisa menor expresa que el conjunto de ratones está incluido en el conjunto de mortales. Suponiendo que ambas premisas sean verdaderas, entonces se tiene que el conjunto de personas está incluido en el conjunto de mortales. Puesto que es imposible que la conclusión sea falsa si las premisas son verdaderas, entonces el argumento es válido.

23. Válido. Las premisas menor y mayor pueden ilustrarse con el siguiente diagrama:

De acuerdo al diagrama, el conjunto de maestros y el conjunto de dioses no pueden tener elementos en común. Así que, si las premisas son verdaderas, entonces la conclusión también debe ser verdadera y entonces el argumento es válido.

25. No válido. Sea que C represente el conjunto de la comida de todas las cafeterías colegiales, sea G el conjunto de toda la buena comida y W el conjunto de todo el desperdicio de comida. Entonces cualquiera de los siguientes diagramas podría representar las premisas dadas.



Sólo el dibujo (1) es la conclusión verdadera. Así que es posible que las premisas sean verdaderas pero que la conclusión sea falsa, entonces el argumento es no válido.

28. (3) *Forma contrapositiva:* Si un objeto es gris, entonces es un círculo.

(2) Si un objeto es un círculo, entonces él está a la derecha de todos los objetos azules.

(1) Si un objeto está a la derecha de todos los objetos azules, entonces él está arriba de todos los triángulos.

$\therefore$ Si un objeto es gris, entonces debe estar arriba de todos los triángulos.

31. 4. Si un animal está en el patio, entonces es mío.
1. Si un animal me pertenece, entonces confío en él.
5. Si confío en un animal, entonces lo admito en mi estudio.
3. Si acepto un animal en mi estudio, entonces él gruñirá cuando se le pida hacerlo.
6. Si un animal gruñe cuando se le pide hacerlo, entonces ese animal es un perro.
2. Si un animal es un perro, entonces ese animal roe huesos;
$\therefore$ Si un animal está en el patio, entonces ese animal roe huesos; es decir, todos los animales en el patio roen huesos.

33. 2. Si un pájaro está en esta pajarera, entonces me pertenece.
4. Si un pájaro me pertenece, entonces tiene al menos 9 pies de alto.
1. Si un pájaro es de al menos 9 pies de alto, entonces es un avestruz.
3. Si un pájaro vive de migajas, entonces no es un avestruz.
Contrapositivo: Si un pájaro es un avestruz, entonces no vive de migajas.
$\therefore$ Si un pájaro está en un pajarera, entonces no vive de migajas; es decir, ningún pájaro en esta pajarera vive de migajas.

Sección 4.1

1. a. Sí. $-17 = 2\,(-9) + 1$
b. Sí. $0 = 2 \cdot 0$
c. Sí: $2k - 1 = 2(k - 1) + 1$ y $k - 1$ es un entero porque es una diferencia de enteros.

2. a. Sí: $6m + 8n = 2(3m + 4n)$ y $(3m + 4n)$ es un entero porque 3, 4, m y n son enteros y productos y sumas de enteros son enteros.
b. Sí: $10mn + 7 = 2(5mn + 3) + 1$ y $5mn + 3$ es un entero ya que 3, 5, m y n son enteros y productos y sumas de enteros son enteros.
c. No necesariamente. Por ejemplo, si $m = 3$ y $n = 2$, entonces $m^2 - n^2 = 9 - 4 = 5$, que es primo. (Observe que $m^2 - n^2$ está compuesto por muchos valores de m y n debido a la identidad $m^2 - n^2 = (m - n)(m + n)$.)

4. Por ejemplo, sean $m = n = 2$. Entonces m y n son enteros tales que $m > 0$ y $n > 0$ y $\frac{1}{m} + \frac{1}{n} = \frac{1}{2} + \frac{1}{2} = 1$, que es un entero.

7. Por ejemplo, sea $n = 7$. Entonces n es un entero tal que $n > 5$ y $2^n - 1 = 127$, que es primo.

9. Por ejemplo, 25, 9 y 16 todos son cuadrados perfectos, porque $25 = 5^2$, $9 = 3^2$ y $16 = 4^2$ y $25 = 9 + 16$. Así 25 es un cuadrado perfecto que se puede escribir como la suma de otros dos cuadrados perfectos.

11. *Contraejemplo:* Sean $a = -2$ y $b = -1$. Entonces $a < b$ porque $-2 < -1$, pero $a^2 \not< b^2$ porque $(-2)^2 = 4$ y $(-1)^2 = 1$ y $4 \not< 1$. *[Así la hipótesis del enunciado es verdadera pero su conclusión es falsa.]*

14. Esta propiedad es verdadera para algunos enteros y es falsa para otros enteros. Por ejemplo, si $a = 0$ y $b = 1$, la propiedad es verdadera porque $(0 + 1)^2 = 0^2 + 1^2$, pero si $a = 1$ y $b = 1$, la propiedad es falsa porque $(1 + 1)^2 = 4$ y $1^2 + 1^2 = 2$ y $4 \neq 2$.

15. *Sugerencia:* Esta propiedad es verdadera para algunos enteros y falsa para otros enteros. Para justificar esta respuesta se necesita encontrar ejemplos de ambos casos.

17. $2 = 1^2 + 1^2,\ 4 = 2^2,\ 6 = 2^2 + 1^2 + 1^2,$
$8 = 2^2 + 2^2,\ 10 = 3^2 + 1^2,\ 12 = 2^2 + 2^2 + 2^2,$
$14 = 3^2 + 2^2 + 1^2,\ 16 = 4^2,$
$18 = 3^2 + 3^2 = 4^2 + 1^2 + 1^2,\ 20 = 4^2 + 2^2,$
$22 = 3^2 + 3^2 + 2^2,\ 24 = 4^2 + 2^2 + 2^2$

19. a. $\forall$ enteros m y n, si m es par y n es impar, entonces $m + n$ es impar.

$\forall$ enteros pares m y enteros impares n, $m + n$ es impar.

Si m es cualquier entero par y n es cualquier entero impar, entonces $m + n$ es impar.

b. (**a**) cualquier entero impar (**b**) entero r
(**c**) $2r + (2s + 1)$ (**d**) $m + n$ es impar

20. a. Si un entero es mayor que 1, entonces su recíproco está entre 0 y 1.

b. *Inicio de la demostración:* Supongamos que m es cualquier entero tal que $m > 1$.
Conclusión a demostrarse: $0 < 1/m < 1$.

22. a. Si el producto de dos enteros es 1, entonces ambos son 1 o ambos son -1.

b. *Inicio de la demostración:* Supongamos que m y n son cualesquiera enteros con $mn = 1$.
Conclusión a demostrarse: $m = n = 1$ o $m = n = -1$.

24. *A continuación se presentan dos versiones de una demostración correcta para ilustrar algo de la variedad existente.*

Demostración 1: Suponga que n es cualquier *[particular arbitrariamente elegido]* entero par. *[Debemos demostrar que $-n$ es par.]* Por definición de número par, $n = 2k$ para algún entero k. Multiplicando ambos lados por -1 se obtiene que:

$$-n = -(2k) = 2(-k).$$

Sea $r = -k$. Entonces r es un entero porque $r = -k = (-1)k$, -1 y k son enteros y el producto de dos enteros es un entero. Así que, $-n = 2r$ para algún entero r y así $-n$ es par *[que era lo que se quería demostrar]*.

Demostración 2: Supongamos que n es cualquier entero par. Por definición de número par, $n = 2k$ para algún entero k. Entonces:

$$-n = -2k = 2(-k).$$

Pero $-k$ es un entero ya que es el producto de los enteros -1 y k. Así $-n$ es igual a dos veces algún entero y entonces $-n$ es par por definición de número par.

25. *Demostración:* Supongamos que a es cualquier entero par y que b es un entero impar arbitrario. *[Debemos demostrar que $a - b$ es impar.]* Por definición de par e impar, $a = 2r$ y $b = 2s + 1$ para algunos enteros r y s. Por sustitución y álgebra,

$$a - b = 2r - (2s + 1) = 2r - 2s - 1 = 2(r - s - 1) + 1.$$

Sea $t = r - s - 1$. Entonces t es un entero porque las diferencias de enteros son enteros. Así $a - b = 2t + 1$, donde t es un entero y así, por definición de impar, $a - b$ es impar *[que era lo que se quería demostrar]*.

26. *Sugerencia:* La conclusión que se demostrará es que la verdadera cantidad es impar. Para demostrar esto, necesita demostrar que la cantidad es igual a dos veces algún entero más uno.

29. *Demostración:* Suponga que n es cualquier *[particular pero arbitrariamente elegido]* entero impar. *[Debemos mostrar que $3n + 5$ es par.]* Por definición de impar, existe un entero r tal que $n = 2r + 1$. Entonces

$$\begin{aligned} 3n + 5 &= 3(2r + 1) + 5 && \text{por sustitución} \\ &= 6r + 3 + 5 \\ &= 6r + 8 \\ &= 2(3r + 4) && \text{por álgebra.} \end{aligned}$$

Sea $t = 3r + 4$. Entonces t es un entero porque productos y sumas de enteros son enteros. Entonces, $3n + 5 = 2t$, en donde t es un entero y así, por definición de par, $3n + 5$ es par *[que era lo que se quería demostrar]*

31. *Demostración:* Supongamos que k es cualquier *[particular pero arbitrariamente elegido]* entero impar y m es un entero par arbitrario. *[Debemos demostrar que $k^2 + m^2$ es impar.]* Por definición de par e impar, $k = 2a + 1$ y $m = 2b$ para algunos enteros a y b. Entonces

$$\begin{aligned} k^2 + m^2 &= (2a + 1)^2 + (2b)^2 && \text{por sustitución} \\ &= 4a^2 + 4a + 1 + 4b^2 \\ &= 4(a^2 + a + b^2) + 1 \\ &= 2(2a^2 + 2a + 2b^2) + 1 && \text{por álgebra.} \end{aligned}$$

Pero $2a^2 + 2a + 2b^2$ es un entero porque es la suma de productos de enteros. Así $k^2 + m^2$ es el doble de un entero más 1, entonces $k^2 + m^2$ es impar *[que era lo que se quería demostrar]*.

33. *Demostración:* Suponga que n es cualquier entero par. Entonces $n = 2k$ para algún entero k. Por tanto:

$$(-1)^n = (-1)^{2k} = ((-1)^2)^k = 1^k = 1$$

[por las leyes de los exponentes del álgebra]. Que era lo que se quería demostrar.

35. La negación del enunciado es "Para todos los enteros $m \geq 3$, $m^2 - 1$ no es primo".

Demostración de la negación: Supongamos que m es un entero arbitrario con $m \geq 3$. Por álgebra básica, $m^2 - 1 = (m-1)(m + 1)$. Como $m \geq 3$, tanto $m - 1$ como $m + 1$ son enteros positivos mayores que 1 y cada uno es más pequeño que $m^2 - 1$. Así $m^2 - 1$ es el producto de dos enteros positivos más pequeños, cada uno mayor que 1 y entonces $m^2 - 1$ no es primo.

38. La prueba incorrecta demuestra justamente que el teorema continua siendo válido en caso de que $k = 2$. Una prueba real debe demostrar que es correcto para *todos* los enteros $k > 0$.

39. El error en la "prueba" es que el mismo símbolo, k, se utiliza para representar dos cantidades diferentes. Colocando $m = 2k$ y $n = 2k + 1$, la prueba implica que $n = m + 1$ y así se deduce la conclusión sólo para esta situación. Cuando $m = 4$ y $n = 17$, por ejemplo, los cálculos en la prueba indican que $n - m = 1$, pero realmente $n - m = 13$. En otras palabras, la prueba no deduce la conclusión para un entero par m y un entero impar n arbitrariamente elegidos, así que es inválida.

40. Esta prueba incorrecta exhibe razonamiento circular. Las palabras *puesto que* en la tercera frase están completamente injustificadas. La segunda frase sólo dice qué pasa *si* $k^2 + 2k + 1$ es compuesta. Pero en ese punto de la prueba, no se ha establecido que $k^2 + 2k + 1$ *es* compuesta. De hecho, eso es exactamente lo que se tiene que demostrar.

43. Verdadero. *Demostración:* Supongamos que m y n son enteros impares arbitrarios. *[Debemos demostrar que mn es impar.]* Por definición de impar, $n = 2r + 1$ y $m = 2s + 1$ para algunos enteros r y s. Entonces

$$\begin{aligned} mn &= (2r + 1)(2s + 1) && \text{por sustitución} \\ &= 4rs + 2r + 2s + 1 \\ &= 2(2rs + r + s) + 1 && \text{por álgebra.} \end{aligned}$$

Ahora $2rs + r + s$ es un entero porque productos y sumas de enteros son enteros y 2, r y s son enteros. Así $mn = 2 \cdot$(algún entero) $+ 1$ y entonces, por definición de impar, mn es impar.

44. Verdadero. *Demostración:* Supongamos que n es cualquier entero impar. *[Debemos demostrar que $-n$ es impar.]* Por definición de impar, $n = 2k + 1$ para algún entero k. Sustituyendo y álgebra,

$$-n = -(2k + 1) = -2k - 1 = 2(-k - 1) + 1.$$

Sea $t = -k - 1$. Entonces t es un entero porque diferencias de enteros son enteras. Así $-n = 2t + 1$, en donde t es un entero y entonces, por definición de impar, $-n$ es impar *[que era lo que se quería demostrar]*.

45. Falso. *Contraejemplo:* Tanto 1 como 3 son impares, pero su diferencia es $3 - 1 = 2$, que es par.

47. Falso. *Contraejemplo:* Sean $m = 1$ y $n = 3$. Entonces $m + n = 4$ es par, pero ni el sumando m o el sumando n son pares.

54. *Demostración:* Sea n un entero arbitrario. Entonces

$$\begin{aligned} 4(n^2 + n + 1) - 3n^2 &= 4n^2 + 4n + 4 - 3n^2 \\ &= n^2 + 4n + 4 = (n + 2)^2 \end{aligned}$$

(por álgebra). Pero $(n + 2)^2$ es un cuadrado perfecto porque $n + 2$ es un entero (siendo la suma de n y 2). Así que $4(n^2 + n + 1) - 3n^2$ es un cuadrado perfecto, que era lo que se quería demostrar.

56. *Sugerencia:* Esto es verdadero.

62. *Sugerencia:* La respuesta es no.

Sección 4.2

1. $\frac{-35}{6} = \frac{-35}{6}$

3. $\frac{4}{5} + \frac{2}{9} = \frac{4\cdot 9+2\cdot 5}{45} = \frac{46}{45}$

4. Sea $x = 0.3737373737\ldots$.
Entonces $100x = 37.37373737\ldots$ y así
$100\,x - x = 37.37373737\ldots - 0.37373737$
Por tanto, $99x = 37$ y entonces $x = 37/99$.

6. Sea $x = 320.5492492492\ldots$.
Entonces $10000x = 3205492.492492\ldots$ y
$10x = 3205.492492492\ldots$, por tanto
$10000x - 10x = 3205492 - 3205$.
Así $9990x = 3202287$, en consecuencia $x = \frac{3202287}{9990}$.

8. **b.** $\forall$ números reales x y y, si $x \neq 0$ y $y \neq 0$ entonces $xy \neq 0$.

9. Como a y b son enteros y $b - a$ y ab^2 también son enteros (ya que las diferencias y productos de enteros también son enteros). Además, por la propiedad del producto cero, $ab^2 \neq 0$ porque ni a o b valen cero. Entonces $(b-a)/ab^2$ es un cociente de dos enteros con denominador distinto de cero, así que es racional.

11. *Demostración:* Supongamos que n es cualquier *[particular arbitrariamente elegido]* entero. Entonces $n = n\cdot 1$ y al dividir ambos lados entre 1 se obtiene que $n = n/1$. Tanto n como 1 son enteros y $1 \neq 0$. Así que n se puede escribir como un cociente de enteros con un denominador distinto de cero, entonces n es racional.

12. (**a**) cualquier número racional *[particular pero arbitrariamente elegido]*.
(b) enteros a y b **(c)** $(a/b)^2$ **(f)** b^2
(e) propiedad del producto cero **(f)** r^2 es racional

13. **a.** $\forall$ número real r, si r es racional entonces $-r$ es racional.
O: $\forall r$, si r es un número racional entonces $-r$ es racional.
O: $\forall$ número racional r, $-r$ es racional.

b. El enunciado es verdadero. *Demostración:* Suponga que r es un número racional *[particular pero arbitrariamente elegido]*. *[Debemos demostrar que $-r$ es racional.]* Por definición de racional, $r = a/b$ para algunos enteros a y b con $b \neq 0$. Entonces

$$-r = -\frac{a}{b} \quad \text{por sustitución}$$
$$= \frac{-a}{b} \quad \text{por álgebra.}$$

Como a es un entero, también lo es $-a$ (siendo el producto de -1 y a). Así que $-r$ es el cociente de enteros con un denominador distinto de cero, entonces $-r$ es racional *[que era lo que se quería demostrar]*.

15. *Demostración:* Supongamos que r y s son números racionales. Por definición de racional, $r = a/b$ y $s = c/d$ para algunos enteros a, b, c y d con b y d distintos de cero. Entonces

$$rs = \frac{a}{b}\cdot\frac{c}{d} \quad \text{por sustitución}$$
$$= \frac{ac}{bd} \quad \text{por las reglas del álgebra para multiplicar fracciones.}$$

Ahora ac y bd son enteros (siendo productos de enteros) y $bd \neq 0$ (por la propiedad del producto cero). Así que rs es el cociente de enteros con denominador distinto de cero, entonces, por definición de racional, rs es racional.

16. *Sugerencia: Contraejemplo:* Sea r cualquier número racional y $s = 0$. Entonces r y s son racionales, pero el cociente de r dividido entre s es indefinido y por tanto no es un número racional.
Enunciado revisado para demostrarse: Para todos los números racionales r y s, si $s \neq 0$ entonces r/s es racional.

17. *Sugerencia:* La conclusión a demostrar es que la verdadera cantidad (la diferencia de dos números racionales) es racional. Para demostrar esto, necesita demostrar que la cantidad se puede expresar como una razón de dos enteros con un denominador distinto de cero.

18. *Sugerencia:* $\frac{a/b+c/d}{2} = \frac{(ad+bc)/(bd)}{2} = \frac{ad+bc}{2bd}$

19. *Sugerencia:* Si $a < b$ entonces $a + a < a + b$ (por T19 del apéndice A), o equivalentemente $2a < a + b$. Así $a < \frac{a+b}{2}$ (por T20 del apéndice A).

21. Verdadero. *Demostración:* Supongamos que m es cualquier entero par y n es un entero impar arbitrario. *[Debemos demostrar que $m^2 + 3n$ es impar.]* Por las propiedades 1 y 3 del ejemplo 4.2.3, m^2 es par (porque $m^2 = m\cdot m$) y $3n$ es impar (porque 3 y n son impares). De la propiedad 5 *[y de la ley conmutativa para la adición]* se tiene que $m^2 + 3n$ es impar *[que era lo que se quería demostrar]*.

24. *Demostración:* Suponga que r y s son números racionales arbitrarios. Por el teorema 4.2.1, tanto 2 como 3 son racionales y así, por el ejercicio 15, tanto $2r$ como $3s$ son racionales. Entonces por el teorema 4.2.2, $2r + 3s$ es racional.

27. Sea

$$x = \frac{1-\frac{1}{2^{n+1}}}{1-\frac{1}{2}} = \frac{1-\frac{1}{2^{n+1}}}{\frac{1}{2}} = \frac{1-\frac{1}{2^{n+1}}}{\frac{1}{2}}\cdot\frac{2^{n+1}}{2^{n+1}} = \frac{2^{n+1}-1}{2^n}\cdot$$

Pero $2^{n+1} - 1$ y 2^n son enteros (porque n es un entero no-negativo) y $2n \neq 0$ por la propiedad de producto cero. Por tanto, x es racional.

31. *Demostración:* Suponga que c es un número real tal que

$$r_3\,c^3 + r_2\,c^2 + r_1\,c + r_0 = 0,$$

en donde r_0, r_1, r_2 y r_3 son números racionales. Por definición de racional, $r_0 = a_0/b_0$, $r_1 = a_1/b_1$, $r_2 = a_2/b_2$ y $r_3 = a_3/b_3$ para algunos enteros, a_0, a_1, a_2, a_3 y enteros b_0, b_1, b_2 y b_3 diferentes de cero. Sustituyendo,

$$\begin{aligned} &r_3c^3 + r_2c^2 + r_1c + r_0 \\ &= \frac{a_3}{b_3}c^3 + \frac{a_2}{b_2}c^2 + \frac{a_1}{b_1}c + \frac{a_0}{b_0} \\ &= \frac{b_0b_1b_2a_3}{b_0b_1b_2b_3}c^3 + \frac{b_0b_1b_3a_2}{b_0b_1b_2b_3}c^2 + \frac{b_0b_2b_3a_1}{b_0b_1b_2b_3}c + \frac{b_1b_2b_3a_0}{b_0b_1b_2b_3} \\ &= 0. \end{aligned}$$

Multiplicando ambos lados por $b_0\,b_1\,b_2\,b_3$ se obtiene

$$b_0b_1b_2a_3\cdot c^3 + b_0b_1b_3a_2\cdot c^2 + b_0b_2b_3a_1\cdot c + b_1b_2b_3a_0 = 0$$

Sean $n_3 = b_0b_1b_3a_3$, $n_2 = b_0b_1b_3a_2$, $n_1 = b_0b_2b_3a_1$ y $n_0 = b_1b_2b_3a_0$. Entonces n_0, n_1, n_2 y n_3 son todos enteros (ya que son productos de enteros). Así que c satisface la ecuación

$$n_3c^3 + n_2c^2 + n_1c + n_0 = 0,$$

en donde n_0, n_1, n_2 y n_3 son enteros. Que era lo que se quería demostrar.

33. a. *Sugerencia:* Observe que $(x - r)(x - s) = x^2 - (r + s)x + rs$. Si r y s son impares, entonces $r + s$ es par y rs es impar. Así el coeficiente de x^2 es 1 (impar), el coeficiente de x es par y el coeficiente constante, rs, es impar.

35. Esta "prueba" supone lo que debe demostrarse.

37. Haciendo r y s iguales a a/b, esta prueba incorrecta viola el requisito de que r y s son números racionales arbitrariamente elegidos. Si r y s son iguales a a/b, entonces $r = s$.

Sección 4.3

1. Sí, $52 = 13 \cdot 4$ **2.** Sí, $56 = 7 \cdot 8$

4. Sí, $(3k + 1)(3k + 2)(3k + 3) = 3\,[(3k + 1)(3k + 2)(k + 1)]$,

y $(3k + 1)(3k + 2)(k + 1)$ es un entero ya que k es un entero y sumas y productos de enteros son enteros.

6. No, $29/3 \cong 9.67$, que no es entero.

7. Sí, $66 = (-3)(-22)$.

8. Sí, $6a(a + b) = 3a[2(a + b)]$ y $2(a + b)$ es un entero porque a y b son enteros y sumas y productos de enteros son enteros.

10. No, $34/7 \cong 4.86$, que no es entero.

12. Sí, $n^2 - 1 = (4k + 1)^2 - 1 = (16k^2 + 8k + 1) - 1 = 16k^2 + 8k = 8(2k^2 + k)$ y $2k^2 + k$ es un entero ya que k es un entero y sumas y productos de enteros son enteros.

14. **(a)** $a \mid b$ **(b)** $b = a \cdot r$ **(c)** $-r$ **(d)** $a \mid (-b)$

15. *Demostración:* Suponga que a, b y c son enteros arbitrarios tales que $a \mid b$ y $a \mid c$. *[Debemos demostrar que $a \mid (b + c)$.]* Por definición de divisibilidad, $b = ar$ y $c = as$ para algunos enteros r y s. Entonces

$$b + c = ar + as = a(r + s) \quad \text{por álgebra.}$$

Sea $t = r + s$. Entonces t es un entero (siendo una suma de enteros) y así $b + c = at$, en donde t es un entero. Por definición de divisibilidad, entonces, $a \mid (b + c)$ *[que era lo que se quería demostrar]*.

16. *Sugerencia:* La conclusión a demostrar es que la verdadera cantidad es divisible por a. Para demostrar esto, Necesita demostrar que la cantidad es igual a a veces algún entero.

17. a. $\forall$ enteros n, si n es un múltiplo de 3, entonces $-n$ es un múltiplo de 3.

b. El enunciado es verdadero. *Demostración:* Supongamos que n es cualquier entero múltiplo de 3. *[Debemos demostrar que $-n$ es un múltiplo de 3.]* Por definición de múltiplo, $n = 3k$ para algún entero k. Entonces

$$\begin{aligned} -n &= -(3k) && \text{por sustitución} \\ &= 3(-k) && \text{por álgebra.} \end{aligned}$$

Así que, por definición de múltiplo, $-n$ es un múltiplo de 3 *[que era lo que se quería demostrar]*.

18. *Contraejemplo:* Sean $a = 2$ y $b = 1$. Entonces $a + b = 2 + 1 = 3$ y así $3 \mid (a + b)$ porque $3 = 3 \cdot 1$. Por otro lado, $a - b = 2 - 1 = 1$ y 3 no divide a 1 porque $1/3$ no es un entero. Por tanto, 3 no divide a $(a - b)$. *[Así la hipótesis del enunciado es verdadera pero su conclusión es falsa.]*

19. *Inicio de la demostración:* Suponga que a, b y c son enteros arbitrarios tales que a divide a b. *[Debemos demostrar que a divide a bc.]*

22. *Sugerencia:* El enunciado dado se puede reescribir formalmente como "$\forall$ enteros n, si n es divisible entre 6, entonces n es divisible entre 2". Este enunciado es verdadero.

24. El enunciado es verdadero. *Demostración:* Suponga que a, b y c son cualesquiera enteros tales que $a \mid b$ y $a \mid c$. *[Debemos demostrar que $a \mid (2b - 3c)$.]* Por definición de divisibilidad, sabemos que $b = am$ y $c = an$ para algunos enteros m y n. Se tiene que $2b - 3c = 2(am) - 3(an)$ *(sustituyendo)* $= a(2m - 3n)$ *(por álgebra básica)*. Sea $t = 2m - 3n$. Entonces t es un entero porque es la diferencia de productos de enteros. Por tanto, $2b - 3c = at$, en donde t es un entero y así $a \mid (2b - 3c)$ por definición de divisibilidad *[que era lo que se quería demostrar]*.

25. El enunciado es falso. *Contraejemplo:* Sean $a = 2$, $b = 3$ y $c = 8$. Entonces $a \mid c$ porque 2 divide a 8, pero ab no divide a c porque $ab = 6$ y 6 no divide a 8.

26. *Sugerencia:* El enunciado es verdadero.

27. *Sugerencia:* El enunciado es falso.

32. No. Cada uno de esos números es divisible por 3 y entonces su suma también es divisible entre 3. Pero 100 no es divisible entre 3. Así que la suma no puede ser igual a \$100.

36. a. La suma de los dígitos es 54, que es divisible por 9. Por tanto, 637, 425, 403, 705, 125 es divisible por 9 y entonces también es divisible por 3 (por la transitividad de la divisibilidad). Como el dígito más a la derecha es 5, entonces 637, 425, 403, 705, 125 no es divisible por 5. Y como los dígitos más a la derecha son 25, que no es divisible por 4, entonces 637, 425, 403, 705, 125 no es divisible por 4.

37. a. $1176 = 2^3 \cdot 3 \cdot 7^2$

38. a. $p_1^{2e_1} p_2^{2e_2} \cdots p_k^{2e_k}$

b. $n = 42$, $2^5 \cdot 3 \cdot 5^2 \cdot 7^3 \cdot n = 5880^2$

40. a. Como $12a = 25b$, entonces el teorema de factorización única garantiza que las formas estándar factorizadas de $12a$ y $25b$ deben ser las mismas. Así $25b$ contiene los factores $2^2 \cdot 3 (= 12)$. Pero puesto que 2 ni 3 dividen a 25, entonces los factores $2^2 \cdot 3$ deben ocurrir en b, Por tanto $12 \mid b$. Similarmente, $12a$ contiene los factores $5^2 = 25$ y como 5 no es factor de 12, entonces los factores 5^2 deben ocurrir en a. Así $25 \mid a$.

41. *Sugerencia:* $45^8 \cdot 88^5 = (3^2 \cdot 5)^8 \cdot (2^3 \cdot 11)^5 = 13^{16} \cdot 5^8 \cdot 2^{15} \cdot 11^5$. ¿Cuántos factores de 10 contiene este número?

42. a. $6! = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 2 \cdot 3 \cdot 5 \cdot 2 \cdot 2 \cdot 3 \cdot 2 = 2^4 \cdot 3^2 \cdot 5$

44. *Demostración:* Suponga que n es un entero no-negativo cuya representación decimal termina en 0. Entonces $n = 10m + 0 = 10m$ para algún entero m. Al factorizar un 5 se obtiene $n = 10m = 5(2m)$ y $2m$ es un entero porque m es un entero. En consecuencia $10m$ es divisible por 5, que era lo que se quería demostrar.

47. *Sugerencia:* Puede tomar como un hecho que para cualquier entero positivo k,

$10^k = \underbrace{99\ldots9}_{k \text{ de estos}} + 1$; es decir,

$10^k = 9\cdot10^{k-1} + 9\cdot10^{k-2} + \cdots + 9\cdot10^1 + 9\cdot10^0 + 1.$

Sección 4.4

1. $q = 7, r = 7$ **3.** $q = 0, r = 36$

5. $q = -5, r = 10$ **7. a.** 4 **b.** 7

11. a. Cuando hoy es sábado, 15 días a partir de hoy son dos semanas (será sábado) más un día (que será domingo). Así que *DíaN* sería 0. De acuerdo a la fórmula, cuando hoy es sábado, *DíaT* = 6 y así cuando $N = 15$,

$$\begin{aligned} \textit{DíaN} &= (\textit{DíaT} + N) \textit{ mod } 7 \\ &= (6 + 15) \textit{ mod } 7 \\ &= 21 \textit{ mod } 7 = 0, \text{ que concuerda.} \end{aligned}$$

13. *Solución 1:* $30 = 4\cdot7 + 2$. Entonces la respuesta es dos días después del lunes, es decir, el miércoles.

Solución 2: Por la fórmula, la respuesta es $(1 + 30)$ *mod* $7 = 31$ *mod* $7 = 3$, que es miércoles.

14. *Sugerencia:* Existen dos maneras de resolver este problema. Una es encontrar que $1\,000 = 7\cdot142 + 6$ y observar que si hoy es martes, entonces 1 000 días a partir de hoy son 142 semanas más 6 días a partir de hoy. La otra manera es emplear la fórmula *DíaN* = (*DíaT* + *N*) *mod* 7, con *DíaT* = 2(martes) y $N = 1\,000$.

16. Como $d \mid n$, $n = dq + 0$ para algún entero q. Así el residuo es 0.

18. *Demostración:* Suponga que n es cualquier entero impar. Por definición de impar, $n = 2q + 1$ para algún entero q. Entonces $n^2 = (2q + 1)^2 = 4q^2 + 4q + 1 = 4(q^2 + q) + 1 = 4q(q + 1) + 1$. Por el resultado del ejercicio 17, el producto $q(q + 1)$ es par, por tanto $q(q + 1) = 2m$ para algún entero m. Entonces, sustituyendo, $n^2 = 4\cdot2m + 1 = 8m + 1$.

20. Como a *mod* $7 = 4$, el residuo que se obtiene cuando a se divide entre 7 es 4 y así $a = 7q + 4$ para algún entero q. Multiplicando esta ecuación por 5 se obtiene $5a = 35q + 20 = 35q + 14 + 6 = 7(5q + 2) + 6$. Como q es un entero, $5q + 2$ también es un entero, entonces $5a = 7\cdot$(un entero) $+ 6$. Así, como $0 \le 6 < 7$, el residuo que se obtiene al dividir $5a$ por 7 es 6. Por tanto $5a$ *mod* $7 = 6$.

23. *Demostración:* Suponga que n es cualquier entero *[particular pero arbitrariamente elegido]* tal que n *mod* $5 = 3$. Entonces el residuo que se obtiene al dividir n por 5 es 3, así $n = 5q + 3$ para algún entero q. Sustituyendo,

$$\begin{aligned} n^2 &= (5q + 3)^2 = 25q^2 + 30q + 9 \\ &= 25q^2 + 30q + 5 + 4 = 5(5q^2 + 6q + 1) + 4. \end{aligned}$$

Como los productos y sumas de enteros son enteros, entonces $5q^2 + 6q + 1$ es un entero, Por tanto $n^2 = 5\cdot$(un entero) $+ 4$.

Así, como $0 \le 4 < 5$, el residuo que se obtiene al dividir n^2 por 5 es 4, entonces n^2 *mod* $5 = 4$.

26. *Sugerencia:* Necesita demostrar 1): que para todos los enteros no-negativos n y enteros positivos d, si n es divisible por d entonces n *mod* $d = 0$; y 2): que para todos los enteros no-negativos n y enteros positivos d, si n *mod* $d = 0$ entonces n es divisible por d.

27. *Demostración:* Suponga que n es un entero arbitrario. Por el teorema del cociente-residuo con $d = 3$, existen enteros q y r tales que $n = 3q + r$ y $0 \le r < 3$. Pero los únicos enteros no-negativos r que son menores que 3 son 0, 1 y 2. Por tanto, $n = 3q + 0 = 3q$ o $n = 3q + 1$ o $n = 3q + 2$ para algún entero q.

28. a. *Demostración:* Suponga que n, $n + 1$ y $n + 2$ son cualesquiera tres enteros consecutivos. *[Debemos demostrar que $n(n + 1)$ es divisible entre 3.]* Por el teorema del cociente-residuo, n se puede escribir en una de las tres formas, $3q$, $3q + 1$ o $3q + 2$ para algún entero q. Lo separamos en tres casos.

***Caso 1* ($n = 3q$ para algún entero q)**: En este caso,

$$\begin{aligned} n(n + 1)(n + 2) & \\ &= 3q(3q + 1)(3q + 2) && \text{sustituyendo} \\ &= 3\cdot[q(3q + 1)(3q + 2)] && \text{por factorización de un 3.} \end{aligned}$$

Sea $m = q(3q + 1)(3q + 2)$. Entonces m es un entero porque q es un entero y sumas y productos de enteros son enteros. Sustituyendo,

$n(n + 1)(n + 2) = 3m$ donde m es un entero.

Y así, por definición de divisible, $n(n + 1)(n + 2)$ es divisible por 3.

***Caso 2* ($n = 3q + 1$ *para algún entero* q)**: En este caso,

$$\begin{aligned} n(n + 1)(n + 2) & \\ &= (3q + 1)((3q + 1) + 1)((3q + 1) + 2) && \text{sustituyendo} \\ &= (3q + 1)(3q + 2)(3q + 3) & \\ &= (3q + 1)(3q + 2)3(q + 1) & \\ &= 3\cdot[(3q + 1)(3q + 2)(q + 1)] && \text{por álgebra.} \end{aligned}$$

Sea $m = (3q + 1)(3q + 2)(q + 1)$. Entonces m es un entero porque q es un entero y sumas y productos de enteros son enteros. Sustituyendo,

$n(n + 1)(n + 2) = 3m$ donde m es un entero.

Y así, por definición de divisible, $n(n + 1)(n + 2)$ es divisible por 3.

***Caso 3* ($n = 3q + 2$ *para algún entero* q)**: En este caso,

$$\begin{aligned} n(n + 1)(n + 2) & \\ &= (3q + 2)((3q + 2) + 1)((3q + 2) + 2) && \text{sustituyendo} \\ &= (3q + 2)(3q + 3)(3q + 4) & \\ &= (3q + 2)3(q + 1)(3q + 4) & \\ &= 3\cdot[(3q + 2)(q + 1)(3q + 4)] && \text{por álgebra.} \end{aligned}$$

Sea $m = (3q + 2)(q + 1)(3q + 4)$. Entonces m es un entero porque q es un entero y sumas y productos de enteros son enteros. Sustituyendo,

$$n(n + 1)(n + 2) = 3m \text{ en donde } m \text{ es un entero.}$$

Y así, por definición de divisible, $n(n + 1)(n + 2)$ es divisible por 3.

En cada uno de los tres casos, $n(n + 1)(n + 2)$ resultó ser divisible por 3. Pero por el teorema del cociente-residuo, uno de esos casos debe ocurrir. Por tanto, el producto de cualesquiera tres enteros consecutivos es divisible por 3.

b. Para todos los enteros n, $n(n + 1)(n + 2)\ mod\ 3 = 0$.

29. a. *Sugerencia:* Dado cualquier entero n, empezamos utilizando el teorema del cociente-residuo para decir que n se puede escribir en una de las tres formas: $n = 3q$ o $n = 3q + 1$ o $n = 3q + 2$ para algún entero q. Entonces separamos en tres casos de acuerdo a esas tres posibilidades. Demostrar que en cada caso $n^2 = 3k$ para algún entero k o $n^2 = 3k + 1$ para algún entero k. Por ejemplo, cuando $n = 3q + 2$, entonces $n^2 = (3q + 2)^2 = 9q^2 + 12q + 4 = 3(3q^2 + 4q + 1) + 1$ y $3q^2 + 4q + 1$ es un entero porque es la suma de productos de enteros.

31. b. Si $m^2 - n^2 = 56$, entonces $56 = (m + n)(m - n)$. Ahora $56 = 2^3 \cdot 7$ y por el teorema de factorización única, esta factorización lo es. Así que las únicas representaciones de 56 como un producto de dos enteros positivos son $56 = 7 \cdot 8 = 14 \cdot 4 = 28 \cdot 2 = 56 \cdot 1$. Por el inciso *a*), m y n deben ser ambos impares o pares. Entonces las únicas soluciones son $m + n = 14$ y $m - n = 4$ o $m + n = 28$ y $m - n = 2$. Esto da $m = 9$ y $n = 5$ o $m = 15$ y $n = 13$ como las únicas soluciones.

32. Bajo las condiciones dadas, $2a - (b + c)$ es par.

Demostración: Supongamos que a, b y c son enteros arbitrarios tales que $a - b$ y $b - c$ son pares. *[Debemos demostrar que $2a - (b + c)$ es par.]* Primero observe que $(a - b) + (b - c)$ es la suma de dos enteros pares, así que es par por el ejemplo 4.2.3.#1. Pero $(a - b) + (b - c) = a - c$, Por tanto $a - c$ es par. En consecuencia $2a - (b + c)$ es par ya que es la suma de dos enteros pares *[que era lo que se quería demostrar]*.

34. *Sugerencia:* Exprese n utilizando el teorema del cociente-residuo con $d = 3$.

36. *Sugerencia:* Use el teorema del cociente-residuo (como en el ejemplo 3.4.5) para tener que $n = 4q$, $n = 4q + 1$, $n = 4q + 2$, o $n = 4q + 3$ y separe en estos casos.

38. *Sugerencia:* Dado cualquier entero n, considere los dos casos en donde n es par y en donde n es impar.

39. *Sugerencia:* Dado cualquier entero n, analice la suma $n + (n + 1) + (n + 2) + (n + 3)$.

42. *Sugerencia:* Use el teorema del cociente-residuo para expresar que n debe tener una de las formas $6q$, $6q + 1$, $6q + 2$, $6q + 3$, $6q + 4$, o $6q + 5$ para algún entero q.

44. *Sugerencia:* Hay tres casos: Ya sea x y y son ambos positivos o negativos, o uno es positivo y el otro es negativo.

47. a. $7\,609 + 5 = 7\,614$

49. *Respuesta a la primera pregunta:* No. *Contraejemplo:* Sea $m = 1$, $n = 3$ y $d = 2$. Entonces $m\ mod\ d = 1$ y $n\ mod\ d = 1$ pero $m \neq n$.

Respuesta a la segunda pregunta: Sí. *Demostración:* Suponga que m, n y d son enteros tales que $m\ mod\ d = n\ mod\ d$. Sea $r = m\ mod\ d = n\ mod\ d$. Por definición de *mod*, $m = dp + r$ y $n = dq + r$ para algunos enteros p y q. Entonces $m - n = (dp + r) - (dq + r) = d(p - q)$. Pero $p - q$ es un entero (es una diferencia de enteros) y así $m - n$ es divisible por d por definición de divisible.

Sección 4.5

1. $\lfloor 37.999 \rfloor = 37$, $\lceil 37.999 \rceil = 38$

3. $\lfloor -14.00001 \rfloor = -15$, $\lceil -14.00001 \rceil = -14$

8. $[n/7]$. La notación piso es más apropiada. Si se emplea la notación techo, entonces se necesitan dos fórmulas diferentes, dependiendo si $n/7$ es o no un entero. (¿Cuáles son dichas fórmulas?)

10. a. (i) $\left(2\,050 + \left\lfloor \frac{2049}{4} \right\rfloor - \left\lfloor \frac{2049}{100} \right\rfloor + \left\lfloor \frac{2049}{400} \right\rfloor\right) mod\ 7$

$= (2\,050 + 512 - 20 + 5)\ mod\ 7 = 2\,547\ mod\ 7$

$= 6$, que corresponde a sábado

b. *Sugerencia:* Cada cuatro años se agrega un día, excepto que a cada centuria no se agrega el día a menos que la centuria sea múltiplo de 400.

12. *Demostración:* Suponga que n es cualquier entero par. Por definición de par, $n = 2k$ para algún entero k. Entonces

$$\left\lfloor \frac{n}{2} \right\rfloor = \left\lfloor \frac{2k}{2} \right\rfloor = \lfloor k \rfloor = k \qquad \text{porque } k \text{ es un entero y } k \leq k < k - 1.$$

$$k = \frac{n}{2} \qquad \text{ya que } n = 2k.$$

Pero

Así, por un lado, $\left\lfloor \frac{n}{2} \right\rfloor = k$ y por el otro $k = \frac{n}{2}$. Entonces se tiene que $\left\lfloor \frac{n}{2} \right\rfloor = \frac{n}{2}$ *[que era lo que se quería demostrar]*.

14. Falso. *Contraejemplo:* Sea $x = 2$ y $y = 1.9$. Entonces $[x - y] = [2 - 1.9] = [0.1] = 0$, mientras que $[x] - [y] = [2] - [1.9] = 2 = 1$.

15. Verdadero. *Demostración:* Suponga que x es cualquier número real. Sea $m = [x]$. Por definición de piso, $m \leq x < m + 1$. Restando 1 de todas las partes de la desigualdad resulta que

$$m - 1 \leq x - 1 < m,$$

y así, por definición de piso, $[x - 1] = m - 1$. Entonces sustituyendo se tiene que $[x - 1] = [x] - 1$.

17. *Demostración para el caso donde $n\ mod\ 3 = 2$:*
En el caso donde $n\ mod\ 3 = 2$, entonces $n = 3q + 2$ para algún entero q por definición de *mod*. Sustituyendo,

$$\left\lfloor \frac{n}{3} \right\rfloor = \left\lfloor \frac{3q+2}{3} \right\rfloor$$
$$= \left\lfloor \frac{3q}{3} + \frac{2}{3} \right\rfloor$$
$$= \left\lfloor q + \frac{2}{3} \right\rfloor = q \quad \text{porque } q \text{ es un entero y } q \le q + 2/3 < q + 1.$$

Pero

$$q = \frac{n-2}{3} \quad \text{al resolver } n = 3q + 2 \text{ para } q.$$

Así, por un lado, $\left\lfloor \frac{n}{3} \right\rfloor = q$ y por el otro $q = \frac{n-2}{3}$ Se tiene que $\left\lfloor \frac{n}{3} \right\rfloor = \frac{n-2}{3}$.

18. *Sugerencia:* Esto es falso.

19. *Sugerencia:* Esto es verdadero.

23. *Demostración:* Suponga que x es un número real que no es entero. Sea $[x] = n$. Entonces, por definición de piso y porque n no es un entero, $n < x < n + 1$. Multiplicando ambos lados por -1 se obtiene $-n > -x > -n - 1$ o equivalentemente, $-n - 1 < -x < -n$. Como $-n - 1$ es un entero, se tiene por definición de piso que $[-x] = -n - 1$. Así que:

$$\lfloor x \rfloor + \lfloor -x \rfloor = n + (-n - 1) = n - n - 1 = -1,$$

que era lo que se quería demostrar.

25. *Sugerencia:* Sea $n = \left\lfloor \frac{x}{2} \right\rfloor$ y considere los dos casos: n par e impar.

26. *Demostración:* Suponga que x es cualquier número real tal que $x - \lfloor x \rfloor < \frac{1}{2}$. Multiplicando ambos lados por 2 se obtiene

$$2x - 2\lfloor x \rfloor < 1 \quad \text{o} \quad 2x < 2\lfloor x \rfloor + 1.$$

Ahora por definición de piso, $\lfloor x \rfloor \le x$. Así que, $2\lfloor x \rfloor \le 2x$. Con las dos desigualdades que implican a $2x$ se obtiene:

$$2\lfloor x \rfloor \le 2x < 2\lfloor x \rfloor + 1.$$

Entonces, por definición de piso (y porque $2\lfloor x \rfloor$ es un entero), $2\lfloor x \rfloor = 2\lfloor x \rfloor$. Que era lo que se quería demostrar.

30. Esta prueba incorrecta exhibe razonamiento circular. La igualdad $\left\lfloor \frac{n}{2} \right\rfloor = \frac{(n-1)}{2}$ es lo que se debe demostrar. Sustituyendo $2k + 1$ para n en ambos lados de la igualdad y trabajando a partir del resultado como si fuera verdadero, la prueba asume la verdad de la conclusión que se intenta demostrar.

Sección 4.6

1. **a.** Una contradicción.
b. Un número real positivo.
c. x
d. Ambos lados por 2
e. Contradicción.

3. *Demostración:* Suponga que no. Es decir, suponga que existe un entero n tal que $3n + 2$ es divisible por 3. *[Debemos obtener una contradicción.]* Por definición de divisibilidad, $3n + 2 = 3k$ para algún entero k. Restando $3n$ de ambos lados resulta que $2 = 3k - 3n = 3(k - n)$. Así, por definición de divisibilidad, $3 \mid 2$. Pero por el teorema 4.3.1 esto implica que $3 \le 2$, lo que contradice el hecho de que $3 > 2$. *[Así para todos los enteros n, $3n + 2$ no es divisible por 3.]*

5. *Negación del enunciado:* Existe un entero par que es el más grande. *Demostración del enunciado:* Suponga que no. Es decir, suponga que existe un entero par que es el más grande; llamado N. Entonces N es un entero par y $N \ge n$ para cada entero par n. *[Debemos deducir una contradicción.]* Sea $M = N + 2$. Entonces M es un entero par porque es la suma de enteros pares y $M > N$ porque $M = N + 2$. Esto contradice la suposición de que $N \ge n$ para cada entero par n. [*Así que la suposición es falsa y el enunciado es verdadero.]*

8. **a.** un número racional.
b. un número irracional.
c. $\frac{a}{b}$
d. $\frac{c}{d}$
e. $\frac{a}{b} - \frac{c}{d}$
f. enteros
g. enteros
h. propiedad del producto cero
i. racional

9. **a.** El error en esta prueba se presenta en la segunda frase en donde la negación escrita por el estudiante es incorrecta: En lugar de ser existencial, debe ser universal. El problema es que si el estudiante procede en una manera lógicamente correcta, todo lo que se necesita para lograr una contradicción es un ejemplo de un número racional y uno irracional cuya suma sea irracional. Sin embargo, para demostrar el enunciado dado, es necesario demostrar que no existe algún número racional y ni algún número irracional cuya suma sea racional.

10. *Demostración por contradicción:* Supongamos que no. Es decir, supongamos que existe un número irracional x tal que la raíz cuadrada de x es racional. *[Debemos obtener una contradicción.]* Por definición de racional, $\sqrt{x} = \frac{a}{b}$ para algunos enteros a y b con $b \ne 0$. Sustituyendo,

$$(\sqrt{x})^2 = \left(\frac{a}{b}\right)^2,$$

y así, por álgebra,

$$x = \frac{a^2}{b^2}.$$

Pero a^2 y b^2 ambos son productos de enteros y por tanto son enteros y b^2 distinto de cero por la propiedad del producto cero. Entonces $\frac{a^2}{b^2}$ es racional. Se tiene que x es irracional y racional, lo que es una contradicción. *[Que era lo que se quería demostrar.]*

11. *Demostración:* Supongamos que no. Es decir, suponga que existe un número racional x distinto de cero y un número irracional y tal que xy es racional. *[Debemos lograr una contradicción.]* Por definición de racional, $x = a/b$ y $xy = c/d$ para algunos enteros a, b, c y d con b y d diferentes de cero. También $a \ne 0$ ya que x es distinto de cero. Sustituyendo, $xy = (a/b)y = c/d$. Resolviendo para y se obtiene $y = bc/ad$. Ahora bc y ad son enteros (son productos de enteros) y $ad \ne 0$ (por la propiedad del producto cero).

Así, por definición de racional y es racional, lo que contradice la suposición de que y es irracional. *[Entonces la suposición es falsa y el enunciado es verdadero.]*

13. *Sugerencia:* Suponga que $n^2 - 2$ es divisible por 4 y considere los dos casos en donde n es par e impar. (Una solución alternativa emplea la proposición 4.6.4.)

14. *Sugerencia:* $a^2 = c^2 - b^2 = (c - b)(c + b)$

15. *Sugerencia:* 1) Para cualquier entero c, si 2 divide a c, entonces 4 divide a c^2. 2) El resultado del ejercicio 13 puede ser útil.

16. *Sugerencia:* Suponga que a, b y c son enteros impares, que z es una solución de $ax^2 + bx + c = 0$, con z racional. Entonces $z = p/q$ para algunos enteros p y q con éste distinto de cero. Podemos suponer que p y q no tienen un factor común. (¿Por qué? Si p y q tienen un factor común, podemos dividir para eliminar su más grande factor común para así obtener dos enteros p' y q' que 1) no tienen factor común y 2) satisfacen la ecuación $z = p'/q'$. Entonces podemos redefinir $q = q'$ y $p = p'$). Observe que como p y q no tienen factor común, entonces ambos no son pares. Sustituya p/q en $ax^2 + bx + c = 0$ y multiplique todo por q^2. Demuestre que 1) la suposición de que p es par conduce a una contradicción, 2) la suposición de que q es par implica una contradicción y 3) la suposición de que ambos p y q son impares conduce a una contradicción. La única posibilidad restante es que tanto p como q sean pares, ya ha sido descartado.

18. **a.** $5 \mid n$ **b.** $5 \mid n^2$ **c.** $5k$ **d.** $(5k)^2$ **e.** $5 \mid n^2$

19. *Demostración (por contraposición): [Para efectuar la contraposición, debemos demostrar que* $\forall$ *números reales positivos, r y s, si* $r \leq 10$ *y* $s \leq 10$*, entonces* $rs \leq 100$*.]* Supongamos que r y s son números reales positivos y $r \leq 10$ y $s \leq 10$. Por el álgebra de desigualdades, $rs \leq 100$. *[Para deducir este hecho, multiplique ambos lados de* $r \leq 10$ *por s para obtener que* $rs \leq 10s$*. Y multiplique ambos lados de* $s \leq 10$ *por* 10 *para deducir que* $10s \leq 10 \cdot 10 = 100$*. Por transitividad de* $\leq$*, entonces,* $rs \leq 100$*.]* Y que era lo que se quería demostrar.

21. **a.** *Demostración por contradicción:* Suponga que no. Es decir, acepte que existe un entero n tal que n^2 es impar y n es par. Demuestre que esta suposición conduce lógicamente a una contradicción.

b. *Demostración por contraposición:* Suponga que n es cualquier entero tal que n no es impar. Pruebe que n^2 no es impar.

23. **a.** Lo contrapositivo es el enunciado "$\forall$ números reales x, si $-x$ no es irracional, entonces x no es irracional". Equivalentemente (ya que $-(-x) = x$), "$\forall$ números reales x, si x es racional, entonces $-x$ es racional".
Demostración por contraposición: Supongamos que x es cualquier número racional. *[Debemos demostrar que* $-x$ *también es racional.]* Por definición de racional, $x = a/b$ para algunos enteros a y b, con $b \neq 0$. Entonces $x = -(a/b) = (-a)/b$. Como $-a$ y b son enteros y $b \neq 0$, $-x$ es racional *[que era lo que se quería demostrar]*.

b. *Demostración por contraposición:* Suponga que no. *[Tomamos la negación y suponemos que es verdadera.]* Es decir, suponemos que existe un número irracional x tal que $-x$ es racional. *[Debemos obtener una contradicción.]* Por definición de racional, $-x = a/b$ para algunos enteros a y b con $b \neq 0$. Multiplicando ambos lados por -1 se obtiene $x = -(a/b) = -a/b$. Pero $-a$ y b son enteros (ya que a y b lo son) y $b \neq 0$. Así x es la razón de dos enteros $-a$ y b con $b \neq 0$. Entonces x es racional (por definición de racional), que es una contradicción. *[Esta contradicción muestra que la suposición es falsa y así el enunciado dado es verdadero.]*

25. *Sugerencias:* Vea la respuesta al ejercicio 21 y revise cuidadosamente en las dos pruebas para la proposición 4.6.4.

26. **a.** *Demostración por contraposición:* Supongamos que a, b y c son cualesquiera enteros *[particulares pero arbitrariamente elegidos]* tales que $a \mid b$. *[Debemos demostrar que* $a \mid bc$*.]* Por definición de división, $b = ak$ para algún entero k. Entonces $bc = (ak)c = a(kc)$. Pero kc es un entero (porque es el producto de los enteros k y c). Así que $a \mid bc$ por definición de divisibilidad *[que era lo que se quería demostrar]*.

b. *Demostración por contradicción:* Suponemos que no. *[Tomamos la negación y la suponemos válida.]* Suponga que existen enteros a, b y c tales que a no divide a bc y $a \mid b$. Como $a \mid b$, existe un entero k tal que $b = ak$ por definición de división. Entonces $bc = (ak)c = a(kc)$ *[por la ley asociativa del álgebra]*. Pero kc es un entero (ya que es un producto de enteros) y así $a \mid bc$ por definición de división. Así a no divide a bc y $a \mid bc$, que es una contradicción. *[Esta contradicción muestra que la suposición es falsa, entonces el enunciado dado es verdadero.]*

27. **a.** *Sugerencia:* El contrapositivo es "Para todos los enteros m y n, si m y n no son ambos pares o impares, entonces $m + n$ no es par". Equivalentemente: "Para todos los enteros m y n, si m o n es par y el otro es impar, entonces $m + n$ es impar".

b. *Sugerencia:* La negación del enunciado dado es el siguiente: Existen enteros m y n tales que $m + n$ es par y m es par y n impar o conversa, m es impar y n es par.

30. La negación de "Cada entero es racional" es "Existe al menos un entero que es irracional" y no "Cada entero es irracional". Deducir una contradicción a partir de una negación incorrecta del enunciado no prueba que éste sea verdadero.

31. **a.** *Demostración:* Supongamos que r, s y n son enteros y $r > \sqrt{n}$ y $s > \sqrt{n}$. Observe que r y s son ambos positivos porque $\sqrt{n}$ no es negativo. Multiplicando ambos lados de la primera desigualdad por s y ambos lados de la segunda desigualdad por $\sqrt{n}$ (apéndice A, T20), tenemos que $rs > \sqrt{n}s$ y $\sqrt{n}s > \sqrt{n}\sqrt{n} = n$. Así, por la ley transitiva de la desigualdad (apéndice A, T18), $rs > n$.

32. **a.** $\sqrt{667} \cong 25.8$ y así los posibles factores primos que deben checarse son 2, 3, 5, 7, 11, 13, 17, 19 y 23. Probando cada uno a la vez se obtiene que 667 no es primo porque $667 = 23 \cdot 29$.

b. $\sqrt{557} \cong 23.6$ y entonces los posibles factores primos que deben verificarse son 2, 3, 5, 7, 1, 13, 17, 19 y 23. Probando con cada uno resulta que ninguno divide a 557. Por tanto, 557 es primo.

34. a. $\sqrt{9\,269} \cong 96.3$ y así los posible factores primos para ser checados son todos aquellos encontrados en el ejercicio 33. Probando cada uno de resulta que 9 269 no es primo ya que $9\,269 = 13 \cdot 713$.

b. $\sqrt{9\,103} \cong 95.4$, entonces los posibles factores primos para ser verificados son aquellos que se encontraron en el ejercicio 33. Checando cada uno de ellos se obtiene que ninguno divide a 9 103. Por tanto, 9 103 es primo.

35. *Sugerencia:* ¿Es posible que sean primos los tres números $n - 4$, $n - 6$ y $n - 8$?

Sección 4.7

1. El valor de $\sqrt{2}$ dado por una calculadora es una aproximación. Las calculadoras pueden dar valores exactos sólo para números que se pueden representar empleando al máximo la cantidad de dígitos decimales en su pantalla. En particular, cada número en la pantalla es racional, pero aún muchos números racionales no pueden ser representados exactamente. Por ejemplo, considere el número formado al escribir el punto decimal y después el primer millón de dígitos de $\sqrt{2}$. Por el análisis de la sección 4.2, este número es racional, pero no podría inferir esto de la pantalla de la calculadora.

3. *Demostración por contradicción:* Suponga que no. Es decir, suponga que $6 - 7\sqrt{2}$ es racional. *[Debemos demostrar una contradicción.]* Por definición de racional, existen enteros a y $b \neq 0$ con

$$6 - 7\sqrt{2} = \frac{a}{b}.$$

$$\text{Entonces } \sqrt{2} = \frac{1}{-7}\left(\frac{a}{b} - 6\right) \quad \text{restando 6 de ambos lados y dividiendo ambos miembros entre } -7,$$

$$\text{y así } \sqrt{2} = \frac{a - 6b}{-7b} \quad \text{por las reglas del álgebra.}$$

Pero $a - 6b$ y $-7b$ son enteros (ya que a y b son enteros y los productos y diferencias de enteros son enteros y $-7b \neq 0$ por la propiedad del producto cero. Así que $\sqrt{2}$ es una razón de los dos enteros $a - 6b$ y $-7b$ con $-7b \neq 0$, entonces $\sqrt{2}$ es un número racional (por definición de racional). Esto contradice el hecho de que $\sqrt{2}$ es irracional, por tanto la suposición es falsa y $6 - 7\sqrt{2}$ es irracional.

4. Esto es falso. $\sqrt{4} = 2 = 2/1$, que es racional.

7. *Contraejemplo:* Sean $x = \sqrt{2}$ y $y = -\sqrt{2}$. Entonces x y y son irracionales, pero $x + y = 0 = 0/1$, que es racional.

9. Verdadero.

Versión formal del enunciado: ∀ números reales positivos r, si r es irracional, entonces $\sqrt{r}$ es irracional.

Demostración por contraposición: Supongamos que r es cualquier número real positivo tal que $\sqrt{r}$ es racional. *[Debemos demostrar que r es racional.]* Por definición de racional, $\sqrt{r} = \frac{a}{b}$ para algunos enteros a y b con $b \neq 0$. Entonces $r = \left(\sqrt{r}\right)^2 = \left(\frac{a}{b}\right)^2 = \frac{a^2}{b^2}$.

Pero a^2 y b^2 son enteros porque son productos de enteros y $b^2 \neq 0$ por la propiedad del producto cero. Así r es racional *[que era lo que se quería demostrar]*.

(El enunciado también puede demostrarse por contradicción.)

13. *Sugerencia:* ¿Puede pensar acerca de enteros "agradables" x y y que sean más grandes que 1 y tengan la propiedad $x^2 = y^2$?

16. a. *Demostración por contradicción:* Suponga que no. Es decir, suponga que existe un entero n tal que $n = 3q_1 + r_1 = 3q_2 + r_2$, en donde q_1, q_2, r_1 y r_2 son enteros, $0 \leq r_1 < 3$, $0 \leq r_2 < 3$ y $r_1 \neq r_2$. Intercambiando los subíndices en r_1 y r_2, si es necesario, podemos suponer que $r_2 > r_1$. Entonces $3(q_1 - q_2) = r_2 - r_1 > 0$ y como r_1 y r_2 son menores que 3, por tanto $r_2 - r_1 = 1$ o $r_2 - r_1 = 2$. Así $3(q_1 - q_2) = 1$ o $3(q_1 - q_2) = 2$. El primer caso implica que $3 \mid 1$ y así que, por el teorema 4.3.1, que $3 \leq 1$ y el segundo caso implica que $3 \mid 2$, entonces, por el teorema 4.3.1, que $3 \leq 2$. Esos resultados contradicen el hecho de que 3 es mayor que 1 y 2. Por tanto, en cualquier caso hemos llegado a una contradicción, que demuestra que la suposición es falsa y el enunciado dado es verdadero.

b. *Demostración por contradicción:* Suponga que no. Es decir, suponga que existe un entero n tal que n^2 es divisible entre 3 y n no es divisible entre 3. *[Debemos deducir una contradicción.]* Por definición de divisible, $n^2 = 3q$ para algún entero q y por el teorema del cociente-residuo y la parte (a), $n = 3k + 1$ o $n = 3k + 2$ para algún entero k.

Caso 1 ($n = 3k + 1$ para algún entero k): En este caso

$$n^2 = (3k + 1)^2 = 9k^2 + 6k + 1 = 3(3k^2 + 2k) + 1.$$

Sea $s = 3k^2 + 2k$. Entonces $n^2 = 3s + 1$ y s es un entero ya que es una suma de productos de enteros. Se tiene que $n^2 = 3q = 3s + 1$ para algunos enteros q y s, que contradice el resultado del inciso *a*).

Caso 2 ($n = 3k + 2$ para algún entero k): En este caso

$$n^2 = (3k + 2)^2 = 9k^2 + 12k + 4 = 3(3k^2 + 6k + 1) + 1.$$

Sea $t = 3k^2 + 6k + 1$. Entonces $n^2 = 3t + 1$ y t es un entero porque es una suma de productos de enteros. Se tiene que $n^2 = 3q = 3t + 1$ para algunos enteros q y t, que contradice el resultado del inciso *a*).

Por tanto, en ambos casos, se llega a una contradicción, que muestra que la suposición es falsa y el enunciado dado es verdadero.

c. *Demostración por contradicción:* Suponga que no. Es decir, suponga que $\sqrt{3}$ es racional. Por definición de racional, $\sqrt{3} = \frac{a}{b}$ para algunos enteros a y b con $b \neq 0$. Sin pérdida de generalidad, acepte que a y b no tienen un factor en común. (Si no, entonces divida a y b entre su más grande factor común para obtener enteros a' y b' con la propiedad de que a' y b' no tienen un factor común y $\sqrt{3} = \frac{a'}{b'}$. Entonces redefina $a = a'$ y $b = b'$). Elevando al cuadrado ambos lados de $\sqrt{3} = \frac{a}{b}$ se obtiene $3 = \frac{a^2}{b^2}$ y multiplicando ambos lados por b^2 se obtiene

$$3b^2 = a^2 (*).$$

Así a^2 es divisible por 3 y entonces, por el inciso *b*), a también es divisible por 3. Por definición de divisibilidad, se tiene que $a = 3k$ para algún entero k y así

$$a^2 = 9k^2 (**).$$

Sustituyendo la ecuación (**) en la ecuación (*) se obtiene $3b^2 = 9k^2$ y dividiendo ambos lados por 3 se tiene que $b^2 = 3k^2$.

$$b^2 = 3k^2.$$

Así que b^2 es divisible por 3 y entonces por el inciso *b*), b también es divisible por 3. Consecuentemente, tanto a como b son divisibles por 3, lo que contradice la suposición de que a y b no tienen un factor en común. Por tanto, la suposición es falsa y entonces $\sqrt{3}$ es irracional.

18. *Sugerencia:* La prueba es una generalización de la expuesta en la solución del ejercicio 16*a*).

19. *Sugerencia:* 1) Los incisos de la prueba son similares a los del ejercicio 16*b*) y 16*c*). 2) Use el resultado del ejercicio 18.

20. *Sugerencia:* Este enunciado es verdadero. Si $a^2 - 3 = 9b$, entonces $a^2 = 9b + 3 = 3(3b + 1)$ y así a^2 es divisible por 3. Entonces, por el ejercicio 16*b*), a es divisible por 3. En consecuencia $a^2 = (3c)^2$ para algún entero c.

21. *Demostración por contradicción:* Suponga que no. Es decir, supóngase que $\sqrt{2}$ es racional. *[Demostraremos que esta suposición conduce a una contradicción.]* Por definición de racional, podemos escribir para algunos enteros a y b con $b \neq 0$. Entonces $2 = a^2/b^2$ y así $a^2 = 2b^2$. Considere las factorizaciones primas de a^2 y $2b^2$. Por el teorema de factorización única de los enteros, esas factorizaciones son únicas excepto por el orden en que se escriben los factores. Ahora, como cada factor primo de a se presenta dos veces en la factorización prima de a^2, en la factorización prima de a^2 el número 2 aparece un número par de veces. (Si 2 es un factor de a, entonces este número par de veces es positivo y si 2 no es un factor de a, entonces este número par es 0.) Por otro lado, como cada factor primo de b ocurre doble en la factorización prima de b^2, el número 2 aparece un número impar de veces en la factorización prima de $2b^2$. Por tanto, la ecuación $a^2 = 2b^2$ no puede ser verdadera. Entonces la suposición es falsa y así $\sqrt{2}$ es irracional.

23. *Sugerencia:* Por el resultado del ejercicio 22, $\sqrt{6}$ es irracional.

25. *Sugerencia:* $\dfrac{2\cdot3\cdot5\cdot7+1}{2} = 3\cdot5\cdot7 + \dfrac{1}{2}$ y

$\dfrac{2\cdot3\cdot5\cdot7+1}{3} = 2\cdot5\cdot7 + \dfrac{1}{3}$.

26. *Sugerencia:* Puede deducir que $p = 3$.

27. **a.** *Sugerencia:* Por ejemplo, $N_4 = 2\cdot3\cdot5\cdot7 + 1 = 211$.

29. *Sugerencia:* Por el teorema 4.3.4 (divisibilidad por un primo) existe un número primo p tal que $p \mid (n! - 1)$. Demuestre que la suposición $p \leq n$ conduce a una contradicción. Entonces se tiene que $n < p < n!$.

30. *Sugerencia:* Cada entero impar se puede escribir como $4k + 1$ o como $4k + 3$ para algún entero k. (¿Por qué?) Si $p_1p_2 \ldots p_n + 1 = 4k + 1$, entonces $4 \mid p_1 p_2 \ldots p_n$. ¿Esto es posible?

31. **a.** *Sugerencia:* Pruebe el contrapositivo: Si para algún entero $n > 2$ que no es potencia de 2, $x^n + y^n = z^n$ tiene solución en los enteros positivos, entonces para algún número primo $p > 2$, $x^p + y^p = z^p$ tiene solución en los enteros positivos. Observe que si $n = kp$, entonces $x^n = x^{kp} = (x^k)^p$.

32. *Demostración de existencia:* Cuando $n = 2$, entonces $n^2 - 1 = 3$, que es primo. Así que existe un número primo de la forma $n^2 - 1$, en donde n es un entero y $n \geq 2$.

Demostración de unicidad (por contradicción): Suponga lo que es contrario, que m es otro entero satisfaciendo las condiciones dadas. Es decir, $m > 2$ y $m^2 - 1$ es primo. *[Debemos deducir una contradicción.]* Factorice $m^2 - 1$ para obtener $m^2 - 1 = (m - 1)(m + 1)$. Pero $m > 2$ y así $m - 1 > 1$ y $m + 1 > 1$. Así que $m^2 - 1$ no es primo, que es una contradicción. *[Esta contradicción demuestra que la suposición es falsa y entonces no existe otro entero $m > 2$ tal que $n^2 - 1$ sea primo.]*

Demostración de unicidad (directa): Supongamos que m es cualquier entero tal que $m \geq 2$ y $m^2 - 1$ es primo. *[Debemos demostrar que $m = 2$.]* Factorizando, $m^2 - 1 = (m - 1)(m + 1)$. Como $m^2 - 1$ es primo, entonces $m - 1 = 1$ o $m + 1 = 1$. Pero $m + 1 \geq 2 + 1 = 3$. Por tanto, por eliminación, $m - 1 = 1$, así $m = 2$.

34. *Demostración (por contradicción):* Suponga que no. Es decir, suponga que existen dos números reales distintos a_1 y a_2 tales que para todos los números reales r,

$$1)\ a_1 + r = r \quad \text{y} \quad 2)\ a_2 + r = r$$

Entonces

$$a_1 + a_2 = a_2 \ \text{ por (1) con } \ r = a_2$$

y

$$a_2 + a_1 = a_1 \ \text{ por (2) con } \ r = a_1.$$

Se tiene que

$$a_2 = a_1 + a_2 = a_2 + a_1 = a_1$$

que implica que $a_2 = a_1$. Pero esto contradice la suposición de que a_1 y a_2 son distintas. *[Así la suposición es falsa y a lo más existe un número real a tal que $a + r = r$ para todos los números r.]*

Demostración (directa): Suponga que a_1 y a_2 son números reales tales que para todos los números reales r,

$$1)\ a_1 + r = r \quad \text{y} \quad 2)\ a_2 + r = r$$

Entonces

$$a_1 + a_2 = a_2 \ \text{ por (1) con } \ r = a_2$$

y

$$a_2 + a_1 = a_1 \ \text{ por (2) con } \ r = a_1.$$

Se tiene que

$$a_2 = a_1 + a_2 = a_2 + a_1 = a_1.$$

Así $a_2 = a_1$. *[Entonces, a lo más existe un número real a tal que $a + r = r$ para todos los números reales r.]*

Sección 4.8

1. $z = 0$ **3. a.** $z = 18$ **4.** $a = \frac{17}{12}$

6.

	Número de iteración			
	0	1	2	3
a	26			
d	7			
q	0	1	2	3
r	26	19	12	5

8. a.

A	69	19	9	
q	2			
d		1		
n			1	
p				4

9. mcd(27, 72) = 9 **10.** mcd(5, 9) = 1

13. Divida el número más grande, 1 188, por el más pequeño, 385, para obtener un cociente de 3 y un residuo de 33. A continuación divida 385 entre 33 para obtener un cociente de 11 y un residuo de 22. Después divida 33 por 22 para lograr un cociente de 1 y un residuo de 11. Finalmente, divida 22 por 11 para obtener un cociente de 2 y un residuo de 0. Así, por el lema 4.8.2, mcd(1 188, 385) = mcd(385, 33) = mcd(33, 22) = mcd(22, 11) = mcd(11, 0) y por el lema 4.8.1, mcd(11, 0) = 11. Entonces mcd(1 188, 385) = 11.

14. Divida el número más grande, 1 177, entre el más pequeño, 509, para obtener un cociente de 2 y un residuo de 159. En seguida divida 509 por 159 para lograr un cociente de 3 y un residuo de 32. Después divida 159 por 32 para deducir un cociente de 4 y un residuo de 31. Entonces divida 32 por 31 para deducir un cociente de 1 y un residuo de 1. Finalmente, divida 31 por 1 para lograr un cociente de 31 y un residuo de cero. Así, por el lema 4.8.2, mcd(1 177, 509) = mcd(509, 159) = mcd(159, 32) = mcd(32, 31) = mcd(31, 1) = mcd(1, 0) y por el lema 4.8.1, mcd(1, 0) = 1. Así mcd(1 177, 509) = 1.

17.

A	1 001					
B	871					
r		130	91	39	13	0
b	871	130	91	39	13	0
a	1 001	871	130	91	39	13
mcd						13

19. *Sugerencia:* Divida la demostración en dos partes. En la parte 1 suponga que a y b son cualesquiera enteros positivos tales que $a \mid b$ y deduzca la conclusión de que mcd$(a, b) = a$. Para hacer esto, observe que $a \mid a$, entonces a es un divisor común de a y b. Así, por definición de máximo común divisor, a es menor que o igual que el máximo común divisor de a y b. En símbolos, $a \leq$ mcd(a, b). Después muestre que $a \geq$ mcd(a, b) utilizando el teorema 4.3.1. En la parte 2 de la prueba, suponga que a y b son cualesquiera enteros positivos tales que mcd$(a, b) = a$ y deduzca que $a \mid b$.

22. a. *Sugerencia 1:* Si $a = dq - r$, entonces $-a = -dq + r = -dq - d + d - r = d(-q - 1) + (d - r)$.

Sugerencia 2: Si $0 \leq r < d$, entonces $0 \geq -r > -d$. Sume d a todas las partes de esta desigualdad y vea qué resulta.

23. a. *Demostración:* Suponga que a, d, q y r son enteros tales que $a = dq + r$ y $0 \leq r < d$. *[Debemos demostrar que* $q = \left\lfloor \frac{a}{d} \right\rfloor$ y $r = a - d\left\lfloor \frac{a}{d} \right\rfloor$.*]* Resolviendo $a = dq + r$ para r resulta que $r = a - dq$ y sustituyendo en $0 \leq r < d$ se obtiene $0 \leq a - dq < d$. Sumando dq en ambos lados se obtiene $dq \leq a < d + dq = d(q + 1)$. Entonces dividiendo por d para deducir $q \leq \frac{a}{d} < q + 1$. Por tanto, por definición de piso, $\left\lfloor \frac{a}{d} \right\rfloor = q$. Finalmente, el sustituir en $a = dq + r$ implica $a = d\left\lfloor \frac{a}{d} \right\rfloor + r$, y al restar $d\left\lfloor \frac{a}{d} \right\rfloor$ en ambos lados resulta que $r = a - d\left\lfloor \frac{a}{d} \right\rfloor$ *[que era lo que se quería demostrar].*

24. b.

	Número de iteración				
	0	1	2	3	4
a	630	294	294	252	210
b	336	336	42	42	42
mcd					

	Número de iteración				
	5	6	7	8	9
a	168	126	84	42	0
b	42	42	42	42	42
mcd					42

25. a. mcm (12, 18) = 36

26. *Demostración: Parte 1:* Sean a y b enteros positivos y suponga que $d =$ mcd$(a, b) =$ mcm(a, b). Por definición de máximo común divisor y de mínimo común múltiplo, $d > 0$, $d \mid a$, $d \mid b$, $a \mid d$ y $b \mid d$. Así, en particular, $a = dm$ y $d = an$ para algunos enteros m y n. Sustituyendo, $a = dm = (an)m = anm$. Dividiendo ambos lados por a resulta que $1 = nm$. Pero los únicos divisores de 1 son 1 y -1 (teorema 4.3.2) y así $m = n = \pm 1$. Como a y d son positivos, entonces $m = n = 1$ y así $a = d$. Un razonamiento similar demuestra también que $b = d$ y en consecuencia $a = b$.

Parte 2: Dados cualesquiera dos enteros positivos a y b tales que $a = b$, tenemos que mcd$(a, b) =$ mcd$(a, a) = a$ y mcm$(a, b) =$ mcm$(a, a) = a$ y por tanto mcd$(a, b) =$ mcm(a, b).

29. *Sugerencia:* Divida la demostración en dos partes. En la parte 1, suponga que a y b son cualesquiera dos enteros positivos y deduzca que:

$$\text{mcd}(a, b) \cdot \text{mcm}(a, b) \leq ab.$$

Obtenga este resultado probando que mcm $(a, b) \leq \frac{ab}{\text{mcm}(a,b)}$.

Para hacer esto, demuestre que $\frac{ab}{\text{mcm}(a, b)}$, es un múltiplo de

a y b. Por ejemplo, para ver que $\frac{ab}{\text{mcd}(a,b)}$ es un múltiplo de b, observe que puesto que $\text{mcd}(a, b)$ divide a, entonces $a = \text{mcd}(a, b)\cdot k$ para algún entero k y así $ab = \text{mcd}(a, b)\cdot kb$. Divida ambos lados entre $\text{mcd}(a, b)$ para obtener que $\frac{ab}{\text{mcd}(a,b)} = kb$. Pero como k es un entero, esta ecuación implica que $\frac{ab}{\text{mcd}(a,b)}$ es un múltiplo de b. El argumento de que $\frac{ab}{\text{mcd}(a,b)}$ es un múltiplo de a es casi idéntico. En la parte 2 de la prueba, use la definición de mínimo común múltiplo para demostrar que $\frac{ab}{\text{mcm}(a,b)} \mid a$ y $\frac{ab}{\text{mcm}(a,b)} \mid b$. Concluya que $\frac{ab}{\text{mcm}(a,b)} \le \text{mcd}(a, b)$ y en consecuencia $ab \le \text{mcd}(a, b)\cdot\text{mcm}(a, b)$.

Sección 5.1

1. $\frac{1}{11}, \frac{2}{12}, \frac{3}{13}, \frac{4}{14}$ **3.** $1, -\frac{1}{3}, \frac{1}{9}, -\frac{1}{27}$ **5.** 0, 0, 2, 2

8. $g_1 = \lfloor\log_2 1\rfloor = 0$
$g_2 = \lfloor\log_2 2\rfloor = 1, \quad g_3 = \lfloor\log_2 3\rfloor = 1$
$g_4 = \lfloor\log_2 4\rfloor = 2, \quad g_5 = \lfloor\log_2 5\rfloor = 2$
$g_6 = \lfloor\log_2 6\rfloor = 2, \quad g_7 = \lfloor\log_2 7\rfloor = 2$
$g_8 = \lfloor\log_2 8\rfloor = 3, \quad g_9 = \lfloor\log_2 9\rfloor = 3$
$g_{10} = \lfloor\log_2 10\rfloor = 3, \quad g_{11} = \lfloor\log_2 11\rfloor = 3$
$g_{12} = \lfloor\log_2 12\rfloor = 3, \quad g_{13} = \lfloor\log_2 13\rfloor = 3$
$g_{14} = \lfloor\log_2 14\rfloor = 3, \quad g_{15} = \lfloor\log_2 15\rfloor = 3$

Cuando n es una potencia entera de 2, g_n es el exponente de esa potencia. Por ejemplo, $8 = 2^3$ y $g_8 = 3$. Más generalmente, si $n = 2^k$, donde k es un entero, entonces $g_n = k$. Todos los términos de la sucesión desde g_n hasta g_m, en donde $m = 2^{k+1}$ es la siguiente potencia entera de 2, tienen el mismo valor como g_n, a saber, k. Por ejemplo, todos los términos de la sucesión desde g_8 hasta g_{15} tienen el valor 3.

Los ejercicios del 10 al 16 tienen más de una respuesta correcta.

10. $a_n = (-1)^n$, en donde n es un entero y $n \ge 1$.

11. $a_n = (n-1)(-1)^n$, tal que n es un entero y $n \ge 1$.

12. $a_n = \dfrac{n}{(n+1)^2}$, en donde n es un entero y $n \ge 1$.

14. $a_n = \dfrac{n^2}{3^n}$, tal que n es un entero y $n \ge 1$.

18. **a.** $2 + 3 + (-2) + 1 + 0 + (-1) + (-2) = 1$
b. $a_0 = 2$
c. $a_2 + a_4 + a_6 = -2 + 0 + (-2) = -4$
d. $2\cdot 3\cdot(-2)\cdot 1\cdot 0\cdot(-1)\cdot(-2) = 0$

19. $2 + 3 + 4 + 5 + 6 = 20$ **20.** $2^2\cdot 3^2\cdot 4^2 = 576$

23. $1(1 + 1) = 2$

27. $\left(\frac{1}{1} - \frac{1}{2}\right) + \left(\frac{1}{2} - \frac{1}{3}\right) + \left(\frac{1}{3} - \frac{1}{4}\right) + \left(\frac{1}{4} - \frac{1}{5}\right)$
$+ \left(\frac{1}{5} - \frac{1}{6}\right) + \left(\frac{1}{6} - \frac{1}{7}\right) + \left(\frac{1}{7} - \frac{1}{8}\right) + \left(\frac{1}{8} - \frac{1}{9}\right)$
$+ \left(\frac{1}{9} - \frac{1}{10}\right) + \left(\frac{1}{10} - \frac{1}{11}\right) = 1 - \frac{1}{11} = \frac{10}{11}$

29. $(-2)^1 + (-2)^2 + (-2)^3 + \cdots + (-2)^n$
$= -2 + 2^2 - 2^3 + \cdots + (-1)^n 2^n$

31. $\sum_{k=0}^{n+1} \frac{1}{k!} = \frac{1}{0!} + \frac{1}{1!} + \frac{1}{2!} + \cdots + \frac{1}{(n+1)!}$

33. $\frac{1}{1!} = 1$

35. $\left(\frac{1}{1+1}\right)\left(\frac{2}{2+1}\right)\left(\frac{3}{3+1}\right) = \left(\frac{1}{2}\right)\left(\frac{2}{3}\right)\left(\frac{3}{4}\right) = \frac{1}{4}$

37. $\sum_{k=1}^{k+1} i(i!) = \sum_{k=1}^{k} i(i!) + (k+1)(k+1)!$

40. $\sum_{k=1}^{k} i^3 + (k+1)^3 = \sum_{k=1}^{k+1} i^3$

Los ejercicios del 43 al 52 tienen más de una respuesta correcta.

43. $\sum_{k=1}^{7}(-1)^{k+1}k^2$ o $\sum_{k=0}^{6}(-1)^k(k+1)^2$

46. $\sum_{j=2}^{6} \frac{(-1)^j j}{(j+1)(j+2)}$ o $\sum_{k=3}^{7} \frac{(-1)^{k+1}(k-1)}{k(k+1)}$

47. $\sum_{i=0}^{5}(-1)^i r^i$ **49.** $\sum_{k=1}^{n} k^3$

51. $\sum_{i=0}^{n-1}(n-i)$

53. Cuando $k = 0$, entonces $i = 1$. Cuando $k = 5$, entonces $i = 6$. Como $i = k + 1$, entonces $k = i - 1$. Así,

$$k(k-1) = (i-1)(i-1-1) = (i-1)(i-2),$$

y entonces

$$\sum_{k=0}^{5} k(k-1) = \sum_{i=1}^{6}(i-1)(i-2)$$

55. Cuando $i = 1$, entonces $j = 0$. Cuando $i = n + 1$, entonces $j = n$. Como $j = i - 1$, entonces $i = j + 1$. Así,

$$\frac{(i-1)^2}{i\cdot n} = \frac{((j+1)-1)^2}{(j+1)\cdot n} = \frac{j^2}{jn+n}.$$

(Observe que n es constante en cuanto a la suma se refiere).

Así $\text{So}\sum_{i=1}^{n+1} \frac{(i-1)^2}{i\cdot n} = \sum_{j=0}^{n} \frac{j^2}{jn+n}$.

56. Cuando $i = 3$, entonces $j = 2$. Cuando $i = n$ entonces $j = n - 1$. Como $j = i - 1$, entonces $i = j + 1$. Así,

$$\sum_{i=3}^{n} \frac{i}{i+n-1} = \sum_{j=2}^{n-1} \frac{j+1}{(j+1)+n-1}$$
$$= \sum_{j=2}^{n-1} \frac{j+1}{j+n}.$$

59. $\sum_{k=1}^{n}[3(2k-3) + (4-5k)]$
$= \sum_{k=1}^{n}[(6k-9) + (4-5k)] = \sum_{k=1}^{n}(k-5)$

62. $\dfrac{4\cdot 3\cdot \cancel{2\cdot 1}}{3\cdot \cancel{2\cdot 1}} = 4$

65. $\dfrac{n(n-1)\cancel{(n-2)\cdots 3\cdot 2\cdot 1}}{\cancel{(n-1)(n-2)\cdots 3\cdot 2\cdot 1}} = n$

66. $\dfrac{\cancel{(n-1)(n-2)\cdots 3\cdot 2\cdot 1}}{(n+1)n\cancel{(n-1)(n-2)\cdots 3\cdot 2\cdot 1}} = \dfrac{1}{n(n+1)}$

68. $\dfrac{[(n+1)n(n-1)(n-2)\cdots 3\cdot 2\cdot 1]^2}{[n(n-1)(n-2)\cdots 3\cdot 2\cdot 1]^2} = (n+1)^2$

69.
$$\frac{n(n-1)(n-2)\cdots(n-k+1)\cancel{(n-k)(n-k-1)\cdots 2\cdot 1}}{\cancel{(n-k)(n-k-1)\cdots 2\cdot 1}} = n(n-1)(n-2)\cdots(n-k+1)$$

71. $\binom{5}{3} = \dfrac{5!}{(3!)(5-3)!} = \dfrac{5\cdot 4\cdot \cancel{3\cdot 2\cdot 1}}{\cancel{(3\cdot 2\cdot 1)}(2\cdot 1)} = 10$

73. $\binom{3}{0} = \dfrac{3!}{(0!)(3-0)!} = \dfrac{\cancel{3!}}{(1)\cancel{(3!)}} = 1$

75. $\binom{n}{n-1} = \dfrac{n!}{(n-1)!(n-(n-1))!} = \dfrac{n\cancel{(n-1)!}}{\cancel{(n-1)!}(n-n+1)!} = \dfrac{n}{1} = n$

77. a. *Demostración:* Sea n un entero tal que $n \geq 2$. Por definición de factorial,

$$n! = \begin{cases} 2\cdot 1 & \text{si } n = 2 \\ 3\cdot 2\cdot 1 & \text{si } n = 3 \\ n\cdot(n-1)\cdots 2\cdot 1 & \text{si } n > 3. \end{cases}$$

En cada caso, $n!$ tiene un factor de 2 y así $n! = 2k$ para algún entero k. Entonces

$$\begin{aligned} n! + 2 &= 2k + 2 && \text{sustituyendo} \\ &= 2(k+1) && \text{factorizando el 2.} \end{aligned}$$

Como $k + 1$ es un entero, entonces $n! + 2$ es divisible por 2 *[que era lo que se quería demostrar]*.

c. *Sugerencia:* Considere la secuencia $m! + 2$, $m! + 3$, $m! + 4$, …, $m! + m$.

78. *Demostración:* Suponga que n y r son enteros no-negativos con $r + 1 \leq n$. El lado derecho de la ecuación a demostrarse es

$$\begin{aligned} \frac{n-r}{r+1}\cdot\binom{n}{r} &= \frac{n-r}{r+1}\cdot\frac{n!}{r!(n-r)!} \\ &= \frac{n-r}{r+1}\cdot\frac{n!}{r!(n-r)\cdot(n-r-1)!} \\ &= \frac{n!}{(r+1)!\cdot(n-r-1)!} \\ &= \frac{n!}{(r+1)!\cdot(n-(r+1))!} \\ &= \binom{n}{r+1}, \end{aligned}$$

que es el lado izquierdo de la ecuación a demostrar.

80. a. $m - 1$, suma $+ a[i+1]$

81.

2 | 90	0	residuo $= r[6] = 1$
2 | 45	1	residuo $= r[5] = 0$
2 | 22	1	residuo $= r[4] = 1$
2 | 11	2	residuo $= r[3] = 1$
2 | 5	5	residuo $= r[2] = 0$
2 | 2	10	residuo $= r[1] = 1$
2 | 1	20	residuo $= r[0] = 0$
	0	

Así que $90_{10} = 1011010_2$.

84.

a	23					
i	0	1	2	3	4	5
q	23	11	5	2	1	0
$r[0]$		1				
$r[1]$			1			
$r[2]$				1		
$r[3]$					0	
$r[4]$						1

88.

16 | 287	0	residuo 1 $= r[2] = 1_{16}$
16 | 17	1	residuo 1 $= r[1] = 1_{16}$
16 | 1	1	residuo 15 $= r[0] = \mathrm{F}_{16}$
	0	

Así que $287_{10} = 11\mathrm{F}_{16}$.

Sección 5.2

1. *Demostración:* Sea $P(n)$ la propiedad "n centavos se pueden obtener empleando monedas de 3 y de 8 centavos".

Demostración que P(14) es verdadero:

Catorce centavos se pueden obtener utilizando dos monedas de 3 centavos y una moneda de 8 centavos.

Demostración que para todos los enteros k ≥ 14, si P(k) es verdadera, entonces P(k + 1) también es verdadera:

Supóngase que pueden obtenerse k centavos (en donde $k \geq 14$) usando monedas de 3 y 8 centavos. *[Hipótesis inductiva.]* Debemos demostrar que se pueden obtener $k + 1$ centavos empleando monedas de 3 y 8 centavos. Si los k centavos incluyen una moneda de 8 centavos, reemplácela por tres monedas de 3 centavos para obtener un total de $k + 1$ centavos. De otra manera los k centavos consisten exclusivamente de monedas de 3 centavos y así al menos deben tenerse cinco monedas de 3 centavos (porque la suma total al menos es de 14 centavos). En este caso, sustituya cinco de las monedas de 3 centavos por dos monedas de 8 centavos para obtener un total de $k + 1$ centavos. Así, en cualquier caso, $k + 1$ centavos pueden obtenerse mediante monedas de 3 y 8 centavos. *[Que es lo que se quería demostrar.]*

[Como hemos demostrado el paso básico y el paso inductivo, concluimos que el enunciado dado es verdadero para todos los enteros $n \geq 4$.]

3. a. $P(1)$ es "$1^2 = \frac{1\cdot(1+1)\cdot(2\cdot1+1)}{6}$." $P(1)$ es verdadero ya que $1^2 = 1$ y $\frac{1\cdot(1+1)\cdot(2+1)}{6} = \frac{2\cdot3}{6} = 1$ también.

b. $P(k)$ es "$1^2 + 2^2 + \cdots + k^2 = \frac{k(k+1)(2k+1)}{6}$."

c. $P(k+1)$ es "$1^2 + 2^2 + \cdots + (k+1)^2 = \frac{(k+1)((k+1)+1)(2\cdot(k+1)+1)}{6}$."

d. *Debe demostrarse que:* Si para algún entero $k \geq 1$,

$$1^2 + 2^2 + \cdots + k^2 = \frac{k(k+1)(2k+1)}{6}, \text{ entonces}$$
$$1^2 + 2^2 + \cdots + (k+1)^2 = \frac{(k+1)[(k+1)+1][(2(k+1)+1)]}{6}.$$

5. a. 1^2 **b.** k^2
c. $1 + 3 + 5 + \cdots + [2(k+1) - 1]$
d. $(k+1)^2$

a. el entero impar justo antes de $2k+1$ es $2k-1$.

f. hipótesis inductiva.

6. *Demostración:* Para el enunciado dado, la propiedad $P(n)$ es la ecuación

$$2 + 4 + 6 + \cdots + 2n = n^2 + n. \quad \leftarrow P(n)$$

Demostración de que P(1) es verdadera:

Para demostrar $P(1)$, debemos demostrar que cuando se sustituye 1 en la ecuación en el lugar de n, el lado izquierdo es igual al lado derecho. Pero cuando 1 es sustituido para n, el lado izquierdo es la suma de todos los enteros pares de 2 a $2\cdot1$, que es justamente 2 y el lado derecho es $1^2 + 1$, que también es igual a 2. Así $P(1)$ es verdadera.

Demostración que para todos los enteros $k \geq 1$, si P(k) es verdadera entonces $P(k+1)$ también es verdadera:

Aceptemos que k es cualquier entero con $k \geq 1$ y supongamos que $P(k)$ es verdadera. Es decir, suponemos que

$$2 + 4 + 6 + \cdots + 2k = k^2 + k. \quad \leftarrow P(k) \text{ hipótesis inductiva}$$

Debemos demostrar que $P(k+1)$ es verdadera. Es decir, debemos demostrar que

$$2 + 4 + 6 + \cdots + 2(k+1) = (k+1)^2 + (k+1).$$

Porque $(k+1)^2 + (k+1) = k^2 + 2k + 1 + k + 1 = k^2 + 3k + 2$, esto es equivalente a demostrar que

$$2 + 4 + 6 + \cdots + 2(k+1) = k^2 + 3k + 2. \quad \leftarrow P(k+1)$$

Pero el lado izquierdo de $P(k+1)$ es

$$\begin{aligned} &2 + 4 + 6 + \cdots + 2(k+1) \\ &= 2 + 4 + 6 + \cdots + 2k + 2(k+1) && \text{haciendo explícito el penúltimo término} \\ &= (k^2 + k) + 2(k+1) && \text{sustituyendo la hipótesis inductiva} \\ &= k^2 + 3k + 2, && \text{por álgebra,} \end{aligned}$$

y este es el lado derecho de $P(k+1)$. Entonces $P(k+1)$ es verdadera.

[Como el paso básico y el paso inductivo han sido demostrados, $P(n)$ es verdadero para todos los enteros $n \geq 1$.]

8. *Demostración:* Para el enunciado dado, la propiedad $P(n)$ es la ecuación

$$1 + 2 + 2^2 + \cdots + 2^n = 2^{n+1} - 1. \quad \leftarrow P(n)$$

Demostración de que P(0) es verdadera:

El lado izquierdo de $P(0)$ es 1 y el lado derecho es $2^{0+1} - 1 = 2 - 1 = 1$. Así $P(0)$ es verdadero.

Demostración de que para todos los enteros $k \geq 0$, si P(k) es verdadera entonces $P(k+1)$ es verdadera:

Aceptemos que k sea cualquier entero con $k \geq 0$ y supongamos que $P(k)$ es verdadera. Es decir, suponemos que:

$$1 + 2 + 2^2 + \cdots + 2^k = 2^{k+1} - 1. \quad \leftarrow P(k) \text{ hipótesis inductiva}$$

Debemos demostrar que $P(k+1)$ es verdadera. Es decir, debemos demostrar que

$$1 + 2 + 2^2 + \cdots + 2^{k+1} = 2^{(k+1)+1} - 1,$$

o equivalentemente

$$1 + 2 + 2^2 + \cdots + 2^{k+1} = 2^{k+2} - 1. \quad \leftarrow P(k+1)$$

Pero el lado izquierdo de $P(k+1)$ es

$$\begin{aligned} &1 + 2 + 2^2 + \cdots + 2^{k+1} \\ &= 1 + 2 + 2^2 + \cdots + 2^k + 2^{k+1} && \text{haciendo explícito el penúltimo término} \\ &= (2^{k+1} - 1) + 2^{k+1} && \text{sustituyendo la hipótesis inductiva} \\ &= 2\cdot2^{k+1} - 1 && \text{combinando términos semejantes} \\ &= 2^{k+2} - 1, && \text{por las leyes de los exponentes,} \end{aligned}$$

y esto es el lado derecho de $P(k+1)$. Así que la propiedad es verdadera para $n = k+1$.

[Como el paso básico y el paso inductivo se han demostrado, entonces $P(n)$ es verdadero para todos los enteros $n \geq 0$.]

10. *Demostración:* Para el enunciado dado, la propiedad es la ecuación

$$1^2 + 2^2 + 3^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}. \quad \leftarrow P(n)$$

Demostración de que P(1) es verdadera:

El lado izquierdo de $P(1)$ es $1^2 = 1$ y el lado derecho es $\frac{1(1+1)(2\cdot1+1)}{6} = \frac{2\cdot3}{6} = 1$. Así $P(1)$ es verdadera.

Demostración de que para todos los enteros $k \geq 1$, si P(k) es verdadera entonces $P(k+1)$ es verdadera:

Sea k un entero arbitrario con $k \geq 1$ y supongamos que $P(k)$ es verdadera. Es decir, suponemos

$$1^2 + 2^2 + 3^2 + \cdots + k^2 = \frac{k(k+1)(2k+1)}{6}. \quad \leftarrow P(k)$$

hipótesis de inducción

Debemos demostrar que $P(k+1)$ es verdadera. Es decir, debemos demostrar que

$$1^2 + 2^2 + 3^2 + \cdots + (k+1)^2 = \frac{(k+1)((k+1)+1)(2(k+1)+1)}{6},$$

o, equivalentemente

$$1^2 + 2^2 + 3^2 + \cdots + (k+1)^2 = \frac{(k+1)(k+1)(2k+3)}{6}. \quad \leftarrow P(k+1)$$

Pero el lado izquierdo de $P(k+1)$ es

$$\begin{aligned}
&1^2 + 2^2 + 3^2 + \cdots + (k+1)^2 \\
&= 1^2 + 2^2 + 3^2 + \cdots + k^2 + (k+1)^2 && \text{haciendo explícito el penúltimo término sustituyendo la hipótesis de inducción} \\
&= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \\
&= \frac{k(k+1)(2k+1)}{6} + \frac{6(k+1)^2}{6} && \text{ya que } \frac{6}{6} = 1 \\
&= \frac{k(k+1)(2k+1) + 6(k+1)^2}{6} && \text{por suma de fracciones} \\
&= \frac{(k+1)[k(2k+1) + 6(k+1)]}{6} && \text{factorizando } (k+1) \\
&= \frac{(k+1)(2k^2 + 7k + 6)}{6} && \text{multiplicando y agrupando términos semejantes} \\
&= \frac{(k+1)(k+2)(2k+3)}{6} && \text{porque } (k+2)(2k+3) = 2k^2 + 7k + 6,
\end{aligned}$$

y esto es el lado derecho de $P(k+1)$. Entonces la propiedad es verdadera para $n = k+1$.

[Como los pasos básico e inductivo han sido demostrados, entonces P(n) es verdadero para todos los enteros $n \geq 1$.]

13. *Demostración:* Para el enunciado dado, la propiedad $P(n)$ es la ecuación

$$\sum_{i=1}^{n-1} i(i+1) = \frac{n(n-1)(n+1)}{3}. \quad \leftarrow P(n)$$

Demostración de que P(2) es verdadero:

El lado izquierdo de $P(2)$ es $\sum_{i=1}^{1} i(i+1) = 1 \cdot (1+1) = 2$ y también el lado derecho es $\frac{2(2-1)(2+1)}{3} = \frac{6}{3} = 2$. Así $P(2)$ es verdadero.

Demostración de que para todos los enteros $k \geq 2$, si P(k) es verdadero entonces P(k + 1) también es verdadero:

Sea k un entero arbitrario con $k \geq 2$ y suponga que $P(k)$ es verdadera. Es decir, acepte que

$$\sum_{i=1}^{k-1} i(i+1) = \frac{k(k-1)(k+1)}{3} \quad \leftarrow P(k)$$

hipótesis de inducción

Debemos demostrar que $P(k+1)$ es verdadera. Es decir, debemos demostrar que

$$\sum_{i=1}^{(k+1)-1} i(i+1) = \frac{(k+1)((k+1)-1)((k+1)+1)}{3},$$

o, equivalentemente,

$$\sum_{i=1}^{k} i(i+1) = \frac{(k+1)k(k+2)}{3}. \quad \leftarrow P(k+1)$$

Pero el lado izquierdo de $P(k+1)$ es

$$\begin{aligned}
&\sum_{i+1}^{k} i(i+1) \\
&= \sum_{i=1}^{k-1} i(i+1) + k(k+1) && \text{escribiendo por separado el último término} \\
&= \frac{k(k-1)(k+1)}{3} + k(k+1) && \text{sustituyendo la hipótesis de inducción} \\
&= \frac{k(k-1)(k+1)}{3} + \frac{3k(k+1)}{3} && \text{ya que } \frac{3}{3} = 1 \\
&= \frac{k(k-1)(k+1) + 3k(k+1)}{3} && \text{por suma de fracciones} \\
&= \frac{k(k+1)[(k-1)+3]}{3} && \text{factorizando } k(k+1) \\
&= \frac{k(k+1)(k+2)}{3}, && \text{por álgebra,}
\end{aligned}$$

y esto es el lado derecho de $P(k+1)$. Entonces $P(k+1)$ es verdadero.

[Como los pasos básico e inductivo han sido demostrados, entonces P(n) es verdadero para todos los enteros $n \geq 0$.]

15. *Sugerencia:* Para demostrar el paso básico, demuestre que $\sum_{i=1}^{1} i(i!) = (1+1)! - 1$. Para demostrar el paso inductivo, suponga que $\sum_{i=1}^{k} i(i!) = (k+1)! - 1$ para algún entero $k \geq 1$ y demuestre que $\sum_{i=1}^{k+1} i(i!) = (k+2)! - 1$. Observe que $[(k+1)! - 1] + (k+1)[(k+1)!] = (k+1)![1 + (k+1)] - 1$.

18. *Sugerencias:* $\operatorname{sen}^2 x + \cos^2 x = 1$, $\cos(2x) = \cos^2 x - \operatorname{sen}^2 x = 1 - 2\operatorname{sen}^2 x$, $\operatorname{sen}(a+b) = \operatorname{sen} a \cos b + \cos a \operatorname{sen} b$, $\operatorname{sen}(2x) = 2 \operatorname{sen} x \cos x$, $\cos(a+b) = \cos a \cos b - \operatorname{sen} a \operatorname{sen} b$.

20. $4 + 8 + 12 + 16 + \cdots + 200 = 4(1 + 2 + 3 + \cdots + 50) = 4\left(\frac{50 \cdot 51}{2}\right) = 5\,100$

22. $3 + 4 + 5 + 6 + \cdots + 1\,000 = (1 + 2 + 3 + 4 + \cdots + 1\,000) - (1 + 2) = \left(\frac{1\,000 \cdot 1\,001}{2}\right) - 3 = 500\,497$

24. $\frac{(k-1)((k-1)+1)}{2} = \frac{k(k-1)}{2}$

25. **a.** $\dfrac{2^{26}-1}{2-1} = 2^{26} - 1 = 67\,108\,863$

b. $2 + 2^2 + 2^3 + \cdots + 2^{26}$
$= 2(1 + 2 + 2^2 + \cdots + 2^{25})$
$= 2 \cdot (67\,108\,863)$ por el inciso (a)
$= 134\,217\,726$

28. $\dfrac{\left(\frac{1}{2}\right)^{n+1} - 1}{\frac{1}{2} - 1} = \dfrac{\frac{1}{2^{n+1}} - 1}{-\frac{1}{2}} = \left(\dfrac{1}{2^{n+1}} - 1\right)(-2)$

$$= -\frac{2}{2^{n+1}} + 2 = 2 - \frac{1}{2^n}$$

30. *Sugerencia:* $c + (c + d) + (c + 2d) + \cdots + (c + nd)$
$= (n + 1)\, c + d \cdot \frac{n(n+1)}{2}$.

33. En el paso inductivo, tanto la hipótesis de inducción como lo que se quiere demostrar están equivocados. La hipótesis de inducción debería de ser:

Supongamos que para algún entero $k \geq 1$,

$$1^2 + 2^2 + \cdots + k^2 = \frac{k(k+1)(2k+1)}{6}.$$

y el resultado a demostrar sería

$$1^2 + 2^2 + \cdots + (k+1)^2 = \frac{(k+1)((k+1)+1)(2(k+1)+1)}{6}.$$

34. *Sugerencia:* Vea la nota de precaución del ejemplo 5.1.8.

35. *Sugerencia:* Vea la subsección "Demostración de una igualdad" en la página 254.

37. *Sugerencia:* Forme la suma $n^2 + (n+1)^2 + (n+2)^2 + \cdots + (n + (p-1))^2$ y demuestre que es igual a

$$pn^2 + 2n(1 + 2 + 3 + \cdots + (p-1)) + (1 + 4 + 9 + 16 + \cdots + (p-1)^2).$$

Sección 5.3

1. *Fórmula general:* $\prod_{i=2}^{n}\left(1 - \frac{1}{i}\right) = \frac{1}{n}$ para todos los enteros $n \geq 2$. *Demostración (por inducción matemática):* Aceptemos que la propiedad $P(n)$ sea la ecuación

$$\prod_{i=2}^{n}\left(1 - \frac{1}{i}\right) = \frac{1}{n}. \qquad \leftarrow P(n)$$

Demostración de que P(2) es verdadera:

El lado izquierdo de $P(2)$ es $\prod_{i=2}^{2}\left(1 - \frac{1}{i}\right) = 1 - \frac{1}{2} = \frac{1}{2}$, que es igual al lado derecho.

Demostración de que para todos los enteros $k \geq 2$, si $P(k)$ es verdadero entonces $P(k+1)$ también es verdadero.

Suponga que k es cualquier entero con $k \geq 2$ tal que

$$\prod_{i=2}^{k}\left(1 - \frac{1}{i}\right) = \frac{1}{k}. \quad \leftarrow P(k)$$
hipótesis de inducción

Debemos demostrar que

$$\prod_{i=2}^{k+1}\left(1 - \frac{1}{i}\right) = \frac{1}{k+1}. \quad \leftarrow P(k+1)$$

Pero por las leyes del álgebra y sustituyendo la hipótesis de inducción, el lado izquierdo de $P(k+1)$ es

$$\prod_{i=2}^{k+1}\left(1 - \frac{1}{i}\right) = \prod_{i=2}^{k}\left(1 - \frac{1}{i}\right)\left(1 - \frac{1}{k+1}\right) = \left(\frac{1}{k}\right)\left(1 - \frac{1}{k+1}\right) = \left(\frac{1}{k}\right)\left(\frac{(k+1)-1}{k+1}\right)$$
$$= \frac{1}{k+1} \text{ que es el lado derecho de } P(k+1)$$

[que era lo que se quería demostrar].

3. *Fórmula general:* $\frac{1}{1\cdot 3} + \frac{1}{3\cdot 5} + \cdots + \frac{1}{(2n-1)(2n+1)} = \frac{n}{2n+1}$ para todos los enteros $n \geq 1$.

Demostración (por inducción matemática): Aceptemos que la propiedad $P(n)$ sea la ecuación

$$\frac{1}{1\cdot 3} + \frac{1}{3\cdot 5} + \cdots + \frac{1}{(2n-1)(2n+1)} = \frac{n}{2n+1}.$$

Demostración de que P(1) es verdadero:

El lado izquierdo de $P(1)$ es igual a $\frac{1}{1\cdot 3}$, y el lado derecho es igual a $\frac{1}{2\cdot 1+1}$. Pero ambos valen $\frac{1}{3}$, entonces $P(1)$ es verdadero.

Demostración que para cualquier entero $k \geq 1$, si $P(k)$ es verdadera entonces $P(k+1)$ es verdadera:

Suponga que k es cualquier entero con $k \geq 1$ y

$$\frac{1}{1\cdot 3} + \frac{1}{3\cdot 5} + \cdots + \frac{1}{(2k-1)(2k+1)} = \frac{k}{2k+1}$$
$\uparrow P(k)$ hipótesis de inducción

Debemos demostrar que

$$\frac{1}{1\cdot 3} + \frac{1}{3\cdot 5} + \cdots + \frac{1}{(2(k+1)-1)(2(k+1)+1)} = \frac{k+1}{2(k+1)+1}.$$

o equivalentemente

$$\frac{1}{1\cdot 3} + \frac{1}{3\cdot 5} + \cdots + \frac{1}{(2k+1)(2k+3)} = \frac{k+1}{2k+3}.$$
$\uparrow P(k+1)$

Pero el lado izquierdo de $P(k+1)$ es:

$$\begin{aligned}
&\frac{1}{1\cdot 3}+\frac{1}{3\cdot 5}+\cdots+\frac{1}{(2k+1)(2k+3)}\\
&\quad=\frac{1}{1\cdot 3}+\frac{1}{3\cdot 5}+\cdots+\frac{1}{(2k-1)(2k+1)}\\
&\qquad\qquad+\frac{1}{(2k+1)(2k+3)}\\
&\quad=\frac{k}{2k+1}+\frac{1}{(2k+1)(2k+3)} \qquad \text{por hipótesis de inducción}\\
&\quad=\frac{k(2k+3)}{(2k+1)(2k+3)}+\frac{1}{(2k+1)(2k+3)}\\
&\quad=\frac{2k^2+3k+1}{(2k+1)(2k+3)}\\
&\quad=\frac{(2k+1)(k+1)}{(2k+1)(2k+3)}\\
&\quad=\frac{k+1}{2k+3} \qquad \text{por álgebra,}
\end{aligned}$$

y esto es el lado derecho de $P(k+1)$ *[que era lo que se quería demostrar]*.

4. *Sugerencia 1:* La fórmula general es

$$\begin{aligned}
&1-4+9-16+\cdots+(-1)^{n-1}n^2\\
&\quad=(-1)^{n-1}(1+2+3+\cdots+n) \qquad \text{en forma desarrollada}
\end{aligned}$$

$$O:\ \sum_{i=1}^{n}(-1)^{i-1}i^2=(-1)^{n-1}\left(\sum_{i=1}^{n}i\right) \qquad \text{en notación de suma}$$

Sugerencia 2: En la demostración, use el hecho de que

$$1+2+3+\cdots+n=\sum_{i=1}^{n}i=\frac{n(n+1)}{2}.$$

6. a. $P(0)$ es "5^0-1 es divisible por 4". $P(0)$ es verdadera porque $5^0-1=0$, que es divisible por 4.

b. $P(k)$ es "5^k-1 es divisible por 4".

c. $P(k+1)$ es "$5^{k+1}-1$ es divisible por 4".

d. *Se debe demostrar:* Si para algún entero $k\geq 0$, 5^k-1 es divisible entre 4, entonces $5^{k+1}-1$ es divisible por 4.

8. *Demostración (por inducción matemática):* Para el enunciado dado, la propiedad es la frase "5^n-1 es divisible por 4".

Demostración de que P(0) es verdadero:

$P(0)$ es la frase "5^0-1 es divisible por 4". Pero $5^0-1=1-1=0$ y 0 es divisible por 4 porque $0=4\cdot 0$. Entonces $P(0)$ es verdadero.

Demostración de que para todos los enteros $k\geq 0$, si $P(k)$ es verdadero entonces $P(k+1)$ también es verdadero:

Sea k cualquier entero con $k\geq 0$ y suponga que $P(k)$ es verdadera. Es decir, supóngase que 5^k-1 es divisible por 4. *[Esta es la hipótesis de inducción.]* Debemos demostrar que $P(k+1)$ es verdadera. Es decir, debemos demostrar que $5^{k+1}-1$ es divisible por 4. Ahora

$$\begin{aligned}
5^{k+1}-1&=5^k\cdot 5-1\\
&=5^k\cdot(4+1)-1=5^k\cdot 4+(5^k-1). \qquad (*)
\end{aligned}$$

Por la hipótesis de inducción 5^k-1 es divisible entre 4 y entonces $5^k-1=4r$ para algún entero r. Sustituyendo en la ecuación (*),

$$5^{k+1}-1=5^k\cdot 4+4r=4(5^k+r).$$

Pero 5^k+r es un entero porque k y r son enteros. Así que, por definición de divisibilidad, $5^{k+1}-1$ es divisible por 4 *[que era lo que se quería demostrar]*.

Una demostración alternativa del paso inductivo va como sigue: Suponga que para algún entero $k\geq 0$, 5^k-1 es divisible por 4. Entonces $5^k-1=4r$ para algún entero r y así $5^k=4r+1$.

Se tiene que $5^{k+1}=5^k\cdot 5=(4r+1)\cdot 5=20r+5$. Restando 1 en ambos lados se obtiene $5^{k+1}-1=20r+4=4(5r+1)$. Pero $5r+1$ es un entero y así, por definición de divisibilidad, $5^{k+1}-1$ es divisible por 4.

11. *Demostración (por inducción matemática):* Para el enunciado dado, la propiedad $P(n)$ es la frase "$3^{2n}-1$ es divisible por 8".

Demostración de que P(0) es verdadero:

$P(0)$ es la frase "$3^{2\cdot 0}-1$ es divisible por 8". Pero $3^{2\cdot 0}-1=1-1=0$ y 0 es divisible por 8 porque $0=8\cdot 0$. Así $P(0)$ es verdadera.

Demostración de que para todos los enteros $k\geq 0$, si $P(k)$ es verdadero entonces $P(k+1)$ también es verdadero:

Sea k cualquier entero con $k\geq 0$ y supóngase que $P(k)$ es verdadero. Es decir, que $3^{2k}-1$ es divisible por 8. *[Esta es la hipótesis de inducción.]* Debemos demostrar que $P(k+1)$ es verdadero. Es decir, debemos demostrar que $3^{2(k+1)}-1$ es divisible por 8, o equivalentemente, $3^{2k+2}-1$ es divisible por 8. Ahora

$$\begin{aligned}
3^{2k+2}-1&=3^{2k}\cdot 3^2-1=3^{2k}\cdot 9-1\\
&=3^{2k}\cdot(8+1)-1=3^{2k}\cdot 8+(3^{2k}-1)\cdot \qquad (*)
\end{aligned}$$

Por la hipótesis inductiva $3^{2k}-1$ es divisible por 8 y entonces $3^{2k}-1=8r$ para algún entero r. Sustituyendo en la ecuación (*),

$$3^{2k+2}-1=3^{2k}\cdot 8+8r=8(3^{2k}+r).$$

Pero $3^{2k}+r$ es un entero porque k y r son enteros. Por tanto, por definición de divisibilidad, $3^{2k+2}-1$ es divisible por 8 *[que era lo que se quería demostrar]:*

13. *Sugerencia:* $\begin{aligned}x^{k+1}-y^{k+1}&=x^{k+1}-x\cdot y^k+x\cdot y^k-y^{k+1}\\&=x\cdot(x^k-y^k)+y^k\cdot(x-y)\end{aligned}$

14. *Sugerencia 1:* $\begin{aligned}(k+1)^3-(k+1)&=k^3+3k^2+3k+1-k-1\\&=(k^3-k)+3k^2+3k\\&=(k^3-k)+3k(k+1)\end{aligned}$

Sugerencia 2: $k(k+1)$ es el producto de dos enteros consecutivos. Por el teorema 4.4.3, uno debe ser par.

16. *Demostración (por inducción matemática):* Para el enunciado dado, permitamos que la propiedad $P(n)$ sea la desigualdad ¡$2^n < (n + 1)!$

Demostración de que P(2) es verdadera:

$P(2)$ dice que ¡$2^2 < (2 + 1)!$ El lado izquierdo es $2^2 = 4$ y el lado derecho es $3! = 6$. Así, como $4 < 6$, entonces $P(2)$ es verdadera.

Demostración de que para todos los enteros $k \geq 2$, si P(k) es verdadero entonces P(k + 1) también es verdadero:

Sea k cualquier entero con $k \geq 2$ y supongamos que $P(k)$ es verdadero. Es decir, supóngase que $2^k < (k + 1)!$ *[Esta es la hipótesis de inducción.]* Debemos demostrar que $P(k + 1)$ es verdadero. Es decir, debemos demostrar que $2^{k+1} < ((k + 1) + 1)!$, o, equivalentemente, $2^{k+1} < (k + 2)!$ Por las leyes de los exponentes y la hipótesis de inducción

$$2^{k+1} = 2 \cdot 2^k < 2(k + 1)! \qquad (*)$$

Como $k \geq 2$, entonces $2 < k + 2$ y así

$$2(k + 1)! < (k + 2)(k + 1)! = (k + 2)! \qquad (**)$$

La combinación de (*) y (**) da

$$2^{k+1} < (k + 2)!$$

[que era lo que se quería demostrar].

19. *Demostración (por inducción matemática):* Para el enunciado dado, aceptemos que la propiedad $P(n)$ sea la desigualdad $n^2 < 2^n$.

Demostración de que P(5) es verdadera:

$P(5)$ dice que $5^2 < 2^5$. Pero $5^2 = 25$ y $2^5 = 32$ y $25 < 32$. Entonces $P(5)$ es verdadera.

Demostración de que para cualquier entero $k \geq 5$, si P(k) es verdadero entonces P(k + 1) también es verdadero.

Sea k cualquier entero con $k \geq 5$ y aceptemos que $P(k)$ es verdadero. Es decir, supóngase que $k^2 < 2^k$. *[Esta es la hipótesis de inducción.]* Debemos demostrar que $P(k + 1)$ es verdadero. Es decir, debemos demostrar que $(k + 1)^2 < 2^{k+1}$. Pero

$$(k + 1)^2 = k^2 + 2k + 1 < 2^k + 2k + 1$$

por hipótesis de inducción.

También, por la proposición 5.3.2,

$2k + 1 < 2^k$ la Prop. 5.3.2 se aplica porque $k \geq 5 \geq 3$.

Juntando estas desigualdades se obtiene

$$(k + 1)^2 < 2^k + 2k + 1 < 2^k + 2^k = 2^{k+1}$$

[que era lo que se quería demostrar].

24. *Demostración (por inducción matemática):* Para el enunciado dado, dejemos que $P(n)$ sea la ecuación $a_n = 3 \cdot 7^{n-1}$.

Demostración de que P(1) es verdadero:

El lado izquierdo de $P(1)$ es a_1, que es igual a 3 por definición de la sucesión. El lado derecho es $3 \cdot 7^{1-1} = 3$. Así $P(1)$ es verdadera.

Demostración de que para todos los enteros $k \geq 1$, si P(k) es verdadero entonces P(k + 1) también es verdadero:

Sea k un entero arbitrario con $k \geq 1$ y suponemos que $P(k)$ es verdadera. Es decir, supóngase que $a_k = 3 \cdot 7^{k-1}$. *[Esta es la hipótesis de inducción.]* Debemos demostrar que $P(k + 1)$ es verdadera. Es decir, debemos demostrar que $a_{k+1} = 3 \cdot 7^{(k+1)-1}$, o, equivalentemente, $a_{k+1} = 3 \cdot 7^k$. Pero el lado izquierdo de $P(k + 1)$ es

$$\begin{aligned} a_{k+1} &= 7a_k && \text{por definición de la sucesión } a_1, a_2, a_3, \ldots \\ &= 7(3 \cdot 7^{k-1}) && \text{por la hipótesis de inducción} \\ &= 3 \cdot 7^k && \text{por las leyes de los exponentes.} \end{aligned}$$

y este es el lado derecho de $P(k + 1)$ *[que era lo que se quería demostrar]*.

30. El paso inductivo falla al ir de $n = 1$ a $n = 2$, porque cuando $k = 1$,

$$A = \{a_1, a_2\} \quad \text{y} \quad B = \{a_1\},$$

y ningún conjunto C se puede definir teniendo las propiedades solicitadas para C en la demostración. La razón es que $C = \{a_1\} = B$ y así un elemento de A, a saber, a_2, no está en B ni en C.

Como el paso inductivo falla al ir de $n = 1$ a $n = 2$, nunca queda demostrada la verdad del siguiente enunciado: "Todos los números en un conjunto de dos números son iguales uno al otro". Esto rompe la sucesión de pasos inductivos y así no se demuestra la verdad de ninguno de los enunciados para $n > 2$.

A continuación se presenta una explicación de lo que ocurre en términos de una analogía con el dominó. La primer ficha de dominó se empuja hacia atrás (el paso básico es demostrado). También, si cualquier ficha de la segunda en adelante se empuja hacia atrás, entonces golpeará a la que tiene inmediatamente atrás (el paso inductivo trabaja para $n \geq 2$). Sin embargo, cuando la primera ficha es empujada hacia atrás, *no* golpea a otra ficha. Así solamente la primera ficha cae, las fichas restantes permanecen paradas.

31. *Sugerencia:* ¿Es verdadero el paso básico?

32. *Sugerencia:* Considere el problema de intentar cubrir un tablero 3×3 con trominos. Coloque una marca en ciertos cuadros como se muestra en la siguiente figura.

✓		✓
✓		✓

Observe que ninguno de los dos cuadrados que tienen marcas no pueden cubrirse con el mismo tromino. Como hay cuatro marcas, se necesitarían cuatro trominos para cubrir esos cuadros. Pero, como cada tromino cubre tres cuadros, entonces cuatro trominos cubrirían doce cuadros y no los nueve cuadros del tablero. Por tanto, se concluye que es imposible tal cubrimiento.

34. a. *Sugerencia:* Para el paso inductivo, observe que un tablero $3 \times (2(k + 1))$ puede descomponerse en dos tableros, uno $3 \times 2k$ y el otro 3×2.

35. b. *Sugerencia:* Considere un tablero 3×5 y refiérase a la sugerencia para el ejercicio 32. Implemente una manera de colocar seis marcas en los cuadros, tal que cualesquiera dos cuadros con marcas no puedan cubrirse con el mismo tromino.

37. *Sugerencia:* Use demostración por contradicción. Si el enunciado es falso, entonces existe algún ordenamiento de los enteros desde 1 a 30, digamos $x_1, x_2, \ldots, x_{30}$, tales que $x_1 + x_2 + x_3 < 45$,

$x_2 + x_3 + x_4 < 45$,… y $x_{30} + x_1 + x_2 < 45$. Evalúe la suma de todas estas desigualdades utilizando el hecho de que $\sum_{i=1}^{30} x_i = \sum_{i=1}^{30} i$ y el teorema 4.2.2.

38. *Sugerencia:* Dados $k + 1$ a y $k + 1$ b, colocados en la parte externa alrededor del círculo, tiene que haber al menos un lugar en donde una a esté seguida por una b al hacer el recorrido en el sentido de las manecillas del reloj. En el paso inductivo, temporalmente eliminamos esa a y la b que le sigue y aplicamos la hipótesis de inducción.

Sección 5.4

1. *Demostración (por inducción matemática fuerte):* Aceptemos que la propiedad $P(n)$ sea la frase "a_n es impar".

Demostración de que P(1) y P(2) son verdaderos:

Observe que $a_1 = 1$ y $a_2 = 3$ y tanto 1 como 3 son impares. Así $P(1)$ y $P(2)$ son verdaderos.

Demostración de que para cualquier entero $k \geq 2$, si $P(i)$ es verdadero para todos los enteros i con $1 \leq i \leq k$, entonces $P(k + 1)$ también es verdadero.

Sea $k \geq 2$ cualquier entero y supongamos que a_i es impar para todos los enteros i con $1 \leq i \leq k$. *[Esta es la hipótesis de inducción.]* Debemos demostrar que a_{k+1} es impar. Conocemos que $a_{k+1} = a_{k-1} + 2a_k$ por definición de a_1, a_2, a_3,…. Aún más, $k - 1$ es menor que $k + 1$ y es mayor o igual que 1 (porque $k \geq 2$). Así, por la hipótesis de inducción, a_{k-1} es impar. También, cada término de la sucesión es un entero (siendo la suma de un producto de enteros), además $2a_k$ es par por definición de par. Por tanto, a_{k+1} es la suma de un entero impar y de un entero par, así que es impar (por el ejercicio 19, sección 4.1). *[Que era lo que se quería demostrar.]*

4. *Demostración(por inducción matemática fuerte):* Aceptemos que la propiedad $P(n)$ sea la desigualdad $d_n \leq 1$.

Demostración de que P(1) y P(2) son verdaderas:

Observe que $d_1 = \frac{9}{10}$ y $d_2 = \frac{10}{11}$ y que $\frac{9}{10} \leq 1$ y $\frac{10}{11} \leq 1$. Por tanto, $P(1)$ y $P(2)$ son verdaderos.

Demostración de que para cada entero $k \geq 2$, si $P(i)$ es verdadero para todos los enteros i con $1 \leq i \leq k$, entonces $P(k + 1)$ también es verdadero.

Sea k cualquier entero que cumple $k \geq 2$ y suponemos $d_i \leq 1$ para todos los enteros i con $1 \leq i \leq k$. *[Esto es la hipótesis de inducción.]* Debemos demostrar que $d_{k+1} \leq 1$. Pero, por definición de d_1, d_2, d_3,…, $d_{k+1} = d_k \cdot d_{k-1}$. Ahora $d_k \leq 1$ y $d_{k-1} \leq 1$ por hipótesis de inducción *[porque $1 \leq k \leq k + 1$ y $1 \leq k - 1 < k + 1$ ya que $k \geq 2$]*. En consecuencia, $d_{k+1} = d_k \cdot d_{k-1} \leq 1$ porque si dos números positivos son cada uno menor o igual que 1, entonces su producto es menor o igual que 1. *[Si $0 < a \leq 1$ y $0 < b \leq 1$, entonces multiplicando $a \leq 1$ por b da $ab \leq b$ y como $b \leq 1$, entonces por transitividad de orden, $ab \leq 1$.]* Esto es lo que se quería demostrar. *[Hemos demostrado los pasos básico e inductivo, así concluimos que $d_n \leq 1$ para todos los enteros $n \geq 1$.]*

5. *Demostración (por inducción matemática fuerte):* Dejemos que la propiedad $P(n)$ sea la ecuación $e_n = 5 \cdot 3^n + 7 \cdot 2^n$.

Demostración de que P(0) y P(1) son verdaderas.

Debemos demostrar que $e_0 = 5 \cdot 3^0 + 7 \cdot 2^0$ y $e_1 = 5 \cdot 3^1 + 7 \cdot 2^1$. El lado izquierdo de la primera ecuación es 12 (por definición de e_0, e_1, e_2,…) y su lado derecho es $5 \cdot 1 + 7 \cdot 1 = 12$. El lado izquierdo de la segunda ecuación es 29 (por definición de e_0, e_1, e_2,…) y su lado derecho es $5 \cdot 3 + 7 \cdot 2 = 29$. Así $P(0)$ y $P(1)$ son verdaderas.

Demostración de que para cualquier entero $k \geq 1$, si $P(i)$ es verdadero para todos los enteros i con $0 \leq i \leq k$, entonces $P(k + 1)$ también es verdadero:

Sea $k \geq 1$ un entero y supongamos que $e_i = 5 \cdot 3^i + 7 \cdot 2^i$ para todos los enteros i con $0 \leq i \leq k$. *[Hipótesis de inducción.]* Debemos demostrar que $e_{k+1} = 5 \cdot 3^{k+1} + 7 \cdot 2^{k+1}$.

Pero

$$
\begin{aligned}
e_{k+1} &= 5e_k - 6e_{k-1} && \text{por definición de } e_0, e_1, e_2, \ldots \\
&= 5(5 \cdot 3^k + 7 \cdot 2^k) - 6(5 \cdot 3^{k-1} + 7 \cdot 2^{k-1}) && \text{por hipótesis de inducción} \\
&= 25 \cdot 3^k + 35 \cdot 2^k - 30 \cdot 3^{k-1} - 42 \cdot 2^{k-1} \\
&= 25 \cdot 3^k + 35 \cdot 2^k - 10 \cdot 3 \cdot 3^{k-1} - 21 \cdot 2 \cdot 2^{k-1} \\
&= 25 \cdot 3^k + 35 \cdot 2^k - 10 \cdot 3^k - 21 \cdot 2^k \\
&= (25 - 10) \cdot 3^k + (35 - 21) \cdot 2^k \\
&= 15 \cdot 3^k + 14 \cdot 2^k \\
&= 5 \cdot 3 \cdot 3^k + 7 \cdot 2 \cdot 2^k \\
&= 5 \cdot 3^{k+1} + 7 \cdot 2^{k+1} && \text{por álgebra.}
\end{aligned}
$$

[Que era lo que se quería demostrar.]

10. *Sugerencia:* En el paso básico, demuestre que $P(14)$, $P(15)$ y $P(16)$ son verdaderas. Para el paso inductivo, observe que $k + 1 = [(k + 1) - 3] + 3$ y si $k \geq 16$, entonces $(k + 1) - 3 \geq 14$.

11. *Demostración (por inducción matemática fuerte):* Aceptemos que la propiedad $P(n)$ sea la frase:

> "Se necesitan $n - 1$ pasos para armar un rompecabezas de n piezas".

Demostración de que P(1) es verdadero:

Un rompecabezas de una sola pieza no necesita paso alguno para armarlo. Entonces es correcto decir que tome cero pasos armarlo.

Demostración de que para cualquier entero $k \geq 1$, si $P(i)$ es verdadero para todos los enteros i con $1 \leq i \leq k$ entonces $P(k + 1)$ también es verdadera.

Sea $k \geq 1$ un entero y supongamos que para todos los enteros i con $1 \leq i \leq k$, en un rompecabezas de i piezas se necesitan $i - 1$ pasos para armarlo. *[Esto es la hipótesis de inducción.]* Debemos demostrar que para armar un rompecabezas de $k + 1$ piezas se necesitan k pasos. Entonces consideremos el armar un rompecabezas de $k + 1$ piezas. El último paso implica juntar dos bloques. Supongamos que uno de los bloques consiste de r piezas y el otro de s piezas. Así $r + s = k + 1$ y $1 \leq r \leq k$ y $1 \leq s \leq k$. Entonces por hipótesis de inducción, los números de pasos necesarios para armar los bloques son $r - 1$ y $s - 1$, respectivamente. Por tanto, el número total de pasos requeridos para armar el rompecabezas es $(r - 1) + (s - 1) + 1 = (r + s) - 1 = (k + 1) - 1 = k$ *[que era lo que se quería demostrar]*.

12. *Sugerencia:* Para cualquier colección de latas, al menos una debe contener suficiente gasolina para permitir que el auto llegue a la siguiente lata. (¿Por qué?) Imagine tomando toda la gasolina de

esa lata y vaciándola en la lata que inmediatamente la precede en la dirección de viaje alrededor de la ruta.

13. *Esbozo de la demostración:* Dado cualquier entero $k > 1$, entonces k es primo o k es el producto de dos enteros positivos más pequeños, cada uno más grande que 1. En el primer caso, la propiedad es verdadera. En el segundo caso, la hipótesis de inducción asegura que ambos factores de k son productos de primos y entonces esa k también es el producto de primos.

14. *Demostración (por inducción matemática fuerte):* Aceptemos que la propiedad $P(n)$ sea la frase "Cualquier producto de n enteros impares es impar".

Demostración de que P(2) es verdadera:

Debemos demostrar que cualquier producto de dos enteros impares es impar, que fue establecido en el capítulo 4 (ejercicio 43 de la sección 4.1).

Demostración de que para cualquier entero $k \geq 2$, si $P(i)$ es verdadera para todos los enteros i con $2 \leq i \leq k$ entonces $P(k+1)$ también es verdadera.

Sea k cualquier entero con $k \geq 2$ y supongamos que para todos los enteros i con $2 \leq i \leq k$, cualquier producto de i enteros impares es impar. *[Hipótesis de inducción.]* Consideremos cualquier producto M de $k+1$ enteros impares. Para obtener M basta una multiplicación. Así existen enteros A y B tales que $M = AB$ y tanto A como B son el producto de entre 1 y k enteros impares. (Por ejemplo, si $M = ((a_1a_2)a_3)a_4$, entonces $A = (a_1a_2)a_3$ y $B = a_4$). Por la hipótesis de inducción, A y B son impares y, como en el paso básico, conocemos que cualquier producto de dos enteros impares es impar. Por tanto, $M = AB$ es impar.

16. *Sugerencia:* Aceptemos que la propiedad $P(n)$ sea la frase "Si n es par, entonces cualquier suma de n enteros impares es par y si n es impar, entonces cualquier suma de n enteros impares es impar". Para el paso inductivo, consideremos cualquier suma S de $k+1$ enteros impares. Para obtener S basta con alguna suma. Entonces existen enteros A y B tales que $S = A + B$ y A es la suma de r enteros impares y B es la suma de $(k+1) - r$ enteros impares. Deben considerarse los casos en donde $k+1$ es par o impar y para cada uno estudiarse los sub-casos en donde r es par o impar.

17. $4^1 = 4$, $4^2 = 16$, $4^3 = 64$, $4^4 = 256$, $4^5 = 1\,024$, $4^6 = 4\,096$, $4^7 = 16\,384$ y $4^8 = 65\,536$.

Conjetura: El dígito de unidades de 4^n es igual a 4 si n es impar, e igual a 6 si n es par.

Demostración por inducción matemática fuerte: Dejemos que la propiedad $P(n)$ sea la frase "El dígito de unidades de 4^n es igual a 4 si n es impar, e igual a 6 si n es par".

Demostración de que P(1) y P(2) son verdaderas:

Cuando $n = 1$, $4^n = 4^1 = 4$ y el dígito de unidades es 4. Cuando $n = 2$, entonces $4^n = 4^2 = 16$ y el dígito de unidades es 6. Por tanto, $P(1)$ y $P(2)$ son verdaderas.

Demostración de que para cualquier entero $k \geq 2$, si la propiedad es verdadera para todos los enteros i con $1 \leq i \leq k$, entonces es verdadera para $k+1$:

Sea k cualquier entero con $k \geq 2$ y supongamos que para todos los enteros i con $0 \leq i \leq k$, el dígito de unidades de 4^i es igual a 4 si i es impar e igual a 6 si i es par. *[Hipótesis de inducción.]* Debemos demostrar que el dígito de unidades de 4^{k+1} es igual a 4 si $k+1$ es impar e igual a 6 si $k+1$ es par.

Caso 1 ($k+1$ es impar): En este caso, k es par y así, por hipótesis de inducción, el dígito de unidades de 4^k es 6. Entonces $4^k = 10q + 6$ para algún entero q no-negativo. Se tiene que $4^{k+1} = 4^k \cdot 4 = (10q+6)\cdot 4 = 40q + 24 = 10(4q+2) + 4$. Así el dígito de unidades de 4^{k+1} es 4 *[que era lo que se quería demostrar]*.

Caso 2 ($k+1$ es par): En este caso, k es impar y así, por la hipótesis de inducción, el dígito de unidades de 4^k es 4. Así $4^k = 10q + 4$ para algún entero q no-negativo. Se tiene que $4^{k+1} = 4^k \cdot 4 = (10q+4)\cdot 4 = 40q + 16 = 10(4q+1) + 6$. Entonces el dígito de las unidades de 4^{k+1} es 6 *[que era lo que se quería demostrar]*.

20. *Demostración:* Sea n cualquier entero mayor que 1. Consideremos el conjunto S de todos los enteros positivos, diferentes que 1, que dividen a n. Como $n \mid n$ y $n > 1$, entonces existe al menos un elemento en S. Por tanto, por el principio del buen orden para los enteros, S tiene un elemento que es el más pequeño; llamado p. Afirmamos que p es primo. Supongamos que p no es primo. Entonces existen enteros a y b con $1 < a < p$, $1 < b < p$ y $p = ab$. Por definición de división, $a \mid p$. También $p \mid n$ porque p está en S y cada elemento de S divide a n. Por tanto, $a \mid p$ y $p \mid n$ y así, por transitividad de divisibilidad, $a \mid n$. Consecuentemente, $a \in S$. Pero esto contradice el hecho de que $a < p$ y que p sea el elemento más pequeño de S. *[Esta contradicción muestra que la suposición de que p no es primo, es falsa.]* Entonces p es primo y hemos demostrado la existencia de un número primo que divide a n.

22. a. *Demostración:* Supongamos que r es cualquier número racional. *[Necesitamos demostrar que existe un entero n tal que $r < n$.]*

Caso 1 ($r \leq 0$): En este caso, tomamos $n = 1$. Entonces $r < n$.

Caso 2 ($r > 0$): En esta situación, $r = \frac{a}{b}$ para algunos enteros positivos a y b (por definición de racional y porque r es positivo). Observe que $r = \frac{a}{b} < n$ si y sólo si, $a < nb$. Sea $n = 2a$. Multiplicamos ambos lados de la desigualdad $1 < 2$ por a para obtener $a < 2a$ y multiplicamos ambos lados de la desigualdad $1 < b$ por $2a$ para obtener que $2a < 2ab = nb$. Así $a < 2a < nb$, entonces, por transitividad de orden, $a < nb$. Dividiendo ambos lados entre b se tiene que $\frac{a}{b} < n$ o, equivalentemente, que $r < n$.

En consecuencia, en ambos casos, $r < n$ *[que era lo que se quería demostrar]*.

23. *Sugerencia:* Si r es cualquier número racional, sea S el conjunto de todos los enteros n tales que $r < n$. Use los resultados de los ejercicios 22*a*), 22*c*) y el principio del buen orden para los enteros, para demostrar que S tiene un elemento mínimo, digamos v y entonces demostrar que $v - 1 \leq r < v$.

24. *Demostración:* Sea S el conjunto de todos los enteros r tales que $n = 2^i \cdot r$ para algún entero i. Entonces $n \in S$ porque $n = 2^0 \cdot n$ y así $S \neq \emptyset$. También, como $n \geq 1$, cada r en S es positivo y además, por el principio del buen orden, S tiene un elemento mínimo m. Esto significa que $n = 2^k \cdot m$ (*) para algún entero k no-negativo y $m \leq r$ para cada r en S. Afirmamos que m es impar. La razón es que si m fuera par, entonces $m = 2p$ para algún entero p. Sustituyendo en la ecuación (*) resulta:

$$n = 2^k \cdot m = 2^k \cdot 2p = (2^k \cdot 2)p = 2^{k+1} \cdot p.$$

Se tiene que $p \in S$ y $p < m$, que contradice el hecho de que m es el elemento mínimo de S. Así que m es impar y entonces $n = m \cdot 2^k$ para algún entero impar m y un entero k no-negativo.

29. *Sugerencia:* En el paso inductivo, divida en casos dependiendo de si k se puede escribir como $k = 3x$ o $k = 3x + 1$ o $k = 3x + 2$ para algún entero x.

30. *Sugerencia:* En el paso inductivo, sea $k \geq 0$ un entero dado y supongamos que existen enteros q' y r' tales que $k = dq' + r'$ y $0 \leq r' < d$. Debe demostrar que existen enteros q y r tales que:

$$k + 1 = dq + r \text{ y } 0 \leq r < d.$$

Al hacer esto, considera los casos $r' < d - 1$ y $r' = d - 1$.

31. *Sugerencia:* Dado un predicado $P(n)$ que satisface las condiciones (1) y (2) del principio de inducción matemática, sea S el conjunto de todos los enteros mayores o iguales a a para que $P(n)$ es falso. Suponga que S tiene uno o más elementos y use el principio del buen orden para deducir una contradicción.

32. *Sugerencia:* Suponga que S es un conjunto que contiene uno o más enteros, todos mayores o iguales que algún entero a y suponga que S no tiene un elemento mínimo. Deje que la propiedad $P(n)$ sea la frase "i no es elemento de S para cualquier entero i con $a \leq i \leq n$". Use inducción matemática para demostrar que $P(n)$ es verdadero para todos los enteros $n \geq a$ y explique cómo este resultado contradice la suposición de que S no tiene un elemento mínimo.

Sección 5.5

1. *Demostración:* Suponga que el predicado $m + n = 100$ es verdadero antes de entrar al bucle. Entonces

$$m_{\text{antiguo}} + n_{\text{antiguo}} = 100.$$

Después de la ejecución del bucle,

$$m_{\text{nuevo}} = m_{\text{antiguo}} + 1 \text{ y } n_{\text{nuevo}} = n_{\text{antiguo}} - 1,$$

así

$$\begin{aligned} m_{\text{nuevo}} + n_{\text{nuevo}} &= (m_{\text{antiguo}} + 1) + (n_{\text{antiguo}} - 1) \\ &= m_{\text{antiguo}} + n_{\text{antiguo}} = 100. \end{aligned}$$

3. *Demostración:* Suponga que el predicado $m^3 > n^2$ es verdadero antes de la entrada al bucle. Entonces

$$m_{\text{antiguo}}{}^3 > n_{\text{antiguo}}{}^2.$$

Después de la ejecución del bucle,

$$m_{\text{nuevo}} = 3 \cdot m_{\text{antiguo}} \text{ y } n_{\text{nuevo}} = 5 \cdot n_{\text{antiguo}},$$

así

$$m^3_{\text{nuevo}} = (3 \cdot m_{\text{antiguo}})^3 = 27 \cdot m^3_{\text{antiguo}} > 27 \cdot n^2_{\text{antiguo}}.$$

Pero como $n_{\text{nuevo}} = 5 \cdot n_{\text{antiguo}}$, entonces $n_{\text{antiguo}} = \frac{1}{5} n_{\text{nuevo}}$. Por tanto

$$\begin{aligned} m^3_{\text{nuevo}} > 27 \cdot n^2_{\text{antiguo}} &= 27 \cdot \left(\frac{1}{5} n_{\text{nuevo}}\right)^2 = 27 \cdot \frac{1}{25} n^2_{\text{nuevo}} \\ &= \frac{27}{25} \cdot n^2_{\text{nuevo}} > n^2_{\text{nuevo}}. \end{aligned}$$

6. *Demostración: [Las palabras de esta demostración son casi las mismas como en el ejemplo 5.5.2.]*

I. Propiedad básica: *[I(0) es verdadera antes de la primera iteración del bucle.]*

I (0) es "$exp = x^0$ y $i = 0$". De acuerdo a la precondición, antes de la primera iteración del bucle $exp = 1$ e $i = 0$. Como $x^0 = 1$, entonces $I(0)$ es evidentemente verdadera.

II. Propiedad inductiva: *[Si $G \wedge I(k)$ es verdadero antes de una iteración de bucle (donde $k \geq 0$), entonces $I(k + 1)$ es verdadera después de la iteración de bucle.]*

Supongamos que k es un entero no-negativo tal que $G \wedge I(k)$ es verdadero antes de una iteración de bucle. Entonces cuando la ejecución alcanza el tope del bucle, $i \neq m$, $exp = x^k$, e $i = k$. Como $i \neq m$, entonces se pasa a través de la guardia y se ejecuta el enunciado 1. Ahora, antes de la ejecución del enunciado 1,

$$exp_{\text{antiguo}} = x^k,$$

así la ejecución del enunciado 1 tiene el siguiente efecto:

$$exp_{\text{nuevo}} = exp_{\text{antiguo}} \cdot x = x^k \cdot x = x^{k+1}.$$

Similarmente, antes de ejecutar el enunciado 2,

$$i_{\text{antiguo}} = k,$$

y después de ejecutar el enunciado 2,

$$i_{\text{nuevo}} = i_{\text{antiguo}} + 1 = k + 1.$$

Entonces después de la iteración de bucle, los dos enunciados $exp = x^{k+1}$ e $i = k + 1$ son verdaderos y por tanto $I(k + 1)$ es verdadero.

III. Eventual falsedad de la guardia: *[Después de un número finito de iteraciones del bucle, G se convierte en falso.]*

La guardia G es la condición $i \neq m$ y m es un entero no-negativo. Por I y II, se conoce que

> para *todos* los enteros $n \geq 0$, si el bucle es iterado n veces, entonces $exp = x^n$ e $i = n$.

Así, después de m iteraciones del bucle, $i = m$. Entonces se convierte en falso después de m iteraciones del bucle.

IV. Corrección de la post-condición: *[Si N es el número mínimo de iteraciones después de que G es falso e I(N) es verdadero, entonces el valor de las variables algorítmicas será especificado en la post-condición del bucle.]*

De acuerdo a la post-condición, el valor de exp después de la ejecución del bucle debería ser x^m. Pero cuando G es falso, $i = m$. Y cuando $I(N)$ es verdadero, $i = N$ y $exp = x^N$. Como *ambas* condiciones (G falso e $I(N)$ verdadero) se satisfacen, entonces $m = i = N$ y $exp = x^m$, como fue requerido.

8. *Demostración:*

I. Propiedad básica: $I(0)$ es "$i = 1$ y $suma = A[1]$". De acuerdo a la pre-condición, este enunciado es verdadero.

II. Propiedad inductiva: Supongamos que k es un entero no-negativo tal que $G \wedge I(k)$ es verdadero antes de una iteración del bucle. Entonces cuando la ejecución alcanza

el tope del bucle, $i \neq m$, $i = k + 1$ y $suma = A[1] + A[2] + \cdots + A[k + 1]$. Como $i \neq m$, se pasa la guardia y se ejecuta el enunciado 1. Ahora, antes de la ejecución del enunciado 1, $i_{\text{antiguo}} = k + 1$. Así, después de la ejecución del enunciado 1, $i_{\text{nuevo}} = i_{\text{antiguo}} + 1 = (k + 1) + 1 = k + 2$. También, antes de la ejecución del enunciado 2, $suma_{\text{antiguo}} = A[1] + A[2] + \cdots + A[k + 1]$. La ejecución del enunciado 2 agrega $A[k + 1]$ a esta suma y así después de que se ejecuta el enunciado 2, $suma_{\text{nuevo}} = A[1] + A[2] + \cdots + A[k + 1] + A[k + 2]$. Entonces después de la iteración de bucle, $I(k + 1)$ es verdadero.

III. Eventual falsedad de la guardia: La guardia G es la condición $i \neq m$. Por I y II, se conoce que para todos los enteros $n \geq 1$, después de n iteraciones del bucle, $I(n)$ es verdadero. Así que, después de $m - 1$ iteraciones del bucle, $I(m)$ es verdadero, que implica que $i = m$ y G es falso.

IV. Corrección de la post-condición: Suponga que N es el número mínimo de iteraciones después de que G es falso e $I(N)$ es verdadero. Entonces (debido a que G es falso) $i = m$ y (porque $I(N)$ es verdadero) $i = N + 1$ y $suma = A[1] + A[2] + \cdots + A[N + 1]$. Agrupando todo esto da $m = N + 1$ y así $suma = \text{A}[1] + \text{A}[2] + \cdots + \text{A}[m]$, que es la post-condición.

10. *Sugerencia:* Suponga que $G \wedge I(k)$ es verdadero para un entero k no-negativo. Entonces $a_{\text{antiguo}} \neq 0$ y $b_{\text{antiguo}} \neq 0$ y

1) a_{antiguo} y b_{antiguo} son enteros no-negativos con $\text{mcd}(a_{\text{antiguo}}, b_{\text{antiguo}}) = \text{mcd}(A, B)$.

2) A lo más uno de los dos, a_{antiguo} y b_{antiguo}, es igual a 0.

3) $0 \leq a_{\text{antiguo}} + b_{\text{antiguo}} \leq A + B - k$.

Debe demostrarse que $I(k + 1)$ es verdadero después de la iteración del bucle, lo que significa que es necesario demostrar que:

1) a_{nuevo} y b_{nuevo} son enteros no-negativos con $\text{mcd}(a_{\text{nuevo}}, b_{\text{nuevo}}) = \text{mcd}(A, B)$.

2) A lo más uno de los dos, a_{nuevo} y b_{nuevo}, es igual a cero.

3) $0 \leq a_{\text{nuevo}} + b_{\text{nuevo}} \leq A + B - (k + 1)$.

Para demostrar (3), observe que:

$$a_{\text{nuevo}} + b_{\text{nuevo}} = \begin{cases} a_{\text{antiguo}} - b_{\text{antiguo}} + b_{\text{antiguo}} & \text{si } a_{\text{antiguo}} \geq b_{\text{antiguo}} \\ b_{\text{antiguo}} - a_{\text{antiguo}} + a_{\text{antiguo}} & \text{si } a_{\text{antiguo}} < b_{\text{antiguo}} \end{cases}$$

[La razón para esto es que cuando $a_{antiguo} \geq b_{antiguo}$, entonces $a_{nuevo} = a_{antiguo} - b_{antiguo}$ y $b_{nuevo} = b_{antiguo}$ y cuando $a_{antiguo} < b_{antiguo}$, entonces $b_{nuevo} = b_{antiguo} - a_{antiguo}$ y $a_{nuevo} = a_{antiguo}$.] Así

$$a_{\text{nuevo}} + b_{\text{nuevo}} = \begin{cases} a_{\text{antiguo}} & \text{si } a_{\text{antiguo}} \geq b_{\text{antiguo}} \\ b_{\text{antiguo}} & \text{si } a_{\text{antiguo}} < b_{\text{antiguo}} \end{cases}$$

Pero como $a_{\text{antiguo}} \neq 0$, $b_{\text{antiguo}} \neq 0$ y son enteros no-negativos, entonces $a_{\text{antiguo}} \geq 1$ y $b_{\text{antiguo}} \geq 1$. Entonces $a_{\text{antiguo}} - 1 \geq 0$, $b_{\text{antiguo}} - 1 \geq 0$, $a_{\text{antiguo}} \leq a_{\text{antiguo}} + b_{\text{antiguo}} - 1$ y $b_{\text{antiguo}} \leq b_{\text{antiguo}} + a_{\text{antiguo}} - 1$. Se tiene que $a_{\text{nuevo}} + b_{\text{nuevo}} \leq a_{\text{antiguo}} + b_{\text{antiguo}} - 1 \leq (A + B - k) - 1$ porque (3) tiene validez en la k-ésima iteración. Entonces, por simplificación algebraica se obtiene que $a_{\text{nuevo}} + b_{\text{nuevo}} < A + B - (k + 1)$.

Sección 5.6

1. $a_1 = 1, a_2 = 2a_1 + 2 = 2 \cdot 1 + 2 = 4,$
$a_3 = 2a_2 + 3 = 2 \cdot 4 + 3 = 11,$
$a_4 = 2a_3 + 4 = 2 \cdot 11 + 4 = 26$

3. $c_0 = 1, c_1 = 1 \cdot (c_0)^2 = 1 \cdot (1)^2 = 1,$
$c_2 = 2(c_1)^2 = 2 \cdot (1)^2 = 2,$
$c_3 = 3(c_2)^2 = 3 \cdot (2)^2 = 12$

5. $s_0 = 1, s_1 = 1, s_2 = s_1 + 2s_0 = 1 + 2 \cdot 1 = 3,$
$s_3 = s_2 + 2s_1 = 3 + 2 \cdot 1 = 5$

7. $u_1 = 1, u_2 = 1, u_3 = 3u_2 - u_1 = 3 \cdot 1 - 1 = 2,$
$u_4 = 4u_3 - u_2 = 4 \cdot 2 - 1 = 7$

9. Por definición de a_0, a_1, a_2,..., para cada entero $k \geq 1$,

(*) $\quad a_k = 3k + 1$ y

(**) $\quad a_{k-1} = 3(k - 1) + 1.$

Entonces $a_{k-1} + 3$

$$\begin{aligned} &= 3(k - 1) + 1 + 3 \\ &= 3k - 3 + 1 + 3 \\ &= 3k + 1 \\ &= a_k \end{aligned}$$

11. Por definición de c_0, c_1, c_2,..., $c_n = 2^n - 1$, para cada entero $n \geq 0$. Sustituimos k y $k - 1$ en lugar de n para obtener:

(*) $\quad c_k = 2^k - 1$ y

(**) $\quad c_{k-1} = 2^{k-1} - 1$

para todos los enteros $k \geq 1$. Entonces:

$$\begin{aligned} 2c_{k-1} + 1 &= 2(2^{k-1} - 1) + 1 && \text{sustituyendo (**)} \\ &= 2^k - 2 + 1 \\ &= 2^k - 1 && \text{por álgebra básica} \\ &= c_k && \text{sustituyendo (*)} \end{aligned}$$

13. Por definición de t_0, t_1, t_2,..., $t_n = 2 + n$, para cada entero $n \geq 0$. Sustituir k, $k - 1$ y $k - 2$ en lugar de n para obtener

(*) $\quad t_k = 2 + k,$

(**) $\quad t_{k-1} = 2 + (k - 1),$ $\quad$ y

(***) $\quad t_{k-2} = 2 + (k - 2)$

Para cada entero $k \geq 2$. Entonces

$$\begin{aligned} &2t_{k-1} - t_{k-2} \\ &\quad = 2(2 + (k - 1) - (2 + (k - 2))) && \text{sustituyendo (**) y (***)} \\ &\quad = 2(k + 1) - k \\ &\quad = 2 + k && \text{por álgebra} \\ &\quad = t_k && \text{sustituyendo (*).} \end{aligned}$$

15. *Sugerencia:* La inducción matemática no se necesita para la demostración. Inicie con el lado derecho de la ecuación y use álgebra para transformarlo en el lado izquierdo de la ecuación.

17. a. $a_1 = 2$

$a_2 = 2$ (mueve el disco de arriba del polo A al polo C)
$+ 1$ (mueve el disco del fondo del polo A al polo B)
$+ 2$ (mueve el disco de arriba del polo C al polo A)
$+ 1$ (mueve el disco del fondo del polo B al polo C)
$+ 2$ (mueve el disco de arriba del polo A al polo C)
$= 8$

$a_3 = 8 + 1 + 8 + 1 + 8 = 26$

c. Para todos los enteros $k \geq 2$.

$a_k = a_{k-1}$ (mueve el disco $k-1$ de arriba del polo A al polo C)
$+ 1$ (mueve el disco del fondo del polo A al polo B)
$+ a_{k-1}$ (mueve el disco de arriba del polo C al polo A)
$+ 1$ (mueve los discos del fondo del polo B al polo C)
$+ a_{k-1}$ (mueve los discos de arriba del polo A al polo C)

$= 3a_{k-1} + 2.$

18. b. $b_4 = 40$

e. *Sugerencia:* Una solución es utilizar inducción matemática y aplicar la fórmula del inciso c). Otra solución es demostrar, por inducción matemática, que cuando se efectúa una muy eficiente transferencia de n discos de un polo a otro, entonces en algún punto todos los discos están en el polo intermedio.

19. a. $s_1 = 1,\ s_2 = 1 + 1 + 1 = 3,$
$s_3 = s_1 + (1 + 1 + 1) + s_1 = 5$
b. $s_4 = s_2 + (1 + 1 + 1) + s_2 = 9$

20. b. Los polos se denotarán por A, B y C. Calcule c_2 empleando la siguiente secuencia de pasos para transferir dos discos de A a B:

1 (mover el disco de arriba para A a B)
$+ 1$ (mover el disco de arriba de B a C)
$+ 1$ (mover el disco del fondo de A a B)
$+ 1$ (mover el disco de arriba de C a A)
$+ 1$ (mover el disco de arriba de A a B).

La secuencia de pasos es la más pequeña posible y así $c_2 = 5$.

Una torre de 3 discos se puede transferir de A a B utilizando la siguiente secuencia de pasos:

1 (mover el disco de arriba de A a B)
$+ 1$ (mover el disco de arriba de B a C)
$+ 1$ (mover el disco intermedio de A a B)
$+ 1$ (mover el disco de arriba de C a A)
$+ 1$ (mover el disco intermedio de B a C)
$+ 1$ (mover el disco de arriba de A a B)
$+ 1$ (mover el disco de arriba de B a C).

Después que se han completado estos 7 pasos, el disco del fondo se puede mover de A a B. En ese punto dos discos de arriba están sobre C y una versión modificada de los siete pasos iniciales puede usarse para moverlos de C a B. Así el número total de pasos es $7 + 1 + 7 = 15$ y $15 < 21 = 4c_2 + 1$.

21. b. $t_3 = 14$

22. b. $r_0 = 1,\ r_1 = 1,\ r_2 = 1 + 4 \cdot 1 = 5,\ r_3 = 5 + 4 \cdot 1 = 9,$
$r_4 = 9 + 4 \cdot 5 = 29,\ r_5 = 29 + 4 \cdot 9 = 65,$
$r_6 = 65 + 4 \cdot 29 = 181$

23. c. Después de 12 meses existen 904 parejas de conejos, o, 1808 conejos.

25. a. Cada término de la sucesión de Fibonacci, posterior al segundo, es igual a la suma de los dos términos anteriores. Para cualquier entero $k \geq 1$, los dos términos previos a F_{k+1} son F_k y F_{k-1}. Entonces, para todos los enteros $k \geq 1$, $F_{k+1} = F_k + F_{k-1}$.

26. Por repetido uso de la definición de la sucesión de Fibonacci, para todos los enteros $k \geq 4$,

$$\begin{aligned} F_k &= F_{k-1} + F_{k-2} = (F_{k-2} + F_{k-3}) + (F_{k-3} + F_{k-4}) \\ &= ((F_{k-3} + F_{k-4}) + F_{k-3}) + (F_{k-3} + F_{k-4}) \\ &= 3F_{k-3} + 2F_{k-4}. \end{aligned}$$

27. Para todos los enteros $k \geq 1$,

$$\begin{aligned} & F_k^2 - F_{k-1}^2 \\ &= (F_k - F_{k-1})(F_k + F_{k-1}) && \text{por álgebra básica (diferencia cuadrados)} \\ &= (F_k - F_{k-1})F_{k+1} && \text{por definición de la sucesión de Fibonacci.} \\ &= F_k F_{k+1} - F_{k-1}F_{k+1} \end{aligned}$$

32. *Sugerencia:* Use inducción matemática. En el paso inductivo, aplique el lema 4.8.2 y el hecho de que $F_{k+2} = F_{k+1} + F_k$, para así deducir que

$$\text{mcd}(F_{k+2}, F_{k+1}) = \text{mcd}(F_{k+1}, F_k).$$

34. *Sugerencia:* Sea $L = \lim_{n\to\infty} \dfrac{F_{n+1}}{F_n}$ y demuestre que $L = \dfrac{1}{L} + 1$. Deduzca que $L = \dfrac{1+\sqrt{5}}{2}$.

35. *Sugerencia:* Use el resultado del ejercicio 30 para demostrar que la sucesión infinita $\dfrac{F_0}{F_1}, \dfrac{F_2}{F_3}, \dfrac{F_4}{F_5}, \ldots$ es estrictamente decreciente y que la sucesión infinita $\dfrac{F_1}{F_2}, \dfrac{F_3}{F_4}, \dfrac{F_5}{F_6}, \ldots$ es estrictamente creciente. La primera sucesión está acotada por abajo por 0 y la segunda secuencia está acotada por arriba por 1. Deduzca que existen los límites de ambas sucesiones y demuestre que son iguales.

37. a. Como el interés anual de 4% es compuesto trimestralmente, la razón de interés trimestral es $(4\%)/4 = 1\%$. Entonces $R_k = R_{k-1} + 0.01R_{k-1} = 1.01R_{k-1}$.

b. Como un año es igual a 4 trimestres, la cantidad del depósito al final de un año es $R_4 = \$5\,203.02$ (redondeado al centavo más cercano).

c. La razón de porcentaje anual (RPA) para la cuenta es $\frac{\$5\,203.02 - \$5\,000.00}{\$5\,000.00} = 4.0604\%$.

39. Cuando se sube una escalera de n escalones, el mínimo avance es de uno o de dos escalones a la vez. El número de maneras de subir la escalera con un avance de un peldaño es c_{n-1}; el número de formas de subir la escalera con un avance de dos escalones es c_{n-2}. Por tanto, $c_n = c_{n-1} + c_{n-2}$. También observe que $c_1 = 1$ y $c_2 = 2$ *[porque ambas escaleras pueden subirse una por una o subirse de continuo como si fueran una sola unidad]*.

41. *Demostración (por inducción matemática):* Sea la propiedad, $P(n)$, la ecuación $\sum_{i=1}^{n} ca_i = c\sum_{i=1}^{n} a_i$, en donde $a_1, a_2, a_3, \ldots, a_n$ y c son números reales arbitrarios.

Demostración de que P(1) es verdadero:

Sean a_1 y c números reales arbitrarios. Por la definición recursiva de suma, $\sum_{i=1}^{1}(ca_i) = ca_1$ y $\sum_{i=1}^{1} a_i = a_1$. Por tanto, $\sum_{i=1}^{1}(ca_i) = c\sum_{i=1}^{1} a_i$, y así $P(1)$ es verdadera.

Demostración de que para todos los enteros $k \geq 1$, si $P(k)$ es verdadero, entonces $P(k+1)$ también es verdadero:

Sea k cualquier entero con $k \geq 1$. Supongamos que para cualesquiera números reales $a_1, a_2, \ldots, a_k$ y c, $\sum_{i=1}^{k}(ca_i) = c\sum_{i=1}^{k} a_i$. *[Esto es la hipótesis de inducción.][Debemos demostrar que para cualesquiera números reales $a_1, a_2, \ldots, a_{k+1}$ y c, $\sum_{i=1}^{k+1}(ca_i) = c\sum_{i=1}^{k+1} a_i$.]* Sean $a_1, a_2, \ldots, a_{k+1}$ y c números reales arbitrarios.

Entonces

$$\begin{aligned}
\sum_{i=1}^{k+1} ca_i &= \sum_{i=1}^{k} ca_i + ca_{k+1} && \text{por la definición recursiva de } \Sigma \\
&= c\sum_{i=1}^{k} a_i + ca_{k+1} && \text{por la hipótesis de inducción} \\
&= c\left(\sum_{i=1}^{k} a_i + a_{k+1}\right) && \text{por la ley distributiva para los números reales,} \\
&= c\sum_{i=1}^{k+1} a_i && \text{por la definición recursiva de } \Sigma.
\end{aligned}$$

44. *Sugerencia:* Acepta que la propiedad sea la desigualdad

$$\left|\sum_{i=1}^{n} a_i\right| \leq \sum_{i=1}^{n} |a_i|.$$

Para demostrar el paso inductivo, observe que debido a $\left|\sum_{i=1}^{k+1} a_i\right| = \left|\sum_{i=1}^{k} a_i + a_{k+1}\right|$, puede usar la desigualdad del triángulo para el valor absoluto (teorema 4.4.6) para deducir que $\left|\sum_{i=1}^{k} a_i + a_{k+1}\right| \leq \left|\sum_{i=1}^{k} a_i\right| + |a_{k+1}|$.

Sección 5.7

1. a. $1 + 2 + 3 + \cdots + (k-1)$

$$= \frac{(k-1)((k-1)+1)}{2} = \frac{(k-1)k}{2}$$

b. $3 + 2 + 4 + 6 + 8 + \cdots + 2n$

$$\begin{aligned}
&= 3 + 2(1 + 2 + 3 + \cdots + n) \\
&= 3 + 2\frac{n(n+1)}{2} = 3 + n(n+1) \\
&= n^2 + n + 3
\end{aligned}$$

2. a. $1 + 2 + 2^2 + \cdots + 2^{i-1} = \frac{2^{(i-1)+1} - 1}{2 - 1} = 2^i - 1$

c. $2^n + 2^{n-2}\cdot 3 + 2^{n-3}\cdot 3 + \cdots + 2^2\cdot 3 + 2\cdot 3 + 3$

$$\begin{aligned}
&= 2^n + 3(2^{n-2} + 2^{n-3} + \cdots + 2^2 + 2 + 1) \\
&= 2^n + 3(1 + 2 + 2^2 + \cdots + 2^{n-3} + 2^{n-2}) \\
&= 2^n + 3\left(\frac{2^{(n-2)+1} - 1}{2 - 1}\right) \\
&= 2^n + 3(2^{n-1} - 1) \\
&= 2\cdot 2^{n-1} + 3\cdot 2^{n-1} - 3 \\
&= 5\cdot 2^{n-1} - 3
\end{aligned}$$

3. $a_0 = 1$

$a_1 = 1\cdot a_0 = 1\cdot 1 = 1$

$a_2 = 2a_1 = 2\cdot 1$

$a_3 = 3a_2 = 3\cdot 2\cdot 1$

$a_4 = 4a_3 = 4\cdot 3\cdot 2\cdot 1$

$\vdots$

Conjetura:

$a_n = n(n-1)\cdots 3\cdot 2\cdot 1 = n\rightarrow$

5. $c_1 = 1$

$c_2 = 3c_1 + 1 = 3\cdot 1 + 1 = 3 + 1$

$c_3 = 3c_2 + 1 = 3\cdot(3+1) + 1 + 3^2 + 3 + 1$

$c_4 = 3c_3 + 1 = 3\cdot(3^2 + 3 + 1) + 1$

$= 3^3 + 3^2 + 3 + 1$

$\vdots$

Conjetura:

$c_n = 3^{n-1} + 3^{n-2} + \cdots + 3^3 + 3^2 + 3 + 1$

$= \frac{3^n - 1}{3 - 1}$ por el teorema 5.2.3 con $r = 3$.

$= \frac{3^n - 1}{2}$

6. *Sugerencia:*

$d_n = 2^n + 2^{n-2}\cdot 3 + 2^{n-3}\cdot 3 + \cdots + 2^2\cdot 3 + 2\cdot 3 + 3$

$= 5\cdot 2^{n-1} - 3$ para todos los enteros $n \geq 1$

9. *Sugerencia:* Para números reales positivos arbitrarios a y b,

$$\frac{\frac{a}{b}}{\frac{a}{b} + 2} = \frac{\frac{a}{b}}{\frac{a}{b} + 2}\cdot\frac{\frac{b}{b}}{\frac{b}{b}} = \frac{a}{a + 2b}.$$

10. $h_0 = 1$

$h_1 = 2^1 - h_0 = 2^1 - 1$

$h_2 = 2^2 - h_1 = 2^2 - (2^1 - 1) = 2^2 - 2^1 + 1$

$h_3 = 2^3 - h_2 = 2^3 - (2^2 - 2^1 + 1)$

$= 2^3 - 2^2 + 2^1 - 1$

$h_4 = 2^4 - h_3 = 2^4 - (2^3 - 2^2 + 2^2 - 1)$

$= 2^4 - 2^3 + 2^2 - 2^1 + 1$

$\vdots$

Conjetura:

$h_n = 2^n - 2^{n-1} + \cdots + (-1)^n \cdot 1$

$= (-1)^n[1 - 2 + 2^2 - \cdots + (-1)^n \cdot 2^n]$

$= (-1)^n[1 + (-2) + (-2)^2 - \cdots + (-2)^n]$ por álgebra básica

$= (-1)^n \left[\dfrac{(-2)^{n+1} - 1}{(-2) - 1}\right]$ por el teorema 5.2.3

$= \dfrac{(-1)^{n+1} \cdot [(-2)^{n+1} - 1]}{(-1) \cdot (-3)}$

$= \dfrac{2^{n+1} - (-1)^{n+1}}{3}$ por álgebra básica

12. $s_0 = 3$

$s_1 = s_0 + 2 \cdot 1 = 3 + 2 \cdot 1$

$s_2 = s_1 + 2 \cdot 2 = [3 + 2 \cdot 1] + 2 \cdot 2$

$= 3 + 2 \cdot (1 + 2)$

$s_3 = s_2 + 2 \cdot 3 = [3 + 2 \cdot (1 + 2)] + 2 \cdot 3$

$= 3 + 2 \cdot (1 + 2 + 3)$

$s_4 = s_3 + 2 \cdot 4 = [3 + 2 \cdot (1 + 2 + 3)] + 2 \cdot 4$

$= 3 + 2 \cdot (1 + 2 + 3 + 4)$

$\vdots$

Conjetura:

$s_n = 3 + 2 \cdot (1 + 2 + 3 + \cdots + (n-1) + n)$

$= 3 + 2 \cdot \dfrac{n(n \Downarrow 1)}{2}$ por el teorema 5.2.2

$= 3 + n(n \Downarrow 1)$ por álgebra básica

14. $x_1 = 1$

$x_2 = 3x_1 + 2 = 3 + 2$

$x_3 = 3x_2 + 3 = 3(3 + 2) + 3 = 3^2 + 3 \cdot 2 + 3$

$x_4 = 3x_3 + 4 = 3(3^2 + 3 \cdot 2 + 3) + 4$

$= 3^3 + 3^2 \cdot 2 + 3 \cdot 3 + 4$

$x_5 = 3x_4 + 5 = 3(3^3 + 3^2 \cdot 2 + 3 \cdot 3 + 4) + 5$

$= 3^4 + 3^3 \cdot 2 + 3^2 \cdot 3 + 3 \cdot 4 + 5$

$x_6 = 3x_5 + 6$

$= 3(3^4 + 3^3 \cdot 2 + 3^2 \cdot 3 + 4 \cdot 3 + 5) + 6$

$= 3^5 + 3^4 \cdot 2 + 3^3 \cdot 3 + 3^2 \cdot 4 + 3 \cdot 5 + 6$

$\vdots$

Conjetura:

$x_n = 3^{n-1} + 3^{n-2} \cdot 2 + 3^{n-3} \cdot 3 + \cdots = 3(n-1) + n$

$= 3^{n-1} + \underbrace{3^{n-2} + 3^{n-2}}_{2 \text{ veces}} + \underbrace{3^{n-3} + 3^{n-3} + 3^{n-3}}_{3 \text{ veces}} +$

$+ \underbrace{3 + 3 + \cdots + 3}_{(n-1) \text{ veces}} + \underbrace{1 + 1 + \cdots + 1}_{n \text{ veces}}$

$= (3^{n-1} + 3^{n-2} + \cdots + 3^2 + 3 + 1)$

$+ (3^{n-2} + 3^{n-3} + \cdots + 3^2 + 3 + 1) + \cdots$

$+ (3^2 + 3 + 1) + (3 + 1) + 1$

$= \dfrac{3^n - 1}{2} + \dfrac{3^{n-1} - 1}{2} + \cdots + \dfrac{3^3 - 1}{2}$

$+ \dfrac{3^2 - 1}{2} + \dfrac{3 - 1}{2}$

$= \frac{1}{2}[(3^n + 3^{n-1} + \cdots + 3^2 + 3) - n]$

$= \frac{1}{2}[3(3^{n-1} + 3^{n-2} + \cdots + 3 + 1) - n]$

$= \frac{1}{2}\left(3\left(\dfrac{3^n - 1}{3 - 1}\right) - n\right)$

$= \frac{1}{4}(3^{n+1} - 3 - 2n)$

18. *Demostración:* Sea d cualquier constante y aceptemos que a_0, a_1, a_2,… sea la sucesión definida recursivamente por $a_k = a_{k-1} + d$ para todos los enteros $k \geq 1$. La propiedad $P(n)$ es la ecuación $a_n = a_0 + nd$. Por inducción matemática demostremos que $P(n)$ es verdadera para todos los enteros $n \geq 0$.

Demostración de que P(0) es verdadero:

Cuando $n = 0$, el lado izquierdo de la ecuación es a_0 y el lado derecho es $a_0 + 0 \cdot d = a_0$, que es igual al lado izquierdo. Así $P(0)$ es verdadero.

Demostración de que para todos los enteros k ≥ 0, si P(k) es verdadera, entonces P(k + 1) también es verdadera:

Supongamos:

$a_k = a_0 + kd$, para algún entero $k \geq 0$.

[Esto es la hipótesis de inducción.]

Debemos demostrar que $a_{k+1} = a_0 + (k+1)d$. Pero

$a_{k+1} = a_k + d$ por definición de $a_0, a_1, a_2, \ldots$

$= [a_0 + kd] + d$ sustituyendo la hipótesis de inducción

$= a_0 + (k+1)d$ por álgebra básica

19. Sea U_n = el número de unidades producidas el día n. Entonces

$U_k = U_{k-1} + 2$ para todos los enteros $k \geq 1$,
$U_0 = 170$.

Así que U_0, U_1, U_2,… es una sucesión aritmética con una constante fija igual a 2. Se tiene que cuando $n = 30$,

$$U_n = U_0 + n \cdot 2 = 170 + 2n = 170 + 2 \cdot 30$$
$$= 230 \text{ unidades.}$$

Así el trabajador debe producir 230 unidades el día 30.

24. $\sum_{k=0}^{20} 5^k = \frac{5^{21} - 1}{4} \cong 1192 \times 10^{14} \cong$ 119 200 000 000 000 $\cong$ 119 trillones de personas (¡Esto es alrededor de 20 000 veces la población actual de la Tierra!)

26. b. *Sugerencia:* Antes una simplificación,
$A_n = 1\,000(1.0025)^n + 200[(1.0025)^{n-1} + (1.0025)^{n-1} + \cdots + (1.0025)^2 + 1.0025 + 1]$.

d. $A_{240} \cong \$67\,481.15$, $A_{480} \cong \$188\,527.05$

e. *Sugerencia:* Use logaritmos para resolver la ecuación $A_n = 10\,000$, en donde A_n es la expresión encontrada (después de la simplificación) en el inciso *b*).

27. a. *Sugerencia:* APR $\cong$ 19.6%

c. *Sugerencia:* aproximadamente dos años.

28. *Demostración:* Dejemos que $a_0, a_1, a_2, \ldots$ sea la sucesión definida recursivamente por $a_0 = 1$ y $a_k = ka_{k-1}$ para todos los enteros $k \geq 1$. Aceptemos que la propiedad $P(n)$ sea la ecuación $a_n = n!$ Demostremos por inducción matemática que $P(n)$ es verdadero para todos los enteros $n \geq 0$.

Demostración de que P(0) es verdadera:

Cuando $n = 0$, el lado derecho de la ecuación es $0! = 1$ y por definición de $a_0, a_1, a_2, \ldots$, el lado izquierdo de la ecuación, a_0, también es 1. Así la propiedad es verdadera para $n = 0$.

Demostración de que para todos los enteros k ≥ 0, si P(k) es verdadero, entonces P(k + 1) también es verdadero:

Supongamos

$a_k = k!$ para algún entero $k \geq 0$.

[Esto es la hipótesis de inducción.]

Debemos demostrar que $a_{k+1} = (k = 1)!$ Pero

$a_{k+1} = (k + 1) \cdot a_k$ por definición de $a_0, a_1, a_2, \ldots$

$= (k + 1) \cdot k!$ sustituyendo la hipótesis de inducción

$= (k + 1)!$ por definición de factorial.

[Así que, si P(k) es verdadero, entonces P(k + 1) también es verdadero.]

30. *Demostración:* Aceptemos que $c_1, c_2, c_3, \ldots$ sea la sucesión definida recursivamente por $c_1 = 1$ y $c_k = 3c_{k-1} + 1$ para todos los enteros $k \geq 2$. Dejemos que la propiedad $P(n)$ sea la ecuación $c_n = \frac{3^n - 1}{2}$. Por inducción matemática, demostremos que $P(n)$ es verdadero para todos los enteros $n \geq 1$.

Demostración de que P(1) es verdadero:

Cuando $n = 1$, el lado derecho de la ecuación es $\frac{3^1 - 1}{2} = \frac{3-1}{2} = 1$ y por definición de $c_1, c_2, c_3, \ldots$, el lado izquierdo de la ecuación, c_1, también es 1. Así la propiedad es verdadera para $n = 1$.

Demostración de que para todos los enteros k ≥ 1, si P(k) es verdadero, entonces P(k + 1) también es verdadero:

Suponga que

$c_k = \frac{3^k - 1}{2}$ para algún entero $k \geq 1$.

[Esto es la hipótesis de inducción].

Debemos demostrar que $c_{k+1} = \frac{3^{k+1} - 1}{2}$. Pero

$c_{k+1} = 3c_k + 1$ por definición de $c_1, c_2, c_3, \ldots$

$= 3\left(\frac{3^k - 1}{2}\right) + 1$ sustituyendo la hipótesis de inducción

$= \frac{3^{k+1} - 3}{2} + \frac{2}{2}$

$= \frac{3^{k+1} - 1}{2}$ por álgebra básica.

35. *Sugerencia:* $2^{k+1} - \frac{2^{k+1} - (-1)^{k+1}}{3}$

$= \frac{3 \cdot 2^{k+1}}{3} - \frac{2^{k+1} - (-1)^{k+1}}{3}$

$= \frac{2 \cdot 2^{k+1} + (-1)^{k+1}}{3} = \frac{2^{k+2} - (-1)^{k+2}}{3}$

37. *Sugerencia:* $[3 + k(k + 1)] + 2(k + 1)$

$= 3 + k^2 + k + 2k + 2 = 3 + [k^2 + 3k + 2]$

$= 3 + (k + 1)(k + 2)$

$= 3 + (k + 1)[(k + 1) + 1]$

39. *Demostración:* Aceptemos que $x_1, x_2, x_3, \ldots$ sea la sucesión definida recursivamente por $x_1 = 1$ y $x_k = 3x_{k-1} + k$ para todos los enteros $k \geq 2$. Dejemos que la propiedad $P(n)$ sea la ecuación $x_n = \frac{3^{n+1} - 2n - 3}{4}$. Demostremos, por inducción matemática, que $P(n)$ es verdadero para todos los enteros $n \geq 1$.

Demostración de que P(1) es verdadera:

Cuando $n = 1$, el lado derecho de la ecuación es $\frac{3^{1+1} - 2 \cdot 1 - 3}{4} = \frac{3^2 - 2 - 3}{4} = 1$ y por definición de $x_1, x_2, x_3, \ldots$, el lado izquierdo de la ecuación, x_1, también es 1. Así $P(1)$ es verdadero.

Demostración de que para todos los enteros k ≥ 1, si P(k) es verdadero, entonces P(k + 1) también es verdadero.

Supongamos que para algún entero $k \geq 0$, $x_k = \frac{3^{k+1} - 2k - 3}{4}$. *[Hipótesis de indución.]* Debemos demostrar que:

$x_{k+1} = \frac{3^{(k+1)+1} - 2(k + 1) - 3}{4}$, o, equivalentemente

$x_{k+1} = \frac{3^{k+2} - 2k - 5}{4}$. Pero

$x_{k+1} = 3x_k + k$ por definición de $x_1, x_2, x_3,$

$= 3\left(\frac{3^{k+1} - 2k - 3}{4}\right) + k + 1$ por hipótesis de inducción

$= \frac{3 \cdot 3^{k+1} - 3 \cdot 2k - 3 \cdot 3}{4} + \frac{4(k + 1)}{4}$

$$= \frac{3^{k+2} - 6k - 9 + 4k + 4}{4}$$
$$= \frac{3^{k+2} - 2k - 5}{4} \qquad \text{por álgebra.}$$

[Esto es lo que se quería demostrar.]

43. **a.** $a_0 = 2$

$$a_1 = \frac{a_0}{2a_0 - 1} = \frac{2}{2\cdot 2 - 1} = \frac{2}{3}$$
$$a_2 = \frac{a_1}{2a_1 - 1} = \frac{\frac{2}{3}}{2\cdot\frac{2}{3} - \frac{3}{3}} = \frac{\frac{2}{3}}{\frac{1}{3}} = 2$$
$$a_3 = \frac{a_2}{2a_2 - 1} = \frac{2}{2\cdot 2 - 1} = \frac{2}{3}$$
$$a_4 = \frac{a_3}{2a_3 - 1} = \frac{\frac{2}{3}}{2\cdot\frac{2}{3} - \frac{3}{3}} = \frac{\frac{2}{3}}{\frac{1}{3}} = 2$$

Conjetura: $a_n = \begin{cases} 2 & \text{si } n \text{ es par} \\ \frac{2}{3} & \text{si } n \text{ es impar} \end{cases}$.

b. *Demostración:* Sea $a_0, a_1, a_2, \ldots$ la sucesión definida recursivamente por $x_0 = 2$ y $a_k = \frac{a_{k-1}}{2a_{k-1} - 1}$ para todos los enteros $k \geq 1$. Dejemos que la propiedad $P(n)$ sea la ecuación:

$$a_n = \begin{cases} 2 & \text{si } n \text{ es par} \\ \frac{2}{3} & \text{si } n \text{ es impar} \end{cases}.$$

Demostremos, por inducción matemática fuerte, que $P(n)$ es verdadera para todos los enteros $n \geq 1$.

Demostración de que P(0) y P(1) son verdaderos:

Los resultados del inciso *a*) muestran que $P(0)$ y $P(1)$ son verdaderas.

Demostración de que para todos los enteros $k \geq 0$, si $P(k)$ es verdadero para todos los enteros i con $0 \leq i \leq k$, entonces $P(k+1)$ también es verdadero:

Sea k cualquier entero con $k \geq 0$ y supongamos que para todos los enteros i con $0 \leq i \leq k$,

$$a_i = \begin{cases} 2 & \text{si } i \text{ es par} \\ \frac{2}{3} & \text{si } i \text{ es impar} \end{cases}. \quad \textit{[Hipótesis de inducción]}$$

Debemos demostrar que

$$a_{k+1} = \begin{cases} 2 & \text{si } k \text{ es par} \\ \frac{2}{3} & \text{si } k \text{ es impar} \end{cases}.$$

Pero

$$a_{k+1} = \frac{a_k}{2a_k - 1} \qquad \text{por definición de } a_0, a_1, a_2, \ldots$$
$$= \begin{cases} \frac{2}{2\cdot 2 - 1} & \text{si } k \text{ es par} \\ \frac{\frac{2}{3}}{2\cdot\frac{2}{3} - 1} & \text{si } k \text{ es impar} \end{cases} \qquad \text{[por hipótesis de inducción]}$$
$$= \begin{cases} \frac{2}{3} & \text{si } k \text{ es par} \\ \frac{\frac{2}{3}}{\frac{1}{3}} & \text{si } k \text{ es impar} \end{cases}$$
$$= \begin{cases} \frac{2}{3} & \text{si } k+1 \text{ es impar} \quad \text{porque } k+1 \text{ es impar cuando } k \text{ es par} \\ 2 & \text{si } k+1 \text{ es par} \quad \text{y } k+1 \text{ es par cuando } k \text{ es impar.} \end{cases}$$

[Que era lo que se quería demostrar.]

45. $v_1 = 1$

$$v_2 = v_{\lfloor 2/2 \rfloor} + v_{\lfloor 3/2 \rfloor} + 2 = v_1 + v_1 + 2$$
$$= 1 + 1 + 2$$
$$v_3 = v_{\lfloor 3/2 \rfloor} + v_{\lfloor 4/2 \rfloor} + 2 = v_1 + v_2 + 2$$
$$= 1 + (1 + 1 + 2) + 2 = 3 + 2\cdot 2$$
$$v_4 = v_{\lfloor 4/2 \rfloor} + v_{\lfloor 5/2 \rfloor} + 2 = v_2 + v_2 + 2$$
$$= (1 + 1 + 2) + (1 + 1 + 2) + 2$$
$$= 4 + 3\cdot 2$$
$$v_5 = v_{\lfloor 5/2 \rfloor} + v_{\lfloor 6/2 \rfloor} + 2 = v_2 + v_3 + 2$$
$$= (3 + 2\cdot 2) + (1 + 1 + 2) + 2$$
$$= 5 + 4\cdot 2$$
$$v_6 = v_{\lfloor 6/2 \rfloor} + v_{\lfloor 7/2 \rfloor} + 2 = v_3 + v_3 + 2$$
$$= (3 + 2\cdot 2) + (3 + 2\cdot 2) + 2$$
$$= 6 + 5\cdot 2$$
$$\vdots$$

Conjetura:

$v_n = n + 2(n-1) = 3n - 2$ para todos los enteros $n \geq 1$

b. *Demostración:* Sea $v_1, v_2, v_3, \ldots$ la secuencia definida recursivamente por $v_1 = 1$ y $v_k = v_{\lfloor k/2 \rfloor} + v_{\lfloor (k+1)/2 \rfloor} + 2$ para todos los enteros $k \geq 1$. Sea la propiedad $P(n)$ la ecuación

$$v_n = 3n - 2.$$

Demostremos por inducción matemática fuerte que $P(n)$ es verdadera para todos los enteros $n \geq 1$.

Demostración de que P(1) es verdadero:

Cuando $n = 1$, el lado derecho de la ecuación es $3\cdot 1 - 2 = 1$, que es igual a v_1 por definición de $v_1, v_2, v_3, \ldots$ Así $P(1)$ es verdadera.

Demostración de que para todos los enteros $k \geq 1$, si $P(i)$ es verdadera para todos los enteros i con $0 \leq i \leq k$, entonces $P(k+1)$ también es verdadera:

Sea k cualquier entero con $k \geq 1$ y supongamos que para todos los enteros i con $1 \leq i \leq k$, $v_i = 3i - 2$.

[Esto es la hipótesis de inducción.] Debemos demostrar que $v_{k+1} = 3(k+1) - 2 = 3k + 1$.

$$v_{k+1} = v_{\lfloor (k+1)/2 \rfloor} + v_{\lfloor (k+2)/2 \rfloor} + 2 \qquad \text{por definición de } v_1, v_2, v_3, \ldots$$
$$= \left(3\left\lfloor \frac{k+1}{2} \right\rfloor - 2\right) + \left(3\left\lfloor \frac{k+2}{2} \right\rfloor - 2\right) + 2$$

$$= 3\left(\left\lfloor \frac{k+1}{2} \right\rfloor + \left\lfloor \frac{k+2}{2} \right\rfloor\right) - 2$$

$$= \begin{cases} 3\left(\frac{k}{2} + \frac{k+2}{2}\right) - 2 & \text{si } k \text{ es par} \\ 3\left(\frac{k+1}{2} + \frac{k+1}{2}\right) - 2 & \text{si } k \text{ es impar} \end{cases}$$

$$= 3\left(\frac{2k+2}{2}\right) - 2$$

$$= 3(k+1) - 2$$

$$= 3k + 1 \qquad \text{por las leyes del álgebra.}$$

[Que era lo que se quería demostrar.]

46. *Sugerencia:* Demuestre que para todos los enteros $n \geq 0$, $s_{2n} = 2^n$ y $s_{2n+1} = 2^{n+1}$. Después combine esas fórmulas utilizando la función techo para obtener que $s_n = 2^{\lceil n/2 \rceil}$.

48. a. *Sugerencia:* $w_n = \begin{cases} \left(\frac{n+1}{2}\right)^2 & \text{si } n \text{ es impar} \\ \frac{n}{2}\left(\frac{n}{2}+1\right) & \text{si } n \text{ es par} \end{cases}$,

49. a. *Sugerencia:* Exprese la respuesta empleando la sucesión de Fibonacci.

50. La sucesión no satisface la fórmula. De acuerdo a la fórmula, $a_4 = (4-1)^2 = 9$. Pero por la definición de la sucesión, $a_1 = 0$, $a_2 = 2 \cdot 0 + (2+1) = 1$, $a_3 = 2 \cdot 1 + (3-1) = 4$ y así $a_4 = 2 \cdot 4 + (4-1) = 11$. Por tanto, la sucesión no satisface la fórmula para $n = 4$.

52. a. *Sugerencia:* El número máximo de regiones se obtiene cuando cada línea adicional cruza a todas las líneas previas, pero no en puntos que ya son la intersección de dos líneas. Cuando se agrega una nueva línea, ésta divide en dos partes a cada región por la que pasa. El número de regiones con una nueva línea agregada es uno más que el número de líneas que ella cruza.

53. *Sugerencia:* ¡La respuesta implica a los números de Fibonacci!

Sección 5.8

1. (a), (d) y (f).

3. a. $\left.\begin{aligned} a_0 &= C \cdot 2^0 + D = C + D = 1 \\ a_1 &= C \cdot 2^1 + D = 2C + D = 3 \end{aligned}\right\}$

$$\Leftrightarrow \left\{\begin{aligned} D &= 1 - C \\ 2C + (1-C) &= 3 \end{aligned}\right\} \Leftrightarrow \left\{\begin{aligned} C &= 2 \\ D &= -1 \end{aligned}\right.$$

$a_2 = 2 \cdot 2^2 + (-1) = 7$

4. a. $\left.\begin{aligned} b_0 &= C \cdot 3^0 + D \cdot (-2)^0 = C + D = 0 \\ b_1 &= C \cdot 3^1 + D \cdot (-2)^1 = 3C - 2D = 5 \end{aligned}\right\}$

$$\Leftrightarrow \left\{\begin{aligned} D &= -C \\ 3C - 2(-C) &= 5 \end{aligned}\right\} \Leftrightarrow \left\{\begin{aligned} C &= 1 \\ D &= -1 \end{aligned}\right.$$

$b_2 = 3^2 + (-1)(-2)^2 = 9 - 4 = 5$

5. *Demostración:* Dado que $a_n = C \cdot 2^n + D$, entonces para cualquier elección de C, D y el entero $k > 2$,

$$a_k = C \cdot 2^k + D,$$
$$a_{k-1} = C \cdot 2^{k-1} + D,$$
$$a_{k-2} = C \cdot 2^{k-2} + D.$$

Así que

$$\begin{aligned} 3a_{k-1} - 2a_{k-2} &= 3(C \cdot 2^{k-1} + D) - 2(C \cdot 2^{k-2} + D) \\ &= 3C \cdot 2^{k-1} + 3D - 2C \cdot 2^{k-2} - 2D \\ &= 3C \cdot 2^{k-1} - C \cdot 2^{k-1} + D \\ &= 2C \cdot 2^{k-1} + D \\ &= C \cdot 2^k + D = a_k. \end{aligned}$$

8. a. Si para todo $k > 2$, $t^k = 2t^{k-1} + 3t^{k-2}$ y $t \neq 0$, entonces $t^2 = 2t + 3$ *[dividiendo por t^{k-2}]* y así $t^2 - 2t - 3 = 0$. Pero $t^2 - 2t - 3 = (t-3)(t+1)$; entonces $t = 3$ o $t = -1$.

b. Se tiene de *a)* y del teorema para raíces distintas, que para algunas constantes C y D, a_0, a_1, a_2,… se satisface la ecuación

$$a_n = C \cdot 3^n + D \cdot (-1)^n \quad \text{para todos los enteros } n \geq 0.$$

Como $a_0 = 1$ y $a_1 = 2$, entonces

$$\left.\begin{aligned} a_0 &= C \cdot 3^0 + D \cdot (-1)^0 = C + D = 1 \\ a_1 &= C \cdot 3^1 + D \cdot (-1)^1 = 3C - D = 2 \end{aligned}\right\}$$

$$\Leftrightarrow \left\{\begin{aligned} D &= 1 - C \\ 3C - (1-C) &= 2 \end{aligned}\right\}$$

$$\Leftrightarrow \left\{\begin{aligned} D &= 1 - C \\ 4C - 1 &= 2 \end{aligned}\right\}$$

$$\Leftrightarrow \left\{\begin{aligned} C &= 3/4 \\ D &= 1/4 \end{aligned}\right.$$

Así $a_n = \frac{3}{4}(3^n) + \frac{1}{4}(-1)^n$ para todos los enteros $n \geq 0$.

11. *Ecuación característica:* $t^2 - 4 = 0$. Como $t^2 - 4 = (t-2)(t+2)$, entonces $t = 2$ y $t = -2$ son las raíces. Por el teorema para raíces distintas, para algunas constantes C y D

$$d_n = C \cdot (2^n) + D \cdot (-2)^n \quad \text{para todos los enteros } n \geq 0.$$

Como $d_0 = 1$ y $d_1 = -1$, entonces

$$\left.\begin{aligned} d_0 &= C \cdot 2^0 + D \cdot (-2)^0 = C + D = 1 \\ d_1 &= C \cdot 2^1 + D \cdot (-2)^1 = 2C - 2D = -1 \end{aligned}\right\}$$

$$\Leftrightarrow \left\{\begin{aligned} D &= 1 - C \\ 2C - 2(1-C) &= -1 \end{aligned}\right\}$$

$$\Leftrightarrow \left\{\begin{aligned} D &= 1 - C \\ 4C - 2 &= -1 \end{aligned}\right\}$$

$$\Leftrightarrow \left\{\begin{aligned} C &= \tfrac{1}{4} \\ D &= \tfrac{3}{4} \end{aligned}\right.$$

Así, $d_n = \frac{1}{4}(2^n) + \frac{3}{4}(-2)^n$ para todos los enteros $n \geq 0$.

13. *Ecuación característica:* $t^2 - 2t + 1 = 0$. Por la fórmula cuadrática,

$$t = \frac{2 \pm \sqrt{4 - 4 \cdot 1}}{2} = \frac{2}{2} = 1.$$

Por el teorema de raíz única, para algunas constantes C y D

$$\begin{aligned} r_n &= C\cdot(1^n) + Dn\cdot(1^n) \\ &= C + n\,D \text{ para todos los enteros } n \geq 0. \end{aligned}$$

Como $r_0 = 1$ y $r_1 = 4$, entonces

$$\left.\begin{aligned} r_0 &= C + 0\cdot D = C = 1 \\ r_1 &= C + 1\cdot D = C + D = 4 \end{aligned}\right\} \Leftrightarrow \left\{\begin{aligned} C &= 1 \\ 1 + D &= 4 \end{aligned}\right\}$$

$$\Leftrightarrow \left\{\begin{aligned} C &= 1 \\ D &= 3 \end{aligned}\right.$$

Así $r_n = 1 + 3n$ para todos los enteros $n \geq 0$.

16. *Sugerencia:* Para todos los enteros $n \geq 0$,

$$s_n = \frac{\sqrt{3}+2}{2\sqrt{3}}\left(1+\sqrt{3}\right)^n + \frac{\sqrt{3}-2}{2\sqrt{3}}\left(1-\sqrt{3}\right)^n.$$

19. *Demostración:* Supongamos que r, s, a_0 y a_1 son números con $r \neq s$. Considere el sistema de ecuaciones

$$\begin{aligned} C + D &= a_0 \\ Cr + Ds &= a_1. \end{aligned}$$

Resolviendo para D y sustituyendo, encontramos que

$$\begin{aligned} D &= a_0 - C \\ Cr + (a_0 - C)s &= a_1. \end{aligned}$$

Así que

$$C(r - s) = a_1 - a_0 s.$$

Como $r \neq s$, ambos lados pueden dividirse por $r - s$. Entonces el sistema dado de ecuaciones tiene la solución única

$$C = \frac{a_1 - a_0 s}{r - s}$$

y

$$\begin{aligned} D = a_0 - C &= a_0 - \frac{a_1 - a_0 s}{r - s} \\ &= \frac{a_0 r - a_0 s - a_1 + a_0 s}{r - s} = \frac{a_0 r - a_1}{r - s}. \end{aligned}$$

Solución alternativa: Como el determinante del sistema es $1\cdot s - r\cdot 1 = s - r$ y $r \neq s$, entonces el sistema dado tiene determinante distinto de cero y por tanto la solución es única.

21. *Sugerencia:* Use inducción matemática fuerte. Primero observe que la fórmula es válida para $n = 0$ y $n = 1$. Para demostrar el paso inductivo, suponga que para algún $k \geq 2$, la fórmula se cumple para toda i con $0 \leq i \leq k$. Entonces demuestre que la fórmula es válida para $k + 1$. Como un modelo, utilice la demostración del teorema 5.8.3 (teorema para las raíces distintas).

22. La ecuación característica es $t^2 - 2t + 2 = 0$. Por la fórmula cuadrática, sus raíces son

$$t = \frac{2 \pm \sqrt{4-8}}{2} = \frac{2 \pm 2i}{2} = \begin{cases} 1+i \\ 1-i \end{cases}.$$

Por el teorema para raíces distintas, para algunas constantes C y D

$$a_n = C(1+i)^n + D(1-i)^n$$

para todos los enteros $n \geq 0$.

Como $a_0 = 1$ y $a_1 = 2$, entonces

$$\begin{aligned} a_0 &= C(1+i)^0 + D(1-i)^0 = C + D = 1 \\ a_1 &= C(1+i)^1 + D(1-i)^1 \\ &= C(1+i) + D(1-i) = 2 \\ &\Leftrightarrow \left\{\begin{aligned} D &= 1 - C \\ C(1+i) + (1-C)(1-i) &= 2 \end{aligned}\right\} \\ &\Leftrightarrow \left\{\begin{aligned} D &= 1 - C \\ C(1+i-1+i) + 1 - i &= 2 \end{aligned}\right\} \\ &\Leftrightarrow \left\{\begin{aligned} D &= 1 - C \\ C(2i) &= 1 + i \end{aligned}\right\} \\ &\Leftrightarrow \left\{\begin{aligned} D &= 1 - C \\ C &= \frac{1+i}{2i} = \frac{1+i}{2i}\cdot\frac{i}{i} = \frac{i-1}{-2} = \frac{1-i}{2} \end{aligned}\right\} \\ &\Leftrightarrow \left\{\begin{aligned} D &= 1 - \frac{1-i}{2} = \frac{2-1+i}{2} = \frac{1+i}{2} \\ C &= \frac{1-i}{2} \end{aligned}\right\} \end{aligned}$$

Así para todos los enteros $n \geq 0$,

$$a_n = \left(\frac{1-i}{2}\right)(1+i)^n + \left(\frac{1+i}{2}\right)(1-i)^n.$$

Sección 5.9

1. a. 1) p, q, r y s son expresiones booleanas de I.
2) $\sim s$ es una expresión booleana por (1) y II(c).
3) $(r \vee \sim s)$ es una expresión booleana por (1), (2) y II(b).
4) $(q \wedge (r \vee \sim s))$ es una expresión booleana por (1), (3) y II(a).
5) $\sim p$ es una expresión booleana por (1) y II(c).
6) $(\sim p \vee (q \wedge (r \vee \sim s)))$ es una expresión booleana por (4), (5) y II(b).

2. a. 1) $\epsilon \in S$ por I.
2) $a = \epsilon a \in S$ por (1) y II(a).
2) $aa \in S$ por (2) y II(a).
2) $aab \in S$ por (3) y II(b).

3. a. 1) *MI* está en el sistema *MIU* por I.
2) *MII* está en el sistema *MIU* por (1) y II(b).
3) *MIIII* está en el sistema *MIU* por (3) y II(b).
4) *MIIIIIII* está en el sistema *MIU* por (3) y II(b).
5) *MIUIII* está en el sistema *MIU* por (4) y II(c).
6) *MIUUI* está en el sistema *MIU* por (5) y II(c).
7) *MIUI* está en el sistema *MIU* por (6) y II(d).

4. a. 1) 2, 0.3, 4.2 y 7 son expresiones aritméticas por I.
2) $(0.3 - 4.2)$ es una expresión aritmética por (1) y II(d).
3) $(2\cdot(0.3 - 4.2))$ es una expresión aritmética por (1), (2) y II(e).

4) (-7) es una expresión aritmética por (1) y II(b).
5) $((2\cdot(0.3-4.2))+(-7))$ es una expresión aritmética por (3), (4) y II(c).

5. *Demostración por inducción estructural:* Dejemos que la propiedad sea la siguiente frase: La cadena termina en un 1.

Demostración de que cada objeto en la BASE para S satisface la propiedad:

El único objeto en la base es 1 y la cadena finaliza en un 1.

Demostración de que para cada regla en la RECURSIÓN para S, si la regla se aplica a un objeto en S que satisface la propiedad, entonces los objetos definidos por la regla también satisfacen la propiedad:

La recursión para S consiste de dos reglas denotadas por II(a) y II(b). Supongamos que s es una cadena en S que termina en un 1. En el caso en que la regla II(a) se aplique a s, el resultado es la cadena $1s$, que también finaliza en un 1. En el caso en que la regla II(b) sea aplicada a s, el resultado es la cadena $1s$, que también termina en un 1. Así, cuando cada regla en la RECURSIÓN se aplique a una cadena en S que termine en un 1, el resultado también es una cadena finalizando en un 1.

7. *Demostración por inducción estructural:* Dejemos que la propiedad sea la siguiente frase: En la cadena, a aparece un número par de veces.

Demostración de que cada objeto en la BASE para S satisface la propiedad:

El único objeto en la base es ϵ, en que a está 0 veces. Como 0 es un número par, entonces en ϵ a existe un número par de veces.

Demostración de que para cada regla en la RECURSIÓN para S, si la regla se aplica a un objeto en S que satisface la propiedad, entonces los objetos definidos por la regla también satisfacen la propiedad:

La recursión para S consiste de cuatro reglas denotadas por II(a), II(b), II(c) y II(d). Supongamos que s es una cadena en S que contiene un número par de veces a a. En el caso en que la regla II(a) o II(b) se aplique a s, el resultado es la cadena bs o la cadena sb, en las que a y s aparecen el mismo número de veces y por tanto un número par de a. En el caso en que la regla II(c) o II(d) sea aplicada a s, el resultado es la cadena aas o la cadena saa, en las cuales a aparece dos veces más que el número de a en s. Como dos más cualquier entero par da un entero par, entonces aas y saa contienen un número par de a. Así cuando cada regla en la RECURSIÓN se aplica a una cadena en S que contiene un número par de a, el resultado también es una cadena en que a aparece un número par de veces.

9. *Sugerencia:* Aceptemos que la propiedad sea la siguiente frase: La cadena representa un entero impar. En la notación decimal, una cadena representa un entero impar si y sólo si, termina en 1, 3, 5, 7 o 9.

10. *Sugerencia:* Por los resultados sobre divisibilidad del capítulo 3 (los ejercicios 15 y 16 de la sección 3.3), si s y t son divisibles por 5, entonces también lo son $s+t$ y $s-t$.

12. *Sugerencia:* ¿Es múltiplo de 3 el número de I en una cadena en el sistema *MIU*? ¿Cómo se afectan las reglas de la II(a) a la (d) al número de I en una cadena?

13. a. 1) ( ) está en P por I.
2) (( )) está en P por (1) y II(a).
3) ( )(( )) está en P por (1), (2) y II(b).

14. a. Esta estructura no está en P. Defina una función $f: P \to Z$ como sigue: Para cada estructura de paréntesis S en P, sea

$$f(S) = \begin{bmatrix}\text{el número de paréntesis}\\ \text{izquierdos en } S\end{bmatrix} - \begin{bmatrix}\text{el número de paréntesis}\\ \text{derechos en } S\end{bmatrix}.$$

Observe que para todo S en P, $f(S)=0$. Para ver por qué, use el razonamiento de inducción estructural:

1. El elemento base de P es enviado por f a 0: $f[(\,)]=0$ *[ya que existe un paréntesis izquierdo y un derecho en ( )]*.
2. Para todo $S \in P$, si $f[S]=0$ entonces $f[(S)]=0$ *[ya que si $k-m=0$ entonces $(k+1)-(m+1)=0$]*.
3. Para toda S y T en P, si $f[S]=0$ y $f[T]=0$, entonces $f[ST]=0$ *[porque si $k-m=0$ y $n-p=0$, entonces $(k+n)-(m+p)=0$]*.

Los puntos (1), (2) y (3) muestran que todas las estructuras de paréntesis obtenibles de la estructura base ( ) por aplicación repetida de II(a) y II(b) son enviadas a 0 por f. Pero por III (la condición de restricción), no hay otros elementos de P aparte de los obtenibles del elemento base por aplicación de II(a) y II(b). Así que $f(S)=0$ para toda $S \in P$.

Ahora si $(\,)((\,)$ estuviera en P, entonces sería enviado a 0 por f. Pero $f[(\,)((\,)]=3-2=1\neq 0$. Por tanto, $(\,)((\,) \notin P$.

15. Sea S el conjunto de todas las cadenas de 0 y 1 con el mismo número de 0 y 1. Lo siguiente es una definición recursiva de S.

I. BASE: La cadena nula $\epsilon \in S$.

II. RECURSIÓN: si $s \in S$, entonces

a. $01s \in S$ **b.** $s01 \in S$ **c.** $10s \in S$
d. $s10 \in S$ **e.** $0s1 \in S$ **f.** $1s0 \in S$

III. RESTRICCIÓN: No hay elementos de S excepto los obtenidos de I y II.

17. Sea T el conjunto de todas las cadenas de a y b que contienen un número impar de a. Lo siguiente es una definición recursiva de T.

I. BASE: El $a \in T$.

II. RECURSIÓN: Si $t \in T$, entonces

a. $bt \in T$ **b.** $tb \in T$ **c.** $aat \in T$
d. $ata \in T$ **e.** $taa \in T$

III. RESTRICCIÓN: No hay elementos de T excepto los obtenidos de I y II.

19. a.
$$\begin{aligned} M(86) &= M(M(97)) && \text{ya que } 86 \le 100\\ &= M(M)M(108))) && \text{ya que } 97 \le 100\\ &= M(M)98)) && \text{ya que } 108 > 100\\ &= M(M)M(109))) && \text{ya que } 98 < 100\\ &= M(M)99)) && \text{ya que } 109 > 100\\ &= M(91) && \text{por el ejemplo 5.9.6} \end{aligned}$$

21. a.
$$\begin{aligned} A(1,1) &= A(0, A)1, 0)) && \text{por (5.9.3) con } m = 1 \text{ y } n = 1 \\ &= A(1,0) + 1 && \text{por (5.9.1) con } n = A(1,0) \\ &= A(0,1) + 1 && \text{por (5.9.2) con } m = 1 \\ &= (1+1) + 1 && \text{por (5.9.1) con } n = 1 \\ &= 3 \end{aligned}$$

Solución alternativa:

$$\begin{aligned} A(1,1) &= A(0, A(1,0)) && \text{por (5.9.3) con } m = 1 \text{ y } n = 1, \\ &= A(0, A(0,1)) && \text{por (5.9.2) con } m = 1 \\ &= A(0,2) && \text{por (5.9.1) con } n = 1 \\ &= 3 && \text{por (5.9.1) con } n = 2 \end{aligned}$$

22. a. *Demostración por inducción matemática:* Aceptemos que la propiedad $P(n)$ sea la ecuación $A(1, n) = n + 2$.

Demostración de que P(0) es verdadera:

Cuando $n = 0$,

$$\begin{aligned} A(1,n) &= A(1,0) && \text{sustituyendo} \\ &= A(0,1) && \text{por (5.9.2)} \\ &= 1 + 1 && \text{por (5.9.1)} \\ &= 2. \end{aligned}$$

Por otro lado, $n + 2 = 0 + 2$, entonces $A(1, n) = n + 2$ para $n = 0$.

Demostración de que para todos los enteros $k \geq 1$, si P(k) es verdadero, entonces P(k + 1) también es verdadero.

Sea k un entero con $k \geq 1$ y supongamos que $P(k)$ es verdadero. En otras palabras, aceptemos que $A(1, k) = k + 2$. *[Esto es la hipótesis de inducción.]* Debemos demostrar que $P(k + 1)$ es verdadero. Es decir, debemos demostrar que $A(1, k + 1) = (k + 1) + 2 = k + 3$. Pero

$$\begin{aligned} A(1,k+1) &= A(0, A(1,k)) && \text{por (5.9.3)} \\ &= A(1,k) + 1 && \text{por (5.9.1)} \\ &= (k+2) + 1 && \text{por la hipótesis de inducción} \\ &= k + 3. \end{aligned}$$

[Esto es lo que se quería demostrar.]

[Sea han demostrado los pasos básico e inductivo, entonces concluimos que la ecuación es válida para todos los enteros n no-negativos.]

24. Suponga que F es una función. Entonces $F(1) = 1$, $F(2) = F(1) = 1$, $F(3) = 1 + F(5 \cdot 3 - 9) = 1 + F(6) = 1 + F(3)$. Restando $F(3)$ del extremo izquierdo y del extremo derecho de esta secuencia de ecuaciones se obtiene $1 = 0$, que es falso. Así que F no es una función.

Sección 6.1

1. a. $A = \{2, \{2\}, (\sqrt{2})^2\} = \{2, \{2\}, 2\} = \{2, \{2\}\}$ y $B = \{2, \{2\}, \{\{2\}\}\}$. Así $A \subseteq B$ porque cada elemento en A está en B, pero $B \nsubseteq A$ porque $\{\{2\}\} \in B$ y $\{\{2\}\} \notin A$. También A es un subconjunto propio de B porque $\{\{2\}\}$ está en B pero no en A.

c. $A = \{\{1, 2\},\{2, 3\}\}$ y $B = \{1, 2, 3\}$. Así $A \nsubseteq B$ porque $\{1, 2\} \in A$ y $\{1, 2\} \notin B$. También $B \nsubseteq A$ porque $1 \in B$ y $1 \notin A$.

e. $A = \left\{\sqrt{16}, \{4\}\right\} = \{4, \{4\}\}$ y $B = \{4\}$. Entonces $B \subseteq A$ porque el único elemento en B es 4 y B está en A, pero $A \nsubseteq B$ porque $\{4\} \in A$ y $\{4\} \notin B$. También B es un subconjunto propio de A porque $\{4\}$ está en A pero no en B.

2. ***Demostración de que B ⊆ A:***

Supongamos que x es un elemento particular de B pero arbitrariamente elegido.

[Debemos demostrar que $x \in A$. Por definición de A, esto significa que debemos demostrar que $x = 2 \cdot$(algún entero).]

Por definición de B, existe un entero b tal que $x = 2b - 2$.

[Dado que $x = 2b - 2$, ¿podemos expresar a x como $2 \cdot$(algún entero)? Es decir, ¿existe un entero, digamos a, tal que $2b - 2 = 2a$? Resolver para a para obtener que $a = b - 1$. Compruebe que esto funciona.]

Sea $a = b - 1$.

[Primero compruebe que a es un entero.]

Entonces a es un entero porque es la diferencia de enteros.

[Después compruebe que $x = 2a$.]

También $2a = 2(b - 1) = 2b - 2 = x$.

Así, por definición de A, x es un elemento de A,

[que era lo que se quería demostrar].

3. a. No. $R \nsubseteq T$ porque existen elementos en R que no están en T. Por ejemplo, el número 2 está en R pero no está en T porque 2 no es divisible por 6.

b. Sí. $T \subseteq R$ porque cada número divisible por 6 es divisible entre 2. Para ver por qué esto es así, suponga que n es cualquier número divisible por 6. Entonces $n = 6m$ para algún entero m. Como $6m = 2(3m)$ y $3m$ es un entero (que es un producto de enteros), se tiene que $n = 2 \cdot$(algún entero) y, en consecuencia, que n es divisible por 2.

5. a. $C \subseteq D$ *Demostración: [Demostraremos que cada elemento de C está en D.]* Supongamos que n es cualquier elemento de C. Entonces $n = 6r - 5$ para algún entero r. Sea $s = 2r - 2$. Entonces s es un entero (porque productos y diferencias de enteros son enteros) y

$$3s + 1 = 3(2r - 2) + 1 = 6r - 6 + 1 = 6r - 5,$$

que es igual a n. Así n satisface la condición para estar en D. Por tanto, cada elemento de C está en D.

b. $D \nsubseteq C$ porque hay elementos de D que no están en C. Por ejemplo, 4 está en D porque $4 = 3 \cdot 1 + 1$. Pero 4 no está en C porque si estuviera, entonces $4 = 6r - 5$ para algún entero r, que implicaría que $9 = 6r$, o, equivalentemente, que $r = 3/2$ y esto contradice el hecho de que r es un entero.

6. c. *Esbozo de demostración de que $B \subseteq C$:* Si r es cualquier elemento de B entonces existe un entero b tal que $r = 10b - 3$. Para demostrar que r está en C, debe demostrar que hay un entero c tal que $r = 10c + 7$. En breve esbozo, suponga que c existe y use la información de que $10b - 3$ tendría que ser igual a $10c + 7$ para así deducir el único valor posible de c.

Entonces demuestre que este valor es 1) un entero y 2) que satisface la ecuación $r = 10c + 7$, lo que le permitirá concluir que r es un elemento de C.

Esbozo de demostración de que $C \subseteq B$: Si s es cualquier elemento de C entonces existe un entero c tal que $s = 10c + 7$. Para demostrar que s está en B, debe demostrar que existe un entero b tal que $s = 10c - 3$. En breve esbozo, suponga que b existe y use la información de que $10c + 7$ tendría que ser igual a $10b - 3$ para deducir el único valor posible para b. Después demuestre que este valor es 1) un entero y 2) que satisface la ecuación $s = 10b - 3$, lo que le permitirá concluir que s es un elemento de B.

8. a. El conjunto de todas las x en U tales que x está en A y x está en B. La notación corta es $A \cap B$.

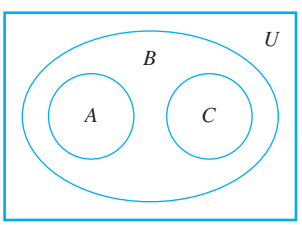
9. a. $x \notin A$ y $x \notin B$

10. a. $\{1, 3, 5, 6, 7, 9\}$ **b.** $\{3, 9\}$
c. $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ **d.** $\emptyset$ **e.** $\{1, 5, 7\}$

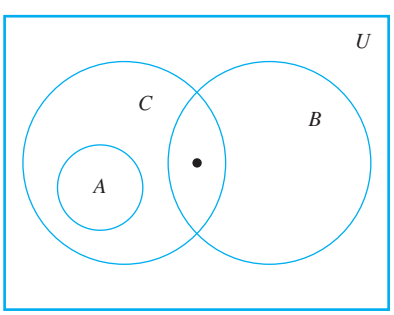
11. a. $A \cup B = \{x \in \mathbf{R} \mid 0 < x < 4\}$
b. $A \cap B = \{x \in \mathbf{R} \mid 1 \le x \le 2\}$
c. $A^c = \{x \in \mathbf{R} \mid x \le 0 \text{ o } x > 2\}$
d. $A \cup C = \{x \in \mathbf{R} \mid 0 < x \le 2 \text{ o } 3 \le x < 9\}$
e. $A \cap C = \emptyset$
f. $B^c = \{x \in \mathbf{R} \mid x < 1 \text{ o } x \ge 4\}$
g. $A^c \cap B^c = \{x \in \mathbf{R} \mid x \le 0 \text{ o } x \ge 4\}$
h. $A^c \cup B^c = \{x \in \mathbf{R} \mid x < 1 \text{ o } x > 2\}$
i. $(A \cap B)^c = \{x \in \mathbf{R} \mid x < 1 \text{ o } x > 2\}$
j. $(A \cup B)^c = \{x \in \mathbf{R} \mid x \le 0 \text{ o } x \ge 4\}$

13. b. Falso. Muchos números reales negativos no son racionales. Por ejemplo, $-\sqrt{2} \in \mathbf{R}$ pero $-\sqrt{2} \notin \mathbf{Q}$.
d. Falso. $0 \in \mathbf{Z}$ pero $0 \notin \mathbf{Z}^- \cup \mathbf{Z}^+$.

14. a.

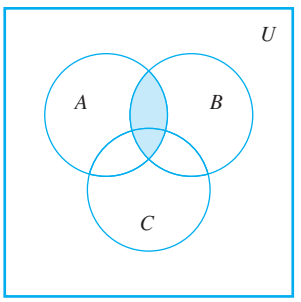


15. a.



16. a. $A \cup (B \cap C) = \{a, b, c\}$, $(A \cup B) \cap C = \{b, c\}$, y $(A \cup B) \cap (A \cup C) = \{a, b, c, d\} \cap \{a, b, c, e\} = \{a, b, c\}$.
Así que $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

17. a.



18. a. El número 0 no está en $\emptyset$ porque $\emptyset$ no tiene elementos.
b. No. El conjunto de la izquierda es el conjunto vacío; no tiene elementos. El conjunto de la derecha es un conjunto con un elemento, a saber, $\emptyset$.

19. $A_1 = \{1, 1^2\} = \{1\}$, $A_2 = \{2, 2^2\} = \{2, 4\}$, $A_3 = \{3, 3^2\} = \{3, 9\}$, $A_4 = \{4, 4^2\} = \{4, 16\}$
a. $A_1 \cup A_2 \cup A_3 \cup A_4 = \{1\} \cup \{2, 4\} \cup \{3, 9\} \cup \{4, 16\} = \{1, 2, 3, 4, 9, 16\}$
b. $A_1 \cap A_2 \cap A_3 \cap A_4 = \{1\} \cap \{2, 4\} \cap \{3, 9\} \cap \{4, 16\} = \emptyset$
c. A_1, A_2, A_3 y A_4, no son mutuamente disjuntos porque $A_2 \cap A_4 = \{4\} = \emptyset$.

21. $C_0 = \{0, -0\} = \{0\}$, $C_1 = \{1, -1\}$, $C_1 = \{2, -2\}$, $C_1 = \{3, -3\}$, $C_1 = \{4, -4\}$
a. $\bigcup_{i=0}^{4} C_i = \{0\} \cup \{1, -1\} \cup \{2, -2\} \cup \{3, -3\} \cup \{4, -4\} = \{-4, -3, -2, -1, 0, 1, 2, 3, 4\}$
b. $\bigcap_{i=0}^{4} C_i = \{0\} \cap \{1, -1\} \cap \}2, -2\} \cap \{3, -3\} \cap \{4, -4\} = \emptyset$
c. $C_0, C_1, C_2, \ldots$ son mutuamente disjuntos porque cualesquiera dos de los conjuntos no tienen elementos en común.
d. $\bigcup_{i=0}^{n} C_i = \{-n, -(n-1), \ldots, -2, -1, 0, 1, 2, \ldots, (n-1), n\}$
e. $\bigcap_{i=0}^{n} C_i = \emptyset$
f. $\bigcup_{i=0}^{\infty} C_i = \mathbf{Z}$, el conjunto de todos los enteros,
g. $\bigcap_{i=0}^{\infty} C_i = \emptyset$

22. $D_0 = [-0, 0] = \{0\}$, $D_1 = [-1, 1]$, $D_2 = [-2, 2]$, $D_3 = [-3, 3]$, $D_4 = [-4, 4]$
a. $\bigcup_{i=0}^{4} D_i = \{0\} \cup [-1, 1] \cup [-2, 2] \cup [-3, 3] \cup [-4, 4] = [-4, 4]$
b. $\bigcap_{i=0}^{4} D_i = \{0\} \cup [-1, 1] \cup [-2, 2] \cup [-3, 3] \cup [-4, 4] = \{0\}$
c. D_0, D_1, $D_2, \ldots$ no son mutuamente disjuntos. En efecto, cada $D_k \subseteq D_{k+1}$.
d. $\bigcup_{i=0}^{n} D_i = [-n, n]$
e. $\bigcap_{i=0}^{n} D_i = \{0\}$

f. $\bigcup_{i=0}^{\infty} D_i = \mathbf{R}$, el conjunto de todos los números reales

g. $\bigcap_{i=0}^{\infty} D_i = \{0\}$

24. $W_0 = (0, \infty)$, $W_1 = (1, \infty)$, $W_2 = (2, \infty)$, $W_3 = (3, \infty)$, $W_4 = (4, \infty)$

a. $\bigcup_{i=0}^{4} W_i = (0, \infty) \cup (1, \infty) \cup (2, \infty) \cup (3, \infty) \cup (4, \infty) = (0, \infty)$

b. $\bigcap_{i=0}^{4} W_i = (0, \infty) \cap (1, \infty) \cap (2, \infty) \cap (3, \infty) \cap (4, \infty) = (4, \infty)$

c. $W_0, W_1, W_2, \ldots$ no son mutuamente disjuntos. En efecto $W_{k+1} \subseteq W_k$ para todos los enteros $k \geq 0$.

d. $\bigcup_{i=0}^{n} W_i = (0, \infty)$

e. $\bigcap_{i=0}^{n} W_i = (n, \infty)$

f. $\bigcup_{i=0}^{\infty} W_i = (0, \infty)$

g. $\bigcap_{i=0}^{\infty} W_i = \emptyset$

27. a. No. El elemento d está en dos de los conjuntos.
b. No. Ningún conjunto contiene al 6.

28. Sí. Cada entero es par o impar, y ningún entero es par e impar.

31. a. $A \cap B = \{2\}$, entonces $\mathscr{P}(A \cap B) = \{\emptyset, \{2\}\}$.
b. $A = \{1, 2\}$, entonces $\mathscr{P}(A) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$.
c. $A \cup B = \{1, 2, 3\}$, entonces $\mathscr{P}(A \cup B) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$.
d. $A \times B = \{(1, 2), (1, 3), (2, 2), (2, 3)\}$, entonces
$\mathscr{P}(A \times B) = \{\emptyset, \{(1, 2)\}, \{(1, 3)\}, \{(2, 2)\}, \{(2, 3)\},$
$\{(1, 2)\ (1, 3)\}, \{(1, 2), (2, 2)\},$
$\{(1, 2)\ (2, 3)\}, \{(1, 3), (2, 2)\}, \{(1, 3), (2, 3)\},$
$\{(2, 2), (2, 3)\}, \{(1, 2), (1, 3)\ (2, 2)\},$
$\{(1, 2)\ (1, 3)\ (2, 3)\},$
$\{(1, 2), (2, 2)\ (2, 3)\}, \{(1, 3), (2, 2)\ (2, 3)\},$
$\{(1, 2), (1, 3), (2, 2)\ (2, 3)\}\}$.

32. a. $\mathscr{P}(A \times B) = \{\emptyset, \{(1, u)\}, \{(1, v)\}, \{(1, u), (1, v)\}\}$

33. b. $\mathscr{P}(\mathscr{P}(\emptyset)) = \mathscr{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$

34. a. $A_1 \times (A_2 \times A_3) = \{(1, (u, m)), (2, (u, m)), (3, (u, m)), (1, (u, n)), (2, (u, n)), (3, (u, n)), (1, (v, m)), (2, (v, m)), (3, (v, m)), (1, (v, n)), (2, (v, n)), (3, (v, n))\}$

35. a. $A \times (B \cup C) = \{a, b\} \times \{1, 2, 3\}$
$= \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3)\}$

b. $(A \times B) \cup (A \times C) = \{(a, 1), (a, 2), (b, 1), (b, 2), (a, 2), (a, 3), (b, 2), (b, 3)\}$
$= \{(a, 1), (a, 2)\ (b, 1), (b, 2), (a, 3)\ (b, 3)\}$

36.

i	1 →			2 →			3 →		4
j		1	2	3	1	2	3	4	1 →	2	
encontrada		no	sí		no		sí		no	sí		
respuesta	$A \subseteq B$											

Sección 6.2

1. a. (1) A (2) $B \cup C$
b. (1) $A \cap B$ (2) C

2. a. (1) $A - B$ (2) A (3) A (4) B
b. (1) $x \in A$ (2) A (3) B (4) A

3. (a.) A **(b)** C **(c)** B **(d)** C **(e)** $B \subseteq C$

5. *Demostración:* Suponga que A y B son conjuntos.
$\boldsymbol{B - A \subseteq B \cap A^c}$: Suponga que $x \in B - A$. Por definición del conjunto diferencia, $x \in B$ y $x \notin A$. Pero entonces por definición de complemento, $x \in B$ y $x \in A^c$ y así por definición de intersección, $x \in B \cap A^c$. *[Por tanto, $B - A \subseteq B \cap A^c$ por definición de subconjunto.]*
$\boldsymbol{B \cap A^c \subseteq B - A}$**:** Suponga que $x \in B \cap A^c$. Por definición de intersección, $x \in B$ y $x \in A^c$. Pero entonces por definición de complemento, $x \in B$ y $x \notin A$ y así por definición de conjunto diferencia, $x \in B - A$. *[Así $B \cap A^c \subseteq B - A$ por definición de subconjunto.]*
[Ya que se han demostrado ambas contenciones de conjuntos, entonces $B - A = B \cap A^c$ por definición de igualdad de conjuntos.]

6. *Respuestas parciales*
a. $(A \cap B) \cup (A \cap C)$ **b.** A **c.** $B \cup C$
d. $x \in C$ **e.** $A \cap B$ **f.** por definición de intersección
$x \in A \cap C$, y entonces por definición de unión
$x \in (A \cap B) \cup (A \cap C)$.

7. *Sugerencia:* Esto es similar a la prueba indicada en el ejemplo 6.2.3.

8. *Demostración:* Supongamos que A y B son conjuntos cualesquiera.
Demostración de que $\boldsymbol{(A \cap B) \cup (A \cap B^c) \subseteq A}$**:** Suponga $x \in (A \cap B) \cup (A \cap B^c)$. *[Debemos demostrar que $x \in A$.]* Por definición de unión, $x \in A \cap B$ o $x \in (A \cap B^c)$.
Caso 1 $\boldsymbol{(x \in A \cap B)}$**:** En este caso x está en A y x está en B, entonces, en particular, $x \in A$.
Caso 2 $\boldsymbol{(x \in A \cap B^c)}$**:** En este caso x está en A y x no está en B, por tanto, en particular, $x \in A$.
Así, en cualquier caso, $x \in A$ *[que es lo que se desea demostrar]. [Así $(A \cap B) \cup (A \cap B^c) \subseteq A$ por definición de subconjunto.]*
Demostración de que $\boldsymbol{A \subseteq (A \cap B)\ U\ (A \cap B^c)}$**:** Supongamos que $x \in A$. *[Debemos demostrar que $x \in (A \cap B) \cup (A \cap B^c)$.]* Entonces $x \in B$ o $x \notin B$.
Caso 1 $\boldsymbol{(x \in B)}$**:** En este caso sabemos que x está en A y también suponemos que x está en B. Así que, por definición de intersección, $x \in A \cap B$.
Caso 2 $\boldsymbol{(x \in \mathbf{A} \cap B^c)}$**:** En este caso sabemos que x está en A y también suponemos que x está en B^c. Entonces, por definición de intersección, $x \in A \cap B^c$.
Así, $x \in A \cap B$ o $x \in A \cap B^c$ y entonces, por definición de unión, $x \in (A \cap B) \cup (A \cap B^c)$. *[que era lo que se quería demostrar. Entonces $A \subseteq (A \cap B) \cup (A \cap B^c)$ por definición de subconjunto].*
Conclusión**:** Como se han demostrado ambas contenciones, entonces se tiene por definición de igualdad entre conjuntos que $(A \cap B) \cup (A \cap B^c) = A$.

9. *Demostración parcial:* Suponga que A, B y C son conjuntos cualesquiera. Para demostrar que $(A - B) \cup (C - B) = (A \cup C) - B$, debemos demostrar que $(A - B) \cup (C - B) \subseteq (A \cup C) - B$ y que $(A \cup C) - B \subseteq (A - B) \cup (C - B)$.

$(A - B) \cup (C - B) \subseteq (A \cup C) - B$: Supongamos que x es cualquier elemento en $(A - B) \cup (C - B)$. *[Debemos demostrar que $x \in (A \cup C) - B$.]* Por definición de unión, $x \in A - B$ o $x \in C - B$.

***Caso 1* ($x \in A - B$):** Entonces, por definición del conjunto diferencia, $x \in A$ y $x \notin B$. Pero $x \in A$, entonces por definición de unión tenemos que $x \in A \cup C$. Por tanto, $x \in A \cup C$ y $x \notin B$ y así, por definición del conjunto diferencia, $x \in (A \cup C) - B$.

***Caso 2* ($x \in C - B$):** Entonces, por definición del conjunto diferencia, $x \in C$ y $x \notin B$. Pero como $x \in C$, por definición de unión tenemos que $x \in A \cup C$. Por tanto, $x \in A \cup C$ y $x \notin B$ y así, por definición del conjunto diferencia, $x \in (A \cup C) - B$.

Así, en ambos casos, $x \in (A \cup C) - B$ *[que era lo que se quería demostrar]*.

Entonces $(A - B) \cup (C - B) \subseteq (A \cup C) - B$.

11. *Demostración parcial:* Supongamos que A y B sean conjuntos arbitrarios. Demostraremos que $A \cup (A \cap B) \subseteq A$. Aceptemos que x sea cualquier elemento en $A \cup (A \cap B)$. *[Debemos demostrar que $x \in A$.]* Por definición de unión, $x \in A$ o $x \in A \cap B$. En este caso en donde $x \in A$, claramente $x \in A$. En el caso en donde $x \in A \cap B$, $x \in A$ y $x \in B$ (por definición de intersección). Así, en particular, $x \in A$. En consecuencia, en ambos casos $x \in A$ *[que era lo que se quería demostrar]*.

Para completar la demostración de que $A \cup (A \cap B) = A$, se debe demostrar que $A \subseteq A \cup (B \cap A)$.

12. *Demostración:* Sea A un conjunto. *[Debemos demostrar que $A \cup \emptyset = A$.]*

$A \cup \emptyset \subseteq A$: Suponga que $x \in A \cup \emptyset$. Entonces, por definición de unión $x \in A$ o $x \in \emptyset$. Pero $x \notin \emptyset$ porque $\emptyset$ no tiene elementos. Así $x \in A$.

$A \subseteq A \cup \emptyset$: Supongamos $x \in A$. Entonces el enunciado "$x \in A$ o $x \in \emptyset$" es verdadero. Así que por definición de unión $x \in A \cup \emptyset$. *[Alternativamente, $A \subseteq A \cup \emptyset$ por la inclusión en la propiedad de la unión.]* Como $A \cup \emptyset \subseteq A$ y $A \subseteq A \cup \emptyset$, entonces por la definición de igualdad de conjuntos $A \cup \emptyset = A$.

13. *Demostración:* Suponga que A, B y C son conjuntos y que $A \subseteq B$. Sea $x \in A \cap C$. Por definición de intersección, $x \in A$ y $x \in C$. Pero como $A \subseteq B$ y $x \in A$, entonces $x \in B$. Por tanto, $x \in B$ y $x \in C$ y así, por definición de intersección, $x \in B \cap C$. *[En consecuencia, por definición de subconjunto $A \cap C \subseteq B \cap C$.]*

16. *Sugerencia:* La demostración tiene el siguiente esbozo:

Supongamos que A, B y C son conjuntos arbitrarios tales que $A \subseteq B$ y $A \subseteq C$.

$\vdots$

Por tanto, $A \subseteq B \cap C$.

18. *Demostración:* Suponga que A, B y C son conjuntos arbitrariamente elegidos.

$A \times (B \cup C) \subseteq (A \times B) \cup (A \times C)$: Aceptemos que $(x, y) \in A \times (B \cup C)$. *[Debemos demostrar que $(x, y) \in (A \times B) \cup (A \times C)$.]* Entonces $x \in A$ y $y \in B \cup C$. Por definición de unión, esto significa que $y \in B$ o $y \in C$.

***Caso 1* ($y \in B$):** Como $x \in A$, entonces por definición de producto cartesiano $(x, y) \in A \times B$. Así que $(x, y) \in (A \times B) \cup (A \times C)$ debido a la inclusión en la propiedad de unión.

***Caso 2* ($y \in C$):** Entonces, como $x \in A$, por la definición de producto cartesiano se tiene que $(x, y) \in A \times C$. Así que, por la inclusión en la propiedad de unión resulta que $(x, y) \in (A \times B) \cup (A \times C)$.

Así, en cualquier caso $(x, y) \in (A \times B) \cup (A \times C)$ *[que era lo que se quería demostrar]*.

Por tanto, $A \times (B \cup C) \subseteq (A \times B) \cup (A \times C)$ por definición de subconjunto.

$(A \times B) \cup (A \times C) \subseteq A \times (B \cup C)$: Suponga $(x, y) \in (A \times B) \cup (A \times C)$. Entonces $(x, y) \in A \times B$ o $(x, y) \in A \times C$.

***Caso 1* ($(x, y) \in A \times B$):** En este caso, $x \in A$ y $y \in B$. Por definición de unión, como $y \in B$, entonces $y \in B \cup C$. Así que $x \in A$ y $y \in B \cup C$, en consecuencia, por definición de producto cartesiano $(x, y) \in A \times (B \cup C)$.

***Caso 2* ($(x,y) \in A \times C$):** En este caso, $x \in A$ y $y \in C$. Por definición de unión, como $y \in C$, entonces $y \in B \cup C$. Por tanto, $x \in A$ y $y \in B \cup C$ y en consecuencia, por definición de producto cartesiano $(x, y) \in A \times (B \cup C)$.

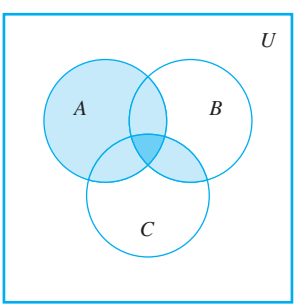
Así, en cualquier caso $(x, y) \in A \times (B \cup C)$. *[Entonces, por definición de subconjunto,* $(A \times B) \cup (A \times C) \subseteq A \times (B \cup C)$*.]*

[Se han demostrado ambas relaciones de subconjuntos, entonces podemos concluir que $A \times (B \cup C) = (A \times B) \cup (A \times C)$ debido a la definición de igualdad de conjuntos.]

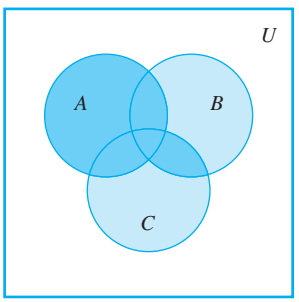
20. Hay más de un error en esta "demostración". El más serio es el uso incorrecto de la definición de subconjunto. Decir que A es un subconjunto de B significa que para toda x, **si** $x \in A$ **entonces** $x \in B$. Ello no significa que existe un elemento de A que también es un elemento de B. El segundo error en la demostración ocurre en la última frase. Justo porque existe un elemento en A que está en B y un elemento en B que está en C, no se tiene que haya un elemento en A que esté en C. Por ejemplo, suponga $A = \{1, 2\}$, $B = \{2, 3\}$ y $C = \{3, 4\}$. Entonces existe un elemento en A que está en B (a saber, 2) y hay un elemento en B que está en C (a saber, 3), pero ningún elemento de A está en C.

21. *Sugerencia:* El enunciado "como $x \notin A$ o $x \notin B$, entonces $x \notin A \cup B$" es una falacia. Intenta pensar de un ejemplo de conjuntos A y B y un elemento x tales que el enunciado "$x \notin A$ o $x \notin B$" sea verdadero pero sea falso el enunciado "$x \notin A \cup B$".

23. a.



Toda la región sombreada es $A \cup (B \cap C)$.



Toda la región más oscura es $(A \cup B) \cap (A \cup C)$.

24. **(a)** $(A - B) \cap (B - A)$ **(b)** intersección **(c)** $B - A$ **(d)** B **(e)** A **(f)** A **(g)** $(A - B) \cap (B - A) = \emptyset$

25. *Demostración por contradicción:* Suponga que no. Es decir, acepte que existen conjuntos A y B tales que $(A \cap B) \cap (A \cap B^c) \neq \emptyset$. Entonces hay un elemento x en $(A \cap B) \cap (A \cap B^c)$. Por definición de intersección, $x \in (A \cap B)$ y $x \in (A \cap B^c)$. Aplicando otra vez la definición de intersección, tenemos que como $x \in (A \cap B)$, entonces $x \in A$ y $x \in B$ y como $x \in (A \cap B^c)$, entonces $x \in A$ y $x \notin B$. Así, en particular, $x \in B$ y $x \notin B$, que es una contradicción. Se tiene que la suposición es falsa y por tanto $(A \cap B) \cap (A \cap B^c) = \emptyset$.

27. *Demostración:* Sea A un subconjunto de un conjunto universal U. Suponga que $A \cap A^c \neq \emptyset$, es decir, acepte que existe un elemento x tal que $x \in A \cap A^c$. Entonces por definición de intersección, $x \in A$ y $x \in A^c$ y por definición de complemento, $x \in A$ y $x \notin A$. Esto es una contradicción. *[Por tanto, la suposición es falsa y así concluimos que $A \cap A^c = \emptyset$.]*

29. *Demostración:* Sea A un conjunto. Suponga que $A \times \emptyset \neq \emptyset$. Entonces debería existir un elemento (x, y) en $A \times \emptyset$. Por definición de producto cartesiano, $x \in A$ y $y \in \emptyset$. Pero no existen elementos y tales que $y \in \emptyset$. Así que no hay elementos (x, y) tales que $x \in A$ y $y \in \emptyset$. En consecuencia, $(x, y) \notin A \times \emptyset$. *[Por tanto, la suposición es falsa y así $A \times \emptyset = \emptyset$.]*

30. *Demostración:* Sean A y B conjuntos tales que $A \subseteq B$. *[Debemos demostrar que $A \cap B^c = \emptyset$.]* Suponga que $A \cap B^c \neq \emptyset$; es decir, acepte que hay un elemento x tal que $x \in A \cap B^c$. Entonces por definición de intersección, $x \in A$ y $x \in B^c$. Así, por definición de complemento, $x \in A$ y $x \notin B$. Pero por hipótesis $A \subseteq B$. Y por definición de subconjunto, $x \in A$ y $x \in B$. En consecuencia, $x \notin B$ y también $x \in B$, que es una contradicción. Entonces es falsa la suposición $A \cap B^c \neq \emptyset$ y por tanto $A \cap B^c = \emptyset$.

33. *Demostración:* Sean A, B y C cualesquiera conjuntos tales que $C \subseteq B - A$. Suponga que $A \cap C \neq \emptyset$. Entonces existe un elemento x tal que $x \in A \cap C$. Por definición de intersección, $x \in A$ y $x \in C$. Como $C \subseteq B - A$, entonces $x \in B$ y $x \notin A$. Así $x \in A$ y $x \notin A$, que es una contradicción. Entonces la suposición es falsa, Por tanto $A \cap C = \emptyset$.

36. **a.** *Inicio de la demostración de que $A \cup B \subseteq (A - B) \cup (B - A) \cup (A \cap B)$:* Dado cualquier elemento x en $A \cup B$, por definición de unión, x al menos está en A o en B. Así x satisface exactamente una de las siguientes tres condiciones:

1) $x \in A$ y $x \notin B$ (x está sólo en A)

2) $x \in B$ y $x \notin A$ (x está sólo en B)

3) $x \in A$ y $x \in B$ (x está en A y en B)

b. Para demostrar que $(A - B)$, $(B - A)$ y $(A \cap B)$ son mutuamente disjuntos, debemos demostrar que la intersección de cualesquiera de los dos es el conjunto vacío. Pero, por definición del conjunto diferencia y del conjunto vacío, decir que $x \in A - B$ significa que 1) $x \in A$ y $x \notin B$ y decir que $x \in B - A$ implica que 2) $x \in B$ y $x \notin A$ y afirmar que $x \in A \cap B$ significa que 3) $x \in A$ y $x \in B$. Las condiciones de la 1) a la 3) son mutuamente excluyentes y así ningún para de estas se puede satisfacer simultáneamente. Entonces, ningún elemento puede estar en la intersección de cualesquiera dos de los conjuntos y, por tanto, la intersección de dos de esos conjuntos da el conjunto vacío. Así que, $(A - B)$, $(B - A)$ y $(A \cap B)$ son mutuamente disjuntos.

37. Supongamos que A y $B_1, B_2, B_3, \ldots, B_n$ son conjuntos arbitrarios.

Demostración de que $A \cap \left(\bigcup_{i=1}^{n} B_i\right) \subseteq \bigcup_{i=1}^{n}(A \cap B_i)$:

Suponga que x es un elemento en $A \cap \left(\bigcup_{i=1}^{n} B_i\right)$. *[Debemos demostrar que $x \in \bigcup_{i=1}^{n}(A \cap B_i)$.]* Por definición de intersección, $x \in A$ y $x \in \bigcup_{i=1}^{n} B_i$. Como $x \in \bigcup_{i=1}^{n} B_i$, la definición de unión general implica que $x \in B_i$ para algún $i = 1, 2, \ldots, n$ y así, como $x \in A$, la definición de intersección implica que $x \in A \cap B_i$. Entonces, por definición de unión general, $x \in \bigcup_{i=1}^{n}(A \cap B_i)$ *[que era lo que se quería demostrar]*.

Demostración de que $\bigcup_{i=1}^{n}(A \cap B_i) \subseteq A \cap \left(\bigcup_{i=1}^{n} B_i\right)$:

Suponga que x es un elemento en $\bigcup_{i=1}^{n}(A \cap B_i)$. *[Debemos demostrar que $x \in A \cap \left(\bigcup_{i=1}^{n} B_i\right)$.]* Por definición de unión general, $x \in A \cap B_i$ para algún $i = 1, 2, \ldots, n$. Así, por definición de intersección, $x \in A$ y $x \in B_i$. Como $x \in B_i$ para algún $i = 1, 2, \ldots, n$, por definición de unión general, $x \in \bigcup_{i=1}^{n} B_i$.

Así tenemos que $x \in A$ y $x \in \bigcup_{i=1}^{n} B_i$, y entonces, por definición de intersección, $x \in A \cap \left(\bigcup_{i=1}^{n} B_i\right)$ *[que era lo que se quería demostrar]*.

Conclusión: Se han demostrado ambas contenciones, entonces por la definición de igualdad entre conjuntos se tiene que $A \cap \left(\bigcup_{i=1}^{n} B_i\right) = \bigcup_{i=1}^{n}(A \cap B_i)$.

38. *Esbozo de la demostración:* Si $x \in \bigcup_{i=1}^{n}(A_i - B)$, entonces $x \in A_i - B$ para algún $i = 1, 2, \ldots, n$ y así, (1) para algún $i = 1, 2, \ldots, n$, $x \in A_i$ (que implica que $x \in \left(\bigcup_{i=1}^{n} A_i\right)$ y (2) $x \notin B$. Inversamente, si $x \in \left(\bigcup_{i=1}^{n} A_i\right) - B$, entonces $x \in \bigcup_{i=1}^{n} A_i$ y $x \notin B$ y por definición de unión general, $x \in A_i$ para algún $i = 1$,

2, …, n y $x \notin B$. Esto implica que existe un entero i tal que $x \in A_i - B$ y en consecuencia, $x \in \bigcup_{i=1}^{n}(A_i - B)$.

40. Supongamos que A y $B_1, B_2, B_3, \ldots, B_n$ son conjuntos arbitrarios.

Demostración de que $\bigcup_{i=1}^{n}(A \times B_i) \subseteq A \times \left(\bigcup_{i=1}^{n} B_i\right)$:

Suponga que (x, y) es cualquier elemento en $\bigcup_{i=1}^{n}(A \times B_i)$. *[Debemos demostrar que* $(x, y) \in A \times \left(\bigcup_{i=1}^{n} B_i\right)$*.]* Por definición de unión general, $(x, y) \in A \times B_i$ para algún $i = 1, 2, \ldots, n$. Por definición de producto cartesiano, esto implica que 1) $x \in A$ y 2) $y \in B_i$ para algún $i = 1, 2, \ldots, n$. Por definición de unión general, 2) implica que $\in \bigcup_{i=1}^{n} B_i$. Así $x \in A$ y $\in \bigcup_{i=1}^{n} B_i$ y así por definición de producto cartesiano, $(x, y) \in A \times \left(\bigcup_{i=1}^{n} B_i\right)$ *[que era lo que se quería demostrar]:*

Demostración de que $A \times \left(\bigcup_{i=1}^{n} B_i\right) \subseteq \bigcup_{i=1}^{n}(A \times B_i)$:

Suponga que (x, y) es cualquier elemento en $A \times \left(\bigcup_{i=1}^{n} B_i\right)$. *[Debemos demostrar que* $(x, y) \in \bigcup_{i=1}^{n}(A \times B_i)$*.]* Por definición de producto cartesiano, 1) $x \in A$ y 2) $\in \bigcup_{i=1}^{n} B_i$. Por definición de unión general, 2) implica que $y \in B_i$ para algún $i = 1, 2, \ldots, n$ y además, por definición de producto cartesiano, $(x, y) \in A \times B_i$ para algún $i = 1, 2, \ldots, n$. De la definición de unión general se tiene que $(x, y) \in \bigcup_{i=1}^{n}(A \times B_i)$ *[que era lo que se quería demostrar]*.

Conclusión: Se han demostrado ambas contenciones, entonces de la definición de igualdad de conjuntos se tiene que $\bigcup_{i=1}^{n}(A \times B_i) = A \times \left(\bigcup_{i=1}^{n} B_i\right)$.

Sección 6.3

1. *Contraejemplo:* Cualesquiera conjuntos A, B y C en donde C contiene elementos que no están en A servirán como un contraejemplo. En efecto, sean $A = \{1, 3\}$, $B = \{2, 3\}$ y $C = \{4\}$. Entonces $(A \cap B) \cup C = \{3\} \cup \{4\} = \{3, 4\}$, mientras que $A \cap (B \cup C) = \{1, 3\} \cap \{2, 3, 4\} = \{3\}$. Como $\{3, 4\} \neq \{3\}$, $(A \cap B) \cup C) \neq A \cap (B \cup C)$.

3. *Contraejemplo:* Sean A, B y C conjuntos arbitrarios en donde $A \subseteq C$ y B contiene al menos un elemento que no está en A ni en C, que servirá como un contraejemplo. En efecto, sean $A = \{1\}$, $B = \{2\}$ y $C = \{1, 3\}$. Entonces $A \nsubseteq B$ y $B \nsubseteq C$ pero $A \subseteq C$.

5. Falso. *Contraejemplo:* Conjuntos arbitrarios A, B y C en donde A y C tienen elementos en común que no están en B servirán como un contraejemplo. En efecto, sean $A = \{1, 2, 3\}$, $B = \{2, 3\}$ y $C = \{3\}$. Entonces $B - C = \{2\}$ y así $A - (B - C) = \{1, 2, 3\} - \{2\} = \{1, 3\}$. Por otro lado, $A - B = \{1, 2, 3\} - \{2, 3\} = \{1\}$ y en consecuencia $(A - B) - C = \{1\} - \{3\} = \{1\}$. Como $\{1, 3\} \neq \{1\}$, $A - (B - C) \neq (A - B) - C$.

6. Verdadero. *Demostración:* Sean A y B conjuntos arbitrarios.

A $\cap$ ***(A*** $\cup$ ***B)*** $\subseteq$ ***A:*** Suponga que $x \in A \cap (A \cup B)$. Por definición de intersección, $x \in A$ y $x \in A \cup B$. En particular $x \in A$. Así, por definición de subconjunto, $A \cap (A \cup B) \subseteq A$.

A $\subseteq$ ***A*** $\cap$ ***(A*** $\cup$ ***B):*** Suponga $x \in A$. Entonces por definición de unión, $x \in A \cup B$. Así $x \in A$ y $x \in A \cup B$, además, por definición de intersección $x \in A \cap (A \cup B)$. En consecuencia, por definición de subconjunto, $A \subseteq A \cap (A \cup B)$.

Ya que se ha demostrado que $A \cap (A \cup B) \subseteq A$ y $A \subseteq A \cap (A \cup B)$, entonces concluimos que $A \cap (A \cup B) = A$.

9. Verdadero. *Demostración:* Suponga que A, B y C son conjuntos con $A \subseteq C$ y $B \subseteq C$. Sea $x \in A \cup B$. Por definición de unión, $x \in A$ o $x \in B$. Pero si $x \in A$ entonces $x \in C$ (porque $A \subseteq C$) y si $x \in B$ entonces $x \in C$ (porque $B \subseteq C$). Por tanto, en cualquier caso, $x \in C$. *[Así, por definición de subconjunto,* $A \cup B \subseteq C$*.]*

11. *Sugerencia:* El enunciado es falso. Considere los siguientes conjuntos U, A, B y C: $U = \{1, 2, 3, 4\}$, $A = \{1, 2\}$, $B = \{1, 2, 3\}$ y $C = \{2\}$.

12. *Sugerencia:* El enunciado es verdadero. *Esbozo de la demostración:* Si $x \in A \cap (B - C)$, entonces $x \in A$, $x \in B$ y $x \notin C$. Por tanto, es verdadero que $x \in A$ y $x \in B$ y que $x \in A$ y $x \notin C$. Inversamente, si $x \in (A \cap B) - (A \cap C)$, entonces $x \in A$ y $x \in B$, pero $x \notin A \cap C$ y así $x \notin C$.

14. *Sugerencia:* El enunciado es falso. Demuestre que lo siguiente es un *Contraejemplo:* $A = \{1, 3\}$, $B = \{1, 2, 3\}$ y $C = \{2, 3\}$.

15. *Sugerencia:* El enunciado es verdadero. *Esbozo de la demostración:* Suponga que $x \in A$. *[Debemos demostrar que* $x \in B$*.]* Entonces $x \in C$ o $x \notin C$. Si $x \in C$, hacemos uso del hecho de que $A \cap C \subseteq B \cap C$ para demostrar que $x \in B$.

17. Verdadero. *Demostración:* Suponga que A y B son conjuntos arbitrarios con $A \subseteq B$. *[Debemos demostrar que* $\mathscr{P}(A) \subseteq \mathscr{P}(B)$*.]* Aceptemos que $X \in \mathscr{P}(A)$. Entonces $X \subseteq A$ por definición de conjunto potencia. Pero como $A \subseteq B$, también tenemos que $X \subseteq B$ por la propiedad transitiva para subconjuntos, Por tanto, por definición de conjunto potencia, $X \in \mathscr{P}(B)$. Esto prueba que para todas las X, si $X \in \mathscr{P}(A)$ entonces $X \in \mathscr{P}(B)$, y así $\mathscr{P}(A) \subseteq \mathscr{P}(B)$ *[que era lo que se quería demostrar]*.

18. Falso. *Contraejemplo:* Para conjuntos arbitrarios A y B, $\mathscr{P}(A) \cup \mathscr{P}(B)$sólo contiene conjuntos que son subconjuntos de A o B, mientras que los conjuntos en $\mathscr{P}(A \cup B)$ pueden contener elementos de A y B. Así, si al menos A o B contienen elementos que no están en otro conjunto, entonces $\mathscr{P}(A) \cup \mathscr{P}(B)$ y $\mathscr{P}(A \cup B)$ no serán iguales. Por ejemplo, sean $A = \{1\}$ y $B = \{2\}$. Entonces $\{1, 2\} \in \mathscr{P}(A \cup B)$ pero $\{1, 2\} \notin \mathscr{P}(A) \cup \mathscr{P}(B)$.

19. *Sugerencia:* El enunciado es verdadero. Para probarlo, suponga que A y B son conjuntos arbitrarios y aceptemos que $X \in \mathscr{P}(A) \cup \mathscr{P}(B)$. Demuestre que $X \subseteq A \cup B$ y obtenga la conclusión de este resultado.

22. a. *Enunciado:* ∀ los conjuntos S, existe un conjunto T tal que $S \cap T = \emptyset$.

Negación: Existe un conjunto S tal que ∀ los conjuntos T, $S \cap T \neq \emptyset$.

El enunciado es verdadero. Dado cualquier conjunto S, tome $T = S^c$.

Entonces $S \cap T = S \cap S^c = \emptyset$ por la ley de complemento para $\cap$. Alternativamente, T podría tomarse igual a $\emptyset$.

25. *Sugerencia:* $S_0 = \{\emptyset\}$, $S_1 = \{\{a\}, \{b\}, \{c\}\}$

a. $S_1 = \{\emptyset, \{t\}, \{u\}, \{v\}, \{t, u\}, \{t, v\}, \{u, v\}, \{t, u, v\}\}$

b. $S_2 = \{\{w\}, \{t^c\, w\}, \{u, w\}, \{v, w\}, \{t, u, w\}, \{t, v, w\}, \{u, v, w\}, \{t, u, v, w\}\}$

c. Si

26. *Sugerencia:* Use inducción matemática. En el paso inductivo, se considerará el conjunto de todos los subconjuntos no vacíos de $\{2,\ldots, k\}$ y el conjunto de todos los subconjuntos no vacíos de $\{2,\ldots, k+1\}$. Cualquier subconjunto de $\{2,\ldots, k+1\}$ contiene o no a $k+1$. Así

$$\begin{bmatrix}\text{la suma de todos los productos}\\ \text{de elementos de subconjuntos}\\ \text{no vacíos de } \{2,\ldots,k+1\}\end{bmatrix}$$

$$= \begin{bmatrix}\text{la suma de todos los productos}\\ \text{de elementos de subconjuntos}\\ \text{no vacíos de } \{2,\ldots,k+1\}\\ \text{que no contienen a } k+1,\end{bmatrix} + \begin{bmatrix}\text{la suma de todos los productos}\\ \text{de elementos de subconjuntos}\\ \text{no vacíos de } \{2,\ldots,k+1\}\\ \text{que contienen a } k+1\end{bmatrix}$$

27. a. ley conmutativa para $\cap$

b. ley distributiva

c. ley conmutativa para $\cap$

28. Respuesta parcial:

a. ley para el conjunto diferencia

b. ley para el conjunto diferencia

c. ley conmutativa para $\cap$

d. ley de De Morgan

29. *Sugerencia:* Recuerde usar las propiedades del teorema 6.2.2, exactamente como fueron escritas. Por ejemplo, la ley distributiva no establece que para todos los conjuntos A, B y C, $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$.

30. *Demostración:* Aceptemos que A, B y C son conjuntos dados. Entonces

$(A \cap B) \cup C$

$= C \cup (A \cap B)$ por la ley conmutativa para $\cup$

$= (C \cup A) \cap (C \cup B)$ por la ley distributiva

$= (A \cup C) \cap (B \cup C)$ por la ley conmutativa para $\cup$.

31. *Demostración:* Suponga que A y B son conjuntos. Entonces

$A \cup (B - A)$

$= A \cup (B \cap A^c)$ por la ley del conjunto diferencia

$= (A \cup B) \cap (A \cup A^c)$ por la ley distributiva

$= (A \cup B) \cap U$ por la ley de complemento para $\cup$

$= A \cup B$ por la ley identidad para $\cap$.

36. *Demostración:* Sean A, B y C conjuntos cualesquiera. Entonces

$((A^c \cup B^c) - A)^c$

$= ((A^c \cup B^c(\cap A^c)^c$ por la ley del conjunto diferencia

$= (A^c \cup B^c(^c \cup (A^c)^c$ por la ley de De Morgan

$= ((A^c)^c \cap (B^c)^c(\cup (A^c)^c$ por la ley de De Morgan

$= (A \cap B(\cup A$ por la ley para el doble complemento

$= A \cup)A \cap B)$ por la ley conmutativa para $\cup$

$= A$ por la ley de absorción

39. *Demostración parcial:* Sean A y B conjuntos arbitrarios. Entonces

$(A - B) \cup (B - A)$

$= (A \cap B^c) \cup (B \cap A^c)$ por la ley del conjunto diferencia

$= [(A \cap B^c) \cup B] \cap [(A \cap B^c) \cup A^c)]$ por la ley distributiva

$= [(B \cup)A \cap B^c)] \cap [A^c \cup (A \cap B^c)$ por la ley conmutativa para $\cup$

$= [(B \cup A) \cap (B \cup B^c)] \cap [(A^c \cup A) \cap (A^c \cup B^c)]$ por la ley distributiva

$= [(A \cup B) \cap (B \cup B^c)] \cap [(A \cup A^c) \cap (A^c \cup B^c)]$ por la ley conmutativa para $\cup$

41. *Sugerencia:* La respuesta es $\emptyset$.

44. a. *Demostración:* Suponga que no. Es decir, acepte que existen conjuntos A y B tales que $A - B$ y B no son disjuntos. *[Debemos obtener una contradicción.]* Entonces $(A - B) \cap B \neq \emptyset$ y así existe un elemento x en $(A - B) \cap B$. Por definición de intersección, $x \in A - B$ y $x \in B$ y por definición de diferencia, $x \in A$ y $x \notin B$. Así que $x \in B$ y también $x \notin B$, que es una contradicción. Por tanto, es falsa la suposición y concluimos que $A - B$ y B son disjuntos.

b. Sean A y B conjuntos arbitrarios. Entonces

$(A - B) \cap B$

$= (A \cap B^c) \cap B$ por la ley del conjunto diferencia

$= A \cap (B^c \cap B)$ por la ley asociativa para $\cap$

$= A \cap (B \cap B^c)$ por la ley conmutativa para $\cap$

$= A \cap \emptyset$ por la ley del complemento para $\cap$

$= \emptyset$ por la ley de cota universal para $\cap$

46. a. $A \Delta B = (A - B) \cup (B - A) = \{1, 2\} \cup \{5, 6\} = \{1, 2, 5, 6\}$

47. *Demostración:* Sean A y B cualesquiera dos subconjuntos de un conjunto universal. Por definición de Δ, demuestre que $A \Delta B = B \Delta A$ es equivalente a demostrar que $(A - B) \cup (B - A) = (B - A) \cup (A - B)$. Pero esto se tiene inmediatamente de la ley conmutativa para $\cup$.

48. *Demostración:* Sea A cualquier subconjunto de un conjunto universal. Entonces

$$\begin{aligned} A\triangle\emptyset & \\ &= (A-\emptyset)\cup(\emptyset-A) && \text{por definición de } \triangle \\ &= (A\cap\emptyset^c)\cup(\emptyset\cap A^c) && \text{por la ley del conjunto diferencia} \\ &= (A\cap U)\cup(A^c\cap\emptyset) && \text{por la ley del complemento de } U \text{ y por la ley conmutativa para } \cap \\ &= A\cup\emptyset && \text{por la ley identidad para } \cap \text{ y la ley de cota universal para } \cap \\ &= A. && \text{por la ley identidad para } \cup \end{aligned}$$

51. *Sugerencia:* Primero demuestre que para conjuntos arbitrarios A y B y para cualquier elemento x,

$$x\in A\triangle B \Leftrightarrow (x\in A \text{ y } x\notin B) \text{ o } (x\in B \text{ y } x\notin A),$$

y

$$x\notin A\triangle B \Leftrightarrow (x\notin A \text{ y } x\notin B) \text{ o } (x\in B \text{ y } x\in A).$$

52. La misma sugerencia que en el ejercicio 51.

53. *Inicio de demostración:* Supongamos que A y B son subconjuntos cualesquiera de un conjunto universal U. Por la ley de cota universal para la unión, $B\cup U=U$ y así, por la ley conmutativa para la unión, $U\cup B=U$. Tome la intersección con A de ambos lados de la ecuación.

Sección 6.4

1. **a.** porque 1 es una identidad para $\cdot$
b. por la ley del complemento para $+$
c. por la ley distributiva para $+$ sobre $\cdot$
d. por la ley del complemento para $\cdot$
e. porque 0 es una identidad para $+$

4. *Demostración:* Para todos los elementos a en B,

$$\begin{aligned} a\cdot 0 &= a\cdot(a\cdot\overline{a}) && \text{por la ley del complemento para } \cdot \\ &= (a\cdot a)\cdot\overline{a} && \text{por la ley asociativa para } \cdot \\ &= a\cdot\overline{a} && \text{por el ejercicio 48} \\ &= 0. && \text{por la ley del complemento para } \cdot \end{aligned}$$

6. **a.** *Demostración:* $0\cdot 1=0$ porque 1 es una identidad para $\cdot$ y $0+1=1+0=1$ porque $+$ es conmutativa y 0 es una identidad para $+$. Así, por la unicidad de la ley del complemento, $\overline{0}=1$.

7. **a.** *Demostración:* Suponga que 0 y $0'$ son elementos de B, siendo ambas identidades para $+$. Entonces satisfacen la identidad, el complemento y las leyes de cota universal. *[Demostraremos que $0=0'$.]* Por la ley de identidad para $+$, para toda $a\in B$,

$$a+0=a \text{ y } a+0'=a.$$

Se tiene que:

$$\begin{aligned} \Rightarrow\quad a+0 &= a+0' && \text{porque ambas cantidades son iguales a } a \\ \Rightarrow\quad \bar{a}\cdot(a+0) &= \bar{a}\cdot(a+0') && \text{“multiplicando” ambos lados por } \bar{a} \\ \Rightarrow\quad (\bar{a}\cdot a)+(\bar{a}\cdot 0) &= (\bar{a}\cdot a)+(\bar{a}\cdot 0') && \text{por la ley distributiva} \\ \Rightarrow\quad (a\cdot\bar{a})+0 &= (a\cdot\bar{a})+0' && \text{por la ley de cota universal para } \cdot \\ \Rightarrow\quad 0\cdot 0 &= 0'\cdot 0' && \text{por la ley del complemento para } \cdot \\ \Rightarrow\quad 0 &= 0' && \text{por la ley de cota universal para } \cdot \end{aligned}$$

[Esto es lo que se quería demostrar.]

b. *Sugerencia:* 1 y $1'$ son elementos de B y ambos son identidades para $\cdot$. Entonces para toda $a\in B$, por la ley de identidad para $\cdot$, $a\cdot 1=a$ y $a\cdot 1'=a$. Se tiene que $a\cdot 1=a\cdot 1'$ y $\bar{a}+a\cdot 1=\bar{a}+a\cdot 1'$, etcétera.

8. *Demostración:* Suponga que B es un álgebra booleana y a y b son elementos cualesquiera de B. Primero demostramos que $(a\cdot b)+(\overline{a}+\overline{b})=1$.

$$\begin{aligned} & a\cdot b+(\overline{a}+\overline{b}) \\ &= (\overline{a}+\overline{b})+(a\cdot b) && \text{por la ley conmutativa para } + \\ &= ((\overline{a}+\overline{b})\Downarrow a)\cdot((\overline{a}+\overline{b})+b) && \text{por la ley distributiva de } + \text{ sobre } \cdot \\ &= ((\overline{b}+\overline{a})+a)\cdot(\overline{a}+(\overline{b}+b)) && \text{por las leyes conmutativa y asociativa para } + \\ &= (\overline{b}+)\overline{a}+a))\cdot(\overline{a}+)b \quad \overline{b})) && \text{por las leyes asociativa y conmutativa para } + \\ &= (\overline{b}+)a+\overline{a}))\cdot(\overline{a}+1) && \text{por las leyes conmutativa y del complemento para } +, \\ &= (\overline{b}+1)\cdot 1 && \text{por las leyes del complemento y de cota universal para } + \\ &= 1\cdot 1 && \text{por la ley de cota universal para} \\ &= 1 && \text{por la ley de identidad para } \cdot \end{aligned}$$

Ahora demostremos que $(a\cdot b)\cdot(\overline{a}+\overline{b})=0$.

$$\begin{aligned} & (a\cdot b)\cdot(\overline{a}+\overline{b}) \\ &= ((a\cdot b)\cdot\overline{a})+(((a\cdot b)\cdot\overline{b}) && \text{por la ley distributiva de } \cdot \text{ respecto a } + \\ &= ((b\cdot a)\cdot\overline{a})+((a\cdot(b\cdot\overline{b})) && \text{por las leyes conmutativa y asociativa para } \cdot \\ &= (b\cdot)a\cdot\overline{a}))+(a\cdot 0) && \text{por las leyes asociativa y del complemento para } \cdot \\ &= (b\cdot 0)+0 && \text{por las leyes del complemento y de cota universal para } \cdot \\ &= 0+0 && \text{por la ley de cota universal para } \cdot \\ &= 0 && \text{por la ley de identidad para } + \end{aligned}$$

Como $(a\cdot b)+(\overline{a}+\overline{b})=1$ y $(a\cdot b)\cdot(\overline{a}+\overline{b})=0$, se tiene, por la unicidad de la ley del complemento, que $\overline{a\cdot b}=\overline{a}+\overline{b}$.

10. *Sugerencia:* Una forma de demostrar el enunciado es utilizar el resultado del ejercicio 3. Algunos pasos en la demostración son los siguientes:

$$y=(y+x)\cdot y=(x\cdot y)+(z\cdot y)=z\cdot(x+y)=z.$$

11. a. (i) Como S sólo tiene dos elementos distintos, 0 y 1, entonces solamente necesitamos checar que $0 + 1 = 1 + 0$. Pero esto es verdadero porque las sumas dan 1.

(v) *Respuesta parcial:*

$0 + (0 \cdot 0) = 0 + 0 = 0$ y $(0 = 0) \cdot (0 + 0) = 0 \cdot 0 = 0$ también
$0 + (0 \cdot 1) = 0 + 0 = 0$ y $(0 = 0) \cdot (0 + 1) = 0 \cdot 1 = 0$ también
$0 + (1 \cdot 0) = 0 + 0 = 0$ y $(0 = 1) \cdot (0 + 0) = 1 \cdot 0 = 0$ también
$0 + (1 \cdot 1) = 0 + 1 = 1$ y $(0 = 1) \cdot (0 + 1) = 1 \cdot 1 = 1$ también

b. *Sugerencia:* Compruebe que $0 + x = x$ y que $1 \cdot x = x$ para todo $x \in S$.

12. *Sugerencias:* 1) Como las demostraciones de las leyes de absorción no utilizan las leyes asociativas, las leyes de absorción se pueden emplear en cualquier paso de la deducción.

2) Demuestre que para todas x, y y z en B, $x\,(x + (y + z)) \cdot x = x$ y $((x + y) + z)) \cdot x = x$.

3) Demuestre que para todas a, b y c en B, tanto $a + (b + c)$ como $(a + b) + c$ son iguales a $((a + b) + c) \cdot (a + (b + c))$.

4) Use las leyes de De Morgan y la ley del doble complemento para deducir la ley asociativa para $\cdot$.

13. La frase no es un enunciado ni verdadero ni falso. Si la frase fuera verdadera, entonces como ella se declara falsa a sí misma, la frase sería falsa. Por tanto, la frase no es verdadera. Por otro lado, si la frase fuera falsa, entonces sería falso que "Esta frase es falsa" y así la frase sería verdadera. En consecuencia, la frase no es falsa.

14. Esta frase es un enunciado porque es verdadera. Recuerde que la única manera en que un enunciado si-entonces sea falso es que la hipótesis sea verdadera y la conclusión falsa. En este caso la hipótesis no es verdadera. Así sin considerar lo que establece la conclusión, la frase es verdadera. (Esto es un ejemplo de un enunciado que es vacuamente verdadero, o verdadero por defecto).

17. Esta frase no es un enunciado porque no es ni verdadera ni falsa. Si la frase fuera verdadera, entonces la frase es falsa o $1 + 1 = 3$. Pero $1 + 1 \neq 3$ y así la frase es falsa. Por tanto, la frase no es verdadera. Por otro lado, si la frase fuera falsa, entonces sería verdadero que "Esta frase es falsa o $1 + 1 = 3$" y así la frase sería verdadera. En consecuencia, la frase no es falsa.

20. *Sugerencia:* Suponga que aparte del enunciado (ii), todas las otras afirmaciones de Nixon sobre Watergate están uniformemente divididas en verdaderas y falsas.

21. No. Suponga que hubiera un programa de computadora P que tuviera como salida una lista de todos los programas de computadoras que no se enumeran a sí mismos en su salida. Si P se enumera a sí mismo como salida, entonces estaría en la lista de salida de P, que consiste de todos los programas de computadoras que no se enumeran a sí mismos en su salida. Así que P no se enumeraría a sí mismo como salida. Pero si P no se enumera a sí mismo como salida, entonces P sería miembro de la lista de todos los programas de computadoras que no se enumeran a sí mismos en su salida y esta lista es exactamente la salida de P. Por tanto, P se enumeraría a sí mismo como salida. Este análisis muestra que la suposición de la existencia de tal programa P es contradictoria, así que no existe tal programa.

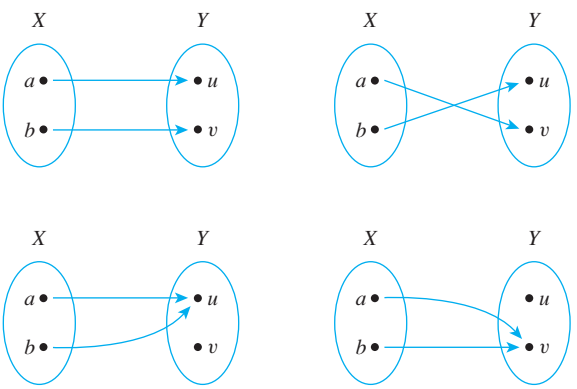
25. *Sugerencia:* Demuestre que cualquier algoritmo que resuelve el problema de impresión se puede adaptar para producir un algoritmo que resuelva el problema del paro.

Sección 7.1:

1. a. dominio de $f = \{1, 3, 5\}$, codominio de $f = \{s, t, u, v\}$
b. $f(1) = v, f(3) = s, f(5) = v$
c. rango de $f = \{s, v\}$
d. sí, no
e. imagen inversa de $s = \{3\}$, imagen inversa de $u = \emptyset$, imagen inversa de $v = \{1, 5\}$
f. $\{(1, v), (3, s), (5, v)\}$

3. a. Verdadero. La definición de función dice que para cualquier entrada sólo existe una salida, así si dos entradas son iguales, entonces sus salidas también deben ser iguales.
c. Verdadero. La definición de función no prohíbe este hecho.

4. a. Hay cuatro funciones, de X a Y, como se muestra a continuación:



5. a. $I_{\mathbf{Z}}(e) = e$
b. $I_{\mathbf{Z}}\left(b_i^{jk}\right) = b_i^{jk}$

6. a. La sucesión está dada por la función f: $\mathbf{Z}^{no\text{-}neg} \to \mathbf{R}$ se define por la regla

$$f(n) = \frac{(-1)^n}{2n + 1}$$ para todos los enteros n no-negativos.

7. a. 1 *[porque existe un número impar de elementos en* $\{1, 3, 4\}$*]*
c. 0 *[porque existe un número par de elementos en* $\{2, 3\}$*]*

8. a. $F(0) = (0^3 + 2 \cdot 0 + 4)\ mod\ 5 = 4\ mod\ 5 = 4$
b. $F(1) = (1^3 + 2 \cdot 1 + 4)\ mod\ 5 = 7\ mod\ 5 = 2$

9. a. $S(1) = 1$ **b.** $S(15) = 1 + 3 + 5 + 15 = 24$
c. $S(17) = 1 + 17 = 18$

10. a. $T(1) = \{1\}$ **b.** $T(15) = \{1, 3, 5, 15\}$
c. $T(17) = \{1, 17\}$

11. a. $F(4, 4) = (2 \cdot 4 + 1, 3 \cdot 4 - 2) = (9, 10)$
b. $F(2, 1) = (2 \cdot 2 + 1, 3 \cdot 1 - 2) = (5, 1)$

12. a. $G(4, 4) = ((2 \cdot 4 + 1)\ mod\ 5, (3 \cdot 4 - 2)\ mod\ 5) = (9\ mod\ 5, 10\ mod\ 5) = (4, 0)$
b. $G(2, 1) = ((2 \cdot 2 + 1)\ mod\ 5, (3 \cdot 1 - 2)\ mod\ 5) = (5\ mod\ 5, 1\ mod\ 5) = (0, 1)$

13.

x	$f(x)$	$g(x)$
0	$4^2 \ mod\ 5 = 1$	$(0^2 + 3\cdot 0 + 1) \ mod\ 5 = 1$
1	$5^2 \ mod\ 5 = 0$	$(1^2 + 3\cdot 1 + 1) \ mod\ 5 = 0$
2	$6^2 \ mod\ 5 = 1$	$(2^2 + 3\cdot 2 + 1) \ mod\ 5 = 1$
3	$7^2 \ mod\ 5 = 4$	$(3^2 + 3\cdot 3 + 1) \ mod\ 5 = 4$
4	$8^2 \ mod\ 5 = 4$	$(4^2 + 3\cdot 4 + 1) \ mod\ 5 = 4$

La tabla muestra que $f(x) = g(x)$ para toda x en J_5. Así, por definición de igualdad de funciones, $f = g$.

15. $F \cdot G$ y $G \cdot F$ son iguales porque para todos los números reales x,

$$\begin{aligned}(F\cdot G)(x) &= F(x)\cdot G(x) && \text{por definición de } F\cdot G\\ &= G(x)\cdot F(x) && \text{por la ley conmutativa para la multiplicación de números reales}\\ &= (G\cdot F)(x) && \text{por definición de } G\cdot F.\end{aligned}$$

17. **a.** $2^3 = 8$ **c.** $4^1 = 4$

18. **a.** $\log_3 81 = 4$ porque $3^4 = 81$

c. $\log_3\left(\frac{1}{27}\right) = -3$ porque $3^{-3} = \frac{1}{27}$

19. Sea b un número real positivo arbitrario con $b \neq 1$. Como $b^1 = b$, entonces por definición de logaritmo, $\log_b b = 1$.

21. *Demostración:* Supongamos que b y u son cualesquiera dos números reales positivos. *[Debemos demostrar que* $\log_b\left(\frac{1}{u}\right) = -\log_b(u)$*.]* Sea $v = \log_b\left(\frac{1}{u}\right)$. Por definición de logaritmo, $b^v = \frac{1}{u}$. Multiplicando ambos lados por u y dividiendo por b^v se obtiene $u = b^{-v}$ y así, por definición de logaritmo, $-v = \log_b(u)$. Ahora multiplicando ambos lados de esta ecuación por -1 para obtener que $v = -\log_b(u)$. Por tanto, $\log_b\left(\frac{1}{u}\right) = -\log_b(u)$ porque ambas expresiones son iguales a v. *[Que era lo que se quería demostrar.]*

22. *Sugerencia:* Use una demostración por contradicción. Suponga que $\log_3 7 = \frac{a}{b}$ para algunos enteros a y b con $b \neq 0$. Aplique la definición de logaritmo para reescribir $\log_3 7 = \frac{a}{b}$ en forma exponencial.

23. Suponga que b y y son números reales positivos con $\log_b y = 3$. Por definición de logaritmo, esto implica que $b^3 = y$. Entonces

$$y = b^3 = \frac{1}{\frac{1}{b^3}} = \frac{1}{\left(\frac{1}{b}\right)^3} = \left(\frac{1}{b}\right)^{-3}.$$

Así, por definición de logaritmo (con base $1/b$), $\log_{1/b}(y) = -3$.

25. **a.** $p_1(2, y) = 2$, $p_1(5, x) = 5$, rango de $p_1 = \{2, 3, 5\}$

26. **a.** $mod(67, 10) = 7$ y $div(67, 10) = 6$ porque $67 = 10\cdot 6 + 7$.

27. $f(aba) = 0$ *[porque no existe b a la izquierda de la a más a la izquierda en aba]*

$f(bbab) = 2$ *[porque hay dos b a la izquierda de la a más a la izquierda en bbab]*

$f(b) = 0$ *[porque la cadena b no contiene a]*

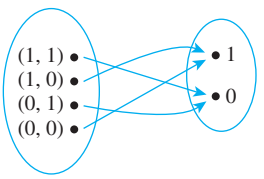
rango de $f = Z^{no\text{-}neg}$

28. **a.** $E(0110) = 000111111000$ y

$D(111111000111) = 1101$

29. **a.** $H(10101,00011) = 3$

30. **a.** Dominio de f Codominio de f



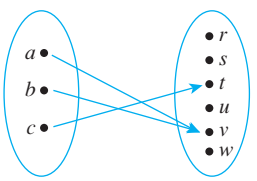
32. **a.** $f(1, 1, 1) = (4\cdot 1 + 3\cdot 1 + 2\cdot 1) \ mod\ 2 = 9 \ mod\ 2 = 1$

$f(0, 0, 1) = (4\cdot 0 + 3\cdot 0 + 2\cdot 1) \ mod\ 2 = 2 \ mod\ 2 = 0$

33. Si g estuviera bien definida, entonces $g(1/2) = g(2/4)$ porque $1/2 = 2/4$. Sin embargo, $g(1/2) = 1 - 2 = -1$ y $g(2/4) = 2 - 4 = -2$. Como $-1 \neq -2$, $g(1/2) \neq g(2/4)$. Así g no está bien definida.

35. El estudiante B está en lo correcto. Si R estuviera bien definida, entonces $R(3)$ tendría un valor unívocamente determinado. Sin embargo, por un lado, $R(3) = 2$ porque $(3\cdot 2) \ mod\ 5 = 1$ y, por otro lado, $R(3) = 7$ porque $(3\cdot 7) \ mod\ 5 = 1$ y así R no está bien definida.

38. **a.**

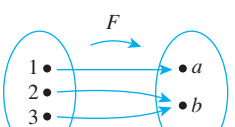


b. $f(A) = \{v\}$, $f(X) = \{t, v\}$, $f^{-1}(C) = \{c\}$, $f^{-1}(D) = \{a, b\}$, $f^{-1}(E) = \emptyset$ $f^{-1}(Y) = \{a, b, c\} = X$

40. *Respuesta parcial:* **(a)** $y \in F(A)$ or $y \in F(B)$, **(b)** alguno, **(c)** $A \cup B$, **(d)** $F(A \cup B)$

41. El enunciado es verdadero. *Demostración:* Sea F una función de X a Y y supongamos que $A \subseteq X$, $B \subseteq X$ y $A \subseteq B$. Sea $y \in F(A)$. *[Debemos demostrar que* $y \in F(B)$*.]* Entonces, por definición de imagen de un conjunto, $y = F(x)$ para algún $x \in A$. Como $A \subseteq B$, $x \in B$, entonces $y = F(x)$ para algún $x \in B$. Por tanto, $y \in F(B)$ *[que era lo que se quería demostrar]*.

43. El enunciado es falso. *Contraejemplo:* Sean $X = \{1, 2, 3\}$, $Y = \{a, b\}$ y defínase una función $F: X \to Y$ mediante el diagrama que se muestra a continuación.



Sean $A = \{1, 2\}$ y $B = \{1,3\}$. Entonces $F(A) = \{a, b\} = F(B)$ y así $F(A) \cap F(B) = \{a, b\}$. Pero $F(A \cap B) = F(\{1\}) = \{a\} \neq \{a, b\}$. Por tanto, $F(A) \cap F(B) \not\subseteq F(A \cap B)$.

(Este es sólo uno de muchos posibles contraejemplos).

45. El enunciado es verdadero. *Demostración:* Sea F una función de un conjunto X a un conjunto Y y supóngase que $C \subseteq Y$, $D \subseteq Y$ y $C \subseteq D$. *[Debe demostrarse que* $F^{-1}(C) \subseteq F^{-1}(D)$*.]* Suponga que $x \in F^{-1}(C)$. Así $F(x) \in C$. Como $C \subseteq D$, entonces también $F(x) \in D$. Por tanto, por definición de imagen inversa, $x \in F^{-1}(D)$. *[Así* $F^{-1}(C) \subseteq F^{-1}(D)$*.]*

46. *Sugerencia:* $x \in F^{-1}(C \cup D) \Leftrightarrow F(x) \in C \cup D \Leftrightarrow F(x) \in C$ o $F(x) \in D$

51. a. $\phi(15) = 8$ *[porque* 1, 2, 4, 7, 8, 11, 13, y 14 *no tienen factores en común con* 15, *excepto* ± 1*]*

b. $\phi(2) = 1$ *[porque* 1 *es el único entero positivo menor o igual que* 2 *no teniendo factores en común con* 2 *excepto* ± 1*]*

c. $\phi(5) = 4$ *[porque* 1,2,3, *y* 4 *no tienen factores en común con* 5 *excepto* $\pm$ 1*]*

52. *Demostración:* Sea p cualquier número primo y n cualquier entero con $n \geq 1$. Hay p^{n-1} enteros positivos menores o iguales que p^n, que tienen un factor común (distinto a $+1$ y -1) con p^n, a saber, p, $2p$, $3p$,…, $(p^{n-1})p$. Así que, por la regla de la diferencia, existen $p^n - p^{n-1}$ enteros positivos menores o iguales que p^n, que no tienen un factor común con p^n excepto ± 1.

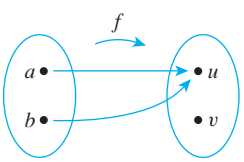
53. *Sugerencia:* Use el resultado del ejercicio 52 con $p = 2$.

Sección 7.2

1. El segundo enunciado es el contrapositivo del primero.

2. a. máximo **b.** mínimo

3. *Sugerencia:* Abajo se da y se explica un contraejemplo. Dar un contraejemplo diferente y acompañarlo con una explicación. *Contraejemplo:* Considere la función definida por el siguiente diagrama:



Observe que a se manda a exactamente un elemento de Y, a saber, u y b también se envía a exactamente un elemento de Y, a saber, también a u. Así es verdadero que cada elemento de X es mapeado a exactamente un elemento de Y. Pero f no es inyectiva porque $f(a) = f(b)$ y $a \neq b$. *[Observe que decir, "Cada elemento de X es enviado a exactamente un elemento de Y", es justamente otra manera de decir que en el diagrama para la función sólo existe una flecha desde cada elemento de X. Pero este enunciado es parte de la definición de cualquier función y no solo de una función inyectiva.]*

4. *Sugerencia:* El enunciado es verdadero.

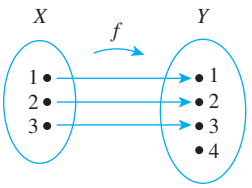
5. *Sugerencia:* Una de las formas incorrectas es b).

6. a. f no es uno a uno porque $f(1) = 4 = f(9)$ y $1 \neq 9$. f no es sobreyectiva porque $f(x) \neq 3$ para cualquier x en X.

b. g es inyectiva porque $g(1) \neq g(5)$, $g(1) \neq g(9)$ y $g(5) \neq g(9)$. g es sobreyectiva porque cada elemento de Y es la imagen de algún elemento de X: $3 = g(5)$, $4 = g(9)$ y $7 = g(1)$.

7. a. F no es inyectiva porque $F(c) = x = F(d)$ y $c \neq d$. F es sobreyectiva porque cada elemento de Y es la imagen de algún elemento de X: $x = F(c) = F(d)$, $y = F(a)$ y $z = F(b)$.

9. a. Un ejemplo de muchos es el siguiente:



10. a. (i) *f es inyectiva:* Supongamos que $f(n_1) = f(n_2)$ para algunos enteros n_1 y n_2. *[Debemos demostrar que* $n_1 = n_2$*.]* Por definición de f, $2n_1 = 2n_2$ y dividiendo ambos lados entre 2 se obtiene $n_1 = n_2$, que era lo que se quería demostrar.

(ii) *f no es sobreyectiva:* Consideremos $1 \in \mathbf{Z}$. Afirmamos que $1 \neq f(n)$, para cualquier entero n, porque si existiera un entero n tal que $1 = f(n)$, entonces, por definición de f, $1 = 2n$. Dividiendo ambos lados entre 2 daría que $n = 1/2$. Pero $1/2$ no es un entero. Así que $1 \neq f(n)$ para cualquier entero n, Por tanto, f no es sobreyectiva.

b. *h es sobreyectiva:* Supongamos que $m \in 2\mathbf{Z}$. *[Debemos demostrar que existe un entero n tal que* $h(n) = m$*.] Como* $m \in 2\mathbf{Z}$*, entonces* $m = 2k$ para algún entero k. Sea $n = k$. Entonces $h(n) = 2n = 2k = m$. Así existe un entero (a saber, n) tal que $h(n) = m$. Esto es lo que se quería demostrar.

11. *Sugerencias:* **a**. (i) g es uno a uno (ii) g no es sobreyectiva

b. G es sobreyectiva. *Demostración:* Suponga que y es cualquier elemento de $\mathbf{R}$. *[Debemos demostrar que existe un elemento* x *en* $\mathbf{R}$ *tal que* $G(x) = y$*. ¿Qué x sería si existe? El análisis muestra que x sería igual a* $(y + 5)/4$*. Entonces la prueba debe demostrar que x tiene las propiedades necesarias.]* Sea $x = (y + 5)/4$. Entonces (1) $x \in \mathbf{R}$ y (2) $(x) = G((y + 5)/4) = 4[(y + 5)/4] - 5 = (y + 5) - 5 = y$ *[que era lo que se quería demostrar].*

13. a. (i) *H no es inyectiva:* $H(1) = 1 = H(-1)$ pero $1 \neq -1$

(ii) *H no es sobreyectiva:* $H(x) \neq -1$ para cualquier número real x (porque ningún número real tiene cuadrado negativo).

14. La "demostración" afirma que f es inyectiva porque para cada entero n sólo existe un valor posible para $f(n)$. Pero decir que para cada entero n sólo existe un valor posible para $f(n)$ es justamente otra forma de decir que f satisface una de las condiciones necesarias para ser una función. Para demostrar que f es inyectiva, se debe demostrar que cualquier entero n tiene un valor funcional diferente a cualquier otro entero m con $n \neq m$.

15. f es inyectiva. *Demostración:* Suponga que $f(x_1) = f(x_2)$ en donde x_1 y x_2 son números reales distintos de cero. *[Debemos demostrar que* $x_1 = x_2$*.]* Por definición de f,

$$\frac{x_1 + 1}{x_1} = \frac{x_2 + 1}{x_2}$$

y al multiplicar en cruz se obtiene

$$x_1x_2 + x_2 = x_1x_2 + x_1,$$

y así

$$x_1 = x_2 \qquad \text{al restar } x_1 \text{ } x_2 \text{ de ambos lados}$$

[que era lo que se quería demostrar].

16. f no es inyectiva. Observe que:

$$\begin{aligned}\frac{x_1}{x_1^2+1} = \frac{x_2}{x_2^2+1} &\Rightarrow x_1x_2^2 + x_1 = x_2x_1^2 + x_2\\ &\Rightarrow x_1x_2^2 - x_2x_1^2 = x_2 - x_1\\ &\Rightarrow x_1x_2(x_2 - x_1) = x_2 - x_1\\ &\Rightarrow x_1 = x_2 \text{ or } x_1x_2 = 1.\end{aligned}$$

Así para un contraejemplo tome cualesquier x_1 y x_2 con $x_1 \neq x_2$ pero $x_1x_2 = 1$. Digamos, tome $x_1 = 2$ y $x_2 = 1/2$. Entonces $f(x_1) = f(2) = 2/5$ y $f(x_2) = f(1/2) = 2/5$, pero $2 \neq 1/2$.

19. a. Observe que $\frac{417302072}{7} \cong 59614581.7$ y

$417302072 - 7 \cdot 59614581 = 5$, $h(417\text{-}30\text{-}2072) = 5$.
Pero la posición 5 ya está ocupada, así se comprueba la siguiente posición. Está libre y entonces el registro se coloca en la posición 6.

20. Recuerde que $\lfloor x \rfloor$ = único entero n tal que $n \leq x < n + 1$.

a. *Piso no es inyectiva:*

Piso(0) = 0 = Piso (1/2) pero $0 \neq 1/2$.

b. *Piso es sobreyectiva:* Supóngase que $m \in \mathbf{Z}$. *[Debemos demostrar que existe un número real y tal que Piso*$(y) = m$*.]* Sea $y = m$. Entonces Piso(y) = Piso$(m) = m$ porque m es un entero. (Realmente, Piso toma el valor m para todos los números reales en el intervalo $m \leq x < m + 1$). Por tanto, existe un número real y tal que Piso$(y) = m$. Esto es lo que se quería demostrar.

21. a. *l no es uno a uno:* $l(0) = l(1) = 1$ pero $1 \neq 0$.

b. *l es sobreyectiva:* Supóngase que n es un entero no-negativo. *[Debemos demostrar que existe una cadena s en S tal que* $l(s) = n$*.]* Sea

$$s = \begin{cases} \epsilon \text{ (la cuerda nula)} & \text{si } n = 0 \\ \underbrace{00\ldots0}_{n \text{ 0's}} & \text{si } n > 0 \end{cases}.$$

Entonces $l(s)$ = la longitud de $s = n$. Que era lo que se quería demostrar.

23. a. *F no es inyectiva:* Sean $A = \{a\}$ y $B = \{b\}$. Entonces $F(A) = F(B) = 1$ pero $A \neq B$.

24. b. *N no es sobreyectiva:* El número -1 está en $\mathbf{Z}$ pero $N(s) \neq -1$ para cualquier cadena s en S porque ninguna cadena tiene un número negativo de a.

26. S no es inyectiva. *Contraejemplo:* $S(6) = 1 + 2 + 3 + 6 = 12$ y $S(11) = 1 + 11 = 12$. Así $S(6) = S(11)$ pero $6 \neq 11$.

S no es sobreyectiva. *Contraejemplo:* Para que exista un entero positivo n tal que $S(n) = 5$, entonces n tendría que ser menor que 5. Pero $S(1) = 1$, $S(2) = 3$, $S(3) = 4$ y $S(4) = 7$. Entonces no existe un entero positivo n tal que $S(n) = 5$.

27. *Sugerencia:* **a**. T no es inyectiva. **b**. T no es sobreyectiva.

28. a. G es uno a uno. *Demostración:* Suponga que (x_1, y_1) y (x_2, y_2) son elementos cualesquiera de $\mathbf{R} \times \mathbf{R}$ tales que $G(x_1, y_1) = G(x_2, y_2)$. *[Debemos demostrar que* $(x_1, y_1) = (x_2, y_2)$*.]* Entonces, por definición de G, $(2y_1, -x_1) = (2y_2, -x_2)$ y, por definición de par ordenado,

$$2y_1 = 2y_2 \text{ y } -x_1 = -x_2.$$

Dividiendo ambos lados de la ecuación de la izquierda por 2 y ambos lados de la ecuación de la derecha por -1, se obtiene que

$$y_1 = y_2 \text{ y } x_1 = x_2,$$

entonces, por definición de par ordenado, $(x_1, y_1) = (x_2, y_2)$ *[que era lo que se quería demostrar]*.

b. G es sobreyectiva. *Demostración:* Suponga que (u, v) es un elemento arbitrario de $\mathbf{R} \times \mathbf{R}$. *[Debemos demostrar que existe un elemento* (x, y) *en* $\mathbf{R} \times \mathbf{R}$ *tal que* $G(x, y) = (u, v)$*.]* Sea $(x, y) = (-v, u/2)$. Entonces 1) $(x, y) \in \mathbf{R} \times \mathbf{R}$ y 2) $G(x, y) = (2y, x) = (2(u/2), -(-v)) = (u, v)$ *[que era lo que se quería demostrar]*.

31. a. *Sugerencia: F* es inyectiva. En la demostración use el teorema de factorización única de los enteros.

32. a. Sean $x = \log_8 27$ y $y = \log_2 3$. *[La pregunta es: ¿*$x = y$*?]* Por definición de logaritmo, ambas ecuaciones se pueden escribir en forma exponencial como

$$8^x = 27 \text{ y } 2^y = 3.$$

Ahora $8 = 2^3$. Así

$$8^x = (2^3)^x = 2^{3x}.$$

También $27 = 3^3$ y $3 = 2^y$. En consecuencia

$$27 = 3^3 = (2^y)^3 = 2^{3y}.$$

Así que, como $8^x = 27$,

$$2^{3x} = 2^{3y}.$$

Por (7.2.5), entonces,

$$3x = 3y,$$

Por tanto

$$x = y.$$

Pero $x = \log_8 27$ y $y = \log_2 3$ y así $\log_8 27 = y = \log_2 3$ y la respuesta a la pregunta es si.

33. *Demostración:* Suponga que b, x y y son números reales positivos con $b \neq 1$. Sean $u = \log_b(x)$ y $v = \log_b(y)$. Por definición de logaritmo, $b^u = x$ y $b^v = y$. Sustituyendo, $\frac{x}{y} = \frac{b^u}{b^v} = b^{u-v}$ *[por (7.2.3) y el hecho de que* $b^{-v} = \frac{1}{b^v}$*]*. Traduciendo $\frac{x}{y} = b^{u-v}$ a su forma logarítmica se obtiene $\log_b\left(\frac{x}{y}\right) = u - v$ y así, sustituyendo, $\log_b\left(\frac{x}{y}\right) = \log_b(x) - \log_b(y)$ *[que era lo que se quería demostrar]*.

35. *Inicio de la demostración:* Suponga que a, b y x son *[particulares pero arbitrariamente elegidos]* números reales tales que b y x son positivos con $b \neq 1$. *[Debemos demostrar que* $\log_b(x^a) = a \log_b x$*.]* Sea

$$r = \log_b(x^a) \text{ y } s = \log_b x.$$

36. No. *Contraejemplo:* Defina f: $\mathbf{R} \to \mathbf{R}$ y g: $\mathbf{R} \to \mathbf{R}$ como sigue: $f(x) = x$ y $g(x) = -x$ para todos los números reales x. Entonces f y g son inyectiva *[porque para todos los números reales* x_1 *y* x_2*, si* $f(x_1) = f(x_2)$ *entonces* $x_1 = x_2$ *y si* $g(x_1) = g(x_2)$*, por tanto* $-x_1 = -x_2$ *y así* $x_1 = x_2$*]*, pero $f + g$ no es inyectiva *[porque* $f + g$

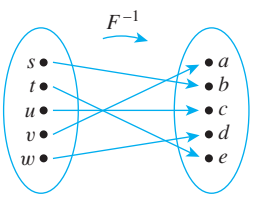
satisface la ecuación $(f + g)(x) = x + (-x) = 0$ *para todos los números reales* x *y así, por ejemplo,* $(f + g)(1) = (f + g)(2)$ *pero* $1 \neq 2$*].*

38. Sí. *Demostración:* Sea b una función inyectiva de $\mathbf{R}$ a $\mathbf{R}$ y aceptemos que c sea cualquier número real distinto de cero. Supóngase que $(cf)(x_1) = (cf)(x_2)$. *[Debemos demostrar que* $x_1 = x_2$*.]* Se tiene por definición de cf que $cf(x_1) = cf(x_2)$. Como $c \neq 0$, podemos dividir ambos lados de la ecuación por c para obtener que $f(x_1) = f(x_2)$. Y como f es uno a uno, esto implica que $x_1 = x_2$ *[que era lo que se quería demostrar].*

40. a. *Sugerencia:* Se necesita la suposición de que F es inyectiva durante la demostración de $F^{-1}(F(A)) \subseteq A$. Si $F(r) \in F(A)$, la definición de imagen de un conjunto implica que existe un elemento x en A tal que $F(r) = F(x)$.

b. *Sugerencia:* Al demostrar que $F(A_1) \cap F(A_2) \subseteq F(A_1 \cap A_2)$ se necesita la suposición de que F es inyectiva. Si $u \in F(A_1)$ y $u \in F(A_2)$, entonces la definición de imagen de un conjunto implica que hay elementos x_1 en A_1 y x_2 en A_2 tales que $F(x_1) = u$ y $F(x_2) = u$ y, así, que $F(x_1) = F(x_2)$.

42.



44. La función no es sobreyectiva. Así que no es una correspondencia inyectiva.

45. La respuesta al ejercicio 10(b) muestra que h es sobreyectiva. Para demostrar que h es inyectiva, supóngase que $h(n_1) = h(n_2)$. Por definición de h, esto implica que $2n_1 = 2n_2$. Dividiendo ambos lados entre 2 se obtiene $n_1 = n_2$. Por tanto, h es inyectiva.

Dado cualquier entero par m, si $m = h(n)$, entonces por definición de h, $m = 2n$ y así $n = m/2$. Entonces

$$h^{-1}(m) = \frac{m}{2} \text{ para todo } m \in 2\mathbf{Z}.$$

46. La función g no es una correspondencia inyectiva porque no es sobreyectiva. Por ejemplo, si $m = 2$, es imposible encontrar un entero n tal que $g(n) = m$. (Esto es porque si $g(n) = m$, entonces $4n - 5 = 2$, que implica que $n = 7/4$. Así el único número n con la propiedad de que $g(n) = m$ es $7/4$. Pero $7/4$ no es un entero.

47. La respuesta al ejercicio 11b muestra que G es sobreyectiva. Además, G es inyectiva. Para demostrar esto, supóngase que $G(x_1) = G(x_2)$ para algunos x_1 y x_2 en $\mathbf{R}$. *[Debemos demostrar que* $x_1 = x_2$*.]* Por definición de G, $4x_1 - 5 = 4x_2 - 5$. Sume 5 en ambos lados de esta ecuación y divida ambos lados entre 4 para obtener que $x_1 = x_2$ *[que era lo que se quería demostrar].* Afirmamos que $G^{-1}(y) = (y + 5)/4$. Por definición de función inversa, esto es verdadero si y sólo si, $G((y + 5)/4) = y$. Pero $G((y + 5)/4) = 4((y + 5)/4) - 5 = (y + 5) - 5 = y$, entonces $G^{-1}(y) = (y + 5)/4$.

50. La función no es inyectiva. Así que no es una correspondencia uno a uno.

52. La respuesta del ejercicio 15 demuestra que f es inyectiva y si el codominio se toma como el conjunto de todos los números reales diferentes de 1, entonces f también es sobreyectiva. *[La razón es que dado cualquier número real* $y \neq 1$*, si tomamos* $x = \frac{1}{y-1}$*, entonces*

$$f(x) = f\left(\frac{1}{y-1}\right) = \frac{\frac{1}{y-1} + 1}{\frac{1}{y-1}} = \frac{1 + (y-1)}{1} = y.]$$

$$f^{-1}(y) = \frac{1}{y-1} \text{ para cada número real } y \neq 1.$$

53. *Sugerencia:* ¿Existe un número real x tal que $f(x) = 1$?

57. *Sugerencia:* Sea una función F dada y supongamos que el dominio de D se representa como un arreglo unidimensional $a[1], a[2],\ldots, a[n]$. Introducimos una variable *respuesta* cuyo valor inicial es "inyectiva". La parte principal del cuerpo del algoritmo se podría escribir como se muestra a continuación:

while ($i \leq n - 1$ y *respuesta* = "uno a uno")
  $j := i + 1$
  while ($j \leq n$ y *respuesta* = "uno a uno")
    if ($F(a[i]) = F(a[j])$ y $a[i] \neq a[j]$)
    then *respuesta*: = "no es uno a uno"
    $j := j + 1$
  end while
  $i := i + 1$
end while

¿Qué puede decirse si la ejecución llega a este punto?

58. *Sugerencia:* Sea F una función dada y supóngase que el dominio y el codominio de F están representados por los arreglos unidimensionales $a[1], a[2],\ldots, a[n]$ y $b[1], b[2],\ldots, b[m]$, respectivamente. Introducir una variable *respuesta* cuyo valor inicial es "sobreyectiva". Para cada $b[i]$ de $i = 1$ a m, realizar una búsqueda a través de $a[1], a[2],\ldots, a[n]$ para checar si $b[i] = F(a[j])$ para algún $a[j]$. Introducir una variable booleana para indicar si una búsqueda ha sido exitosa. (Poner la variable igual a 0 antes del inicio de cada búsqueda y ponerla igual a 1 si la búsqueda tiene éxito). Al final de cada búsqueda, compruebe el valor de la variable booleana. Si ésta es 0, entonces F no es sobreyectiva. Si todas las búsquedas son exitosas, entonces F es sobreyectiva.

Sección 7.3

1. $g \circ f$ está definida como sigue:

$$(g \circ f)(1) = g(f(1)) = g(5) = 1,$$
$$(g \circ f)(3) = g(f(3)) = g(3) = 5,$$
$$(g \circ f)(5) = g(f(5)) = g(1) = 3.$$

$f \circ g$ está definida como sigue:

$$(f \circ g)(1) = f(g(1)) = f(3) = 3,$$
$$(f \circ g)(3) = f(g(3)) = f(5) = 1,$$
$$(f \circ g)(5) = f(g(5)) = f(1) = 5.$$

Entonces $g \circ f \neq f \circ g$ porque, por ejemplo, $(g \circ f)(1) \neq (f \circ g)(1)$.

3. $(G \circ F)(x) = G(F(x)) = G(x^3) = x^3 - 1$ para todos los números reales x.
$(F \circ G)(x) = F(G(x)) = F(x-1) = (x-1)^3$ para todos los números reales x.
$G \circ F \neq F \circ G$ porque, por ejemplo $(G \circ F)(2) = 2^3 - 1 = 7$, mientras que $(F \circ G)(2) = (2-1)^3 = 1$.

6. $(G \circ F)(0) = G(F(0)) = G(7(0) = G(0) = 0 \ mod\ 5 = 0$
$(G \circ F)(1) = G(F(1)) = G(7(1) = G(7) = 7 \ mod\ 5 = 2$
$(G \circ F)(2) = G(F(2)) = G(7(2) = G(14) = 14 \ mod\ 5 = 4$
$(G \circ F)(3) = G(F(3)) = G(7(3) = G(21) = 21 \ mod\ 5 = 1$
$(G \circ F((4) = G(F(4)) = G(7(4) = G(28) = 28 \ mod\ 5 = 3$

8. a.
$$(L \circ M)(12) = L(M(12)) = L(12 \ mod\ 5) = L(2) = 2^2 = 4$$
$$(M \circ L)(12) = M(L(12)) = M(12^2) = M(144) = 144 \ mod\ 5 = 4$$
$$(L \circ M)(9) = L(M(9)) = L(9 \ mod\ 5) = L(4) = 4^2 = 16$$
$$(M \circ L)(9) = M(L(9)) = M(9^2) = M(81) = 81 \ mod\ 5 = 1$$

9.
$$(F^{-1} \circ F)(x) = F^{-1}(F(x)) = F^{-1}(3x+2) = \frac{(3x+2)-2}{3} = \frac{3x}{3} = x = I_{\mathbf{R}}(x)$$

para toda x en $\mathbf{R}$. Así que $F^{-1} \circ F = I_{\mathbf{R}}$ por definición de igualdad de funciones.

$$(F \circ F^{-1})(y) = F(F^{-1}(y)) = F\left(\frac{y-2}{3}\right) = 3\left(\frac{y-2}{3}\right) + 2 = (y-2) + 2 = y = I_{\mathbf{R}}(y)$$

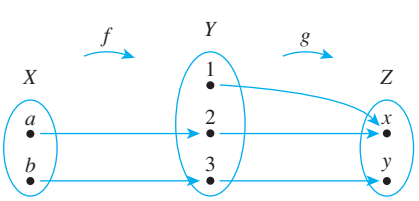
para toda y en $\mathbf{R}$. Entonces $F \circ F^{-1} = I_{\mathbf{R}}$ por definición de funciones.

12. a. Por definición de logaritmo de base b, para cada número real x, $\log_b(b^x)$ es el exponente al cual debe elevarse b para obtener b^x. Pero este exponente es justamente x. Entonces $\log_b(b^x) = x$.

13. *Sugerencia:* Suponga que f es cualquier función de un conjunto X a un conjunto Y y demuestre que para toda x en X, $(I_Y \circ f)(x) = f(x)$.

15. a. $s_k = s_m$

16. No. *Contraejemplo:* Defina f y g por el diagrama que sigue:



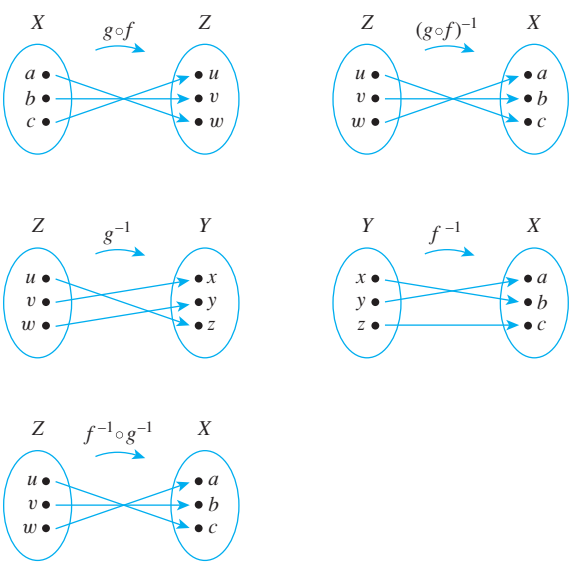
Entonces $g \circ f$ es inyectiva pero g no es inyectiva. (Así que es falso ¡que tanto f como g sean inyectiva por la ley de De Morgan!) (Este es un contraejemplo entre muchos otros. ¿Puede construir uno diferente?)

18. *Sugerencia:* Suponga que $f: X \to Y$ y $g: Y \to Z$ son funciones y que $g \circ f$ es inyectiva. Dados x_1 y x_2 en X, si $f(x_1) = f(x_2)$ Por tanto $(g \circ f)(x_1) = (g \circ f)(x_2)$.(¿Por qué?) Entonces use el hecho de que $g \circ f$ es inyectiva.

19. *Sugerencia:* Suponga que $f: X \to Y$ y $g: Y \to Z$ son funciones y $g \circ f$ es sobreyectiva. Dado $z \in Z$, existe un elemento x en X tal que $(g \circ f)(x) = z$. (¿Por qué?) Sea $y = f(x)$. Entonces $g(y) = z$.

21. *Verdadero. Demostración:* Suponga que X es cualquier conjunto y que f, g y h son funciones de X a X tales que h es inyectiva y $h \circ f = h \circ g$. *[Debemos demostrar que para todo x en X, f (x) = g(x).]* Acepte que x es un elemento arbitrario en X. Como $h \circ f = h \circ g$, tenemos que $(h \circ f)(x) = (h \circ g)(x)$ por definición de igualdad de funciones. Entonces, por definición de composición de funciones, $h(f(x)) = h(g(x))$. Debido a que h es inyectiva, esto implica que $f(x) = g(x)$ *[que era lo que se quería demostrar]*.

23.



Las funciones $(g \circ f)^{-1}$ y $f^{-1} \circ g^{-1}$ son iguales.

26. *Sugerencias:* 1) Los teoremas 7.3.3 y 7.3.4 juntos aseguran que $g \circ f$ es inyectiva y sobreyectiva. 2) Use la propiedad de la función inversa: $F^{-1}(b) = a$ si y sólo si $F(a) = b$, para todo a en el dominio de F y b en el dominio de F^{-1}.

Sección 7.4

1. El estudiante debería haber respondido que si A tiene la misma cardinalidad que B, significa que existe una función de A a B que es inyectiva y sobreyectiva. Un conjunto no puede tener la propiedad de estar en correspondencia uno a uno y sobreyectivo con otro conjunto: sólo una función puede tener esas propiedades.

2. Defina una función $f: \mathbf{Z}^+ \to S$ como sigue: Para todos los enteros positivos k, $f(k) = k^2$.

f es inyectiva: [Debemos demostrar que para todos $k_1, k_2 \in \mathbf{Z}^+$, si $f(k_1) = f(k_2)$ entonces $k_1 = k_2$.] Suponga que k_1 y k_2 son enteros positivos y $f(k_1) = f(k_2)$. Por definición de f, $(k_1)^2 = (k_2)^2$, así $k_1 = \pm k_2$. Pero k_1 y k_2 son *positivos*. Así que $k_1 = k_2$.

f es sobreyectiva: [Debemos demostrar que para todo $n \in S$, existe $k \in Z +$ tal que $n = f(k)$.] Suponga que $n \in S$. Por definición de S, $n = k^2$ para algún entero positivo k. Pero entonces por definición de f, $n = f(k)$.

Como existe f, función inyectiva y sobreyectiva, de $\mathbf{Z}^+$ a S, entonces los dos conjuntos tienen la misma cardinalidad.

3. Defina $f: \mathbf{Z} \to 3\mathbf{Z}$ mediante la regla $f(n) = 3n$ para todos los enteros n. La función f es inyectiva porque para cualesquiera enteros n_1 y n_2, si $f(n_1) = f(n_2)$ entonces $3n_1 = 3n_2$ y así $n_1 = n_2$. También f es sobreyectiva porque si m es un elemento arbitrario de $3\mathbf{Z}$, entonces $m = 3k$ para algún entero k. Pero entonces $f(k) = 3k = m$ por definición de f. Así, como existe una función $f: \mathbf{Z} \to 3\mathbf{Z}$ que es inyectiva y sobreyectiva, Por tanto $\mathbf{Z}$ tiene la misma cardinalidad que $3\mathbf{Z}$.

6. *Sugerencia:* Si $m \in 2\mathbf{Z}$, demuestre que $J(m) = J(m + 1) = m$.

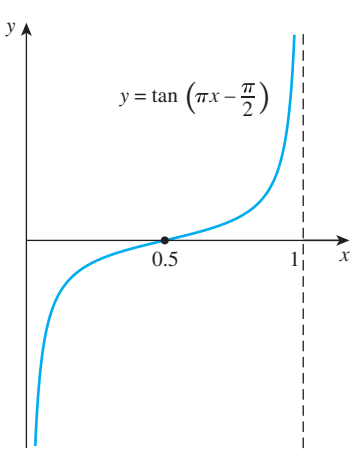
7. b. Para cada entero positivo n, $F(n) = (-1)^n \left\lfloor \frac{n}{2} \right\rfloor$.

8. En el ejemplo 7.4.2 se demostró que $\mathbf{Z}$ es infinito contable, lo que significa que $\mathbf{Z}^+$ tiene la misma cardinalidad que $\mathbf{Z}$. Por el ejercicio 3, $\mathbf{Z}$ tiene la misma cardinalidad que $3\mathbf{Z}$. De la propiedad transitiva de cardinalidad (teorema 7.4.1(c)) se tiene que $\mathbf{Z}^+$ tiene la misma cardinalidad que $3\mathbf{Z}$. Así $3\mathbf{Z}$ es infinito contable *[por definición de infinito contable]* y así que $3\mathbf{Z}$ es contable *[por definición de contable]*.

10. *Demostración:* Defina $f: S \to U$ por la regla $f(x) = 2x$ para todos los números reales x en S. Entonces f es inyectiva por el mismo argumento en el ejercicio 10a de la sección 7.2 con $\mathbf{R}$ en lugar de $\mathbf{Z}$. Aún más, f es sobreyectiva porque si y es un elemento arbitrario en U, entonces $0 < y < 2$ y así $0 < y/2 < 1$. En consecuencia, $y/2 \in S$ y $f(y/2) = 2(y/2) = y$. Por tanto, f es una correspondencia uno a uno, entonces S y U tienen la misma cardinalidad.

11. *Sugerencia:* Defina h: $S \to V$ como sigue: $h(x) = 3x + 2$, para todo $x \in S$.

13.



De la gráfica es claro que f es inyectiva (porque es creciente) y que la imagen de f es todo $\mathbf{R}$ (porque las líneas $x = 0$ y $x = 1$ son asíntotas verticales). Así S y $\mathbf{R}$ tienen la misma cardinalidad.

16. En el ejemplo 7.4.4 se demostró que existe una correspondencia uno a uno de $\mathbf{Z}^+$ a $\mathbf{Q}^+$. Esto implica que los números racionales positivos se pueden escribir como una sucesión infinita: r_1, r_2, r_3, r_4,… Ahora, el conjunto $\mathbf{Q}$ de todos los números racionales consiste de los números en esta sucesión junto con el 0 y los números racionales negativos: $-r_1, -r_2, -r_3, -r_4, \ldots$ Sea $r_0 = 0$. Entonces los elementos del conjunto de todos los números racionales se pueden "contar" como sigue:

$$r_0, r_1, -r_1, r_2, -r_2, r_3, -r_3, r_4, -r_4, \ldots$$

En otras palabras, podemos definir una correspondencia uno a uno:

$$G(n) = \begin{cases} r_{n)2} & \text{si } n \text{ es par} \\ -r_{(n-1)/2} & \text{si } n \text{ es impar} \end{cases} \quad \text{para todos los enteros } n \geq 1.$$

Por tanto, $\mathbf{Q}$ es infinito contable y entonces es contable.

18. *Sugerencia:* No.

19. *Sugerencia:* Suponga que r y s son números reales con $s > r > 0$. Sea n un entero tal que $n > \frac{\sqrt{2}}{s-r}$. Así $s - r > \frac{\sqrt{2}}{n}$. Sea $m = \left\lfloor \frac{nr}{\sqrt{2}} \right\rfloor + 1$. Entonces $m > \frac{nr}{\sqrt{2}} \geq m - 1$. Use el hecho de que $s = r + (s - r)$ para demostrar que $r < \frac{\sqrt{2}m}{n} < s$.

22. *Sugerencia:* Aplique el teorema de factorización única de los enteros (teorema 4.3.5) y el teorema 7.4.3.

23. a. Defina una función G: $\mathbf{Z}^{no\text{-}neg} \to \mathbf{Z}^{no\text{-}neg} \times \mathbf{Z}^{no\text{-}neg}$ como sigue: Sea $G(0) = (0, 0)$ y después siga las flechas del diagrama, dejando que cada par ordenado de enteros sucesivo sea el valor de G para el próximo entero sucesivo. Así, por ejemplo, $G(1) = (1, 0)$, $G(2) = (0, 1)$,…, $G(8) = (1, 2)$ y así sucesivamente.

b. *Sugerencia:* Observe que si el par ordenado de arriba en cualquier diagonal dada es $(k, 0)$, la diagonal completa (moviéndose de arriba hacia abajo) consiste de $(k, 0)$, $(k - 1, 1)$, $(k - 2, 2)$,…, $(2, k - 2)$, $(1, k - 1)$, $(0, k)$. Así para todos los pares ordenados (m, n) dentro de cualquier diagonal dada, el valor de $m + n$ es constante y conforme se mueven hacia abajo los pares ordenados de la diagonal, empezando desde arriba, el valor del segundo elemento del par se mantiene incrementándose en 1.

25. *Sugerencia:* Hay al menos dos enfoques a este problema. Uno es utilizar el método analizado en la sección 4.2. El otro es suponer que 1.9999999 … < 2 y obtener una contradicción. (Demostrar que la diferencia entre 2 y 1.999999 … puede hacerse más pequeña que cualquier número positivo dado).

26. *Demostración:* Sea A un conjunto infinito. Construya un subconjunto infinito contable $a_1, a_2, a_3, \ldots$ de A, dejando que a_1 sea cualquier elemento de A, aceptando que a_2 es otro elemento arbitrario de A diferente que a_1, permitiendo que a_3 sea cualquier otro elemento de A distinto que a_1 y a_2 y así sucesivamente. Este proceso nunca para (entonces $a_1, a_2, a_3, \ldots$ es una sucesión infinita) porque A es un conjunto infinito. Más formalmente,

1. Sea a_1 un elemento arbitrario de A.
2. Para cada entero $n \geq 2$, sea a_n cualquier elemento de $A - \{a_1, a_2, a_3, \ldots, a_{n-1}\}$. Tal elemento existe, porque si no $A - \{a_1, a_2, a_3, \ldots, a_{n-1}\}$ sería vacío y A sería finito.

27. *Demostración:* Suponga que A es cualquier conjunto infinito contable, B es un conjunto arbitrario y $g: A \to B$ es sobreyectiva. Como A es infinito contable, existe una correspondencia uno a uno $f: \mathbf{Z}^+ \to A$. Entonces, en particular, f es sobreyectiva y así por el teorema 7.3.4, $g \circ f$ es una función sobreyectiva de $\mathbf{Z}^+$ a B. Defina una función h: $B \to \mathbf{Z}^+$ como sigue: Suponga que x es cualquier elemento de B. Como $g \circ f$ es sobreyectiva, $\{m \in \mathbf{Z}^+ \mid (g \circ f)(m) = x\} \neq \emptyset$. Así, por el principio del buen orden para los enteros, existe un entero positivo mínimo n con $(g \circ f)(n) = x$. Sea $h(x)$ dicho entero.

Afirmamos que h es uno a uno. Supongamos que $h(x_1) = h(x_2) = n$. Por definición de h, n es el entero positivo mínimo con $(g \circ f)(n) = x_1$. Pero también por definición de h, n es el mínimo entero positivo con $(g \circ f)(n) = x_2$. Así que $x_1 = (g \circ f)(n) = x_2$.

Así h es una correspondencia uno a uno entre B y un subconjunto S de enteros positivos (el rango de h). Cualquier subconjunto de un conjunto contable es contable (teorema 7.4.3), S es contable y entonces existe una correspondencia uno a uno entre B y un conjunto contable. Por tanto, por la propiedad transitiva de cardinalidad, B es contable.

29. *Sugerencia:* Suponga que A y B son conjuntos infinitos contables arbitrarios. Entonces existen correspondencias uno a uno $f: \mathbf{Z}^+ \to A$ y $g: \mathbf{Z}^+ \to$ B.

Caso 1 ($A \cap B = \emptyset$): En este caso defina $h: \mathbf{Z}^+ \to A \cup B$ como sigue: Para todos los enteros $n \geq 1$,

$$h(n) \begin{cases} f(n)2) & \text{si } n \text{ es par} \\ g((n+1)/2) & \text{si } n \text{ es impar.} \end{cases}$$

Demostrar que h es inyectiva y sobreyectiva.

Caso 2 ($A \cap B \neq \emptyset$): En este caso sea $C = B - A$. Entonces $A \cup B = A \cup C$ y $A \cap C = \emptyset$. Si C es infinito pero contable, use el resultado del caso 1 para completar la demostración. Si C es finito, aplique el resultado del ejercicio 28 para terminar la demostración.

30. *Sugerencia:* Implemente la demostración por contradicción y el hecho de que el conjunto de todos los números reales es no contable.

31. *Sugerencia:* Considere los siguientes casos: 1) A y B son finitos, 2) al menos A o B es infinito y $A \cap B = \emptyset$, 3) al menos A o B es infinito y $A \cap B \neq \emptyset$. En el caso 3 use el hecho de que $A \cup B = (A - B) \cup (B - A) \cup (A \cap B)$ y que los conjuntos $(A - B)$, $(B - A)$ y $(A \cap B)$ son mutuamente disjuntos.

32. *Sugerencia:* Aplique la correspondencia uno a uno F: $\mathbf{Z}^+ \to \mathbf{Z}$ del ejemplo 7.4.2 para definir una función G: $\mathbf{Z}^+ \times \mathbf{Z}^+ \to \mathbf{Z} \times \mathbf{Z}$ por la fórmula $G(m, n) = (F(m), F(n))$. Demuestre que G es una correspondencia uno a uno, emplee el resultado del ejercicio 22 y la propiedad transitiva de cardinalidad.

34. *Sugerencia para solución 1:* Defina una función $f: \mathscr{P}(S) \to T$ como sigue: Para cada subconjunto A de S, sea $f(A) = X_A$, la *función característica* de A, en donde X_A: $S \to \{0, 1\}$ está definida por la regla

$$\chi_A(x) = \begin{cases} 1 & \text{si } x \in A \\ 0 & \text{si } x \notin A \text{ para todo } x \in S \end{cases}$$

Demuestre que f es inyectiva (para todos los $A_1, A_2 \subseteq S$, si $X_{A1} = X_{A2}$ entonces $A_1 = A_2$) y que f es sobreyectiva (dada cualquier función $g: S \to \{0, 1\}$, existe un subconjunto A de S tal que $g = X_A$).

Sugerencia para la solución 2: Defina $H: T \to \mathscr{P}(S)$ aceptando que $H(f) = \{x \in S \mid f(x) = 1\}$. Demuestre que H es una correspondencia uno a uno.

35. *Demostración parcial (por contradicción):* Suponga que no. Suponga que existe una función inyectiva y sobreyectiva $f: S \to \mathscr{P}(S)$. Sea

$$A = \{x \in S \mid x \notin f(x)\}$$

Entonces $A \in \mathscr{P}(S)$ y como f es sobreyectiva, existe un $z \in S$ tal que $A = f(z)$. *[¡Ahora deduzca una contradicción!]*

37. *Sugerencia:* A y B son contables, entonces sus elementos se pueden ordenar como

$$A: a_1, a_2, a_3, \ldots \text{ y } B: b_1, b_2, b_3, \ldots$$

Represente los elementos de $A \times B$ en una malla:

$$\begin{array}{lll} (a_1, b_1) & (a_1, b_2) & (a_1, b_3) \ \ldots \\ (a_2, b_1) & (a_2, b_2) & (a_2, b_3) \ \ldots \\ (a_3, b_1) & (a_3, b_2) & (a_3, b_3) \ \ldots \\ \vdots & \vdots & \vdots \end{array}$$

Ahora use un método de conteo similar al del ejemplo 7.4.4.

Sección 8.1

1. a. $0 \; E \; 0$ porque $0 - 0 = 0 = 2 \cdot 0$, así $2 \mid (0 - 0)$.
$5 \not\; E \; 2$ porque $5 - 2 = 3$ y $3 \neq 2k$ para cualquier entero k, así $2 \nmid (5 - 2)$.
$(6, 6) \in E$ porque $6 - 6 = 0 = 2 \cdot 0$, entonces $2 \mid (6 - 6)$.
$(-1, 7) \in E$ porque $-1 - 7 = -8 = 2 \cdot (-4)$, es decir, $2 \mid (-1 - 7)$.

2. *Sugerencia:* Para demostrar un enunciado de la forma $p \leftrightarrow (q \vee r)$, necesita demostrar que $p \to (q \vee r)$ y $(q \vee r) \to p$. Para demostrar un enunciado de la forma $p \to (q \vee r)$, puede mostrar que $(p \wedge \sim q) \to r$ (porque esas dos formas de enunciado son lógicamente equivalentes). Para demostrar un enunciado de la forma $(q \vee r) \to p$, puede demostrar que $(q \to p) \wedge (r \to p)$ (porque esos dos formas de enunciado son lógicamente equivalentes). En este caso, suponer que m y n son enteros arbitrarios, aceptar que p sea "$m - n$ es par" y que q sea "m y n son pares" y sea que r sea "$m - n$ es par".

3. a. $10 \; T \; 1$ porque $10 - 1 = 9 = 3 \cdot 3$, así $3 \mid (10 - 1)$.

$1 \; T \; 10$ porque $1 - 10 = -9 = 3 \cdot (-3)$, entonces $3 \mid (1 - 10)$.

$2 \; T \; 2$ porque $2 - 2 = 0 = 3 \cdot 0$, así $3 \mid (2 - 2)$.

$8 \not\; T \; 1$ porque $8 - 1 = 7 \neq 3k$, para cualquier entero k. Por tanto, $3 \nmid (8 - 1)$.

b. *Una posible respuesta:* 3, 6, 9, −3, −6

e. *Sugerencia:* Todos los enteros de la forma $3k + 1$, para algún entero k, están relacionados por T a 1.

4. a. Sí, porque 15 y 25 son divisibles por 5, que es primo.

b. No, porque 22 y 27 no tienen ningún factor común primo.

5. a. Sí, porque $\{a, b\}$ y $\{b, c\}$ tienen dos elementos.

6. a. No, porque $\{a\} \cap \{c\} = \emptyset$.

7. a. Sí. $1\ R(-9) \Leftrightarrow 5 \mid (1^2 - (-9)^2)$. Pero $1^2 - (-9)^2 = 1 - 81 = -80$ y $5 \mid (-80)$ porque $-80 = 5 \cdot (-16)$.

8. a. Sí, porque *abaa* y *abba* tienen los primeros dos caracteres *ab*.

b. No, porque los primeros dos caracteres de *aabb* son diferentes de los primeros dos caracteres de *bbaa*.

9. a. Sí, porque la suma de los caracteres en 0121 es 4 y la suma de los caracteres en 2200 también es 4.

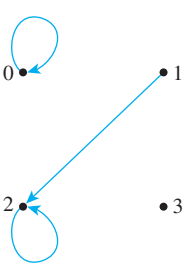
b. No, porque la suma de los caracteres en 1011 es 3 mientras que la suma de los caracteres en 2101 es 4.

10. $R = \{(3, 4), (3, 5), (3, 6), (4, 5), (4, 6), (5, 6)\}$

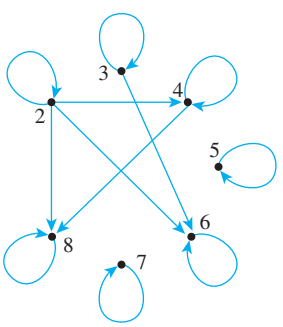
$R^{-1} = \{(4, 3), (5, 3), (6, 3), (5, 4), (6, 4), (6, 5)\}$

12. a. No. Si F: X $\rightarrow$ Y no es sobreyectiva, entonces F^{-1} no está definida sobre todo Y. En otras palabras, existe un elemento y en Y tal que $(y, x) \notin F^{-1}$ para cualquier $x \in X$. En consecuencia, F^{-1} no satisface la propiedad (1) de la definición de función.

13.



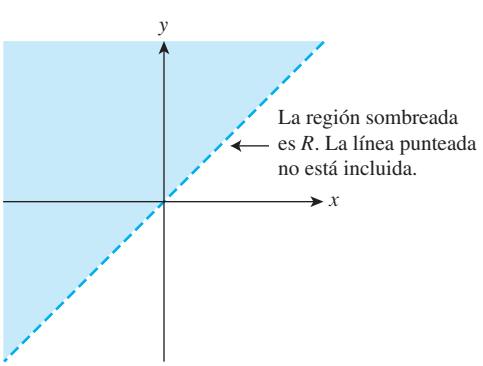
15.

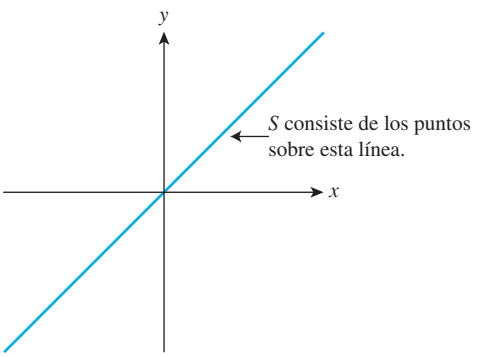


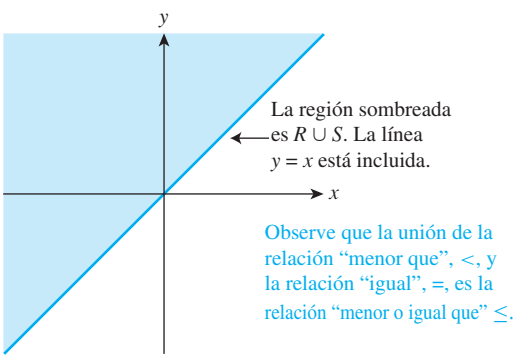
16. *Sugerencia:* Vea el ejemplo 8.1.6.

19. $A \times B = \{(2, 6), (2, 8), (2, 10), (4, 6), (4, 8), (4, 10)\}$
$R = \{(2, 6), (2, 8), (2, 10), (4, 8)\}$
$S = \{(2, 6), (4, 8)\}$
$R \cup S = R$, $R \cap S = S$

21.







Observe que la unión de la relación "menor que", $<$, y la relación "igual", $=$, es la relación "menor o igual que" $\leq$.

La gráfica de la intersección de R y S se obtiene al encontrar todos los puntos comunes a ambas gráficas. Pero no hay puntos en que $x < y$ y $x = y$. Así que $R \cap S = \emptyset$ y la gráfica carece de puntos.

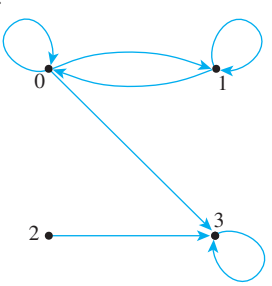
24. a.

574329	Tak Kurosawa
011985	John Schmidt

Sección 8.2

1. R_1:

a.



b. R_1 no es reflexiva: 2 $\not R_1$ 2.

c. R_1 no es simétrica: 2 R_1 3 *pero* 3 $\not R_1$ 2.

d. R_1 no es transitiva: 1 R_1 0 y 0 R_1 3 *pero* 1 $\not R_1$ 3.

3. R_3:

a. 0 • • 1

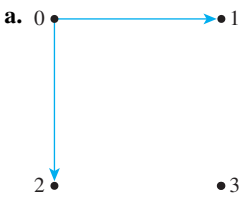
b. R_3 no es reflexiva: $(0, 0) \notin R_3$.

c. R_3 es simétrica. (Si R_3 no fuera simétrica, habrían elementos x y y en $A = \{0, 1, 2, 3\}$ tales que $(x, y) \in R_3$ pero $(y, x) \notin R_3$. Por inspección es claro que no existen tales elementos.)

d. R_3 no es transitiva: $(2, 3) \in R_3$ y $(3, 2) \in R_3$ pero $(2, 2) \notin R_3$.

6. R_6:

a.



b. R_6 no es reflexiva: $(0, 0) \notin R_6$

c. R_6 no es simétrica: $(0, 1) \in R_6$ pero $(1, 0) \notin R_6$.

d. R_6 es transitiva. (Si R_6 no fuera transitiva, habrían elementos x, y y z en $\{0, 1, 2, 3\}$ tales que $(x, y) \in R_6$, $(y, z) \in R_6$ y $(x, z) \notin R_6$. Por inspección es claro que no existen tales elementos.)

9. ***R es reflexiva:*** R es reflexiva si sólo si para todos los números reales x, $x\ R\ x$. Por definición de R, esto significa que para todos los números reales x, $x \geq x$. En otras palabras, para todos los números reales x, $x > x$ o $x = x$. Pero esto es verdadero.

***R no es* simétrica:** R es simétrica si sólo si para todos los números reales x y y, si $x\ R\ y$ entonces $y\ R\ x$. Por definición de R, esto significa que para todos los números reales x y y, si $x \geq y$ entonces $y \geq x$. Pero esto es falso. Como un contraejemplo, tome $x = 1$ y $y = 0$. Entonces $x \geq y$ pero y no es mayor o igual que x porque $1 \geq 0$ pero $0 \ngeq 1$.

R es transitiva: R es transitiva si y sólo si para todos los números reales x, y y z, si $x\ R\ y$ y $y\ R\ z$ entonces $x\ R\ z$. Por definición de R, esto significa que para todos los números reales x, y y z, si $x \geq y$ y $y \geq z$ entonces $x \geq z$. Pero esto es verdadero por definición de $\geq$ y la propiedad transitiva de orden para los números reales. (Vea el apéndice A, T18.)

11. ***D es reflexiva:*** Que D sea reflexiva significa que para todos los números reales x, $x\ D\ x$. Pero por definición de D, esto implica que para todos los números reales x, $xx = x^2 \geq 0$, que es verdadero.

D* es *simétrica: Que D sea simétrica significa que para todos los números reales x y y, si $x\ D\ y$ entonces $y\ D\ x$. Pero por definición de D, esto implica que para todos los números reales x y y, si $xy \geq 0$ entonces $yx \geq 0$, que es verdadero por la ley conmutativa de la multiplicación.

D no es transitiva: Que D sea transitiva significa que para todos los números reales x, y y z, si $x\ D\ y$ y $y\ D\ z$ entonces $x\ D\ z$. Por definición de D, esto implica que para todos los números reales x, y y z, si $xy \geq 0$ y $yz \geq 0$ entonces $xz \geq 0$. Pero esto es falso: existen números reales x, y y z tales que $xy \geq 0$ y $yz \geq 0$ pero con $xz \ngeq 0$. Como un contraejemplo, sean $x = 1$, $y = 0$ y $z = -1$. Entonces $x\ D\ y$ y $y\ D\ z$ porque $1 \cdot 0 \geq 0$ y $0 \cdot (-1) \geq 0$. Pero $x \not D z$ ya que $1 \cdot (-1) \ngeq 0$.

12. ***E es reflexiva:*** *[Debemos demostrar que para todos los enteros m, $m\ E\ m$.]* Suponga que m es un entero arbitrario. Como $m - m = 0$ y $2 \mid 0$, tenemos que $2 \mid (m - m)$. En consecuencia, $m\ E\ m$ por definición de E.

E es simétrica: *[Debemos demostrar que para todos los enteros m y n, si $m\ E\ n$ entonces $n\ E\ m$.]* Suponga que m y n son enteros arbitrarios tales que $m\ E\ n$. Por definición de E, esto significa que $2 \mid (m - n)$ y así, por definición de divisibilidad, $m - n = 2k$ para algún entero k. Además, $n - m = -(m - n)$. Así que, sustituyendo, $n - m = -(2k) = 2(-k)$. Se tiene que $2 \mid (n - m)$ por definición de divisibilidad (porque $-k$ es un entero) y entonces $n\ E\ m$ por definición de E.

E es transitiva: *[Debemos demostrar que para todos los enteros m, n y p si $m\ E\ n$ y $n\ E\ p$ entonces $m\ E\ p$.]* Suponga que m, n y p son enteros arbitrarios tales que $m\ E\ n$ y $n\ E\ p$. Por definición de E esto significa que $2 \mid (m - n)$ y $2 \mid (n - p)$ y así, por definición de divisibilidad, $m - n = 2k$ para algún entero k y $n - p = 2l$ para algún entero l. Además, $m - p = (m - n) + (n - p)$. Así, sustituyendo, $m - p = 2k + 2l = 2(k + l)$. Se tiene que $2 \mid (m - p)$ por definición de divisibilidad (porque $k + l$ es un entero) y así $m\ E\ p$ por definición de E.

15. ***D es reflexiva:*** *[Debemos demostrar que para todos los enteros positivos m, $m\ D\ m$.]* Suponga que m es un entero positivo arbitrario. Como $m = m \cdot 1$, por definición de divisibilidad $m \mid m$. Así $m\ D\ m$ por definición de D.

D no es simétrica: Si D fuera simétrica significaría que para todos los enteros positivos m y n, si $m\ D\ n$ entonces $n\ D\ m$. Por definición de divisibilidad, esto significaría que para todos los enteros positivos m y n, si $m \mid n$ entonces $n \mid m$. Pero esto es falso. Como un contraejemplo, tome $m = 2$ y $n = 4$. Entonces $m \mid n$ porque $2 \mid 4$ pero $n \nmid m$ porque $4 \nmid 2$.

D es transitiva: Para demostrar la transitividad de D, debemos demostrar que para todos los enteros positivos m, n y p, si $m\ D\ n$ y $n\ D\ p$ entonces $m\ D\ p$. Por definición de D, esto implica que para todos los enteros positivos m, n y p, si $m \mid n$ y $n \mid p$ entonces $m \mid p$. Pero esto es verdadero por el teorema 4.3.3 (la transitividad de la divisibilidad).

18. *Sugerencia:* Q es reflexiva, simétrica y transitiva.

20. ***E es reflexiva:*** $\mathbf{E}$ es reflexiva si y sólo si para todos los subconjuntos A de X, A $\mathbf{E}$ A. Por definición de $\mathbf{E}$, esto significa que para todos los subconjuntos A de X, A tiene el mismo número de elementos como A. Pero esto es verdadero.

E es simétrica: $\mathbf{E}$ es simétrica si y sólo si para todos los subconjuntos A y B de X, si A $\mathbf{E}$ B entonces B $\mathbf{E}$ A. Por definición de $\mathbf{E}$, esto significa que si A tiene el mismo número de elementos que B, entonces B tiene el mismo número de elementos que A. Pero esto es verdadero.

E es transitiva: $\mathbf{E}$ es transitiva $\Leftrightarrow$ para todos los subconjuntos A, B y C de X, si A $\mathbf{E}$ B y B $\mathbf{E}$ C, entonces A $\mathbf{E}$ C. Por definición de $\mathbf{E}$, esto implica que para todos los subconjuntos, A, B y C de X, si A tiene el mismo número de elementos que B y éste tiene el mismo número de elementos que C, entonces A tiene el mismo número de elementos que C. Pero esto es verdadero.

23. ***S es reflexiva:*** $\mathbf{S}$ es reflexiva si y sólo si para todos los subconjuntos A de X, A $\mathbf{S}$ A. Por definición de $\mathbf{S}$, esto significa que para todos los subconjuntos A de X, A $\subseteq$ A. Que es verdadero porque cada conjunto es un subconjunto de sí mismo.

S no es simétrica: $\mathbf{S}$ es simétrica si y sólo si para todos los subconjuntos A y B de X, si A $\mathbf{S}$ B entonces B $\mathbf{S}$ A. Por definición de $\mathbf{S}$, esto implica que para todos los subconjuntos A y B de X, si A $\subseteq$ B entonces B $\subseteq$ A. Pero esto es falso porque $X \neq \emptyset$ y así

existe un elemento a en X. Como un contraejemplo, tome $A = \emptyset$ y $B = \{a\}$. Entonces $A \subseteq B$ pero $B \not\subseteq A$.

S es transitiva: **S** es transitiva si y sólo si para todos los subconjuntos A, B y C de X, si A **S** B y B **S** C, entonces A **S** C. Por definición de **S**, esto significa que para todos los subconjuntos A, B y C de X, si $A \subseteq B$ y $B \subseteq C$ entonces $A \subseteq C$. Que es verdadero por la propiedad transitiva de subconjuntos (teorema 6.2.1(3)).

25. ***R es reflexiva:*** Suponga que s es una cadena arbitraria en A. Entonces $s\ R\ s$ porque s tiene los mismos primeros dos caracteres como s.

R es simétrica: Sean s y r son cadenas arbitrarias en A tales que $s\ R\ t$. Por definición de R, s tiene los mismos primeros dos caracteres que t. Se tiene que t tiene los mismos primeros dos caracteres que s y así $t\ R\ s$.

R es transitiva: Suponga que s, t y u, son cadenas cualesquiera en A tales que $s\ R\ t$ y $t\ R\ u$. Por definición de R, s tiene los mismos primeros dos caracteres que t y t tiene los mismos primeros dos caracteres que u. Se tiene que s tiene los mismos primeros dos caracteres que u y así $s\ R\ u$.

27. ***I* es *reflexiva:*** *[Debemos demostrar que para todos los enunciados p, p **I** p.]* Suponga que p es un enunciado. La única forma en que un enunciado condicional pueda ser falso es que su hipótesis sea verdadera y su conclusión falsa. Considere el enunciado $p \rightarrow p$. La hipótesis y la conclusión tienen el mismo valor verdadero. Así es imposible que $p \rightarrow p$ sea falso y entonces $p \rightarrow p$ debe ser verdadero.

I no es simétrica: **I** es simétrica $\Leftrightarrow$ para todos los enunciados p y q, si p **I** q entonces q **I** p. Por definición de **I**, esto significa que todos los enunciados p y q, si $p \rightarrow q$ entonces $q \rightarrow p$. Que es falso. Como un contraejemplo, sea p el enunciado "10 es divisible por 4" y q sea "10 divisible por 2". Entonces $p \rightarrow q$ es el enunciado "si 10 es divisible por 4, entonces 10 es divisible por 2". Esto es verdadero porque su hipótesis, p, es falsa. Por otro lado, $q \rightarrow p$ es el enunciado "si 10 es divisible entre 2, entonces 10 es divisible por 4". Esto es falso porque su hipótesis, q, es verdadera y su conclusión, p, es falsa.

I es transitiva: *[Debemos demostrar que para todos los enunciados p, q, y r, si p **I** q y q **I** r entonces p **I** r.]* Suponga que p, q y r son enunciados tales que p **I** q y q **I** r. Por definición de **I**, esto implica que $p \rightarrow q$ y $q \rightarrow r$ son verdaderos. Por transitividad de si-entonces (ejemplo 2.3.6 y el ejercicio 20 de la sección 2.3), podemos concluir que $p \rightarrow r$ es verdadero. Así que, por definición de **I**, p **I** r.

28. ***F es reflexiva:*** **F** es reflexiva $\Leftrightarrow$ para todos los elementos (x, y) en $\mathbf{R} \times \mathbf{R}$, (x, y) **F** (x, y). Por definición de **F**, esto implica que para todos los elementos (x, y) en $\mathbf{R} \times \mathbf{R}$, $x = x$. Que es verdadero.

F es simétrica: *[Debemos demostrar que para todos los elementos (x_1, y_1) y (x_2, y_2) en $\mathbf{R} \times \mathbf{R}$, si (x_1, y_1) **F** (x_2, y_2) entonces (x_2, y_2) **F** (x_1, y_1).]* Suponga que (x_1, y_1) y (x_2, y_2) son elementos de $\mathbf{R} \times \mathbf{R}$ tales que (x_1, y_1) **F** (x_2, y_2). Por definición de **F**, esto significa que $x_1 = x_2$. Por simetría de la igualdad, $x_2 = x_1$. Así, por definición de **F**, (x_2, y_2) **F** (x_1, y_1).

F es transitiva: *[Debemos demostrar que para todos los elementos (x_1, y_1), (x_2, y_2) y (x_3, y_3) en $\mathbf{R} \times \mathbf{R}$, si (x_1, y_1) **F** (x_2, y_2) y (x_2, y_2) **F** (x_3, y_3) entonces (x_1, y_1) **F** (x_3, y_3).]* Suponga que (x_1, y_1), (x_2, y_2) y (x_3, y_3) son elementos de $\mathbf{R} \times \mathbf{R}$ tales que (x_1, y_1) **F** (x_2, y_2) y (x_2, y_2) **F** (x_3, y_3). Por definición de **F**, esto implica que $x_1 = x_2$ y $x_2 = x_3$. Por transitividad de la igualdad, $x_1 = x_3$. Así que, por definición de **F**, (x_1, y_1) **F** (x_3, y_3).

31. ***R es reflexiva:*** R es reflexiva si y sólo si para toda la gente p en A, $p\ R\ p$. Por definición de R, esto significa que para toda la gente p que vive actualmente en el mundo, p vive dentro de un radio de 100 millas alrededor de p. Que es verdadero.

R es simétrica: *[Debemos demostrar que para toda la gente p y q en A, si $p\ R\ q$ entonces $q\ R\ p$.]* Suponga que p y q son gente en A tales que $p\ R\ q$. Por definición de R, esto significa que p vive dentro de en un radio de 100 millas alrededor de q. Pero esto implica que q vive dentro de un radio de 100 millas alrededor de p. Así, por definición de R, $q\ R\ p$.

R no es transitiva: R es transitiva $\Leftrightarrow$ para toda la gente p, q y r, si $p\ R\ q$ y $q\ R\ r$ entonces $p\ R\ r$. Que es falso. Como un contraejemplo, tome p como un habitante de Chicago, Illinois, q un habitante de Kankakee, Illinois y r un habitante de Champaign, Illinois. Entonces $p\ R\ q$ porque Chicago está a menos de 100 millas de Kankakee y $q\ R\ r$ porque Kankakee está a menos de 100 millas de Champaign, pero $p \not R\ r$ porque Chicago no está a menos de 100 millas de Champaign.

34. *Demostración:* Suponga que R es cualquier relación reflexiva sobre el conjunto A. *[Debemos demostrar que R^{-1} es reflexiva. Para demostrar esto, debemos demostrar que para toda x en A, $x\ R^{-1}\ x$.]* Dado cualquier elemento x en A, como R es reflexiva, $x\ R\ x$ y por definición de la relación, esto implica que $(x, x) \in R$. Se tiene, por definición de la inversa de una relación, que $(x, x) \in R^{-1}$ y así, por definición de la relación, $x\ R^{-1} x$ *[que era lo que se quería demostrar]*.

37. a. ***R* ∩ *S* es reflexiva:** Suponga que R y S son reflexivas. *[Para demostrar que $R \cap S$ es reflexiva, debemos demostrar que $\forall\ x \in A$, $(x, x) \in R \cap S$.]* Así suponga que $x \in A$. Como R es reflexiva, $(x, x) \in R$ y como S es reflexiva, entonces $(x, x) \in S$. Por tanto, por definición de intersección, $(x, x) \in R \cap S$ *[que era lo que se quería demostrar]*.

38. *Sugerencia:* La respuesta es sí.

41. Sí. Para demostrar esto debemos demostrar que para toda x y y en A, si $(x, y) \in R \cup S$ entonces $(y, x) \in R \cup S$. Entonces suponga que (x, y) es un elemento particular pero arbitrariamente elegido en $R \cup S$. *[Debemos demostrar que $(y, x) \in R\ U\ S$.]* Por definición de unión, $(x, y) \in R$ o $(x, y) \in S$. Si $(x, y) \in R$, entonces $(y, x) \in R$ porque R es simétrica. Así que $(y, x) \in R \cup S$ por definición de unión. Además, si $(x, y) \in S$ entonces $(y, x) \in S$ porque S es simétrica. En consecuencia, $(y, x) \in R \cup S$ por definición de unión. Así, en cualquier caso, $(y, x) \in R \cup S$ *[que era lo que se quería demostrar]*.

43. R_1 no es irreflexiva porque $(0, 0) \in R_1$. R_1 no es asimétrica porque $(0, 1) \in R_1$ y $(1, 0) \in R_1$. R_1 no es intransitiva porque $(0, 1) \in R_1$ y $(1, 0) \in R_1$ y $(0, 0) \in R_1$.

45. R_3 es irreflexiva. R_3 no es asimétrica porque $(2, 3) \in R_3$ y $(3, 2) \in R_3$. R_3 es intransitiva.

48. R_6 es irreflexiva. R_6 es asimétrica. R_6 es intransitiva (por defecto).

51. $R^t = R \cup \{(0, 0), (0, 3), (1, 0), (3, 1), (3, 2), (3, 3), (0, 2), (1, 2)\}$
$= \{(0, 0), (0, 1), (0, 2), (0, 3), (1, 0), (1, 1), (1, 2), (1, 3), (2, 2), (3, 0), (3, 1), (3, 2)(3, 3)\}$

54. Algoritmo: Demostración de reflexividad.

[La entrada para este algoritmo es una relación binaria R definida sobre un conjunto A, que está representada como el arreglo unidimensional a[1], a[2],..., a[n]. Para demostrar si R es reflexiva, la variable respuesta se pone inicialmente en "sí" y cada elemento a[i] de A es examinado para ver si está relacionado por R consigo mismo. Si ningún elemento está relacionado consigo mismo por R, entonces la respuesta se pone igual a "no", el bucle ya no se repite y el proceso termina.]

Entrada: *n [un entero positivo], a[1], a[2],..., a[n] [un arreglo unidimensional representando un conjunto A], R [un subconjunto de A × A]*

Cuerpo del algoritmo:

i := 1, *respuesta* := *"sí"*
while (*respuesta* = *"sí"* e $i \leq n$)
if (*a*[i], *a*[i]) $\notin R$ **entonces** *respuesta* := *"no"*
$i := i + 1$
end while

Salida: *respuesta [una cadena]*

Sección 8.3

1. a. cRc **b.** bRa, cRb, eRd **c.** aRc
d. $cRc, bRa, cRb, eRd, aRc, cRa$

2. a. $R = \{(0, 0), (0, 2), (1, 1), (2, 0), (2, 2), (3, 3), (3, 4), (4, 3), (4, 4)\}$

3. $\{0, 4\}, \{1, 3\}, \{2\}$

5. $\{1, 5, 9, 13, 17\}, \{2, 6, 10, 14, 18\}, \{3, 7, 11, 15, 19\}, \{4, 8, 12, 16, 20\}$

7. $\{(1, 3), (3, 9)\}, \{(2, 4), (-4, -8), (3, 6)\}, \{(1, 5)\}$

8. $\{\emptyset\}, \{\{a\}, \{b\}, \{c\}\}, \{\{a, b\}, \{a, c\}, \{b, c\}\}, \{\{a, b, c\}\}$

11. $[0] = \{x \in A \mid 4 \mid (x^2 - 0)\} = \{x \in A \mid 4 \mid x^2\} = \{-4, -2, 0, 2, 4\}$ $[1] = \{x \in A \mid 4 \mid (x^2 - 1^2)\} = \{x \in A \mid 4 \mid (x^2 - 1)\} = \{-3, -1, 1, 3\}$

13. $\{aaaa, aaab, aaba, aabb\}, \{abaa, abab, abba, abbb\}, \{baaa, baab, baba, babb\}, \{bbaa, bbab, bbba, bbbb\}$

15. a. Verdadero. $17 - 2 = 15$ y $5 \mid 15$.

16. a. $[7] = [4] = [19]$, $[-4] = [17]$, $[-6] = [27]$

17. a. *Demostración:* Suponga que m y n son enteros tales que $m = n$ (*mod* 3). *[Debemos demostrar que m mod* $3 = n$ *mod* 3.*]* Por definición de congruencia, $3 \mid (m - n)$ y así por definición de divisibilidad, $m - n = 3k$ para algún entero k. Sea m *mod* $3r =$. Entonces $m = 3l + r$ para algún entero l. Como $m - n = 3k$, entonces sustituyendo, $(3l + r) - n = 3k$, o, equivalentemente, $n = 3(l - k) + r$. Además, $l - k$ es un entero y $0 \leq r < 3$, entonces se tiene, por definición de *mod*, que n *mod* 3 también es igual a r. Así m *mod* $3 = n$ *mod* 3.

Suponga que m y n son enteros tales que m *mod* $3 = n$ *mod* 3. *[Debemos demostrar que* $m = n$ (*mod* 3).*]* Sea $r = m$ *mod* $3 = n$ *mod* 3. Entonces, por definición de *mod*, $m = 3p + r$ y $n = 3q + r$ para algunos enteros p y q. Sustituyendo, $m - n = (3p + r) - (3q + r) = 3(p - q)$. Como $p - q$ es un entero, se tiene que $3 \mid (m - n)$ y entonces, por definición de congruencia, $m \equiv n$ (*mod*)3.

18. a. Por ejemplo, sean $A = \{1, 2\}$ y $B = \{2, 3\}$. Entonces $A \neq B$, así A y B son distintos. Pero A y B no son disjuntos porque $2 \in A \cap B$.

19. a. 1) *Demostración: R* es reflexiva porque es verdad que para cada estudiante x en el colegio, x tiene el mismo principal (o doble principal) como x.
R es simétrica porque es verdadero que para todos los estudiantes x y y en el colegio, si x tiene el mismo principal (o doble principal) como y, entonces y tiene el mismo principal (o doble principal) como x.
R es transitiva porque es verdadera para todos los estudiantes x, y y z en el colegio, si x tiene el mismo principal (o doble principal) como y y y tiene el mismo principal (o doble principal) como z, entonces x tiene el mismo principal (o doble principal) como z. *R* es una relación de equivalencia porque es reflexiva, simétrica y transitiva.

2) Existe una clase de equivalencia para cada principal y cada doble principal en el colegio. Cada clase consiste de todos los estudiantes con determinado principal (o doble principal).

20. 1) *Sugerencia:* Vea la solución al ejercicio 15 de la sección 10.2.

(2) Dos clases distintas:$\{x \in \mathbf{Z} \mid x = 2k$, para algún entero $k\}$ y $\{x \in \mathbf{Z} \mid x = 2k + 1$, para algún entero $k\}$.

25. 1) *Demostración: A* es reflexiva porque cada número real tiene el mismo valor absoluto como mismo.

A es simétrica porque para todos los números reales x y y, si $| x | = | y |$ entonces $| y | = | x |$.

A es transitiva porque para todos los números reales x, y y z, si $| x | = | y |$ y $| y | = | z |$ entonces $| x | = | z |$.

A es una relación de equivalencia porque es reflexiva, simétrica y transitiva.

2) Las distintas clases son conjuntos de la forma $\{x, -x\}$, en donde x es un número real.

26. *Sugerencias:* 1) *D* es reflexiva, simétrica y transitiva. Las pruebas son muy similares a las demostraciones del ejercicio 17.

2) Existen dos clases de equivalencia distintas. Observe que $m^2 - n^2 = (m - n)(m + n)$ para todos los enteros m y n. Además, $3 \mid (m - n)$ o $3 \mid (m + n) \Leftrightarrow$ si $m - n = 3r$ o $m + x = 3r$, para algún entero r.

28. 1) *Demostración: I* es reflexiva porque la diferencia entre cada número real y mismo es 0, que es un entero.

I es simétrica porque para todos los números reales x y y, si $x - y$ es un entero, entonces $y - x = (-1)(x - y)$, también es un entero.

I es transitiva porque para todos los números reales x, y y z, si $x - y$ es un entero y $y - z$ es un entero, entonces $x - z = (x - y) + (y - z)$ es la suma de dos enteros y por tanto es un entero.

I es una relación de equivalencia porque es reflexiva, simétrica y transitiva.

2) Existe una clase para cada número real x con $0 \le x < 1$. Las distintas clases son todos los conjuntos de la forma $\{y \in \mathbf{R} \mid y = n + x$, para algún entero $n\}$, en donde x es un número real tal que $0 \le x < 1$.

29. 1) *Demostración:* P es reflexiva porque cada par ordenado de números reales tiene el mismo primer elemento como mismo.

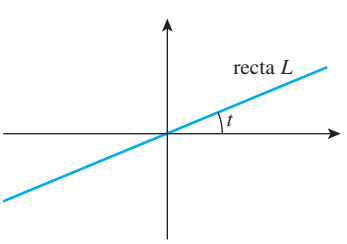
P es simétrica por la siguiente razón: Suponga que (w, x) y (y, z) son pares ordenados de números reales tales que $(w, x)P(y, z)$. Entonces, por definición de P, $w = y$. Pero por la propiedad simétrica de la igualdad, esto implica que $y = w$ y también, por definición de P $(y, z)P(w, x)$.

P es transitiva por la siguiente razón: Suponga que (u, v), (w, x) y (y, z) son pares ordenados de números reales tales que (u, v) $P(w, x)$ y $(w, x)P(y, z)$. Entonces, por definición de P, $u = w$ y $w = y$. Pero por la propiedad transitiva de la igualdad, esto implica que $u = w$ y así, por definición de P $(u, v)P(w, x)$.

P es una relación de equivalencia porque es reflexiva, simétrica y transitiva.

2) Existe una clase de equivalencia para cada número real. Las distintas clases de equivalencia son todos los conjuntos de pares ordenados $\{(x, y) \in \mathbf{R} \times \mathbf{R} \mid x = a\}$, para cada número real a. Equivalentemente, las clases de equivalencia consisten de todas las líneas verticales en el plano cartesiano.

32. *Solución* para *(2):* Existe una clase de equivalencia para cada número real t tal que $0 \le t < \pi$. Una recta en cada clase pasa por el origen y esa línea hace un ángulo t con el eje horizontal positivo.



Alternativamente, existe una clase de equivalencia para cada posible pendiente: todos los números reales más los "indefinidos".

34. No. Si los puntos p, q y r se encuentran sobre una línea recta con q a la mitad y si p está a c unidades de q y éste está a c unidades de r, entonces p está a más de c unidades de r.

36. *Demostración:* Suponga que R es una relación de equivalencia sobre un conjunto A y $a \in A$. Como R es una relación de equivalencia, R es reflexiva y al ser R reflexiva entonces cada elemento de A está relacionado consigo mismo mediante R. En particular, $a\ R\ a$. Así, por definición de clase de equivalencia, $a \in [a]$.

38. *Demostración:* Suponga que R es una relación de equivalencia sobre un conjunto A y a, b y c son elementos de A con $b\ R\ c$ y $c \in [a]$. Como $c \in [a]$, entonces $c\ R\ a$ por definición de clase de equivalencia. Pero R es transitiva porque R es una relación de equivalencia. Por tanto, como $b\ R\ c$ y $c\ R\ a$, entonces $b\ R\ a$. Se tiene que $b \in [a]$ por definición de clase.

40. *Demostración:* Suponga que a, b y x están en A, $a\ R\ b$ y $x \in [a]$. Por definición de clase de equivalencia, $x\ R\ a$. Así $x\ R\ a$ y $a\ R\ b$ y entonces, por transitividad, $x\ R\ b$. Por tanto, $x \in [b]$.

41. *Sugerencia:* Demuestre que $[a] = [b]$, demuestre que $[a] \subseteq [b]$ y $[b] \subseteq [a]$. Compruebe que $[a] \subseteq [b]$, demuestre que para todo x en A, si $x \in [a]$ entonces $x \in [b]$.

42. **c.** Por ejemplo (2, 6), (−2, −6), (3, 9), (−3, −9).

43. **a.** Suponga que (a, b), (a', b'), (c, d) y (c', d') son elementos arbitrarios de A tales que $[(a, b)] = [(a', b')]$ y $[(c, d)] = [(c', d')]$. Por definición de la relación, $ab' = ba'$(*) y $cd' = dc'$(**). Debemos demostrar que $[(a, b)] + [(c, d)] = [(a', b')] + [(c', d')]$. Por definición de la suma, esta ecuación es verdadera si y sólo si,

$$[(ad + bc, bd)] = [(a'd' + b'c', b'd')].$$

Y, por definición de la relación, esta ecuación es verdadera si y sólo si,

$$(ad + bc)b'd' = bd(a'd' + b'c'),$$

que es equivalente a

$$adb'd' + bcb'd' = bda'd' + bdb'c', \quad \text{realizando las multiplicaciones.}$$

Pero esta ecuación es equivalente a

$$(ab')(dd') +)cd')(bb') = (ba')(dd') + (dc')(bb') \quad \text{agrupando}$$

y, sustituyendo (*) y (**), esta última ecuación es verdadera.

c. Suponga que (a, b) es cualquier elemento de A. Debemos demostrar que $[(a, b)] + [(0, 1)] = [(a, b)]$. Por definición de la adición, esta ecuación es verdadera si y sólo si,

$$[(a \cdot 1 + b \cdot 0, b \cdot 1)] = [(a, b)].$$

Esta última ecuación es verdadera porque $a \cdot 1 + b \cdot 0 = a$ y $b \cdot 1 = b$.

e. Acepte que (a, b) es cualquier elemento de A. Debemos demostrar que $[(a, b)] + [(-a, b)] = [(-a, b)] + [(a, b)] = [(0, 1)]$. Por definición de la suma, esta ecuación es verdadera si y sólo si,

$$[(ab + b(-a), bb)] = [(0, 1)],$$

o, equivalentemente,

$$[(0, bb)] = [(0, 1)].$$

Por definición de la relación, esta última ecuación es verdadera si y sólo si, $0 \cdot 1 = bb \cdot 0$, que es verdadera.

44. **a.** Sea (a, b) cualquier elemento de $\mathbf{Z}^+ \times \mathbf{Z}^+$. Debemos demostrar que $(a, b)R(a, b)$. Por definición de R, esta relación es válida si y sólo si, $a + b = b + a$. Pero esta ecuación es verdadera por la ley conmutativa de la suma para números reales. Así que R es reflexiva.

c. *Sugerencia:* Necesitarás demostrar que para cualesquiera enteros positivos a, b, c y d, si $a + d = c + b$ y $c + f = d + e$, entonces $a + f = b + e$.

d. *Una posible respuesta:* (1, 1), (2, 2), (3, 3), (4, 4), (5, 5)

g. Observe que para cualesquier enteros positivos a y b, la clase de equivalencia de (a, b) consiste de todos los pares

ordenados en $\mathbf{Z}^+ \times \mathbf{Z}^+$ para que la diferencia entre la primera y la segunda coordenadas es igual a $a - b$. Así existe una clase de equivalencia para cada entero: positivo, negativo y cero. Cada entero positivo n corresponde a la clase $(n + 1, 1)$; cada entero negativo $-n$ corresponde a la clase de $(1, n + 1)$ y el cero corresponde a la clase $(1, 1)$.

47. c. "Maneras y Medios"

Sección 8.4

1. a. GRQGH QRV HQFRQWUDUHPRV
b. EN LA CAFETERÍA

3. a. La relación $3 \mid (25 - 19)$ es verdadera porque $25 - 19 = 6$ y $3 \mid 6$ $(6 = 3 \cdot 2)$.
b. Por definición de congruencia módulo n, para demostrar que $25 = 19 \pmod 3$, se debe demostrar que $3 \mid (25 - 19)$. Esto se comprobó en el inciso *a*).
c. Para demostrar que $25 = 19 + 3k$ para algún entero k, se resuelve la ecuación para k y se comprueba que el resultado sea un entero. En este caso, $k = (25 - 19)/3 = 2$, que es un entero. Así $25 = 19 + 2 \cdot 3$.
d. Cuando 25 se divide por 3, el residuo es 1 porque $25 = 3 \cdot 8 + 1$. Cuando 19 se divide por 3, el residuo también es 1 porque $19 = 3 \cdot 6 + 1$. Así 25 y 19 tienen el mismo residuo cuando son divididos por 3.
e. Por definición, $25 \; mod \; 3$ es el residuo que se obtiene cuando 25 se divide por 3 y $19 \; mod \; 3$ es el residuo que se obtiene al dividir 19 por 3. En el inciso *d*) se probó que ambos números son iguales.

6. *Sugerencias:* 1) Use el teorema cociente-residuo y el teorema 8.4.1 para demostrar que dado cualquier entero a, éste se encuentra en una de las clases [0], [1], [2], …, [n−1]. 2) Con el teorema 4.3.1 demuestre que si $0 \le a < n$, $0 \le b < n$ y $a = b \pmod n$, entonces $a = b$.

7. a. $128 \equiv 2 \pmod 7$ porque $128 - 2 = 126 = 7 \cdot 18$, y $61 \equiv 5 \pmod 7$ porque $61 - 5 = 56 = 7 \cdot 8$
b. $128 + 61 \equiv (2 + 5) \pmod 7$ porque $128 + 61 = 189$, $2 + 5 = 7$, y $189 - 7 = 182 = 7 \cdot 26$
c. $128 - 61 \equiv (2 - 5) \pmod 7$ porque $128 - 61 = 67$, $2 - 5 = -3$, y $67 - (-3) = 70 = 7 \cdot 10$
d. $128 \cdot 61 \equiv (2 \cdot 5) \pmod 7$ porque $128 \; 61 = 7808$, $2 \cdot 5 = 10$, y $7808 - (10) = 7798 = 7 \cdot 1114$
e. $128^2 \equiv 2^2 \pmod 7$ porque $128^2 = 16384$, $2^2 = 4$, y $16384 - 4 = 16380 = 7 \cdot 2340$.

9. a. *Demostración:* Suponga que a, b, c, d y n son enteros con $n > 1$, $a = c \pmod n$ y $b = d \pmod n$. Por el teorema 8.4.1, $a - c = nr$ y $b - d = ns$ para algunos enteros r y s. Entonces

$$(a + b) - (c + d) = (a - c) + (b - d) = nr + ns$$
$$= n(r + s).$$

Pero $r + s$ es un entero y así, por el teorema 8.4.1, $a + b = (c + d) \pmod n$.

12. a. *Demostración (por inducción matemática):* Aceptemos que la propiedad $P(n)$ sea la congruencia $10^n = 1 \pmod 9$.

Demostración de que P(0) es verdadero:

Cuando $n = 0$, el lado izquierdo de la congruencia es $10^0 = 1$ y el lado derecho también es 1.

Demostración de que para todos los enteros $k \ge 0$, si $P(k)$ es verdadera, entonces $P(k + 1)$ también es verdadera.

Sea k cualquier entero con $k \ge 0$ y suponga que $P(k)$ es verdadero. Es decir, acepte que $10^k \equiv 1 \pmod 9$. (*) *[Esto es la hipótesis inductiva.]* Por el teorema 8.4.1, $10 \equiv 1 \pmod 9$ (**) porque $10 - 1 = 9 = 9 \cdot 1$. Y por el teorema 8.4.3, podemos multiplicar el lado izquierdo y derecho de (*) y (**) para obtener que $10^k \cdot 10 \equiv 1 \cdot 1 \pmod 9$ o, equivalentemente, $10^{k+1} \equiv 1 \pmod 9$. Así que $P(k + 1)$ es verdadera.

Demostración alternativa: Observe que $10 \equiv 1 \pmod 9$ porque $10 - 1 = 9$ y $9 \mid 9$. Entonces por el teorema 8.4.3 $(49, 10^n \equiv 1^n \equiv 1 \pmod 9)$.

14. $14^1 \; mod \; 55 = 14$
$14^2 \; mod \; 55 = 196 \; mod \; 55 = 31$
$14^4 \; mod \; 55 = (14^2 \; mod \; 55)^2 \; mod \; 55 = 31^2 \; mod \; 55 = 26$
$14^8 \; mod \; 55 = (14^4 \; mod \; 55)^2 \; mod \; 55 = 26^2 \; mod \; 55 = 16$
$14^{16} \; mod \; 55 = (14^8 \; mod \; 55)^2 \; mod \; 55 = 16^2 \; mod \; 55 = 36$

15. $4^{27} \; mod \; 55 = 14^{16+8+2+1} \; mod \; 55$
$= \{(14^{16} \; mod \; 55)(14^8 \; mod \; 55)(14^2 \; mod \; 55)$
$(14^1 \; mod \; 55)\} \; mod \; 55$
$= (36 \cdot 16 \cdot 31 \cdot 14) \; mod \; 55 = 249984 \; mod \; 55 = 9$

16. Observe que: $307 = 256 + 32 + 16 + 2 + 1$.
$675^1 \; mod \; 713 = 675$
$675^2 \; mod \; 713 = 18$
$675^4 \; mod \; 713 = 18^2 \; mod \; 713 = 324$
$675^8 \; mod \; 713 = 324^2 \; mod \; 713 = 165$
$675^{16} \; mod \; 713 = 165^2 \; mod \; 713 = 131$
$675^{32} \; mod \; 713 = 131^2 \; mod \; 713 = 49$
$675^{64} \; mod \; 713 = 49^2 \; mod \; 713 = 262$
$675^{128} \; mod \; 713 = 262^2 \; mod \; 713 = 196$
$675^{256} \; mod \; 713 = 196^2 \; mod \; 713 = 627$
Así
$675^{307} \; mod \; 713 \; \Im \; 675^{256+32+16=2+1} \; mod \; 713$
$= (675^{256} \cdot 675^{32} \cdot 675^{16} \cdot 675^2 \cdot 675^1) \; mod \; 713$
$= (627 \cdot 49 \cdot 131 \cdot 18 \cdot 675) \; mod \; 713 = 3.$

19. Las letras HOLA se trasladan numéricamente en 08, 15, 12 y 01. Por el ejemplo 8.4.9, la H se encripta como 17. Para encriptar la O, calculamos $15^3 \; mod \; 55 = 20$. Para encriptar la L, determinamos $12^3 \; mod \; 55 = 23$. Y para encriptar la A, obtenemos $1^3 \; mod \; 55 = 01$. Así el texto cifrado es 17 20 23 01. (En la práctica, las letras individuales del alfabeto se agrupan en bloques durante la encriptación para que así el descifrado no se pueda lograr conociendo los patrones de frecuencia de letras o palabras).

22. Por el ejemplo 8.4.10, la clave para el descifrado es 27. Así, los residuos módulo 55 para 08^{27}, 21^{27}, 15^{27}, 49^{27} y 20^{27} se deben encontrar y traducirse a las letras del alfabeto.

Como $27 = 16 + 8 + 2 + 1$, primero efectuamos las siguientes operaciones:

$08^1 \equiv 8 \pmod{55}$ $21^1 \equiv 21 \pmod{55}$ $15^1 \equiv 15 \pmod{55}$
$08^2 \equiv 9 \pmod{55}$ $21^2 \equiv 1 \pmod{55}$ $15^2 \equiv 5 \pmod{55}$
$08^4 \equiv 26 \pmod{55}$ $21^4 \equiv 1 \pmod{55}$ $15^4 \equiv 25 \pmod{55}$
$08^8 \equiv 16 \pmod{55}$ $21^8 \equiv 1 \pmod{55}$ $15^8 \equiv 20 \pmod{55}$
$08^{16} \equiv 36 \pmod{55}$ $21^{16} \equiv 1 \pmod{55}$ $15^{16} \equiv 15 \pmod{55}$

$49^1 \equiv 49 \pmod{55}$ $20^1 \equiv 20 \pmod{55}$
$49^2 \equiv 36 \pmod{55}$ $20^2 \equiv 15 \pmod{55}$
$49^4 \equiv 31 \pmod{55}$ $20^4 \equiv 5 \pmod{55}$
$49^8 \equiv 26 \pmod{55}$ $20^8 \equiv 25 \pmod{55}$
$49^{16} \equiv 16 \pmod{55}$ $20^{16} \equiv 20 \pmod{55}$

Entonces calculamos

$$08^{27} \textit{ mod } 55 = (36 \cdot 16 \cdot 9 \cdot 8) \textit{ mod } 55 = 2$$
$$21^{27} \textit{ mod } 55 = (16 \cdot 26 \cdot 36 \cdot 49) \textit{ mod } 55 = 21$$
$$15^{27} \textit{ mod } 55 = (15 \cdot 5 \cdot 20 \cdot 15) \textit{ mod } 55 = 5$$
$$49^{27} \textit{ mod } 55 = (16 \cdot 26 \cdot 36 \cdot 49) \textit{ mod } 55 = 14$$
$$20^{27} \textit{ mod } 55 = (20 \cdot 25 \cdot 15 \cdot 20) \textit{ mod } 55 = 15$$

Finalmente, como 2, 21, 5, 14 y 15 se traducen a las letras B, U, E, N y O, vemos que el mensaje es BUENO.

25. *Sugerencia:* Por el teorema 5.2.3, empleando a en lugar de r y $n-1$ en lugar de n, tenemos que $1 + a + a^2 + \cdots + a^{n-1} = \frac{a^n - 1}{a - 1}$. Multiplicando ambos lados por $a - 1$ se obtiene

$$a^n - 1 = (a - 1)(1 + a + a^2 + \cdots + a^{n-1}).$$

26. Paso 1: $6664 = 765 \cdot 8 + 544$ y así $544 = 6664 - 765 \cdot 8$
Paso 2: $765 = 544 \cdot 1 + 221$ y así $221 = 765 - 544$
Paso 3: $544 = 221 \cdot 2 + 102$ y así $102 = 544 - 221 \cdot 2$
Paso 4: $221 = 102 \cdot 2 + 17$ y así $7 = 221 - 102 \cdot 2$
Paso 5: $102 = 17 \cdot 6 + 0$

Así mcd(6664, 765) = 17 (que es el residuo que se obtiene justamente antes de la división final). Sustituya en hacia atrás los pasos 4−1 para expresar 17 como una combinación lineal de 6664 y 765:

$$\begin{aligned} 17 &= 221 - 102 \cdot 2 \\ &= 221 - (544 - 221 \cdot 2) = 221 \cdot 5 - 544 \cdot 2 \\ &= (765 - 544) \cdot 5 - 544 \cdot 2 = 765 \cdot 5 - 544 \cdot 7 \\ &= 765 \cdot 5 - (6664 - 765 \cdot 8) \cdot 7 = (-7) \cdot 6664 + 61 \cdot 765. \end{aligned}$$

(Cuando haya terminado este paso final, es sabio que compruebe que no ha cometido un error comprobando que la expresión final realmente es igual al máximo común divisor.)

28.

a	330	156	18	12	6
b	156	18	12	6	0
r		18	12	6	0
q		2	8	1	2
s	1	0	1	−8	9
t	0	1	−2	17	−19
u	0	1	−8	9	−26
v	1	−2	17	−19	55
nueva		1	−8	9	−26
nueva		−2	17	−19	55
sa + tb	330	18	−6	6	6

31. a. Paso 1: $210 = 13 \cdot 16 + 2$ y así $2 = 210 - 16 \cdot 13$
Paso 2: $13 = 2 \cdot 6 + 1$ y así $1 = 13 - 2 \cdot 6$
Paso 3: $6 = 1 \cdot 6 + 0$ y así $\text{mcd}(210, 13) = 1$

Sustituya hacia atrás los pasos 2−1:

$$\begin{aligned} 1 &= 13 - 2 \cdot 6 \\ &= 13 - (210 - 16 \cdot 13) \cdot 6 = (-6) \cdot 210 + 97 \cdot 13 \end{aligned}$$

Así $210 \cdot (-6) = 1 \pmod{13}$ y entonces -6 es un inverso para 210 módulo 13.

b. Calcule $13 - 6 = 7$ y observe que $7 = -6 \pmod{13}$ porque $7 - (-6) = 13 = 13 \cdot 1$. Así, por el teorema $8 \cdot 4 \cdot 3(3)$, $210 \cdot 7 = 210 \cdot (-6) \pmod{13}$. Se tiene, por la propiedad transitiva de la congruencia, que $210 \cdot 7 \equiv 1 \pmod{13}$ y entonces 7 es un inverso positivo para 210 módulo 13.

c. Este problema puede ser resuelto usando el resultado del inciso *a*) o el del inciso *b*). Por el inciso *b*) $210 \cdot 7 = 1 \pmod{13}$. Multiplicando ambos lados por 8 y aplicando el teorema 8.4.3(3) para obtener que $210 \cdot 56 \equiv 8 \pmod{13}$. Así una solución positiva para $210x \equiv 8 \pmod{13}$ es $x = 56$. Observe que el mínimo residuo positivo correspondiente a esta solución también es una solución. Por el teorema 8.4.1, $56 = 4 \pmod{13}$ porque $56 = 13 \cdot 4 + 4$ y así, por el teorema 8.4.3(3), $210 \cdot 56 = 210 \cdot 4 = 9 \pmod{13}$. Esto muestra que 4 también es una solución para la congruencia y como $0 \leq 4 < 13$, 4 es la mínima solución positiva para la congruencia.

33. *Sugerencia:* Si $as + bt = 1$ y $c = au = bv$, entonces $c = asc + btc = as(bv) + bt(au)$.

35. *Demostración:* Suponga que a, n, s y s' son enteros tales que $as = as' = 1 \pmod{n}$. Considere la cantidad $as's$ y observe que $as's = (as') \cdot s = (as) \cdot s'$. Por el teorema 8.4.3(3), $(as') \cdot s = 1 \cdot s = s \pmod{n}$ y $(as') \cdot s' = 1 \cdot s' = s' \pmod{n}$. Esto prueba que cualesquiera dos inversos de a son congruentes módulo n.

36. Los equivalentes numéricos de A y, U, D, A son 01, 25, 21, 04 y 01. Para encriptar esas letras, se deben calcular las siguientes cantidades. 1^{43} *mod* 713, 25^{43} *mod* 713, 21^{43} *mod* 713, 4^{43} *mod* 713 y 1^{43} *mod* 713. Usamos el hecho de que $43 = 32 + 8 + 2 + 1$.

A: $01^1 \equiv 1 \pmod{713}$
$01^2 \equiv 1 \pmod{713}$
$01^4 \equiv 1 \pmod{713}$
$01^8 \equiv 1 \pmod{713}$
$01^{16} \equiv 1 \pmod{713}$
$01^{32} \equiv 1 \pmod{713}$
Así el texto cifrado es
$1^{43} \textit{ mod } 713$
$= (1 \cdot 1 \cdot 1.1) \textit{ mod } 713 = 001.$

Y: $25^1 \equiv 25 \pmod{713}$
$25^2 \equiv 625 \pmod{713}$
$25^4 \equiv 614 \pmod{713}$
$25^8 \equiv 532 \pmod{713}$
$25^{16} \equiv 676 \pmod{713}$
$25^{32} \equiv 656 \pmod{713}$
Así el texto cifrado es
$25^{43} \textit{ mod } 713$
$= (25 \cdot 625 \cdot 532 \cdot 656) \textit{ mod } 713 = 242.$

U: $21^1 \equiv 21 \pmod{713}$
$21^2 \equiv 441 \pmod{713}$
$21^4 \equiv 545 \pmod{713}$
$21^8 \equiv 417 \pmod{713}$
$21^{16} \equiv 630 \pmod{713}$
$21^{32} \equiv 472 \pmod{713}$
Así el texto cifrado es
21^{43} *mod* 713
$= (21 \cdot 441 \cdot 417 \cdot 472)$ *mod* 713 $= 425$.

D: $04^1 \equiv 4 \pmod{713}$
$04^2 \equiv 16 \pmod{713}$
$04^4 \equiv 256 \pmod{713}$
$04^8 \equiv 653 \pmod{713}$
$04^{16} \equiv 35 \pmod{713}$
$04^{32} \equiv 512 \pmod{713}$
Así el texto cifrado es
4^{43} *mod* 713
$= (4 \cdot 16 \cdot 653 \cdot 512)$ *mod* 713 $= 374$.

Por tanto, el mensaje encriptado es 001 242 425 374 001. (Otra vez, observe que en la práctica, las letras individuales del alfabeto son agrupadas en bloques durante la encriptación para que así no se pueda lograr descifrar mediante el conocimiento de los patrones de frecuencia de letras o palabras. Las hemos mantenido separadas para que los números en los cálculos fueran los más pequeños y fáciles de manejar).

39. Por el ejercicio 38, la clave para descifrar, d, es 307. Así que, para descifrar el mensaje, se deben calcular las siguientes cantidades que deben ser calculadas: 533^{307} *mod* 713, 423^{307} *mod* 713, 018^{307} *mod* 713 y 089^{307} *mod* 713. Empleamos el hecho de que $307 = 256 + 32 + 16 + 2 + 1$.

$533 = 533 \pmod{713}$
$533^2 = 315 \pmod{713}$
$533^4 = 118 \pmod{713}$
$533^8 = 377 \pmod{713}$
$533^{16} = 242 \pmod{713}$
$533^{32} = 98 \pmod{713}$
$533^{64} = 335 \pmod{713}$
$533^{128} = 284 \pmod{713}$
$533^{256} = 87 \pmod{713}$

$423 = 423 \pmod{713}$
$423^2 = 679 \pmod{713}$
$423^4 = 443 \pmod{713}$
$423^8 = 174 \pmod{713}$
$423^{16} = 330 \pmod{713}$
$423^{32} = 524 \pmod{713}$
$423^{64} = 71 \pmod{713}$
$423^{128} = 50 \pmod{713}$
$423^{256} = 361 \pmod{713}$

$18 = 18 \pmod{713}$
$18^2 = 324 \pmod{713}$
$18^4 = 165 \pmod{713}$
$18^8 = 131 \pmod{713}$
$18^{16} = 49 \pmod{713}$
$18^{32} = 262 \pmod{713}$
$18^{64} = 196 \pmod{713}$
$18^{128} = 627 \pmod{713}$
$18^{256} = 266 \pmod{713}$

$89 = 89 \pmod{713}$
$89^2 = 78 \pmod{713}$
$89^4 = 380 \pmod{713}$
$89^8 = 374 \pmod{713}$
$89^{16} = 128 \pmod{713}$
$89^{32} = 698 \pmod{713}$
$89^{64} = 225 \pmod{713}$
$89^{128} = 2 \pmod{713}$
$89^{256} = 4 \pmod{713}$

Así el descifrado para 533,
533^{307} *mod* 713 $= (533^{256+32+16+2+1})$ *mod* 713
$= (87 \cdot 98 \cdot 242 \cdot 315 \cdot 533)$ *mod* 713 $= 6$, que
corresponde a la letra F.

El descifrado para 423,
423^{307} *mod* 713 $= (423^{256+32+16+2+1})$ *mod* 713
$= (361 \cdot 524 \cdot 330 \cdot 679 \cdot 423)$ *mod* 713 $= 18$, que
corresponde a la letra R.

El descifrado para 18,
18^{307} *mod* 713 $= (18^{256+32+16+2+1})$ *mod* 713
$= (266 \cdot 262 \cdot 49 \cdot 324 \cdot 18)$ *mod* 713 $= 9$, que
corresponde a la letra I.

El descifrado para 89,
89^{307} *mod* 713 $= (89^{256+32+16+2+1})$ *mod* 713
$= (4 \cdot 698 \cdot 128 \cdot 78 \cdot 89)$ *mod* 713 $= 15$, que
corresponde a la letra O.

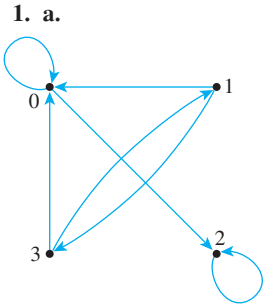
Entonces el mensaje que se obtiene es FRIO.

41. a. *Sugerencia:* Para el paso inductivo, suponga que $p \mid q_1 q_2 \ldots q_{s+1}$ y sea $a = q_1 q_2 \ldots q_s$. Entonces $p \mid aq_{s+1}$ y ya sea que $p = q_{s+1}$ o el lema de Euclides y la hipótesis de inducción se pueden aplicar.

42. a. Cuando $a = 15$ y $p = 7$, $a^{p-1} = 15^6 = 11390625 = 1 \pmod 7$ porque $11390625 - 1 = 7.1627232$.

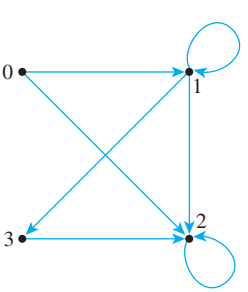
Sección 8.5

1. a.



R_1 no es antisimétrica: $1 R_1 3$ y $3 R_1 1$ pero $1 \neq 3$.

b.



R_2 es antisimétrica: No existen casos en donde $a R b$ y $b R a$ con $a \neq b$.

2. R no es antisimétrica. Sean x y y dos personas diferentes pero de la misma edad. Entonces $x\ R\ y$ y $y\ R\ x$ pero $x \neq y$.

5. R es una relación de orden parcial.

Demostración:

R es reflexiva: Suponga que $(a, b) \in \mathbf{R} \times \mathbf{R}$. Entonces $(a, b)\ R\ (a, b)$ porque $a = a$ y $b \leq b$.

R es antisimétrica: Acepte que (a, b) y (c, d) son pares ordenados de números reales tales que $(a, b)\ R\ (c, d)$ y $(c, d)\ R\ (a, b)$. Entonces

$$a < c \quad \text{o} \quad a = c \text{ y } b \leq d$$

y

$$c < a \quad \text{o} \quad c = a \text{ y } d \leq b.$$

Así

$$a \leq c \quad \text{y} \quad c \leq a$$

de donde

$$a = c.$$

Además,

$$b \leq d \quad \text{y} \quad d \leq b$$

En consecuencia

$$b = d.$$

Así $(a, b) = (c, d)$.

R es transitiva: Suponga que (a, b),(c, d) y (e, f) son pares ordenados de números reales tales que $(a, b)\ R\ (c, d)$ y $(c, d)\ R\ (e, f)$. Entonces

$$a < c \quad \text{o} \quad a = c \text{ y } b \leq d$$

y

$$c < e \quad c \quad = e \text{ y } d \leq f.$$

Se tiene que debe ocurrir uno de los siguientes casos.

Caso 1 ($a < c$ y $c < e$): Entonces por transitividad de $<$, $a < e$ y así $(a, b)\ R\ (e, f)$ por definición de R.

Caso 2 ($a < c$ y $c = e$): Sustituyendo, $a < e$, en consecuencia $(a, b)\ R\ (e, f)$ por definición de R.

Caso 3 ($a = c$ y $c < e$): Entonces sustituyendo, $a < e$ y así $(a, b)\ R\ (e, f)$ por definición de R.

Caso 4 ($a = c$ y $c = e$): Por definición de R, $b \leq d$ y $d \leq f$ y así por transitividad de $\leq$, $b \leq f$. Entonces $a = e$ y $b \leq f$, Por tanto $(a, b)\ R\ (e, f)$ por definición de R.

En cada caso, $(a, b)\ R\ (e, f)$. Por tanto, R es transitiva. Como R es reflexiva, antisimétrica y transitiva, entonces R es una relación de orden parcial.

8. R no es una relación de orden parcial porque R no es antisimétrica.

Contraejemplo: $1\ R\ 3$ (porque $1 + 3$ es par) y $3\ R\ 1$ (porque $3 + 1$ es par) pero $1 \neq 3$.

10. No. *Contraejemplo:* Defina las relaciones R y S sobre el conjunto $\{1, 2\}$ como sigue: $R = \{(1, 2)\}$ y $S = \{(2, 1)\}$. Entonces R y S son antisimétricas, pero $R \cup S = \{(1, 2), (2, 1)\}$ no es antisimétrica porque $(1, 2) \in R \cup S$ y $(2, 1) \in R \cup S$ pero $1 \neq 2$.

11. a. Esto se tiene de (1).

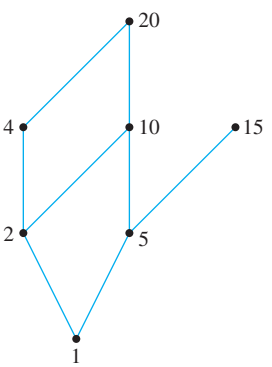
b. Falso. Por (1), $bba \leq bbab$.

13. $R_1 = \{(a, a), (b, b)\}$, $R_2 = \{(a, a), (b, b), (a, b)\}$, $R_3 = \{(a, a), (b, b), (b, a)\}$

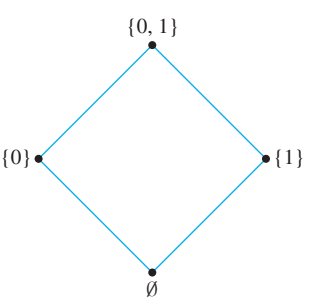
14. a.
$R_1 = \{(a, a), (b, b), (c, c)\}$,
$R_2 = \{(a, a), (b, b), (c, c), (b, a)\}$,
$R_3 = \{(a, a), (b, b), (c, c), (c, a)\}$,
$R_4 = \{(a, a), (b, b), (c, c), (b, a), (c, a)\}$,
$R_5 = \{(a, a), (b, b), (c, c), (c, b), (c, a)\}$,
$R_6 = \{(a, a), (b, b), (c, c), (b, c), (b, a)\}$,
$R_7 = \{(a, a), (b, b), (c, c), (c, b), (b, a), (c, a)\}$,
$R_8 = \{(a, a), (b, b), (c, c), (b, c), (b, a), (c, a)\}$,
$R_9 = \{(a, a), (b, b), (c, c), (b, c)\}$,
$R_{10} = \{(a, a), (b, b), (c, c), (c, b)\}$

15. *Sugerencia:* R es la relación identidad sobre A: $x\ R\ x$ para todo $x \in A$ y $x \not R\ y$ si $x \neq y$.

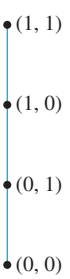
16. a.



17. a.



18.



21. a. *Demostración: [Debemos demostrar que para toda a y b en A, $a \mid b$ o $b \mid a$.]* Sean a y b en A, dados pero arbitrariamente elegidos. Por definición de A, existen enteros no-negativos r y s tales que $a = 2^r$ y $b = 2^s$. Entonces $r \leq s$ o $s < r$. Si $r \leq s$, entonces

$$b = 2^s = 2^r \cdot 2^{s-r} = a \cdot 2^{s-r},$$

en donde $s - r \geq 0$. Se tiene, por definición de divisibilidad, que $a \mid b$. Por un argumento similar, si $s < r$, entonces $b \mid a$. Así, $a \mid b$ o $b \mid a$ *[que era lo que se quería demostrar].*

b.

22. El mayor elemento: ninguno; el menor elemento: 1; Elementos máximos: 15, 20; elementos mínimos: 1.

24. El mayor elemento: {0, 1}; el menor elemento: ∅; Elementos máximos: {0, 1}; elementos mínimos: ∅.

26. El mayor elemento: (1, 1); el menor elemento: (0, 0); Elementos máximos: (1, 1); elementos mínimos: (0, 0).

30. a. No se tienen los elementos mayor ni menor.

b. El menor elemento es 0, el mayor elemento es 1.

31. R es una relación de orden total porque es reflexiva, antisimétrica y transitiva (esto da un orden parcial) y porque $[b, a, c, d]$ es una cadena que contiene a cada elemento de A: bRc, cRa y aRd.

34. *Sugerencia:* Sea R' la restricción de R a B y demuestre que R' es reflexiva, antisimétrica y transitiva. En cada caso, esto se tiene casi inmediatamente del hecho de que R es reflexiva, antisimétrica y transitiva.

35. $\emptyset \subseteq \{w\} \subseteq \{w, x\} \subseteq \{w, x, y\} \subseteq \{w, x, y, z\}$

36. *Demostración:* Suponga que A es un conjunto parcialmente ordenado con respecto a una relación $\preceq$. Por definición de orden total, A está totalmente ordenado si y sólo si, dos elementos cualesquiera de A son comparables. Por definición de cadena, esto es verdadero si y sólo si, A es una cadena.

39. *Demostración (por inducción matemática):* Sea A un conjunto totalmente ordenado con respecto a una relación $\preccurlyeq$ y aceptemos que la propiedad $P(n)$ sea la frase "Cada subconjunto de A con n elementos tiene el menor y el mayor elementos".

Demostración de que P(1) es verdadero:

Si $A = \emptyset$, entonces $P(1)$ es verdadero por defecto. Así aceptemos que A tiene al menos un elemento y supongamos que $S = \{a_1\}$ es un subconjunto de A con un elemento. Como $\preccurlyeq$ es reflexiva, $a_1 \preccurlyeq a_1$. Entonces, por definición de menor y mayor elementos, a_1 es tanto un elemento mínimo como un elemento máximo de S y por tanto la propiedad es verdadera para $n = 1$.

Demostración de que para todos los enteros k ≥ 1, si P(k) es verdadero, entonces P(k + 1) también es verdadero:

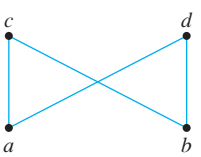
Sea k cualquier entero con $k \geq 1$ y suponga que cualquier subconjunto de A con k elementos tiene un elemento menor y un elemento mayor. *[Hipótesis de inducción.]* Debemos demostrar que cualquier subconjunto de A con $k + 1$ elementos tiene un elemento menor y un elemento mayor. Si A tiene menos de $k + 1$ elementos, entonces el enunciado es verdadero por defecto. Así, supongamos que A al menos tiene $k + 1$ elementos y que $S = \{a_1, a_2, \ldots, a_{k+1}\}$ es un subconjunto de A con $k + 1$ elementos. Por hipótesis inductiva, $S - \{a_{k+1}\}$ tiene un elemento menor s y un elemento mayor b. Como A está totalmente ordenado, entonces a_{k+1} y s son comparables. Si $a_{k+1} \preccurlyeq s$, entonces, por transitividad de $\preccurlyeq$, a_{k+1} es el elemento menor de S; de otra forma, s permanece como el elemento menor de S. Y si $b \preccurlyeq a_{k+1}$, entonces, por transitividad de $\preccurlyeq$, a_{k+1} es el elemento mayor de S; si no, entonces b queda como el elemento mayor de S. Así S tiene un elemento menor y un elemento mayor *[que era lo que se quería demostrar]*.

40. a. *Demostración por contradicción:* Suponga que no. Acepte que A es un conjunto finito que está parcialmente ordenado con respecto a una relación $\preceq$ y que A no tiene elemento mínimo. Construya una secuencia de elementos $x_1, x_2, x_3, \ldots$ de A como sigue:

1. Tome cualquier elemento de A y llámelo x_1.

2. Para cada $i = 2, 3, 4, \ldots$, seleccione a x_i como un elemento de A para el que $x_i \preceq x_{i-1}$ y $x_i \neq x_{i-1}$. *[Tal elemento debe existir porque si no x_{i-1} sería mínimo y estamos suponiendo que ningún elemento de A es mínimo.]* Ahora $x_i \neq x_j$ para cualquier $i \neq j$. *[Si $x_i = x_j$, en donde $i < j$, entonces por otro lado, $x_j \preceq x_{j-1} \preceq \ldots \preceq x_{i+1} \preceq x_i$ y así $x_i \preceq x_{i-1}$, y además, como $x_i = x_j$ entonces $x_j = x_i \succeq x_{i+1}$ y así $x_j \succeq x_{i+1}$. En consecuencia, por antisimetría, $x_j = x_{i+1}$, por tanto $x_i = x_{i+1}$. Pero esto contradice la definición de la secuencia $[x_1, x_2, x_3, \ldots]$.* Así $x_1, x_2, x_3, \ldots$ es una sucesión infinita de elementos distintos y entonces $\{x_1, x_2, x_3, \ldots\}$ es un subconjunto infinito del conjunto finito A. Lo que es imposible. Por tanto, la suposición es falsa y concluimos que cualquier subconjunto parcialmente ordenado de un conjunto finito tiene un elemento mínimo.

42.



44. Uno tal que el orden total es 1, 5, 2, 15, 10, 4, 20.

46. Uno tal que el orden total es (0, 0),(1, 0), (0, 1), (1, 1).

50. a. *Una respuesta posible*: 1, 6, 10, 9, 5, 7, 2, 4, 8, 3.

51. b. Trayectoria crítica: 1, 2, 5, 8, 9.

Sección 9.1

2. 3/4, 1/2, 1/2

3. {1♦, 2♦, 3♦, 4♦, 5♦, 6♦, 7♦, 8♦, 9♦, 10♦, 1♥, 2♥, 3♥, 4♥, 5♥, 6♥, 7♥, 8♥, 9♥, 10♥}, probabilidad = 20/52 ≅ 38.5%

5. {10♣, J♣, Q♣, K♣, A♣, 10♦, J♦, Q♦, K♦, A♦, 10♥, J♥, Q♥, K♥, A♥, 10♠, J♠, Q♠, K♠, K♠, A♠}, probabilidad = 20/52 = 5/13 ≅ 38.5%.

7. {26, 35, 44, 53, 62}, probabilidad = 5/36 ≅ 13.9%

9. {11, 12, 13, 14, 15, 21, 22, 23, 24, 31, 32, 33, 41, 42, 51} probabilidad = 15/36 = $41\frac{2}{3}$%

11. a. {*HHH*, *HHT*, *HTH*, *HTT*, *THH*, *THT*, *TTH*, *TTT*}

b. (i) {*HTT*, *THT*, *TTH*}, probabilidad = 3/8 ≅ 37.5%

12. a. {*BBB*, *BBG*, *BGB*, *BGG*, *GBB*, *GBG*, *GGB*, *GGG*}

b. (i) {*GBB*, *BGB*, *BBG*} probabilidad = 3/8 = 37.5%

13. a. {*CCC*, *CCW*, *CWC*, *CWW*, *WCC*, *WCW*, *WWC*, *WWW*}

b. (i) {*CWW*, *WCW*, *WWC*}, probabilidad = 3/8 = 37.5%

14. a. probabilidad $= 3/8 = 37.5\%$

16. a. $\{RRR, RRB, RRY, RBR, RBB, RBY, RYR, RYB, RYY, BRR, BRB, BRY, BBR, BBB, BBY, BYR, BYB, BYY, YRR, YRB, YRY, YBR, YBB, YBY, YYR, YYB, YYY\}$

b. $\{RBY, RYB, YBR, BRY, BYR, YRB\}$, probabilidad $= 6/27 = 2/9 \cong 22.2\%$

c. $\{RRB, RBR, BRR, RRY, RYR, YRR, BBR, BRB, RBB, BBY, BYB, YBB, YYR, YRY, RYY, YYB, YBY, BYY\}$ probabilidad $= 18/27 = 2/3 = 66\frac{2}{3}\%$

18. a. $\{B_1B_1, B_1B_2, B_1W, B_2B_1, B_2B_2, B_2W, WB_1, WB_2, WW\}$

b. $\{B_1B_1, B_1B_2, B_2B_1, B_2B_2\}$ probabilidad $= 4/9 \cong 44.4\%$

c. $\{B_1W, B_2W, WB_1, WB_2\}$ probabilidad $= 4/9 \cong 44.4\%$

21. a.

10	11	12	13	14	15	16	17	18	...	96	97	98	99
		↕			↕			↕		↕			↕
		$3\cdot4$			$3\cdot5$			$3\cdot6$		$3\cdot32$			$3\cdot33$

El diagrama anterior muestra que hay tantos posibles enteros de dos dígitos, que son múltiplos de 3, como enteros de 4 a 33 inclusive. Por el teorema 9.1.1, existen $33 - 4 + 1$, o 30, de dichos enteros.

b. En total existen $99 - 10 + 1 = 90$ enteros positivos de dos dígitos y por el inciso *a*), 30 de éstos son múltiplos de 3. Así la probabilidad de que un entero positivo de dos dígitos seleccionado aleatoriamente sea un múltiplo de 3 es $30/90 = 1/3 = 33\frac{1}{3}\%$.

c. De los enteros del 10 al 99 que son múltiplos de 4, el más pequeño es 12 $(= 4\cdot3)$ y el más grande es 96 $(= 4\cdot24)$. Entonces hay $24 - 3 + 1 = 22$ enteros de dos dígitos que son múltiplos de 4. Por tanto, la probabilidad de que un entero de dos dígitos seleccionado aleatoriamente sea múltiplo de 4 es $22/90 = 36\frac{2}{3}\%$.

23. c. Probabilidad $= \dfrac{m-3+1}{n} = \dfrac{m-2}{n}$

d. Porque $\left\lfloor \frac{39}{2} \right\rfloor = 19$, la probabilidad es $\dfrac{39-19+1}{39} = \dfrac{21}{39}$.

24. a. (i) Si n es par, hay $\left\lfloor \frac{n}{2} \right\rfloor = \frac{n}{2}$ elementos en el sub-arreglo.

(ii) Si n es impar, existen $\left\lfloor \frac{n}{2} \right\rfloor = \frac{n-1}{2}$ elementos en el sub-arreglo.

b. Hay n elementos en el arreglo, así

(i) La probabilidad de que un elemento esté en el sub-arreglo dado cuando n es par es $\dfrac{\frac{n}{2}}{n} = \frac{1}{2}$,

(ii) La probabilidad de que un elemento esté en el sub-arreglo dado cuando n es impar es $\dfrac{\frac{n-1}{2}}{n} = \dfrac{n-1}{2n}$.

26. Aceptemos que k sea el 27-ésimo elemento en el arreglo. Por el teorema 9.1.1, $k - 42 + 1 = 27$ y así $k = 42 + 27 - 1 = 68$. Entonces el 27-ésimo elemento en el arreglo es $A[68]$.

28. Sea m el más pequeño de los enteros. Por el teorema 9.1.1, $279 - m + 1 = 56$, Por tanto, $m = 279 - 56 + 1 = 224$. Así, el más pequeño de los enteros es 224.

31.

1	2	3	4	5	6	7	8	9	...	999	1000	1001
		↕			↕			↕			↕	
		$3\cdot1$			$3\cdot2$			$3\cdot3$			$3\cdot333$	

Entonces, entre 1 y 1001 hay 333 múltiplos de 3.

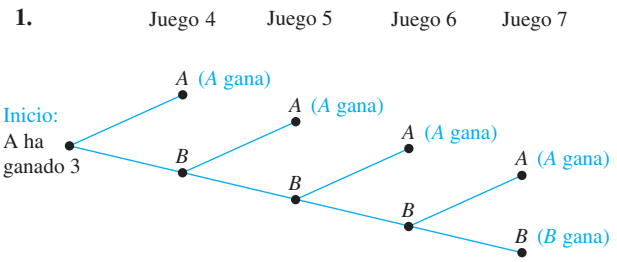
32. a.

M	Tu	W	Th	F	Sa	Su	M	Tu	W	Th	F	Sa	Su	⋯	F	Sa	Su	M
1	2	3	4	5	6	7	8	9	10	11	12	13	14		362	363	364	365
						↕							↕				↕	
						$7\cdot1$							$7\cdot2$				$7\cdot52$	

Los domingos ocurren en el séptimo día del año, en el 14avo día del año y en efecto en todos los días que son múltiplos de 7. Entre 1 y 365 existen 52 múltiplos de 7 y por tanto hay 52 domingos en el año.

Sección 9.2

1.



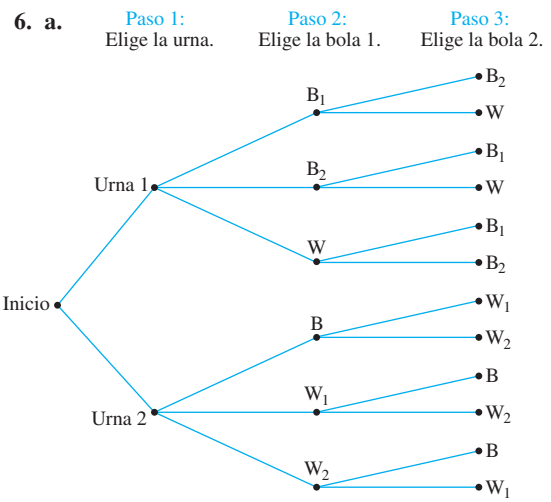
Hay cinco maneras de completar la serie:

A, $B{-}A$, $B{-}B{-}A$, $B{-}B{-}B{-}A$, y $B{-}B{-}B{-}B$.

3. Cuatro maneras: $A{-}A{-}A{-}A$, $B{-}A{-}A{-}A{-}A$, $B{-}B{-}A{-}A{-}A{-}A$ y $B{-}B{-}B{-}A{-}A{-}A{-}A$.

4. Dos maneras: $A{-}B{-}A{-}B{-}A{-}B{-}A$ y $B{-}A{-}B{-}A{-}B{-}A{-}B$.

6. a.



b. Hay 12 salidas igualmente probables en el experimento.

c. $2/12 = 1/6 = 16\frac{2}{3}\%$ **d.** $8/12 = 2/3 = 66\frac{2}{3}\%$

8. Por la regla de la multiplicación, la respuesta es $3 \cdot 2 \cdot 2 = 12$.

9. a. Al ir de la ciudad A a la ciudad B, se puede tomar cualquiera de 3 caminos. Al viajar de la ciudad B a la ciudad C, se puede elegir cualquiera de 5 rutas. Así, por la regla de la multiplicación, existen $3 \cdot 5 = 15$ formas de ir de la ciudad A a la ciudad C pasando por B.

b. Una jornada de viaje redondo puede pensarse como una operación de cuatro pasos:

Paso 1: Ir de A a B.

Paso 2: Ir de B a C.

Paso 3: Ir de C a B.

Paso 4: Ir de B a A.

Existen 3 formas de realizar el paso 1, 5 maneras de hacer el paso 2, 5 opciones de efectuar el paso 3 y 3 formas de realizar el paso 4, entonces por la regla de la multiplicación, hay $3 \cdot 5 \cdot 5 \cdot 3 = 225$ rutas de viaje redondo.

c. En este caso los pasos para hacer el viaje redondo son los mismos que en el inciso *b*), pero como ningún segmento de ruta puede repetirse, entonces sólo hay 4 maneras de efectuar el paso 3 y sólo 2 formas de realizar el paso 4. Así, por la regla de la multiplicación, existen $3 \cdot 5 \cdot 4 \cdot 2 = 120$ rutas de viaje redondo en las cuales ningún camino se viaja dos veces.

11. a. Imagine la construcción de una cadena de longitud 8 como un proceso de ocho pasos:

Paso 1: Elige un 0 o un 1 para la siguiente posición más a la izquierda.

Paso 2: Selecciona un 0 o un 1 para la siguiente posición a la derecha.

Paso 3: Elige un 0 o un 1 para la siguiente posición a la derecha.

Como hay 2 maneras de efectuar cada paso, entonces el número total de formas de ejecutar la operación entera, que es el número de diferentes eslabones en la cadena de longitud 8, es $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 2^8 = 256$.

b. Imagine que hay tres 0 en las tres posiciones más a la izquierda, e imagine el llenado de las restantes 5 posiciones como un proceso de 5 pasos, en donde el paso i significa llenar la posición $(i + 3)$. Puesto que existen 2 maneras de realizar cada uno de los 5 pasos, entonces hay 2^5 formas para ejecutar la operación completa. Así que hay 2^5, o 32, cadenas de 8 eslabones que empiezan con tres 0.

12. a. Existen 9 dígitos hexadecimales de 3 a través de B y 11 dígitos hexadecimales de 5 que pasan por F. Así, la respuesta es $9 \cdot 16 \cdot 16 \cdot 16 \cdot 11 = 405\,504$.

13. a. En cada una de las cuatro tiradas hay dos posibles resultados: cara (C) o cruz (T). Así, por la regla de la multiplicación, el número de resultados es $2 \cdot 2 \cdot 2 \cdot 2 = 2^4 = 16$.

b. Hay seis resultados con dos caras:

$$CCTT, CTCT, CTTC, TCCT, TCTC, TTTT.$$

Por tanto, la probabilidad de obtener exactamente dos caras es $6/16 = 3/8$.

14. a. Aceptemos que cada uno de los pasos 1-4 consista en elegir una letra del alfabeto para colocarla en las posiciones 1-4 y que cada uno de los pasos 5-7 sea seleccionar un dígito para ponerlo en las posiciones 5-7. Como hay 26 letras y 10 dígitos (0–9), entonces la cantidad de placas de licencia es

$$26 \cdot 26 \cdot 26 \cdot 26 \cdot 10 \cdot 10 \cdot 10 = 456\,976\,000.$$

b. En este caso sólo hay una manera de efectuar el paso 1 (porque la primera letra debe ser una A) y sólo una forma de realizar el paso 7 (porque el último dígito debe ser un 0).Por tanto, el número de placas de licencia es $26 \cdot 26 \cdot 26 \cdot 10 \cdot 10 = 17\,576\,000$.

d. En este caso tenemos 26 opciones para efectuar el paso 1, 25 maneras de realizar el paso 2, 24 formas de hacer el paso 3, 10 alternativas para ejecutar el paso 4, 9 opciones para realizar el paso 5 y 8 maneras de efectuar el paso 6, entonces el número de placas de licencia es $26 \cdot 25 \cdot 24 \cdot 23 \cdot 10 \cdot 9 \cdot 8 = 258\,336\,000$.

16. a. Dos soluciones:

(i) número de enteros.

$$= \begin{bmatrix}\text{número de maneras}\\ \text{de elegir el primer}\\ \text{dígito}\end{bmatrix}\begin{bmatrix}\text{número de formas}\\ \text{de seleccionar el}\\ \text{segundo dígito}\end{bmatrix} = 9 \cdot 10 = 90$$

(ii) Usando el teorema 9.1.1,número de enteros $= 99 - 10 + 1 = 90$.

b. Los enteros impares terminan en 1, 3, 5, 7, o en 9.
número de enteros impares

$$= \begin{bmatrix}\text{número de maneras}\\ \text{de elegir el primer}\\ \text{dígito}\end{bmatrix}\begin{bmatrix}\text{número de formas}\\ \text{de seleccionar el}\\ \text{segundo dígito}\end{bmatrix} = 9 \cdot 5 = 45$$

Solución alternativa: Aplique el método de listado indicado en la solución del ejemplo 9.1.4.

c.
$$\begin{bmatrix}\text{número de enteros}\\ \text{con dígitos distintos}\end{bmatrix} = \begin{bmatrix}\text{número de maneras}\\ \text{de elegir el primer}\\ \text{dígito}\end{bmatrix}\begin{bmatrix}\text{número de formas}\\ \text{de seleccionar el}\\ \text{segundo dígito}\end{bmatrix}$$
$$= 9 \cdot 9 = 81$$

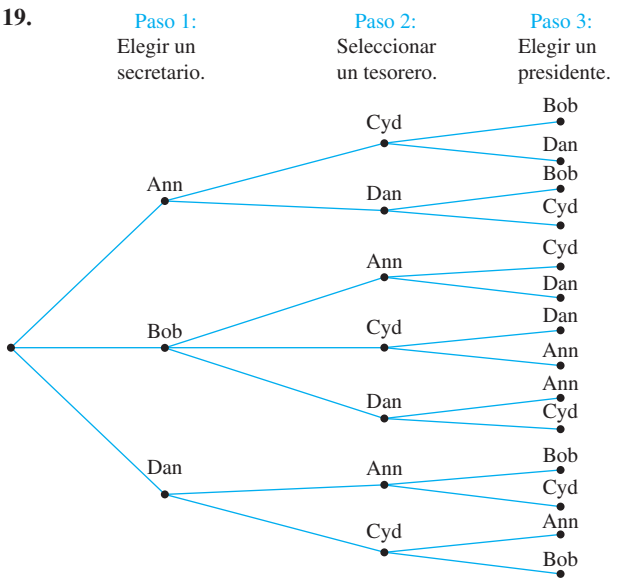
d.
$$\begin{bmatrix}\text{número de enteros impares}\\ \text{con dígitos distintos}\end{bmatrix} = \begin{bmatrix}\text{número de maneras}\\ \text{de elegir el segundo}\\ \text{dígito}\end{bmatrix}\begin{bmatrix}\text{número de formas}\\ \text{de seleccionar el}\\ \text{primer dígito}\end{bmatrix}$$
$$= 5 \cdot 8 = 40$$ porque el primer dígito no puede ser igual a 0, ni puede ser igual al segundo dígito

e. $81/90 = 9/10$, $40/90 = 4/9$.

18. a. Aceptemos que el paso 1 sea elegir el número 2 o una de las letras correspondientes al número 2 en el tablero, que el paso 2 consista en seleccionar el número 1 o una de las letras asociadas en el tablero y que los pasos 3 y 4 sean elegir el número 3 o una de las letras correspondientes al número 3 en el tablero. Hay 4 maneras de efectuar el paso 1, 3 formas de realizar el paso 2 y 4 opciones para ejecutar cada uno de los pasos 3 y 4.

Así por la regla de multiplicación, existen $4 \cdot 3 \cdot 4 \cdot 4 = 192$ formas de realizar la operación completa. Entonces hay 192 diferentes NIPs que son tecleados igual como 2133. Observe que en el tablero de una computadora, esos NIPs no serían tecleados de la misma manera.

19.



En este árbol de probabilidades existen 14 rutas para ir de "raíz" a "hoja", por lo que hay 14 formas de elegir a los funcionarios. Como $14 = 2 \cdot 7$, entonces reordenar los pasos no hará posible emplear únicamente la regla de multiplicación para resolver este problema.

20. a. No es constante el número de maneras de realizar el paso 4; eso depende de qué pasos previos fueron efectuados. Por ejemplo, si en los pasos del 1 al 3 se eligieron 3 dígitos, entonces habrían $10 - 3 = 7$ opciones para hacer el paso 4, pero si 3 letras fueron seleccionadas en los pasos del 1 al 3, entonces habrían 10 maneras de realizar el paso 4.

21. *Sugerencia:*

a. La respuesta es 2^{mn}. **b.** La respuesta es n^m.

22. a. La respuesta es $4 \cdot 4 \cdot 4 = 4^3 = 64$. Imagina que la creación de una función, de un conjunto de 3 elementos a un conjunto de 4 elementos, sea un proceso de tres pasos: el paso 1 consiste en enviar el primer elemento del conjunto de 3 elementos a un elemento del conjunto de 4 elementos (hay cuatro maneras de realizar esto); el paso 2 es enviar el segundo elemento del primer conjunto a un elemento del segundo conjunto (también hay cuatro opciones); y en el paso 3 se mapea el tercer elemento del conjunto inicial sobre un elemento del segundo conjunto (se tienen cuatro maneras para efectuar esto). Entonces, el proceso completo puede realizarse en $4 \cdot 4 \cdot 4$ formas distintas.

24. El bucle externo se itera 30 veces y durante cada iteración del bucle externo hay 15 iteraciones del bucle interior. Así que, por la regla de la multiplicación, el número total de iteraciones del bucle interno es $30 \cdot 15 = 450$.

27. El bucle externo es iterado $50 - 5 + 1 = 46$ veces y en cada iteración del bucle exterior hay $20 - 10 + 1 = 11$ iteraciones del bucle interior. Entonces, por la regla de la multiplicación. El número total de iteraciones del bucle interno es $46 \cdot 11 = 506$.

29. *Sugerencias:* Una solución es agregar ceros al frente, tantos como sean necesarios, para hacer que cada número tenga 5 dígitos. Por ejemplo, escribir 1 como 00001. Aceptemos que algunos de los pasos consistan en elegir posiciones para los dígitos dados. La respuesta es 720. Otra solución es considerar por separado los casos de números con cuatro y cinco dígitos.

31. a. Hay $a + 1$ divisores: $1, p, p^2, \ldots, p^a$.

b. Un divisor es un producto de cualquiera de los $a + 1$ números listados en el inciso *a*) por uno de los $b + 1$ números $1, q, q^2, \ldots, q^b$. Así, por la regla de multiplicación, en total existen $(a + 1)(b + 1)$ divisores.

32. a. Como son distintas las nueve letras de la palabra *ALGORITMO*, entonces hay tantos arreglos de esas letras como permutaciones de un conjunto de nueve elementos: $9! = 362\,880$.

b. En este caso existen efectivamente ocho símbolos para ser permutados (porque *AL* puede considerarse como un solo símbolo). Así el número de arreglos es $8! = 40\,320$.

34. El mismo razonamiento como en el ejemplo 9.2.9 da una respuesta de $4! = 24$.

35. $WX, WY, WZ, XW, XY, XZ, YW, YX, YZ, ZW, ZX, ZY$

37. a. $P(6, 4) = \dfrac{6!}{(6-4)!} = \dfrac{6 \cdot 5 \cdot 4 \cdot 3 \cdot \cancel{2 \cdot 1}}{\cancel{2 \cdot 1}} = 360$

38. a. $P(5, 3) = \dfrac{5 \cdot 4 \cdot 3 \cdot \cancel{2!}}{\cancel{2!}} = 60$

39. a. $P(9, 3) = \dfrac{9 \cdot 8 \cdot 7 \cdot \cancel{6!}}{\cancel{6!}} = 504$

c. $P(8, 5) = \dfrac{8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot \cancel{3!}}{\cancel{3!}} = 6{,}720$

41. *Demostración:* Sea n un entero con $n \geq 2$. Entonces

$$\begin{aligned} &P(n+1, 2) - P(n, 2) \\ &= \frac{(n+1)!}{[(n+1)-2]!} - \frac{n!}{(n-2)!} = \frac{(n+1)!}{(n-1)!} - \frac{n!}{(n-2)!} \\ &= \frac{(n+1) \cdot n \cdot \cancel{(n-1)!}}{\cancel{(n-1)!}} - \frac{n \cdot (n-1) \cdot \cancel{(n-2)!}}{\cancel{(n-2)!}} \\ &= n^2 + n - (n^2 - n) = 2n = 2 \cdot \frac{n \cdot (n-1)!}{(n-1)!} \\ &= 2 \cdot \frac{n!}{(n-1)!} = 2P(n, 1). \end{aligned}$$

Esto es lo que se quería demostrar.

45. *Sugerencia:* En el paso inductivo, suponga que existen $k!$ permutaciones de un conjunto de k elementos. Sea X un conjunto con $k + 1$ elementos. El proceso de formar una permutación de los elementos de X puede considerarse como una operación de dos pasos, en donde el paso 1 es elegir el elemento que primero debe escribirse. El paso 2 consiste en escribir, en algún orden, los elementos restantes de X.

47. a.

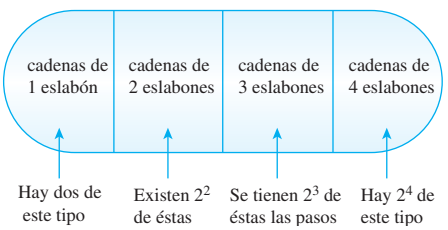
1	2	3	1	2	3	1	2	3
↓	↓	↓	↓	↓	↓	↓	↓	↓
1	2	3	2	1	3	3	2	1

c.

1	2	3	1	2	3	1	2	3
↓	↓	↓	↓	↓	↓	↓	↓	↓
1	3	2	2	3	1	3	1	2
1	2	3	1	2	3			
↓	↓	↓	↓	↓	↓			
2	3	1	3	1	2			

Sección 9.3

1. a. Conjunto de cadenas, éstas pueden tener de 1 a 4 eslabones



Aplicando la regla de suma a la figura anterior se muestra que existen $2 + 2^2 + 2^3 + 2^4 = 30$ cadenas de 1 a 4 eslabones.

b. Por un razonamiento similar al del inciso *a*), hay $2^5 + 2^6 + 2^7 + 2^8 = 480$ cadenas de 5 a 8 eslabones.

3. a. [número de enteros del 1 al 999 con ningún dígito repetido]

= [número de enteros del 1 al 9 con ningún dígito repetido] + [número de enteros del 10 al 99 con ningún dígito repetido] + [número de enteros del 100 al 999 con ningún dígito repetido]

$= 9 + 9 \cdot 9 + 9 \cdot 9 \cdot 8 = 738$

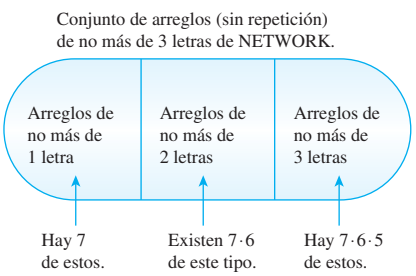
b. [número de enteros del 1 al 999 con al menos un dígito repetido]

= [número total de enteros del 1 al 999] − [número de enteros del 1 al 999 con ningún dígito repetido]

$= 999 - 738 = 261$

c. La probabilidad de que un entero que se elija aleatoriamente tenga al menos un digito repetido es $261/999 \cong 26.1\%$.

4.



Aplicando la regla de suma para la figura anterior, se muestra que existen $7 + 7 \cdot 6 + 7 \cdot 6 \cdot 5 = 259$ arreglos de tres letras de la palabra NETWORK si no está permitida la repetición de letras.

6. a. Hay $1 + 26 + 26^2 + 26^3$ arreglos de 0 a 3 letras del alfabeto. Cualesquiera de éstos se puede asociar con todas menos un arreglo de 0 a 4 dígitos y existen $1 + 10 + 10^2 + 10^3 + 10^4$ arreglos de 0 a 4 dígitos. Así, por la regla de multiplicación y la regla de la diferencia, el número de placas es

$$(1 + 26 + 26^2 + 26^3) \cdot (1 + 10 + 10^2 + 10^3 + 10^4) - 1 = 203{,}097{,}968$$

(↑ placa en blanco)

b. $(1 + 26 + 26^2 + 26^3 - 85) \cdot (1 + 10 + 10^2 + 10^3 + 10^4) - 1 = 202{,}153{,}533$

7. c. *Sugerencia:* La respuesta es 774,372,096.

8. a. $50^3 + 50^4 + 50^5 = 318{,}875{,}000$

9. a. Cada columna de la tabla de abajo corresponde a un par de valores de i y j, para el cual el bucle interior será iterado.

i	1	2 →		3 →			4 →			
j	1	1	2	1	2	3	1	2	3	4
		1		2			3			4

Como existen $1 + 2 + 3 + 4 = 10$ columnas, el bucle interior será iterado diez veces.

11. a. La respuesta es el número de permutaciones de las cinco letras en *QUICK*, que es igual a $5! = 120$.

b. Ya que a *QU* (en orden) se le considera como una sola unidad, entonces la respuesta es el número de permutaciones de los cuatro símbolos $\boxed{QU}, I, C, K$. Esto es $4! = 24$.

c. Por el inciso *b*), hay 4! arreglos de $\boxed{QU}, I, C, K$. Similarmente, existen 4! arreglos de $\boxed{UQ}, I, C, K$. Por tanto, por la regla de suma, tenemos un total de $4! + 4! = 48$ arreglos.

13. a. [número de maneras de colocar ocho personas en una fila manteniendo juntos a A y B.]

= [número de formas de arreglar $\boxed{AB}CDEFGH$] + [número de maneras de arreglar $\boxed{BA}CDEFGH$]

$= 7! + 7! = 5\,040 + 5\,040 = 10\,080$

b. [número de opciones para ubicar a ocho personas en una fila manteniendo separados a A y B.]

= [número total de maneras de colocar a ocho personas en una fila] − [número de formas de ubicar a ocho personas en una fila manteniendo juntas a A y B.]

$= 8! - 10\,080 = 40\,320 - 10\,080$
$= 30\,240$

14. Número de nombres de variables

$$= \begin{bmatrix}\text{número de nombres de}\\ \text{variables numéricas}\end{bmatrix} + \begin{bmatrix}\text{número de cadenas de}\\ \text{nombres de variables}\end{bmatrix}$$
$$= (26 + 26\cdot 36) + (26 + 26\cdot 36) = 1\,924$$

15. *Sugerencia:* En el ejercicio 14 observamos que

$$26 + 26\cdot 36 = 26\sum_{k=0}^{1} 36^k.$$

Aquí generalice esta idea. Use el teorema 5.2.3 para evaluar la expresión que obtenga.

16. a. $10\cdot 9\cdot 8\cdot 7\cdot 6\cdot 5\cdot 4 = 604\,800$

b. $\begin{bmatrix}\text{cantidad de números telefónicos con}\\ \text{al menos un dígito repetido}\end{bmatrix}$

$$= \begin{bmatrix}\text{cantidad total de}\\ \text{números telefónicos}\end{bmatrix} - \begin{bmatrix}\text{cantidad de números telefónicos}\\ \text{con ningún dígito repetido}\end{bmatrix}$$
$$= 10^7 - 604\,800 = 9\,395\,200$$

c. $9\,395\,200/10^7 \cong 93.95\%$

18. a. *Demostración:* Sean A y B eventos mutuamente disjuntos en un espacio muestral. Por la regla de suma, $N(A \cup B) = N(A) + N(B)$. Por tanto, por la fórmula para eventos equiprobables,

$$P(A \cup B) = \frac{N(A \cup B)}{N(S)} = \frac{N(A) + N(B)}{N(S)}$$
$$= \frac{N(A)}{N(S)} + \frac{N(B)}{N(S)} = P(A) + P(B).$$

19. *Sugerencia:* Justifique la siguiente respuesta: $39\cdot 38\cdot 38$.

20. a. Identifique los enteros del 1 al 100 000 que contengan el dígito 6 exactamente una vez con cadenas de cinco dígitos. Así, por ejemplo, 306 sería identificado con 00306. No es necesario emplear cadenas de seis dígitos porque 100 000 no contiene el dígito 6. El proceso de construir una cadena de cinco dígitos que exactamente contiene un 6, puede imaginarse como una operación de cinco pasos que consiste en llenar las posiciones de cinco dígitos $\underset{1}{\_}\ \underset{2}{\_}\ \underset{3}{\_}\ \underset{4}{\_}\ \underset{5}{\_}$.

Paso 1: Para el 6 elija una de las cinco posiciones.
Paso 2: Seleccione un dígito para la posición en el extremo izquierdo.
Paso 3: Elija un dígito para la siguiente posición a la derecha.
Paso 4: Seleccione un dígito para el siguiente lugar a la derecha.
Paso 5: Elija un dígito para la posición en el extremo derecho.

Hay 5 opciones para el paso 1 (cualquiera de la cinco posiciones) y 9 posibilidades para cada paso 2-5 (cualquier dígito excepto 6), por la regla de multiplicación, el número de maneras de efectuar esta operación es $5\cdot 9\cdot 9\cdot 9\cdot 9 = 32\,805$. Entonces existen 32 805 enteros de 1 a 100 000 que contienen el 6 exactamente una vez.

21. *Sugerencia:* La respuesta es 2/3.

23. a. Sean A = conjunto de enteros que son múltiplos de 4 y B = conjunto de enteros que son múltiplos de 7. Entonces $A \cap B$ = conjunto de enteros que son múltiplos de 28.

Pero $n(A) = 250$ porque $1\ 2\ 3\ 4\ 5\ 6\ 7\ 8\ \ldots 999\ 1000$,
$\updownarrow\quad\ \updownarrow\qquad\ \updownarrow$
$4\cdot 1\quad 4\cdot 2\ldots\quad 4\cdot 250$

equivalentemente ya que $1000 = 4\cdot 250$.

Además $n(B) = 142$ porque $1\ 2\ 3\ 4\ 5\ 6\ 7\ \ldots 14\ \ldots \quad 994\ 995\ \ldots 1000$
$\updownarrow\quad\ \updownarrow\qquad\ \updownarrow$
$7\cdot 1\quad 7\cdot 2\ \ldots\ 7\cdot 142$

o equivalentemente ya que $1000 = 7\cdot 142 + 6$.

Y $n(A \cap B) = 35$ porque $1\ 2\ 3\ \ldots 28\ \ldots 56\ \ldots \quad 980\ \ldots 1000$,
$\updownarrow\quad\ \updownarrow\quad\ \updownarrow$
$28\cdot 1\quad 28\cdot 2\ldots\quad 28\cdot 35$

o equivalentemente ya que $1000 = 28\cdot 35 + 20$.

Por tanto, $n(A \cup B) = 250 + 142 - 35 = 357$.

25. a. Longitud 0: ϵ
Longitud 1: 0, 1
Longitud 2: 00, 01, 10, 11
Longitud 3: 000, 001, 010, 011, 100, 101, 110
Longitud 4: 0000, 0001, 0010, 0011, 0100, 0101, 0110, 1000, 1001, 1010, 1011, 1100, 1101

b. Por el inciso *a*), $d_0 = 1$, $d_1 = 2$, $d_2 = 4$, $d_3 = 7$ y $d_4 = 13$.

c. Sea k un entero con $k \geq 3$. Cualquier cadena de longitud k que no contiene el eslabón patrón 111 empieza con un 0 o con un 1. Si inicia con un 0, esto puede ser seguido por cualquier cadena de $k - 1$ eslabones que no contienen el patrón 111. Hay d_{k-1} de éstas. Si la cadena empieza con un 1, entonces los primeros dos eslabones son 10 o 11. Si los primeros dos eslabones son 10, entonces pueden ser seguidos por cualquier cadena de los $k - 2$ eslabones que no contienen el patrón 111. Existen d_{k-2} de éstos. Si la cadena inicia con un 11, entonces el tercer eslabón debe ser 0 (porque la cuerda no contiene 111) y esos tres eslabones pueden ser seguidos por cualquier cadena de $k - 3$ eslabones que no contienen el patrón 111. Hay d_{k-3} de éstas. Por tanto, para todos los enteros $k \geq 3$, $d_k = d_{k-1} + d_{k-2} + d_{k-3}$.

d. Por los incisos *b*) y *c*), $d_5 = d_4 + d_3 + d_2 = 13 + 7 + 4 = 24$. Este es el número de cadenas de longitud cinco que no contienen el patrón 111.

26. c. *Sugerencia:* $s_k = 2s_{k-1} + 2s_{k-2}$.

e. *Sugerencia:* Para todos los enteros $n \geq 0$,

$$s_n = \frac{\sqrt{3}+2}{2\sqrt{3}}(1+\sqrt{3})^n + \frac{\sqrt{3}-2}{2\sqrt{3}}(1-\sqrt{3})^n.$$

28. a. $a_3 = 3$ (Las tres permutaciones que no se mueven más de un lugar de sus posiciones "naturales" son 213, 132 y 123).

29. a. $11001010_2 = 2 + 2^3 + 2^6 + 2^7 = 202$,
$00111000_2 = 2^3 + 2^4 + 2^5 = 56$,
$01101011_2 = 1 + 2 + 2^3 + 2^5 + 2^6 = 107$,
$11101110_2 = 2 + 2^2 + 2^3 + 2^5 + 2^6 + 2^7 = 238$
Así la respuesta es 202.56.107.238.

b. La ID de la red para una red Clase A consiste de 8 bits (eslabones) e inicia con 0. Si fueran permitidas todas las posibles combinaciones de ocho 0 y 1 que empiezan con un 0, habrían dos opciones (0 o 1) para cada una de las 7 posiciones del segundo miembro de los ocho. Esto daría $2^7 = 128$ posibles ID. Pero como 00000000 ni 01111111 están permitidos, entonces el total se reduce por 2, así que hay 126 posibles redes Clase A.

c. Sea $w.x.y.z$ la forma decimal punteada de la dirección IP de una computadora en una red Clase A. Como las ID de la red para una red Clase A van de 00000001 ($= 1$) a 01111110 ($= 126$), entonces w puede ser cualquier entero de 1 a 126. Además, x, y y z pueden ser cualquier entero de 0 ($= 00000000$) a 255 ($= 11111111$), excepto que x, y y z no pueden ser 0 simultáneamente y tampoco pueden ser 255 a la vez.

d. Se disponen 24 posiciones para alojar el ID de una red Clase A. Si cada una puede ser 0 o 1, habrían $2^{24} = 16\,777\,216$ posibles opciones. Pero no se permiten el 0 ni el 1, lo que reduce el total en 2. Así que hay 16 777 214 posibles opciones para el ID en una red Clase A.

i. Observe que $140 = 128 + 8 + 4 = 10001100_2$, que empieza con 10. Así la dirección IP viene de una red Clase B. Una solución alternativa utiliza el resultado del ejemplo 9.3.5: ID de redes de Clase B varían de 128 a 191. Como $128 \leq 140 \leq 191$, entonces la dirección IP dada es de una red Clase B.

31. a. Existen 12 posibles meses de nacimiento para A, 12 para B, 12 para C y 12 para D, así el total es $12^4 = 20\,736$.

b. Si ninguna pareja de personas comparten el mismo mes de nacimiento, hay 12 posibles meses de nacimiento para A, 11 para B, 10 para C y 9 para D. Así el total es $12 \cdot 11 \cdot 10 \cdot 9 = 11\,880$.

c. Si al menos dos personas comparten el mismo mes de nacimiento, entonces el número total de maneras en que los meses de nacimiento podrían ser asociados con A, B, C y D es $20\,736 - 11\,,880 = 8\,856$.

d. La probabilidad de que al menos dos de las cuatro personas compartan el mismo mes de nacimiento es $\frac{8856}{20736} \cong 42.7\%$.

e. Cuando hay cinco personas, la probabilidad de que al menos dos compartan el mismo mes de nacimiento es $\frac{12^5 - 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8}{12^5} \cong 61.8\%$ y cuando existen más de cinco personas, la probabilidad es aún más grande. Así, como la probabilidad para cuatro personas es menor que 50%, entonces el grupo debe tener cinco o más personas para que la probabilidad llegue al menos a 50% si deseamos que dos o más compartan el mismo mes de nacimiento.

32. *Sugerencia:* Estudie la solución al ejercicio 31.

33. a. El número de estudiantes que comprobaron al menos uno de los enunciados es $N(H) + N(C) + N(D) - N(H \cap C) - N(N \cap D) - N(C \cap D) + N(H \cap C \cap D) = 28 + 26 + 14 - 14 - 4 - 8 + 2 = 45$

b. Por la regla de la diferencia, el número de estudiantes que no comprobaron ninguno de los enunciados es el número total de estudiantes menos el número de quienes comprobaron al menos un enunciado. Esto es $100 - 45 = 55$.

d. El número de estudiantes que verificaron #1 y #2 pero no #3 es $N(H \cap C) - N(N \cap C \cap D) = 14 - 2 = 12$.

35. Sean

M = el conjunto de gente casada en la muestra,

Y = el conjunto de personas entre 20 y 30 en la muestra y

F = el conjunto de personas femeninas en la muestra.

Entonces el número de personas en el conjunto $M \cup Y \cup F$ es menor o igual al tamaño de la muestra. Y así

$$\begin{aligned} 1\,200 \geq N(M \cup Y \cup F) &= N(M) + N(Y) + N(F) - N(M \cap Y) \\ &\quad - N(M \cap F) - N(Y \cap F) + N(M \cap Y \cap F) \\ &= 675 + 682 + 684 - 195 - 467 - 318 + 165 \\ &= 1\,226. \end{aligned}$$

Esto es imposible porque $1\,200 < 1\,226$, así que las figuras son inconsistentes. No podrían haber ocurrido como resultado de un muestreo real.

37. Sea A el conjunto de todos los enteros positivos menores que 1 000 que no son múltiplos de 2 y sea B el conjunto de todos los enteros positivos menores que 1 000 que no son múltiplos de 5. Los únicos factores primos de 1 000 son 2 y 5, entonces el número de enteros positivos que no tienen factores comunes con 1 000 es $N(A \cap B)$. Sea el universo U el conjunto de todos los enteros positivos menores que 1 000. Entonces A^c es el conjunto de enteros positivos menores que 1 000 que son múltiplos de 2 y B^c es el conjunto de enteros positivos menores que 1 000 que son múltiplos de 5 y $A^c \cap B^c$ es el conjunto de enteros positivos menores que 1 000 que son múltiplos de 10. Por uno de los procedimientos analizado en la sección 9.1 o 9.2, es fácil encontrar que $N(A^c) = 499$, $N(B^c) = 199$ y $N(A^c \cap B^c) = 99$. Así, por la regla de inclusión/exclusión,

$$\begin{aligned} N(A^c \cup B^c) &= N(A^c) + N(B^c) - N(A^c \cap B^c) \\ &= 499 + 199 - 99 = 599. \end{aligned}$$

Pero por la ley de De Morgan, $N(A^c \cup B^c) = N((A \cap B)^c)$ y por tanto

$$N((A \cap B)^c) = 599. \qquad (*)$$

Ahora, como $(A \cap B)^c = U - (A \cap B)$, por la regla de resta tenemos

$$N((A \cap B)^c) = N(U) - N(A \cap B). \qquad (**)$$

Igualando los miembros derechos de (*) y (**) obtenemos que $N(U) - N(A \cap B) = 599$. Y como $N(U) = 999$, concluimos que $999 - N(A \cap B) = 599$, o, equivalentemente, $N(A \cap B) = 999 - 599 = 400$. Entonces hay 400 enteros positivos menores que 1 000 que no tienen factores comunes con 1 000.

40. *Sugerencia:* Sean A y B los conjuntos de todos los enteros positivos, menores o iguales que n, que son divisibles entre p y q, respectivamente. Entonces $\phi(n) = n - (N(A \cup B))$.

42. c. *Sugerencia:* Si $k \geq 6$, cualquier secuencia de k juegos debe empezar con W, LW, o LLW, en donde L indica "perder" y W expresa "ganar".

43. c. *Sugerencia:* Divida en dos subconjuntos al conjunto de todos los desarreglos: Un subconjunto que consiste de todos los desarreglos en que el número 1 cambia de lugar con otro número y el otro subconjunto se forma con todos los desarreglos en que el número 1 va a la posición $i \neq 1$ pero i no va a la posición 1. La respuesta es $d_k = (k-1)d_{k-1} + (k-1)d_{k-2}$. ¿Puede justificarla?

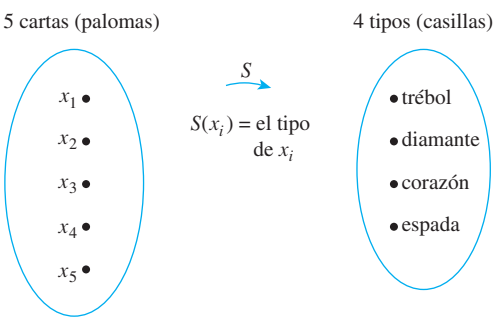
48. *Sugerencia:* Use la ley asociativa para conjuntos y la ley distributiva generalizada para conjuntos del ejercicio 37, sección 6.2.

49. *Sugerencia:* Aplique el método de solución descrito en la sección 5.8. La respuesta es $s_k = 2s_{k-1} + 3s_{k-2}$ para $k \geq 4$.

Sección 9.4

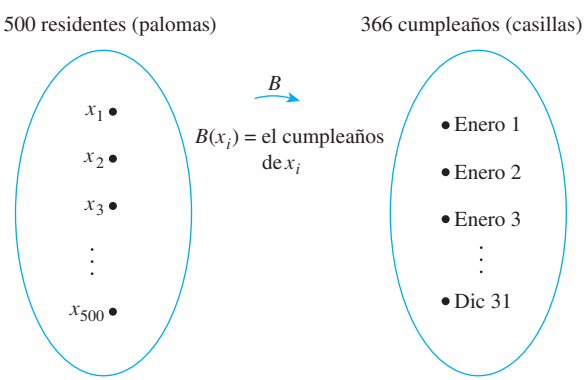
1. a. No. Por ejemplo, los ases de los cuatro diferentes tipos podrían ser seleccionados.

b. Sí. Sean x_1, x_2, x_3, x_4, x_5, las cinco cartas. Considere la función S que envía cada carta a su tipo.



Por el principio de las casillas, S no es inyectiva: $S(x_i) = S(x_j)$ para algunas dos cartas x_i y x_j. Así que al menos dos cartas son del mismo palo.

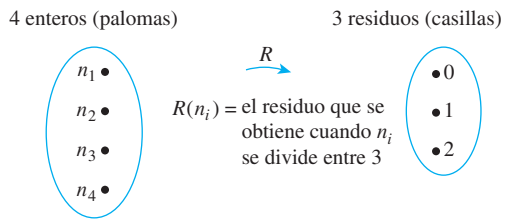
3. Sí. Los residentes se denotan por $x_1, x_2, \ldots, x_{500}$. Considere la función B de residentes a cumpleaños que envía a cada residente a su cumpleaños:



Por el principio de las casillas, B no es inyectiva: $B(x_i) = B(x_j)$ para algunos dos residentes x_i y x_j. Así que al menos dos residentes tienen el mismo cumpleaños.

5. a. Sí. Sólo hay tres posibles residuos que se pueden obtener cuando se divide un entero entre 3: 0, 1 y 2. Entonces, por el principio de las casillas, si cuatro enteros son divididos entre 3, entonces al menos dos deben tener el mismo residuo.

Más formalmente, denotemos a los enteros por n_1, n_2, n_3 y n_4 y considere la función R que envía a cada entero al residuo que se obtiene al dividirlo entre 3:



Por el principio de las casillas, R no es inyectiva, $R(n_i) = R(n_j)$ para algunos dos enteros n_i y n_j. Entonces al menos dos enteros deben tener el mismo residuo.

b. No. Por ejemplo, $\{0, 1, 2\}$ es un conjunto de tres enteros y ninguna pareja tiene el mismo residuo al dividirse entre 3.

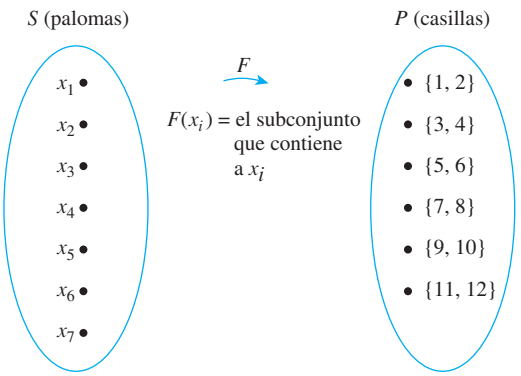
7. *Sugerencia:* Mire el ejemplo 9.4.3

9. a. Sí.

Solución 1: Sólo seis de los números del 1 al 12 son pares (a saber, 2, 4, 6, 8, 10, 12), así a lo más pueden elegirse seis números pares entre 1 y 12 inclusive. Por tanto, si se seleccionan siete números, entonces al menos uno debe ser impar.

Solución 2: Particione el conjunto de todos los enteros de 1 a 12, en 6 subconjuntos (las casillas), cada uno consistiendo de un número par y uno impar: $\{1, 2\}$, $\{3, 4\}$, $\{5, 6\}$, $\{7, 8\}$, $\{9, 10\}$, $\{11, 12\}$. Si se eligen siete enteros entre 1 y 12, entonces, por el principio de las casillas, al menos dos deben ser del mismo subconjunto. Pero cada subconjunto contiene un número par y uno impar. Por tanto, al menos uno de los siete números es impar.

Solución 3: Sea $S = \{x_1,\ldots,x_7\}$ un conjunto de siete números seleccionados del conjunto $T = \{1,\ldots,12\}$ y sea P la siguiente partición de T:$\{1, 2\}$, $\{3, 4\}$, $\{5, 6\}$, $\{7, 8\}$, $\{9, 10\}$ y $\{11, 12\}$. Cada elemento de S está en exactamente uno de los subconjuntos de la partición, entonces podemos definir una función F de S a P permitiendo que $F(x_i)$ sea el subconjunto que contiene a x_i.



S tiene 7 elementos y P tiene 6 elementos, entonces por el principio de las casillas, F no es uno a uno. Así, dos números distintos de los siete números son enviados al mismo subconjunto, lo que implica que esos dos números son los dos elementos distintos del subconjunto. Por tanto, ya que cada par consiste de un entero par y un impar, entonces uno de los siete números es impar.

b. No. Por ejemplo, ninguno de los 10 números 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, es par.

10. Sí. Hay n enteros pares en el conjunto $\{1, 2, 3,\ldots, 2n\}$, a saber $2(= 2\cdot\underline{1}), 4(= 2\cdot\underline{2}), 6(= 2\cdot\underline{3}), \ldots, 2\underline{n}(= 2\cdot n)$. Así el número máximo de enteros pares que se puede seleccionar es n. Entonces si se eligen $n + 1$ enteros, al menos uno debe ser impar.

12. La respuesta es 27. Sólo existen 26 cartas negras en una baraja estándar, así a lo más pueden seleccionarse 26 cartas negras. Entonces si se toman 27 cartas, al menos una debe ser roja.

14. Existen 61 enteros del 0 al 60 inclusive. De esos, 31 son pares $(0 = 2\cdot\underline{0}, 2 = 2\cdot\underline{1}, 4 = 2\cdot\underline{2}, \ldots, 60 = 2\cdot\underline{30})$ y así 30 son impares. Por tanto, si se eligen 32 cartas, al menos una debe ser impar y si se toman 31 enteros, al menos uno debe ser par.

17. La respuesta es 8. (Sólo hay siete posibles residuos al dividir entre 7: 0, 1, 2, 3, 4, 5, 6).

20. La respuesta es 20 483 *[a saber*, 0, 1, 2,…, 20 482*]*.

22. Este número es irracional; la expansión decimal ni termina ni se repite.

24. Sea A el conjunto de los trece números seleccionados y sea B el conjunto de todos los números primos entre 1 y 40. Observe que $B = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37\}$. Para cada x en A, sea $F(x)$ el número primo más pequeño que divide a x. Como A tiene 13 elementos y B tiene 12 elementos, entonces por el principio de las casillas F no es uno a uno. Así $F(x_1) = F(x_2)$ para algún $x_1 \neq x_2$ en A. Por definición de F, esto significa que el número primo más pequeño que divide a x_1 es igual al número primo más pequeño que divide a x_2. Por tanto, dos números en A, a saber x_1 y x_2, tienen un divisor común mayor que 1.

25. Sí. Esto se tiene del principio de las casillas generalizado con 30 elementos, 12 casillas y $k = 2$, empleando el hecho de que $30 > 2\cdot 12$.

26. No. Por ejemplo, los cumpleaños de las 30 personas se podrían distribuir como sigue: tres cumpleaños en cada uno de los seis meses de enero a junio y dos cumpleaños en cada uno de los seis meses de julio a diciembre.

29. La respuesta es $x = 3$. Hay 18 años del 17 al 34. Ahora $40 > 18\cdot 2$, así por el principio de las casillas generalizado, se puede asegurar que al menos existen $x = 3$ estudiantes de la misma edad. Sin embargo, como $18\cdot 3 > 40$, entonces no se puede asegurar que tenga más de tres estudiantes con la misma edad. (Por ejemplo, tres estudiantes podrían tener edades entre 17 y 20 y dos estudiantes podrían tener edades entre 21 y 34). Entonces x no puede seleccionarse mayor que 3.

31. *Sugerencia:* Use el mismo tipo de razonamiento que en el ejemplo 9.4.6.

32. *Sugerencias:* 1) El número de subconjuntos de los seis enteros es $2^6 = 64$. 2) Como cada entero es menor que 13, entonces la mayor suma posible es 57. (¿Por qué? y ¿qué origina esta suma?)

33. *Sugerencia:* El conjunto de potencias de A tiene $2^6 = 64$ elementos, entonces hay 63 subconjuntos no vacíos de A. Sea k el más pequeño número en el conjunto A. Así las sumas sobre los elementos en los subconjuntos no vacíos de A están en el rango de k a $k + 10 + 11 + 12 + 13 + 14 = k + 60$. ¿Cuántos números están en este rango?

35. *Sugerencia:* Sea X el conjunto consistente de los 52 enteros positivos dados y sea Y el conjunto que contiene los siguientes elementos: {00}, {50}, {01, 99}, {02, 98}, {03, 97},…, {48, 52},{49, 51}. Defina una función F de X a Y por la regla $F(x)$ = conjunto que contiene a los dos últimos dígitos de x. Use el principio de las casillas para argumentar que F no es uno a uno y demuestre cómo se obtiene la conclusión deseada.

36. *Sugerencia:* Represente a cada uno de los 101 enteros x_i como a_i 2^{ki}, en donde a_i es impar y $k_i \geq 0$. Ahora $1 \leq x_i \leq 200$ y entonces $1 \leq a_i \leq 199$ para toda i. Sólo existen 100 enteros impares del 1 al 199 inclusive.

37. b. *Sugerencia:* Para cada $k = 1, 2,\ldots, n$, aceptemos que $a_k = x_1 + x_2 + \ldots + x_k$. Si algún a_k es divisible entre n, entonces el problema está resuelto: la subsucesión consecutiva es x_1, $x_2,\ldots, x_k$. Si ningún a_k es divisible por n, entonces a_1, a_2, $a_3,\ldots, a_n$ satisface la hipótesis del inciso *a*). Así que $a_j - a_i$ es divisible por n para algunos enteros i y j con $j > i$. Escriba $a_j - a_i$ en términos de las x para deducir la conclusión dada.

38. *Sugerencia:* Sea $a_1, a_2,\ldots, an^2{}_{+1}$ cualquier sucesión de $n^2 + 1$ números reales distintos y suponga que esta sucesión no contiene una subsucesión estrictamente creciente de longitud $n + 1$ y tampoco contiene una subsucesión estrictamente decreciente de longitud $n + 1$. Sea S el conjunto de todos los pares ordenados de enteros (i, d), en donde $1 \leq i \leq n$ y $1 \leq d \leq n$. Para cada término a_k en la sucesión, sea $F(a_k) = (i_k, d_k)$, tal que i_k es la longitud de la más grande sucesión creciente empezando por a_k y d_k es la longitud de la mayor sucesión decreciente iniciando en a_k. Suponga que F es uno a uno para así deducir una contradicción.

Sección 9.5

1. a. 2-combinaciones $\{x_1, x_2\}, \{x_1, x_3\}, \{x_2, x_3\}$.

Así, $\binom{3}{2} = 3$.

b. Selecciones no ordenadas: $\{a, b, c, d\}$, $\{a, b, c, e\}$, $\{a, b, d, e\}$, $\{a, c, d, e\}$, $\{b, c, d, e\}$.

Entonces, $\binom{5}{4} = 5$.

3. $P(7, 2) = \binom{7}{2} \cdot 2!$

5. a. $\binom{6}{0} = \frac{6!}{0!(6-0)!} = \frac{6!}{1(6!)} = 1$

b. $\binom{6}{1} = \frac{6!}{1!(6-1)!} = \frac{6(5!)}{1(5!)} = 6$

6. a. número de comités de 6

$$= \binom{15}{6} = \frac{15!}{(15-6)!6!}$$

$$= \frac{\overset{7}{\cancel{15}} \cdot \cancel{14} \cdot 13 \cdot \cancel{12} \cdot 11 \cdot \cancel{10} \cdot \overset{5}{\cancel{9}}!}{\cancel{9!} \cdot \cancel{6} \cdot \cancel{5} \cdot \cancel{4} \cdot \cancel{3} \cdot \cancel{2}} = 5{,}005$$

b. [número de comités que no contienen a A y B juntos,]

$$= \begin{bmatrix}\text{número de comités con } A \text{ y otros cinco, ninguno de éstos es } B\end{bmatrix} + \begin{bmatrix}\text{número de comités con } B \text{ y otros cinco, ninguno de éstos es } A\end{bmatrix} + \begin{bmatrix}\text{número de comités que no tienen ni a } A \text{ ni a } B\end{bmatrix}$$

$$= \binom{13}{5} + \binom{13}{5} + \binom{13}{6}$$

$$= 1\,287 + 1\,287 + 1\,716 = 4\,290$$

Solución alternativa:

[número de comités que no contienen a A y B juntos]

$$= \begin{bmatrix}\text{número total de comités}\end{bmatrix} - \begin{bmatrix}\text{número de comités que contienen tanto a } A \text{ como a } B\end{bmatrix}$$

$$= \binom{15}{6} - \binom{13}{4}$$

$$= 5\,005 - 715 = 4\,290$$

c. [número de comités con A y B juntos] + [número de comités sin A ni B]

$$= \binom{13}{4} + \binom{13}{6} = 715 + 1\,716 = 2\,431$$

d. (i) [número de subconjuntos de tres hombres elegidos de ocho] · [número de subconjuntos de tres mujeres seleccionadas de siete]

$$= \binom{8}{3}\binom{7}{3} = 56 \cdot 35 = 1{,}960$$

(ii) [número de comités con al menos una mujer]

$$= \begin{bmatrix}\text{número total de comités}\end{bmatrix} - \begin{bmatrix}\text{número de comités totalmente femeninos}\end{bmatrix}$$

$$= \binom{15}{6} - \binom{8}{6} = 5{,}005 - 28$$

$$= 4{,}977$$

e. [número de formas de elegir a dos estudiantes de primer año] · [número de maneras de seleccionar a dos alumnos de segundo año] · [número de opciones de elegir a dos estudiantes de penúltimo año] · [número de maneras de seleccionar a dos alumnos del último año]

$$= \binom{3}{2}\binom{4}{2}\binom{3}{2}\binom{5}{2}$$

8. *Sugerencia:* Las respuestas son **a**. 1001, **b**. (i) 420, (ii) todas las 1001, requieren prueba, (iii) 175, **c**. 506, **d**. 561.

9. b. $\binom{24}{3}\binom{16}{3} + \binom{24}{4}\binom{16}{2} + \binom{24}{5}\binom{16}{1} + \binom{24}{6}\binom{16}{0} =$ 3 223 220

11. a. 1) 4 (porque hay tantas escaleras reales como tipos de cartas).

2) $\frac{4}{\binom{52}{5}} = \frac{4}{2\,598\,960} \cong 0.0000015$

c. 1) $13 \cdot \binom{48}{1} = 624$ (porque primero se puede elegir la denominación de las cuatro de un tipo y después seleccionar una carta adicional de las 48 restantes)

2) $\frac{624}{\binom{52}{5}} = \frac{624}{2\,598\,960} = 0.00024$

f. 1) Imagine que construye una escalera (que incluye una escalera de color y una escalera real como un proceso de seis pasos: paso 1 es seleccionar la más baja denominación de cualquier carta de las cinco (que puede ser cualquiera de A, 2,…, 10), el paso 2 es elegir una carta de esa denominación, el paso 3 es tomar una carta de la siguiente más alta denominación y así continuar hasta que se hayan tomado cinco cartas. Por la regla de la multiplicación, el número de maneras para efectuar este proceso es

$$10 \cdot \binom{4}{1}\binom{4}{1}\binom{4}{1}\binom{4}{1}\binom{4}{1} = 10 \cdot 4^5 = 10\,240.$$

Por los incisos *a*) y *b*), 40 de esos números representan escaleras real y de color, así hay $10\,240 - 40 = 10\,200$ escaleras en total.

2) $\frac{10\,200}{\binom{52}{5}} = \frac{10\,200}{2\,598\,960} \cong 0.0039$

13. a. $2^{10} = 1\,024$

d. $\begin{bmatrix}\text{número de resultados}\\ \text{con al menos una cara}\end{bmatrix}$

$$= \begin{bmatrix}\text{número total}\\ \text{de resultados}\end{bmatrix} - \begin{bmatrix}\text{número de resultados}\\ \text{con ninguna cara}\end{bmatrix}$$

$$= 1\,024 - 1 = 1\,023$$

15. a. 50 **b.** 50

c. Para obtener una suma par, ambos números deben ser pares o impares. Entonces

$$\begin{bmatrix}\text{número de subconjuntos de dos enteros}\\ \text{del 1 al 100 inclusive cuya suma es par}\end{bmatrix}$$

$$= \begin{bmatrix}\text{número de subconjuntos}\\ \text{de dos enteros pares}\\ \text{seleccionados de 50}\\ \text{opciones}\end{bmatrix} + \begin{bmatrix}\text{número de subconjuntos}\\ \text{de dos enteros impares}\\ \text{elegidos de 50}\\ \text{posibilidades}\end{bmatrix}$$

$$= \binom{50}{2} + \binom{50}{2} = 2\,450.$$

d. Para lograr una suma impar, uno de los números debe ser par y el otro impar. Así que la respuesta es $\binom{50}{1}\cdot\binom{50}{1} = 2\,500$. Alternativamente, observe que la respuesta es igual al número total de subconjuntos de dos enteros seleccionados del 1 al 100 menos el número de tales subconjuntos para que la suma de los elementos sea par. Entonces la respuesta es $\binom{100}{2} - 2\,450 = 2\,500$.

17. a. Dos puntos determinan una recta. Por tanto,

$$\begin{bmatrix}\text{número de rectas}\\ \text{determinadas por}\\ \text{los diez puntos}\end{bmatrix} = \begin{bmatrix}\text{número de subconjuntos}\\ \text{de dos puntos}\\ \text{elegidos de diez}\end{bmatrix}$$

$$= \binom{10}{2} = 45.$$

19. a. $\dfrac{10!}{2!1!1!3!2!1!} = 151\,200$ porque hay 2 A's, 1 B, 1 H, 3 L's, 2 O's, y 1 U

b. $\dfrac{8!}{2!1!1!2!2!} = 5\,040$ **c.** $\dfrac{9!}{1!2!1!3!2!} = 15\,120$

23. La torre debe moverse siete cuadros a la derecha y siete cuadros hacia arriba, así

$$\begin{bmatrix}\text{número de rutas}\\ \text{que la torre}\\ \text{puede tomar,}\end{bmatrix} = \begin{bmatrix}\text{número de}\\ \text{ordenamientos}\\ \text{de siete}\\ \text{R y siete U}\end{bmatrix}$$

en donde R significa "a la derecha" y U denota "hacia arriba"

$$= \frac{14!}{7!7!} = 3\,432.$$

24. b. *Solución 1*: Un factor puede ser 1 y el otro factor puede ser el producto de todos los primos. (Esto da 1 factorización). Un factor puede ser un primo y el otro factor puede ser el producto de los otros tres. (Esto da $\binom{4}{1} = 4$ factorizaciones). Un factor puede ser un producto de dos primos y el otro factor puede ser el producto de los otros dos primos. El número $\binom{4}{2} = 6$ cuenta todos los posibles conjuntos de dos primos seleccionados de los cuatro primos y cada conjunto de primos corresponde a una factorización. Observe, sin embargo, que el conjunto $\{p_1, p_2\}$ corresponde a la misma factorización como el conjunto $\{p_3, p_4\}$, a saber, $p_1\,p_2\,p_3\,p_4$ (justamente escrita en un orden diferente). En general, cada elección de dos primos corresponde a la misma factorización como alguna otra selección de dos primos. Así el número de factorizaciones en las cuales cada factor es el producto de dos primos es $\dfrac{\binom{4}{2}}{2} = 3$. (Esto da tres factorizaciones). Los casos anteriores cuentan para todas las posibilidades $4 + 3 + 1 = 8$.

Solución 2: Sea $S = \{p_1, p_2, p_3, p_4\}$. Aceptemos que $p_1\,p_2\,p_3\,p_4 = P$ y $f_1\,f_2$ sea cualquier factorización de P. El producto de los números en cualquier subconjunto $A \subseteq S$ se puede emplear para f_1, con el producto de los números en A^c siendo f_2. Hay tantas maneras de escribir $f_1 f_2$ como subconjuntos de S, a saber $2^4 = 16$ (por el teorema 6.3.1). Pero dados cualesquiera factores f_1 y f_2, entonces $f_1 f_2 = f_2 f_1$. Así, contando el número de maneras de escribir $f_1 f_2$ se cuenta dos veces cada factorización, entonces la respuesta es $\frac{16}{2} = 8$.

25. a. Existen cuatro elecciones hacia dónde enviar al primer elemento del dominio (se puede elegir cualquier elemento del codominio), tres opciones hacia dónde mandar al segundo (como la función es uno a uno, entonces el segundo elemento del dominio debe ir a un elemento $\neq 1$ codominio, distinto al asociado con el primero) y dos posibilidades hacia dónde enviar al tercer elemento (nuevamente, ya que la función es uno a uno). Así la respuesta es $4 \cdot 3 \cdot 2 = 24$.

b. ninguno.

e. *Sugerencia:* La respuesta es $n(n-1)\cdots(n-m+1)$.

26. a. Los elementos del dominio se denotan por a, b y c y los elementos del codominio son u y v. Para que una función de $\{a, b, c\}$ a $\{u, v\}$ sea sobreyectiva, dos elementos del dominio deben ser enviados a u y uno a v, o dos elementos deben ser mapeados a v y uno a u. Hay tantas maneras de enviar dos elementos del dominio a u y uno a v como formas de elegir cuáles elementos de $\{a, b, c\}$ se enviarán a u, a saber, $\binom{3}{2} = 3$. Similarmente, existen $\binom{3}{2} = 3$ maneras de enviar dos elementos del dominio a v y uno a u. Por tanto, existen $3 + 3 = 6$ funciones sobre de un conjunto de tres elementos a un conjunto con dos elementos.

c. *Sugerencia:* La respuesta es 6.

d. Considere funciones de un conjunto con cuatro elementos a un conjunto de dos elementos. Denote el conjunto de cuatro elementos por $X = \{a, b, c, d\}$ y al conjunto de dos elementos por $Y = \{u, v\}$. Divida el conjunto de todas las funciones sobre de X a Y en dos categorías. La primera categoría consiste de todas aquellas que envían a los tres elementos en $\{a, b, c\}$ a $\{u, v\}$ y que mapean a d en u o v. Las funciones en esta categoría pueden definirse mediante un proceso de dos pasos.

Paso 1: Construir una función sobreyectiva de $\{a, b, c\}$ a $\{u, v\}$.

Paso 2: Elegir si d se envía a u o a v.

Por el inciso *a*), hay seis maneras de efectuar el paso 1 y, como existen dos formas de enviar a d, entonces se tienen dos opciones para realizar el paso 2. Así, por la regla de multiplicación, hay $6 \cdot 2 = 12$ maneras de definir las funciones en la primera categoría.

La segunda categoría consiste de todas aquellas funciones sobreyectivas de X a Y que envían a los tres elementos en $\{a, b, c\}$ a u o v y que mandan a d al u o v que no haya sido imagen de los otros. Sólo hay dos maneras hacia dónde mandar los elementos en $\{a, b, c\}$ y como d es simplemente enviada a donde los otros no hayan ido, entonces existen justamente dos funciones en la segunda categoría.

Cada función sobreyectiva de X a Y, envía o no, al menos dos elementos de X a $f(d)$. Si manda al menos dos elementos de X a $f(d)$ entonces está en la segunda categoría. Si no lo hace, Por tanto la imagen de $\{a, b, c\}$ es $\{u, v\}$ y así la "restricción" de la función a $\{a, b, c\}$ es sobreyectiva. En consecuencia, la función es una de aquellas incluidas en la primera categoría. Así todas las funciones sobreyectivas de A a Y están en una de las dos categorías y ninguna función está en ambas categorías, entonces el número total de funciones sobreyectivas es $12 + 2 = 14$.

Sugerencias: **a**. (i) g es inyectiva (ii) g no es sobreyectiva

b. G es sobreyectiva. *Demostración:* Suponga que y es cualquier elemento de $\mathbf{R}$. *[Debemos demostrar que existe un elemento x en $\mathbf{R}$ tal que $G(x) = y$. Trabajo desde el principio para determinar qué sería x si existiera y muestre que tendría que ser igual a $(y + 5)/4$. La demostración debe establecer que x tiene las propiedades necesarias.]* Sea $x = (y + 5)/4$. Entonces (1) $x \in \mathbf{R}$ y (2) $G(x) = G((y + 5)/4) = 4[(y + 5)/4] - 5 = (y + 5) - 5 = y$ *[que era lo que se quería demostrar].*

27. a. Una relación sobre A es cualquier subconjunto de $A \times A$ y $A \times A$ tiene $8^2 = 64$ elementos. Así hay 2^{64} relaciones binarias sobre A.

c. Forme una relación simétrica mediante un proceso de dos pasos: 1) tome un conjunto de elementos de la forma (a, a) (hay ocho de tales elementos, así 2^8 conjuntos); 2) seleccione un conjunto de pares de elementos de la forma (a, b) y (b, a) en donde $a \neq b$ (existen $(64 - 8)/2 = 28$ de tales pares, así 2^{28} de esos conjuntos). Por tanto, la respuesta es $2^8 \cdot 2^{28} = 2^{36}$.

28. *Sugerencia:* Use la regla de diferencia y la generalización de la regla de inclusión/exclusión para 4 conjuntos. (Vea el ejercicio 48 de la sección 9.3.)

31. Al conjunto lo llamamos X y suponemos que $X = \{x_1, x_2, \ldots, x_n\}$. Para cada entero $i = 0, 1, 2, \ldots, n - 1$, podemos considerar al conjunto de todas las particiones de X (llamémoslas particiones de tipo i) en donde uno de los subconjuntos de la partición es un $(i + 1)$ elemento que contiene a x_n e i elementos elegidos de $\{x_1, \ldots, x_{n-1}\}$. Los restantes subconjuntos de la partición será una partición de los restantes $(n - 1) - i$ elementos de $\{x_1, \ldots, x_{n-1}\}$. Por ejemplo, si $X = \{x_1, x_2, x_3\}$, hay cinco particiones de los diversos tipos, a saber,

Tipo 0: dos particiones en donde un conjunto es un conjunto que contiene sólo a x_3: $[\{x_3\},\{x_1\},\{x_2\}]$, $[\{x_3\},\{x_1,x_2\}]$

Tipo 1: dos particiones en donde un conjunto es un conjunto de dos elementos que contiene a x_3: $[\{x_1, x_3\},\{x_2\}]$, $[\{x_2, x_3\},\{x_1\}]$

Tipo 2: una partición en donde un conjunto es un conjunto de tres elementos que contiene a x_3: $\{x_1, x_2, x_3\}$.

En general, podemos imaginar que la construcción de una partición del tipo i es un proceso de dos pasos:

Paso 1: Seleccione i elementos de $\{x_1, \ldots, x_{n-1}\}$ para colocarlos junto con x_n.

Paso 2: Elija cualquier partición de los restantes $(n - 1) - i$ elementos de $\{x_1, \ldots, x_{n-1}\}$ para ponerlos con el conjunto formado en el paso 1.

Existen $\binom{n-1}{i}$ maneras de ejecutar el paso 1 y $P_{(n-1)-i}$ opciones para realizar el paso 2. Por tanto, por la regla de multiplicación, hay $\binom{n-1}{i} \cdot P_{(n-1)-i}$ particiones del tipo i. Cualquier partición de X es del tipo i para algún $i = 0, 1, 2, \ldots, n - 1$, entonces de la regla de adición se tiene que el número total de particiones es

$$\binom{n-1}{0} P_{n-1} + \binom{n-1}{1} P_{n-2} + \binom{n-1}{2} P_{n-3} + \cdots + \binom{n-1}{n-1} P_0.$$

33. $S_{5,2} = S_{4,1} + 2S_{4,2} = 1 + 2 \cdot 7 = 15$

36. *Demostración (por inducción matemática):* Aceptemos que la propiedad $P(n)$ sea la ecuación $S_{n,2} = 2^{n-1} - 1$.

***Demostración de que P(2) es verdadero*:**

Debemos demostrar que $S_{2,2} = 2^{2-1} - 1$. Por el ejemplo 9.5.13, $S_{2,2} = 1$ y $2^{2-1} - 1 = 2 - 1 = 1$. Entonces $P(2)$ es verdadero.

Demostración de que para todos los enteros $k \geq 2$, si $P(k)$ es verdadero, entonces $P(k + 1)$ también es verdadero:

Sea k cualquier entero con $k \geq 2$ y suponga que $S_{k,2} = 2^{k-1} - 1$. *[Hipótesis inductiva.]* Debemos demostrar que $S_{k+1,2} = 2^{(k+1)-1} - 1 = 2^k - 1$. Pero de acuerdo con el ejemplo 9.5.13, $S_{k+1,2} = S_{k,1} + 2\,S_{k,2}$ y $S_{k,1} = 1$. Así, sustituyendo y la hipótesis inductiva,

$$\begin{aligned} S_{k+1,2} &= 1 + 2S_{k,2} = 1 + 2(2^{k-1} - 1) \\ &= 1 + 2^k - 2 = 2^k - 1 \end{aligned}$$

[que era lo que se quería demostrar].

38. *Sugerencia:* Observe que el número de funciones sobreyectivas de $X = \{x_1, x_2, x_3, x_4\}$ a $Y = \{y_1, y_2, y_3\}$ es $S_{4,3} \cdot 3!$ porque la construcción de una función sobreyectiva puede pensarse como un proceso de dos pasos en donde el paso 1 es elegir una partición de X en tres subconjuntos y el paso 2 es seleccionar, para cada subconjunto de la partición, un elemento de Y para los elementos del conjunto a ser enviado.

Sección 9.6

1. a. $\binom{5+3-1}{5} = \binom{7}{5} = \frac{7\cdot 6}{2} = 21.$

a. Los tres elementos del conjunto son 1, 2 y 3. Las 5-combinaciones son [1, 1, 1, 1, 1], [1, 1, 1, 1, 2], [1, 1, 1, 1, 3], [1, 1, 1, 2, 2], [1, 1, 1, 2, 3], [1, 1, 1, 3, 3], [1, 1, 2, 2, 2], [1, 1, 2, 2, 3], [1, 1, 2, 3, 3], [1, 1, 3, 3, 3], [1, 2, 2, 2, 2], [1, 2, 2, 2, 3], [1, 2, 2, 3, 3], [1, 2, 3, 3, 3], [1, 3, 3, 3, 3], [2, 2, 2, 2, 2], [2, 2, 2, 2, 3], [2, 2, 2, 3, 3], [2, 2, 3, 3, 3], [2, 3, 3, 3, 3] y [3, 3, 3, 3, 3].

2. a. $\binom{4+3-1}{4} = \binom{6}{4} = \frac{6\cdot 5}{2} = 15$

3. a. $\binom{20+6-1}{20} = \binom{25}{20} = 53{,}130$

b. Si al menos tres son choux, entonces los 17 panes adicionales son seleccionados de seis tipos. El número de selecciones es $\binom{17+6-1}{17} = \binom{22}{17} = 26{,}334.$

Nota: En los incisos *a*) y *b*), se supone que las selecciones contadas no tienen orden.

c. Sea T el conjunto de selecciones de panes que pueden ser de cualquiera de los seis tipos, $E_{\geq 3}$ es el conjunto de selecciones con tres o más choux y $E_{\leq 2}$ es el conjunto de selecciones que contiene dos o menos chouxs. Entonces

$$\begin{aligned} N(E_{\leq 2}) &= N(T) - N(E_{\geq 3}) && \text{porque } T = E_{\leq 2} \cup E_{\geq 3} \text{ y } E_{\leq 2} \cap E_{\geq 3} = \emptyset \\ &= 53,130 - 26,334 && \text{por los incisos } a) \text{ y } b) \\ &= 26,796. \end{aligned}$$

Así hay 26,796 selecciones de panes que tienen a lo más dos chouxs.

5. La respuesta es igual al número de 4-combinaciones, con repetición permitida, que se pueden formar de un conjunto de n elementos. Entonces

$$\begin{aligned} \binom{4+n-1}{4} &= \binom{n+3}{4} \\ &= \frac{(n+3)(n+2)(n+1)n(\cancel{n-1)!}}{4!(\cancel{n-1)!}} \\ &= \frac{n(n+1)(n+2)(n+3)}{24}. \end{aligned}$$

8. Como en el ejemplo 9.6.4, la respuesta es la misma como el número de cuádruplas de enteros (i, j, k, m) para las que $1 \leq i \leq j \leq k \leq m \leq n$. Por el ejercicio 5, este número es $\binom{n+3}{4} = \frac{n(n+1)(n+2)(n+3)}{24}$.

10. Pensar en el número 20 como dividido en 20 unidades individuales y en las variables x_1, x_2 y x_3 como tres categorías en las cuales esas unidades son colocadas. El número de unidades en la categoría x_i indica el valor de x_i en una solución de la ecuación. Por el teorema 9.6.1, el número de maneras de seleccionar 20 objetos de las tres categorías es $\binom{20+3-1}{20} = \binom{22}{20} = \frac{22\cdot 21}{2} = 231$, entonces la ecuación tiene 231 soluciones enteras no-negativas.

11. El análisis para este ejercicio es el mismo como en el ejercicio 10 excepto que como cada $x_i \geq 1$, podemos imaginar que se toman 3 de las 20 unidades, colocando una en cada categoría x_1, x_2 y x_3 y entonces distribuir las restantes 17 unidades en las tres categorías. El número de formas de hacer esto es $\binom{17+3-1}{17} = \binom{19}{17} = \frac{19\cdot 18}{2} = 171$, entonces la ecuación tiene 171 posibles soluciones enteras positivas.

16. a. Sea $L_{\geq 7}$ el conjunto de selecciones que incluyen al menos siete frascos de limonada. En este caso unos ocho frascos adicionales pueden seleccionarse de los cinco tipos de bebidas, entonces

$$N(L_{\geq 7}) = \binom{8+5-1}{8} = \binom{12}{8} = 495.$$

Sea T el conjunto de selecciones de frascos en que la bebida puede ser cualquiera de los cinco tipos y sea $L_{\leq 6}$ el conjunto de selecciones que contienen a lo más seis frascos de limonada. Por tanto,

$$\begin{aligned} N(L_{\leq 6}) &= N(T) - N(L_{\geq 7}) && \text{porque } T = L_{\leq 6} \cup L_{\geq 7} \text{ y } L_{\leq 6} \cap L_{\geq 7} = \emptyset \\ &= 3,876 - 495 && \text{por lo anterior y la parte (a) del ejemplo 9 .6.2} \\ &= 3,381. \end{aligned}$$

Entonces, hay 3,381 selecciones de quince frascos de bebidas que contienen a lo más seis frascos de limonada.

b. Sea $R_{\leq 5}$ el conjunto de selecciones que contiene a lo más cinco frascos de cerveza de raíz y sea $L_{\leq 6}$ el conjunto de selecciones con a lo más seis frascos de limonada. La respuesta a la pregunta puede representarse como $N(R_{\leq 5} \cap L_{\leq 6})$. Como en el inciso *a*), sea T el conjunto de todas las selecciones de quince frascos en las cuales la bebida puede ser cualquiera de los cinco tipos. Si en T elimina todas las selecciones que contiene al menos seis frascos de cerveza de raíz o al menos siete frascos de limonada, entonces se queda con todas las selecciones que contienen a lo más cinco frascos de cerveza y a lo más seis frascos de limonada. Así, en la notación del inciso *a*) y del ejemplo 9.6.2, $N(R_{<5} \cap L_{<6}) = N(T) - N(R_{\geq 6} \cup L_{\geq 7})$.

Use la regla de inclusión/exclusión como sigue para calcular $N(R_{\geq 6} \cup L_{\geq 7})$:

$$N(R_{\geq 6} \cup L_{\geq 7}) = N(R_{\geq 6}) + N(L_{\geq 7}) - N(R_{\geq 6} \cap L_{\geq 7}).$$

Para encontrar $N(R_{\geq 6} \cap L_{\geq 7})$, observe que si se seleccionan al menos seis frascos de cerveza y al menos siete frascos de limonada, entonces a lo más se pueden elegir dos frascos adicionales de bebida de los otros tres tipos para hacer un total de quince frascos. Una selección de dos de tales frascos puede representarse por una cadena de $2\times$ y $3\,|$ y una elección de un frasco se puede representar por una cadena de $1\times$ y $3\,|$. Entonces

$$\begin{aligned} N(R_{\geq 6} \cap L_{\geq 7}) &= \binom{2+3-1}{2} = \binom{1+3-1}{1} \\ &= \binom{4}{2} + \binom{3}{1} = 6 + 3 = 9. \end{aligned}$$

Se tiene que

$$\begin{aligned} N(R_{\geq 6} \cup L_{\geq 7}) &= N(R_{\geq 6}) + N(L_{\geq 7}) \\ &\quad - N(R_{\geq 6} \cap L_{\geq 7}) \\ &= 715 + 495 - 15 \\ &= 1\,201. \end{aligned}$$

por la regla de inclusión/exclusión

por el inciso *a*), el cálculo anterior, y el inciso *b*) del ejemplo 9.6.2

Juntando toda la información anterior en la solución se obtiene:

$$\begin{aligned} N(R_{\leq 5} \cap L_{\leq 6}) &= N(T) - N(R_{\geq 6} \cup L_{\geq 7}) \\ &= 3\,876 - 1\,201 = 2\,675. \end{aligned}$$

Así, existen 2 681 selecciones de quince bebidas que contienen a lo más cinco frascos de cerveza de raíz y a lo más seis frascos de limonada.

17. *Sugerencias:* **a.** La respuesta es 10 295 472. **b.** Vea la solución del inciso *c*) del ejemplo 9.6.2. La respuesta es 9 949 368. **c.** La respuesta es 9 111 432.

d. Aceptemos que T denote el conjunto de todas las selecciones de treinta balones, $R_{\leq 12}$ representa el conjunto de selecciones que contiene a lo más doce balones rojos, $B_{\leq 8}$ es el conjunto de elecciones con a lo más ocho balones azules, $R_{\geq 13}$ denota el conjunto de selecciones que contiene al menos trece balones rojos y $B_{\geq 9}$ representa el conjunto de selecciones con al menos nueve balones azules. Entonces la respuesta a la pregunta puede representarse como $N(R_{\leq 12} \cap B_{\leq 8})$. Si del total de todas las selecciones de balones, se eliminan aquellas que contiene al menos trece balones rojos o al menos nueve azules, entonces se queda con las selecciones con a lo más doce balones rojos y a lo más ocho azules. Así $N(R_{\leq 12} \cap B_{\leq 8}) = N(T) - N(R_{\geq 13} \cup B_{\geq 9})$. Calcule $N(R_{\geq 13} \cap B_{\geq 9})$ y use la regla de inclusión/exclusión para encontrar $N(R_{\geq 13} \cap B_{\geq 9})$.

19. *Sugerencia:* Las respuestas son **a.** 51 128 **b.** 46 761

Sección 9.7

1. $\binom{n}{0} = \dfrac{n!}{0!(n-0)!} = \dfrac{n!}{1 \cdot n!} = 1$

3. $\binom{n}{2} = \dfrac{n!}{(n-2)! \cdot 2!} = \dfrac{n \cdot (n-1) \cdot \cancel{(n-2)!}}{\cancel{(n-2)!} \cdot 2!}$

$= \dfrac{n(n-1)}{2}$

5. *Demostración:* Suponga que n y r son enteros no-negativos con $r \leq n$. Entonces

$$\begin{aligned} \binom{n}{r} &= \frac{n!}{r!(n-r)!} && \text{por el teorema 9.5.1} \\ &= \frac{n!}{(n-(n-r))!(n-r)!} && \text{porque } n-(n-r) = n-n+r = r \\ &= \frac{n!}{(n-r)!(n-(n-r))!} && \text{por intercambio de factores en el denominador} \\ &= \binom{n}{n-r} && \text{por el teorema 9.5.1} \end{aligned}$$

6. *Solución 1*: Aplique la fórmula (9.7.2) con $m+k$ en lugar de n. Esto es legal porque $m+k \geq 1$.
Solución 2:

$$\begin{aligned} \binom{m+k}{m+k-1} &= \frac{(m+k)!}{(m+k-1)![(m+k)-(m+k-1)]!} \\ &= \frac{(m+k) \cdot (m+k-1)!}{(m+k-1)!(m+k-m-k+1)!} \\ &= \frac{(m+k) \cdot (m+k-1)!}{(m+k-1)! \cdot 1!} = m+k \end{aligned}$$

10. a. $\binom{6}{2} = \binom{5}{2} + \binom{5}{1} = 10 + 5 = 15,$

$\binom{6}{3} = \binom{5}{3} + \binom{5}{2} = 10 + 10 = 20$

b. $\binom{6}{4} = \binom{5}{4} + \binom{5}{3} = 5 + 10 = 15,$

$\binom{6}{5} = \binom{5}{5} + \binom{5}{4} = 1 + 5 = 6,$

$\binom{7}{3} = \binom{6}{3} + \binom{6}{2} = 20 + 15 = 35,$

$\binom{7}{4} = \binom{6}{4} + \binom{6}{3} = 15 + 20 = 35,$

$\binom{7}{5} = \binom{6}{5} + \binom{6}{4} = 6 + 15 = 21$

c. Fila para $n = 7$: 1 7 21 35 35 21 7 1

13. *Demostración por inducción matemática:* Aceptemos que la propiedad $P(n)$ sea la fórmula

$$\sum_{i=2}^{n+1} \binom{i}{2} = \binom{n+2}{3}. \quad \leftarrow P(n)$$

Demostración de que P(1) es verdadero:

Para demostrar $P(1)$ debemos demostrar que

$$\sum_{i=2}^{1+1} \binom{i}{2} = \binom{1+2}{3}. \quad \leftarrow P(1)$$

Pero

$$\sum_{i=2}^{1+1} \binom{i}{2} = \sum_{i=2}^{2} \binom{i}{2} = \binom{2}{2} = 1 = \binom{3}{3} = \binom{1+2}{3},$$

así $P(1)$ es verdadera.

Demostración que para todos los enteros k ≥ 1, si P(k) es verdadero, entonces P(k + 1) también es verdadero:

Sea k cualquier entero con $k \geq 1$ y suponga que

$$\sum_{i=2}^{k+1} \binom{i}{2} = \binom{k+2}{3} \quad \leftarrow P(k)$$

hipótesis de inducción

Debemos demostrar que

$$\sum_{i=2}^{(k+1)+1} \binom{i}{2} = \binom{(k+1)+2}{3},$$

o equivalentemente

$$\sum_{i=2}^{k+2}\binom{i}{2}=\binom{k+3}{3}. \qquad \leftarrow P(k+1)$$

Pero el lado izquierdo de $P(k+1)$ es

$$\begin{aligned}\sum_{i=2}^{k+2}\binom{i}{2}&=\sum_{i=1}^{k+1}\binom{i}{2}=\binom{k+2}{2} && \text{escribiendo el último término por separado}\\ &=\binom{k+2}{3}+\binom{k+2}{2} && \text{por la hipótesis de inducción}\\ &=\binom{(k+2)+1}{3} && \text{por la fórmula de Pascal}\\ &=\binom{k+3}{3},\end{aligned}$$

que es el lado derecho de $P(k+1)$ *[que era lo que se quería demostrar]. [Se han demostrado el paso básico y el paso inductivo, entonces concluimos que P(n) es verdadero para todo* $n \geq 1$.*]*

14. *Sugerencia:* Use los resultados de los ejercicios 3 y 13.

17. *Sugerencia:* Esto se obtiene haciendo $m = n = r$ en el ejercicio 16 y usando el resultado del ejemplo 9.7.2.

19. $1+\binom{7}{1}7x+\binom{7}{2}x^2+\binom{7}{3}x^3+\binom{7}{4}x^4+\binom{7}{5}x^5+\binom{7}{6}x^6+x^7=1+7x+21x^2+35x^3+35x^4+21x^5+7x^6+x^7$

21. $1+6(-x)+\binom{6}{2}(-x)^2+\binom{6}{3}(-x)^3+\binom{6}{4}(-x)^4+\binom{6}{5}(-x)^5+(-x)^6=1-6x+15x^2-20x^3+15x^4-6x^5+x^6$

23.
$$\begin{aligned}(p-2q)^4&=\sum_{k=0}^{4}\binom{4}{k}p^{4-k}(-2q)^k\\ &=\binom{4}{0}p^4(-2q)^0+\binom{4}{1}p^3(-2q)^1\\ &\quad+\binom{4}{2}p^2(-2q)^2+\binom{4}{3}p^1(-2q)^3\\ &\quad+\binom{4}{4}p^0(-2q)^4\\ &=p^4-8p^3q+24p^2q^2-32pq^3+16q^4\end{aligned}$$

25.
$$\begin{aligned}\left(x+\frac{1}{x}\right)^5&=\sum_{k=0}^{5}\binom{5}{k}x^{5-k}\left(\frac{1}{x}\right)^k\\ &=\binom{5}{0}x^5\left(\frac{1}{x}\right)^0+\binom{5}{1}x^4\left(\frac{1}{x}\right)^1\\ &\quad+\binom{5}{2}x^3\left(\frac{1}{x}\right)^2+\binom{5}{3}x^2\left(\frac{1}{x}\right)^3\\ &\quad+\binom{5}{4}x^1\left(\frac{1}{x}\right)^4+\binom{5}{5}x^0\left(\frac{1}{x}\right)^5\\ &=x^5+5x^3+10x+\frac{10}{x}+\frac{5}{x^3}+\frac{1}{x^5}\end{aligned}$$

29. El término es $\binom{9}{3}x^6y^3=84x^6y^3$, entonces el coeficiente es 84.

31. El término es $\binom{12}{7}a^5(-2b)^7=792a^5(-128)b^7=-101\,376a^5$, así el coeficiente es $-101\,376$.

33. El término es $\binom{15}{8}(3p^2)^8(-2q)^7=\binom{15}{8}3^8(-2)^7p^{16}q^7$, por tanto el coeficiente es $\binom{15}{8}3^8(-2)^7=-5,404,164,480$.

36. *Demostración:* Sean $a = 1$, $b = -1$ y n un entero positivo. Sustituya en el teorema binomial para obtener

$$\begin{aligned}(1+(-1))^n&=\sum_{k=0}^{n}\binom{n}{k}\cdot 1^{n-k}\cdot(-1)^k\\ &=\sum_{k=0}^{n}\binom{n}{k}(-1)^k \quad \text{porque } 1^{n-k}=1.\end{aligned}$$

Pero $(1+(-1))^n=0^n=0$, so

$$\begin{aligned}0&=\sum_{k=0}^{n}\binom{n}{k}(-1)^k\\ &=\binom{n}{0}-\binom{n}{1}+\binom{n}{2}-\binom{n}{3}+\cdots+(-1)^n\binom{n}{n}.\end{aligned}$$

37. *Sugerencia:* $3 = 1 + 2$.

38. *Demostración:* Sea m cualquier entero con $m \geq 0$ y aplique el teorema binomial con $a = 2$ y $b = -1$. El resultado es

$$\begin{aligned}1=1^m=(2+(-1))^m&=\sum_{i=0}^{m}\binom{m}{i}2^{m-i}(-1)^i\\ &=\sum_{i=0}^{m}(-1)^i\binom{m}{i}2^{m-i}.\end{aligned}$$

41. *Sugerencia:* Aplique el teorema binomial con $a=-\frac{1}{2}$ y $b = 1$ y analice la ecuación resultante cuando n es par y cuando n es impar.

43. $\displaystyle\sum_{k=0}^{n}\binom{n}{k}5^k=\sum_{k=0}^{n}\binom{n}{k}1^{n-k}5^k=(1+5)^n=6^n$

45. $\displaystyle\sum_{i=0}^{n}\binom{n}{i}x^i=\sum_{i=0}^{n}\binom{n}{i}1^{n-i}x^i=(1+x)^n$

47. $\displaystyle\sum_{j=0}^{2n}(-1)^j\binom{2n}{j}x^j=\sum_{j=0}^{2n}\binom{2n}{j}1^{2n-j}(-x)^j=(1-x)^{2n}$

51.
$$\begin{aligned}\sum_{i=0}^{m}(-1)^i\binom{m}{i}\frac{1}{2^i}&=\sum_{i=0}^{m}\binom{m}{i}1^{m-i}\left(-\frac{1}{2}\right)^i\\ &=\left(1-\frac{1}{2}\right)^m=\frac{1}{2^m}\end{aligned}$$

53. $\displaystyle\sum_{i=0}^{n}(-1)^i\binom{n}{i}5^{n-i}2^i=\sum_{i=0}^{n}\binom{n}{i}5^{n-i}(-2)^i=(5-2)^n=3^n$

55. b. $\displaystyle n(1+x)^{n-1}=\sum_{k=1}^{n}\binom{n}{k}kx^{k-1}$.

[El término correspondiente a $k = 0$ *es cero porque* $\frac{d}{dx}(x^0)=0$.*]*

c. (i) Sustituya $x = 1$ en el inciso *b*) anterior para obtener

$$n(1+1)^{n-1} = \sum_{k=1}^{n} \binom{n}{k} k \cdot 1^{k-1} = \sum_{k=1}^{n} \binom{n}{k} k$$
$$= \binom{n}{1} \cdot 1 + \binom{n}{2} \cdot 2 + \binom{n}{3} \cdot 3 + \cdots + \binom{n}{n} n.$$

Dividiendo ambos lados por n y simplificando se obtiene

$$2^{n-1} = \frac{1}{n}\left[\binom{n}{1} + 2\binom{n}{2} + 3\binom{n}{3} + \cdots + n\binom{n}{n}\right].$$

Sección 9.8

1. Por el axioma 2 de probabilidad, $P(\emptyset) = 0$.

2. a. Por el axioma 3 de probabilidad, $P(A \cup B) = P(A) + P(B) = 0.3 + 0.5 = 0.8$

b. Como $A \cup B \cup C = S$, entonces $C = S - (A \cup B)$. Así, por la fórmula para la probabilidad del complemento de un evento, $P(C) = P((A \cup B)^c) = 1 - P(A \cup B) = 1 - 0.8 = 0.2$.

4. Por la fórmula para la probabilidad de la unión general de dos eventos, $P(A \cup B) = P(A) + P(B) - P(A \cap B) = 0.8 + 0.7 - 0.6 = 0.9$.

7. a. $P(A \cup B) = 0.4 + 0.3 = 0.7$
b. $P(C) = P((A \cup B)^c) = 1 - P(A \cup B) = 1 - 0.7 = 0.3$
c. $P(A \cup C) = 0.4 + 0.3 = 0.7$
d. $P(A^c) = 1 - P(A) = 1 - 0.4 = 0.6$
e. $P(A^c \cap B^c) = P((A \cup B)^c) = 1 - P(A \cup B) = 1 - 0.7 = 0.3$
f. $P(A^c \cup B^c) = P((A \cap B)^c) = P(\emptyset^c) = P(S) = 1$

9. a. $P(A \cup B) = P(A) + P(B) - P(A \cap B) = 0.4 + 0.5 - 0.2 = 0.7$
d. $P(A^c \cap B^c) = P((A \cup B)^c) = 1 - P(A \cup B) = 1 - 0.7 = 0.3$

11. *Sugerencia:* $V = (U \cup (V - U))$

12. *Sugerencia:* Use el hecho de que para todos los conjuntos U y V, es válido que $U \cup (V - U) = U \cup V$.

13. *Sugerencia:* $(A_1 \cup A_2 \cup \cdots \cup A_k) \cap A_{k+1} = \emptyset$ y $A_1 \cup A_2 \cup \cdots \cup A_k \cup A_{k+1} = (A_1 \cup A_2 \cup \cdots \cup A_k) \cup A_{k+1}$.

14. *Solución 1:* La ganancia neta del ganador del gran premio es \$2 000 000 − \$2 = \$1 999 998. Cada uno de los 10 000 ganadores del segundo premio tiene una ganancia neta de \$20 − \$2 = \$18 y cada uno de los 50 000 ganadores del tercer premio tiene una ganancia neta de \$4 − \$2 = \$2. El número de personas que no ganaron nada es 1 500 000 − 1 − 10 000 − 50 000 = 1 439 999 y cada una de esas gentes tiene una pérdida neta de \$2. Todos los 1 500 000 boletos tienen igual oportunidad de ganar un premio, entonces la ganancia o pérdida esperada de un boleto es

$$\frac{1}{1\,500\,000}(\$1\,999\,998 \cdot 1 + \$18 \cdot 10\,000 + \$2 \cdot 50\,000 + (-\$2) \cdot 1\,439\,999) = -\$0.40.$$

Solución 2: El ingreso total del organizador de la lotería es \$2 (por boleto). 1 500 00 (boletos) = \$3 000 000. El pago que el organizador de la lotería debe hacer es \$2 000 000 + (\$20)(10 000) + (\$4)(50 000) = \$2 400 000, así la ganancia neta para el organizador es \$600 000, que da $\frac{\$600\,000}{1\,500\,000} = \$0.40$ por boleto. Entonces la pérdida neta esperada del comprador de un boleto es \$0.40.

16. Aceptemos que 2_1 y 2_2 denoten las dos bolas con el número 2 y que 5 y 6 representen a las otras dos bolas. Hay $\binom{6}{2} = 4$ subconjuntos de 2 bolas que se pueden elegir de la urna. La siguiente tabla muestra las sumas de los números sobre las bolas en cada conjunto y las correspondientes probabilidades:

Subconjunto	Suma s	Probabilidad de que la suma = s
$\{2_1, 2_2\}$	4	1, 6
$\{2_1, 5\}, \{2_2, 5\}$	7	2, 6
$\{2_1, 6\}\{2_2, 6\}$	8	2, 6
$\{5^c 6\}$	11	1, 6

Así el valor esperado es $4 \cdot \frac{1}{6} + 7 \cdot \frac{2}{6} + 8 \cdot \frac{2}{6} + 11 \cdot \frac{1}{6} = 7.5$

19. La siguiente tabla muestra la suma de los números en las caras superiores de los dados

	1	2	3	4	5	6
1	2	3	4	5	6	7
2	3	4	5	6	7	8
3	4	5	6	7	8	9
4	5	6	7	8	9	10
5	6	7	8	9	10	11
6	7	8	9	10	11	12

Cada cuadro en la tabla representa un resultado cuya probabilidad es 1/36. Entonces el valor esperado de la suma es

$$2\left(\frac{1}{36}\right) + 3\left(\frac{2}{36}\right) + 4\left(\frac{3}{36}\right) + 5\left(\frac{4}{36}\right) + 6\left(\frac{5}{36}\right) + 7\left(\frac{6}{36}\right) + 8\left(\frac{5}{36}\right) + 9\left(\frac{4}{36}\right) + 10\left(\frac{3}{36}\right) + 11\left(\frac{2}{36}\right) + 12\left(\frac{1}{36}\right) = \frac{252}{36} = 7.$$

20. *Sugerencia:* La respuesta es alrededor de 7.7 centavos.

22. *Sugerencia:* La respuesta es 1.875.

23. *Sugerencia:* Para obtener P_{20}, use el teorema para raíces distintas de la sección 5.8. La respuesta es $P_{20} = \frac{5^{300} - 5^{20}}{5^{300} - 1} \cong 1$.

Sección 9.9

1. $P(B) = \dfrac{P(A \cap B)}{P(A \mid B)} = \dfrac{1/6}{1/2} = \dfrac{1}{3}$

3. *Sugerencia:* La respuesta es 60%.

4. a. *Demostración:* Suponga que S es cualquier espacio muestral con A y B eventos arbitrarios en S tales que $P(B) \neq 0$. Observe que
1) $A \cup A^c = S$ por la ley de complemento para $\cup$.
2) $B \cap S = B$ por la ley identidad para $\cap$.

3) $B \cap (A \cup A^c) = (A \cap B) \cup (A^c \cap B)$ por las leyes distributiva y conmutativa para conjuntos.
4) $(A \cap B) \cap (A^c \cap B) = \emptyset$ por la ley de complemento para $\cap$ y las leyes conmutativas y asociativa para conjuntos.

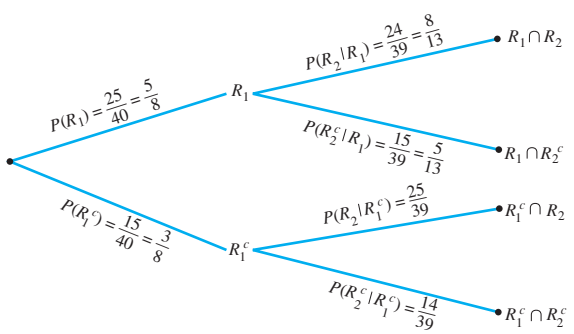
Así $B = (A \cap B) \cup (A^c \cap B)$ y, por el axioma 3 de probabilidad, $P(B) = P(A \cap B) + P(A^c \cap B)$. Por tanto, $P(A^c \cap B) = P(B) - P(A \cap B)$. Por definición de probabilidad condicional, se tiene que

$$P(A^c \mid B) = \frac{P(A^c \cap B)}{P(B)} = \frac{P(B) - P(A \cap B)}{P(B)} = 1 - \frac{P(A \cap B)}{P(B)} = 1 - P(A|B).$$

5. *Sugerencias:* 1) $A = (A \cap B) \cup (A \cap B^c)$.

2) La respuesta es $P(A \mid B^c) = \dfrac{P(A) - P(A \mid B)P(B)}{1 - P(B)}$.

6. a. Aceptemos que R_1 sea la probabilidad de que la primera bola sea roja y que R_2 denote la probabilidad de que la segunda bola sea roja. Entonces $R_1{}^c$ es la probabilidad de que la primera bola no sea roja y $R_2{}^c$ es la probabilidad de que la segunda bola no sea roja. El diagrama de árbol muestra las diversas relaciones entre las probabilidades.



Entonces

$$\begin{aligned}
P(R_1 \cap R_2) &= P(R_2 \mid R_1) \cdot P(R_1) \\
&= \frac{8}{13} \cdot \frac{5}{8} = \frac{5}{13} \cong 38.5\%, \\
P(R_1 \cap R_2^c) &= P(R_2^c \mid R_1) \cdot P(R_1) \\
&= \frac{5}{13} \cdot \frac{5}{8} = \frac{25}{104} \cong 24\%, \\
P(R_1^c \cap R_2) &= P(R_2 \mid R_1^c) \cdot P(R_1^c) \\
&= \frac{25}{39} \cdot \frac{3}{8} = \frac{25}{104} \cong 24\%, \\
P(R_1^c \cap R_2^c) &= P(R_2^c \mid R_1^c) \cdot P(R_1^c) \\
&= \frac{14}{39} \cdot \frac{3}{8} = \frac{14}{104} \cong 13.5\%
\end{aligned}$$

Así la probabilidad de que ambas bolas sean rojas es 5/13, la probabilidad de que la primera sea roja y la segunda no, es 25/104, la probabilidad de que la primera no sea roja y la segunda sí, es 25/104 y la probabilidad de que ninguna sea roja es 14/104.

b. Observe que

$$R_2 = (R_2 \cap R_1) \cup (R_2 \cap R_1^c) \quad \text{y} \quad (R_2 \cap R_1) \cap (R_2 \cap R_1^c) = \emptyset.$$

Entonces la probabilidad de que la segunda bola sea roja es

$$P(R_2) = P(R_2 \cap R_1) + P(R_2 \cap R_1^c) = \frac{5}{13} + \frac{25}{104} = \frac{65}{104} \cong 62.5\%.$$

c. Si exactamente una bola es roja, entonces la primera bola es roja y la segunda no, o la primera bola no es roja pero la segunda sí lo es y esas posibilidades son mutuamente excluyentes. Por tanto

$$\begin{aligned}
P(\text{exactamente una bola es roja}) &= P(R_1 \cap R_2^c) + P(R_1^c \cap R_2) \\
&= \frac{25}{104} + \frac{25}{104} = \frac{50}{104} \\
&= \frac{25}{52} \cong 48.1\%.
\end{aligned}$$

La probabilidad de que ambas bolas sean rojas es $P(R_1 \cap R_2) = \frac{5}{13} \cong 38.5\%$. Entonces

P (al menos una bola es roja) = P (exactamente una bola es roja) + P (ambas bolas son rojas)

$$= \frac{25}{52} + \frac{5}{13} = \frac{45}{52} \cong 86.5\%.$$

8. a. Sean W_1 el evento de que una mujer sea elegida en el primer intento,
W_2 el evento de que una mujer sea seleccionada en el segundo intento,
M_1 el evento de que un hombre sea electo en el primer intento,
M_2 el evento de que un hombre sea seleccionado en el segundo intento.
Entonces $P(W_1) = \frac{3}{10}$ y $P(W_2 \mid W_1) = \frac{2}{9}$ y así

$P(W_1 \cap W_2) = P(W_2 \mid W_1)P(W_1) = \frac{2}{9} \cdot \frac{3}{10} = \frac{1}{15} = 6\frac{2}{3}\%$.

c. *Sugerencia:* La respuesta es $\frac{7}{15} = 46\frac{2}{3}\ \%$.

9. *Sugerencia:* Use los resultados $P(B_k \mid A) = \dfrac{P(B_k \cap A)}{P(A)}$ y que $(A \cap B_1) \cup (A \cap B_2) = A$.

11. a. Sean U_1 el evento de que la primera urna sea seleccionada, U_2 el evento de que la segunda urna sea elegida y B el evento de que la bola seleccionada sea azul. Entonces

$$P(B \mid U_1) = \frac{12}{19} \quad \text{y} \quad P(B \mid U_2) = \frac{8}{27}.$$

$$P(B \cap U_1) = P(B \mid U_1)P(U_1) = \frac{12}{19} \cdot \frac{1}{2} = \frac{12}{38}.$$

También

$$P(A \cap U_2) = P(B \mid U_2)P(U_2) = \frac{8}{27} \cdot \frac{1}{2} = \frac{8}{54}.$$

Ahora B es la unión disjunta de $B \cap U_1$ y $B \cap U_2$. Así

$$P(B) = P(B \cap U_1) + P(B \cap U_2) = \frac{12}{38} + \frac{8}{54} \cong 46.4\%.$$

Por tanto, la probabilidad de que la bola seleccionada sea azul es aproximadamente 46.4%.

b. Dado que la bola elegida es azul, la probabilidad de que ella venga de la primera urna es $P(U_1 \mid B)$. Por el teorema de Bayes y los cálculos en el inciso *a*),

$$P(U_1 \mid B) = \frac{P(B \mid U_1)P(U_1)}{P(B \mid U_1)P(U_1) + P(B \mid U_2)P(U_2)} = \frac{(12/19)(0.5)}{(12/19)(0.5) + (8/27)(0.5)} \cong 68.1\%$$

13. *Sugerencia:* Las respuestas a los incisos *a*) y *b*) son aproximadamente 52.9% y 54.0%, respectivamente.

14. Sean A el evento de que una persona elegida aleatoriamente dé positivo en drogas, B_1 el evento de que una persona seleccionada aleatoriamente use drogas y B_2 el evento de que una persona elegida aleatoriamente no utilice drogas. Entonces A^c es el evento de que una persona elegida aleatoriamente no dé positivo en el examen de drogas y $P(B_1) = 0.04$, $P(B_2) = 0.96$, $P(A \mid B_2) = 0.03$ y $P(A^c \mid B_1) = 0.02$. Así que $P(A \mid B_1) = 0.97$ y $P(A^c \mid B_2) = 0.98$.

a. $$P(B_1 \mid A) = \frac{P(A \mid B_1)P(B_1)}{P(A \mid B_1)P(B_1) + P(A \mid B_2)P(B_2)} = \frac{(0.97)(0.04)}{(0.97)(0.04) + (0.03)(0.96)} \cong 57.4\%$$

b. $$P(B_2 \mid A^c) = \frac{P(A^c \mid B_2)P(B_2)}{P(A^c \mid B_1)P(B_1) + P(A^c \mid B_2)P(B_2)} = \frac{(0.98)(0.96)}{(0.02)(0.04) + (0.98)(0.96)} \cong 99.9\%$$

16. *Sugerencia:* Las respuestas a los incisos *a*) y *b*) son 11.25% y $21\frac{1}{3}\%$, respectivamente.

17. *Demostración:* Suponga que A y B sean eventos en el espacio muestral S y $P(A \mid B) = P(A) \neq 0$. Entonces

$$P(B|A) = \frac{P(B \cap A)}{P(A)} = \frac{P(A|B)P(B)}{P(A)} = \frac{P(A)P(B)}{P(A)} = P(B).$$

19. Como en el ejemplo 6.9.1, el espacio muestral es el conjunto de todos los 36 resultados al lanzar los dos dados y anotando los números sobre las caras superiores de cada uno. Sean A el evento de que el número sobre el dado azul es 2 y B el evento de que el número sobre el dado gris es 4 o 5. Entonces

$$A = \{21, 22, 23, 24, 25, 26\},$$
$$B = \{14, 24, 34, 44, 54, 64, 15, 25, 35, 45, 55, 65\}, \text{ y}$$
$$A \cap B = \{24, 25\}.$$

Los dados son imparciales (así los resultados son equiprobables), $P(A) = \frac{6}{36}$, $P(B) = \frac{12}{36}$ y $P(A \cap B) = \frac{2}{36}$. Por definición de probabilidad condicional,

$$P(A \mid B) = \frac{P(A \cap B)}{P(B)} = \frac{\frac{2}{36}}{\frac{12}{36}} = \frac{1}{6} \quad \text{y}$$

$$P(B|A) = \frac{P(A \cap B)}{P(A)} = \frac{\frac{2}{36}}{\frac{6}{36}} = \frac{1}{3}.$$

Pero $P(A) = \frac{6}{36} = \frac{1}{6}$ y $P(B) = \frac{12}{36} = \frac{1}{3}$. Entonces $P(A \mid B) = P(A)$ y $P(B \mid A) = P(B)$.

23. Sean A el evento de que el estudiante responda correctamente a la primera pregunta y B el evento de que el alumno conteste correctamente la segunda pregunta. Se pueden eliminar dos elecciones en la primera pregunta, entonces $P(A) = \frac{1}{3}$ y ninguna elección puede eliminarse en la segunda pregunta, $P(B) = \frac{1}{5}$. Entonces $P(A^c) = \frac{2}{3}$ y $P(B^c) = \frac{4}{5}$.

a. *Sugerencia:* La probabilidad de que el estudiante responda correctamente ambas preguntas es:

$$P(A \cap B) = P(A)P(B) = \frac{1}{3} \cdot \frac{1}{5} = \frac{1}{15} = 6\frac{2}{3}\%.$$

b. La probabilidad de que el estudiante conteste correctamente exactamente una cuestión es

$$\begin{aligned} &P((A \cap B^c) \cup (A^c \cap B)) \\ &\quad = P(A \cap B^c) + P(A^c \cap B) \\ &\quad = P(A)P(B^c) + P(A^c)P(B) \\ &\quad = \frac{1}{3} \cdot \frac{4}{5} + \frac{2}{3} \cdot \frac{1}{5} = \frac{6}{15} = \frac{2}{5} = 40\%. \end{aligned}$$

c. Una solución es decir que la probabilidad de que el alumno responda incorrectamente ambas preguntas es $P(A^c \cap B^c)$ y $P(A^c \cap B^c) = P(A^c)P(B^c)$ por el resultado del ejercicio 22. Así la respuesta es

$$P(A^c)P(B^c) = \frac{2}{3} \cdot \frac{4}{5} = \frac{8}{15} = 53\frac{1}{3}\%.$$

Otra solución utiliza el hecho de que el evento de que el estudiante conteste incorrectamente ambas cuestiones, es el complemento del evento de que el alumno responda correctamente al menos una pregunta. Así, por los resultados de los incisos *a*) y *b*), la respuesta es $1 - \left(\frac{1}{15} + \frac{2}{5}\right) = \frac{8}{15} = 53\frac{1}{3}\%$.

25. H_i es el evento de que el resultado del lanzamiento i sea cara, T_i es el evento de que el resultado del lanzamiento i sea cruz. Entonces $P(H_i) = 0.7$ y $P(T_i) = 0.3$ para $i = 1, 2$.

b. La probabilidad de obtener exactamente una cara es

$$\begin{aligned} &P((H_1 \cap T_2) \cup (T_1 \cap H_2)) \\ &\quad = P(H_1 \cap T_2) + P(T_1 \cap H_2) \\ &\quad = P(H_1)P(T_2) + P(T_1)P(H_2) \\ &\quad = (0.7)(0.3) + (0.3)(0.7) = 42\%. \end{aligned}$$

27. *Sugerencia:* La respuesta es $\frac{1}{2}$.

28. a. P(siete caras)

$$= \begin{bmatrix}\text{número de diferentes maneras}\\ \text{en que se pueden obtener siete}\\ \text{caras en diez lanzamientos}\end{bmatrix} (0.7)^7(0.3)^3$$
$$= 120(0.7)^7(0.3)^3 \cong 0.267 = 26.7\%.$$

29. a. P(ninguna es defectuosa)

$$= \begin{bmatrix}\text{número de distintas formas}\\ \text{de tener 0 objetos defectuosos}\\ \text{en la muestra de 10}\end{bmatrix} (0.03)^0(0.97)^{10}$$
$$= 1 \cdot (0.3.)^0(0.97)^{10} \cong 0.737 = 73.7\%$$

30. b. La probabilidad de que una mujer tendrá al menos un resultado positivo falso en un periodo de diez años es $1 - (0.96)^{10} \cong 33.5\%$.

31. a. P(ninguna persona es masculino) $\cong 1.3\%$

b. P(al menos una es masculino) $= 1 - P$(ninguna es masculino) $\cong 1 - 0.013 = 98.7\%$

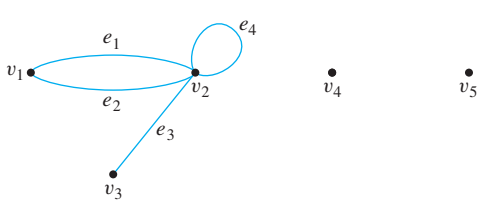
Sección 10.1

1. $V(G) = \{v_1, v_2, v_3, v_4\}$, $E(G) = \{e_1, e_2, e_3\}$

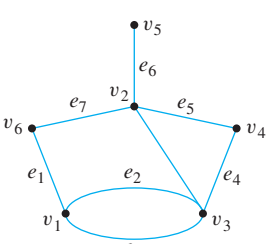
Función extremo-puntos extremos:

Extremo	Puntos extremos
e_1	$\{v_1, v_2\}$
e_2	$\{v_1, v_3\}$
e_3	$\{v_3\}$

3.



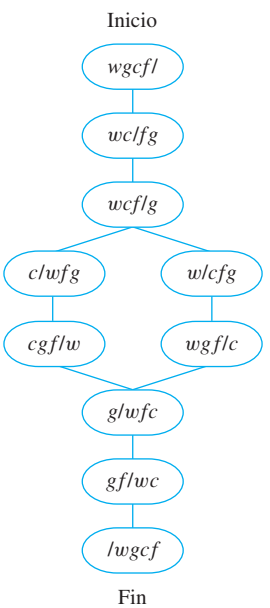
5. Imagine que los extremos son cadenas y los vértices son nudos. Puede tomar la figura del lado izquierdo y ponerla para formar la figura del lado derecho como se muestra a continuación.



8.
(i) e_1, e_2 y e_3 inciden sobre v_1.
(ii) v_1, v_2 y v_3 son adyacentes a v_3.
(iii) e_2, e_8, e_9 y e_3 son adyacentes a e_1.
(iv) Los bucles son e_6 y e_7.
(v) e_8 y e_9 son paralelos; e_4 y e_5 son paralelos.
(vi) v_6 es un vértice aislado.
(vii) grado de $v_3 = 5$.
(viii) grado total $= 20$.

10. a. Sí. De acuerdo a la gráfica, *Deportes Ilustrados* es un ejemplo de una revista deportiva, que es de tipo periódica y ésta contiene escritura impresa.

12. Resuelva este problema utilizando un grafo, introduzca una notación en la que, por ejemplo, wc/fg significa que el lobo y la col están en la orilla izquierda del río y el lanchero y la cabra están en la orilla derecha. Después dibuje los posibles arreglos de lobo, col, cabra y lanchero que pueden obtenerse a partir del arreglo inicial ($wgcf/$) y que no sean arreglos a eliminarse (tales como (wg/fc)). En cada paso pregúntate, ¿de aquí a dónde puedo ir? y dibuja líneas o flechas apuntando hacia esos arreglos. Este método da el grafo que se muestra arriba de la próxima columna.



Un examen del diagrama muestra las soluciones

$$(wgcf/) \to (wc/gf) \to (wcf/g) \to (w/gcf) \to (wgf/c) \to (g/wcf) \to (gf/wc) \to (/wgcf)$$

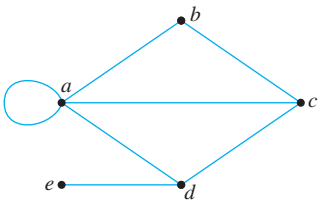
y

$$(wgcf/) \to (wc/gf) \to (wcf/g) \to (c/wgf) \to (gcf/w) \to (g/wcf) \to (gf/wc) \to (/wgcf)$$

14. *Sugerencia:* La respuesta es sí. Con pares ordenados represente las posibles cantidades de agua en las jarras A y B. Por ejemplo, el par ordenado (1, 3) indicaría que hay un cuarto de agua en la jarra A y tres cuartos en la jarra B. Iniciando con (0, 0), dibuje flechas de un par ordenado a otro si es posible ir de la situación representada por un par hacia la representada por el otro par, ya sea llenando o vaciando una jarra, o transfiriendo agua de una jarra a otra. Sólo necesita trazar flechas de estados que tienen flechas apuntándolos; los otros estados no se pueden alcanzar. Después encuentre una trayectoria dirigida (secuencia de extremos dirigidos) del estado inicial (0, 0) a un estado final (1, 0) o (0, 1).

15. El grado total del grafo es $0 + 2 + 2 + 3 + 9 = 16$, así por el teorema 10.1.1, el número de extremos es $16/2 = 8$.

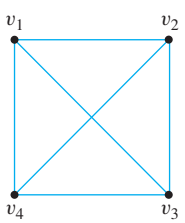
17. Dicho grafo es



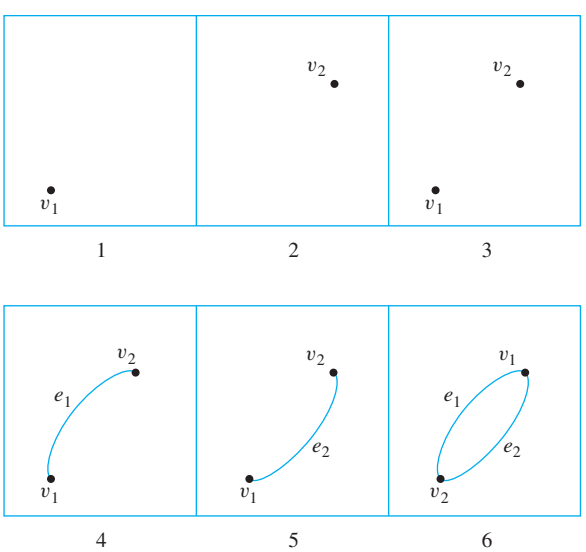
18. Si hubiera un grafo con cuatro vértices de grados 1, 2, 3 y 3, entonces su grado total sería 9, que es impar. Pero por el corolario 10.1.2, el grado total del grafo debe ser par. *[Esto es una contradicción.]* Así que no existe dicho grafo. (Alternativamente, si hubiera tal grafo, tendría un número impar de vértices de grado impar. Pero esto es imposible por la proposición 10.1.3.)

21. Suponga que hubiera un grafo simple con cuatro vértices de grados 1, 2, 3 y 4. Entonces el vértice de grado 4 tendría que estar conectado por extremos a cuatro vértices distintos a sí mismo, esto debido a la suposición de que el grafo es simple (así que no tiene bucles o extremos paralelos). Esto contradice la suposición de que el grafo tiene cuatro vértices en total. Entonces no existe un grafo simple con cuatro vértices de grados 1, 2, 3 y 4.

24.



26. a. Los subgrafos no vacíos son los siguientes:



27. a. Suponga que, en un grupo de 15 personas, cada persona tuvo exactamente tres amigos. Entonces podría dibujar un grafo representando a cada persona por un vértice y conectando dos vértices por un extremo si las correspondientes personas fueron amigos. Pero tal grafo tendría 15 vértices, cada uno de grado 3, para un grado total de 45. Esto sería una contradicción para el hecho de que el grado total de cualquier grafo es par. Así que la suposición debe ser falsa y en un grupo de 15 personas no es posible que cada uno haya tenido exactamente tres amigos.

31. Demos dos demostraciones para el siguiente enunciado, uno menos y el otro más formal.

> Para todos los enteros $n \geq 0$, si $a_1, a_2, a_3, \ldots, a_{2n+1}$ son enteros impares, entonces $\sum_{i=1}^{2n+1} a_i$ es impar.

Demostración 1 (por inducción matemática: Es verdadero que la "suma" de un entero impar es impar. Suponga que para verdadero entero impar positivo r, la suma de r enteros impares es impar. Debemos demostrar que la suma de $r + 2$ enteros impares es impar (porque $r + 2$ es el siguiente entero impar después de r). Pero cualquier suma de $r + 2$ enteros impares es igual a una suma de r enteros impares (que es impar por la hipótesis inductiva) más una suma de dos enteros impares (que es par). Así la suma total es un entero impar más un entero par, que es impar. *[Que era lo que se quería demostrar.]*

Demostración 2 (por inducción matemática): Aceptemos que la propiedad $P(n)$ sea la siguiente frase: "Si $a_1, a_2, a_3, \ldots, a_{2n+1}$ son enteros impares, entonces $\sum_{i=1}^{2n+1} a_i$ es impar".

Demostración de que P(0) es verdadero:

Suponga que a_1 es un entero impar. Entonces $\sum_{i=1}^{2 \cdot 0+1} a_i = \sum_{i=1}^{1} a_i = a_1$, que es impar.

Demostración de que para todos los enteros $k \geq 0$, si $P(k)$ es verdadero entonces $P(k+1)$ también es verdadero:

Sea k un entero con $k \geq 0$ y suponga que

> si $a_1, a_2, \ldots, a_{2k+1}$ son enteros impares, entonces $\sum_{i=1}^{2k+1} a_i$ es impar.

[Esto es la hipótesis de inducción $P(k)$.]

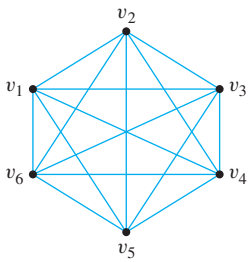
Suponga que $a_1, a_2, a_3, \ldots, a_{2(k+1)+1}$ son enteros impares. *[Debemos demostrar que $P(k+1)$, a saber que $\sum_{i=1}^{2(k+1)+1} a_i$ es impar, o, equivalentemente, que $\sum_{i=1}^{2k+3} a_i$ es impar.]* Pero

$$\sum_{i=1}^{2k+3} a_i = \sum_{i=1}^{2k+1} a_i = (a_{2k+2} + a_{2k+3}).$$

La suma de cualesquiera dos números impares es par, entonces $a_{2k+2} + a_{2k+3}$ es par y, por la hipótesis de inducción, $\sum_{i=1}^{2k+1} a_i$ es impar. Por tanto, $\sum_{i=1}^{2k+3} a_i$ es la suma de un entero impar y un entero par, que es impar. *[Que era lo que se quería demostrar.]*

32. *Sugerencia:* Demuestre por contradicción.

33. a. K_6:



b. Una demostración de este hecho fue dada en la sección 5.6 utilizando recursividad. Intente encontrar una demostración diferente.

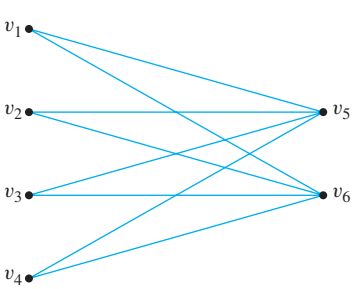
Sugerencia para la demostración 1: Hay tantos extremos en K_n como subconjuntos de dos vértices (los puntos extremos) que pueden elegirse de un conjunto de n vértices.

Sugerencia para la demostración 2: Use inducción matemática. Un grafo completo de $n + 1$ vértices puede obtenerse de un grafo completo de k vértices agregando un vértice y conectando a éste con k extremos a cada uno de los otros vértices.

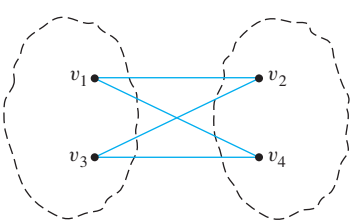
Sugerencia para la prueba 3: Implemente el hecho de que el número de extremos de un grafo es la mitad del grado total. ¿Cuál es el grado de cada vértice de K_n?

35. Suponga que G es un grafo simple con n vértices y $2n$ extremos en donde n es un entero positivo. Por el ejercicio 34, su número de extremos no puede exceder $\frac{n(n-1)}{2}$. Así2 $2n \leq \frac{n(n-1)}{2}$, o $4n \leq n^2 - n$. Equivalentemente, $n^2 - 5n \geq 0$, o $n(n - 5) \geq 0$. Esto implica que $n \geq 5$ ya que $n > 0$. Entonces un grafo simple con el doble de extremos que de vértices debe tener al menos cinco vértices. Pero un grafo completo con cinco vértices tiene $\frac{5(5-1)}{2} = 10$ extremos y $10 = 2 \cdot 5$. En consecuencia, la respuesta a la pregunta es sí porque K_5 es un grafo con dos veces más extremos que vértices.

36. a. $K_{4,2}$:

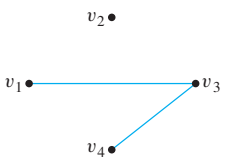


37. a. Este grafo es bipartito.

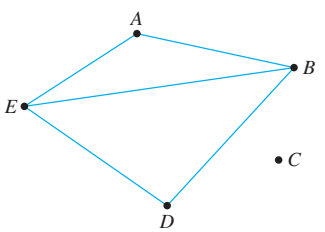


b. Suponga que este grafo es bipartito. Entonces el conjunto de vértices puede ser particionado en dos subconjuntos mutuamente disjuntos, tales que los vértices en cada subconjunto estén conectados por extremos solamente a vértices en el otro subconjunto y no a vértices en el mismo subconjunto. Ahora v_1 está en un subconjunto de la partición, digamos V_1. Como v_1 está conectado por extremos a v_2 y v_3, entonces v_2 y v_3 deben estar en el otro subconjunto, V_2. Pero v_2 y v_3 están conectados entre sí por un extremo. Esto contradice el hecho de que ningún vértice en V_2 está conectado por extremos a otros vértices en V_2. Así que la suposición es falsa y entonces el grafo no es bipartito.

39. a.



41. b.

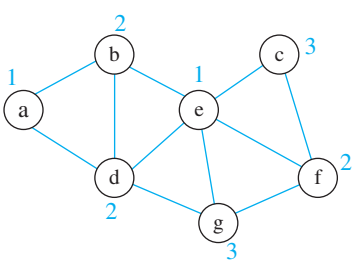


42. *Sugerencia:* Considere el grafo obtenido al tomar los vértices y extremos de G más todos los extremos de G'. Use el ejercicio 33(b).

44. c. *Sugerencia:* Suponga que hubiera un grafo simple con n vértices (en donde $n \geq 2$) y cada uno de los cuales con diferente grado. Entonces ningún vértice podría tener un grado mayor que $n - 1$ (¿por qué?), así los grados de los n vértices deben ser 0, 1, 2,…, $n - 1$ (¿por qué?). Esto es imposible (¿por qué?).

45. *Sugerencia:* Use el resultado del ejercicio 44(c).

46.



El vértice e tiene un grado máximo, así se colorea con el color #1. El vértice a no comparte un extremo con e y en consecuencia el color #1 también puede emplearse para éste. De los restantes vértices no coloreados, d, g y f tienen grado máximo. Elija cualquiera de estos, digamos d y use el color #2 para éste. Observe que los vértices b, c y f no comparten un extremo con d, pero c y f sí comparten entre sí un extremo, lo que significa que el color #2 se puede usar sólo para c o f. Así se colorea b con el color #2 y se elije colorear a f con el color #2 porque el grado de f es mayor que el grado de c. De los restantes vértices no coloreados, g tiene grado máximo, Por tanto, se colorea con el color #3.Observe que como g no comparte un extremo con c, entonces el color #3 se puede emplear para c. En este paso, todos los vértices ya han sido coloreados.

47. *Sugerencia:* Existen dos soluciones:

1) Tiempo 1: alquiler, biblioteca
   Tiempo 2: personal, educación a nivel superior, coloquio
   Tiempo 3: educación a nivel graduados
2) Tiempo 1: alquiler, biblioteca
   Tiempo 2: educación a nivel graduados, coloquio
   Tiempo 3: personal, educación a nivel superior

Sección 10.2

1. a. sendero (no un extremo repetido), no una trayectoria (vértice repetido $-v_1$), no un bucle.

b. caminar, no un sendero (tiene un extremo repetido $-e_9$), no un bucle.

c. camino cerrado (inicia y termina en el mismo vértice), sendero (ningún extremo repetido porque no hay extremos), ni una trayectoria o un bucle (porque no hay extremo).

d. bucle, no un simple bucle (vértice repetido, v_4).

e. camino cerrado (inicia y termina en el mismo vértice pero tiene extremos repetidos $-\{v_2,v_3\}$ y $\{v_3,v_4\}$)

f. trayectoria.

3. a. No. La notación $v_1v_2v_1$ podría igualmente referirse a $v_1e_1v_2e_2v_1$ o a $v_1e_2v_2e_1v_1$, que son caminos diferentes.

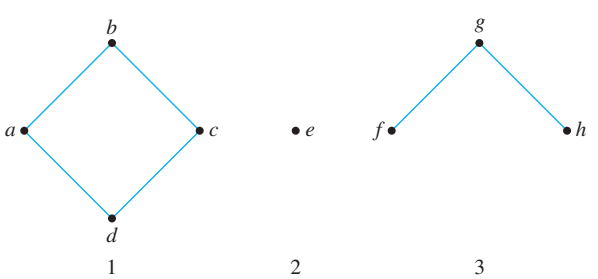
4. a. Tres (existen tres maneras de elegir el extremo de en medio).

b. $3! + 3 = 9$ (Además de los tres caminos, hay 3! con vértices v_1, v_2, v_3, v_4. La razón es que de v_2 existen tres posibilidades para ir a v_3, entonces dos elecciones de diferentes extremos para retornar a v_2 y una opción de distinto extremo para regresar a v_3. Esto da 3! senderos de v_2 a v_3.

c. Una infinidad (un camino puede tener extremos repetidos, entonces un camino de v_1 a v_4 puede tener un número arbitrariamente grande de repeticiones de extremos uniendo un par de vértices a lo largo del avance).

6. a. $\{v_1, v_3\}$, $\{v_2, v_3\}$, $\{v_4, v_3\}$ y $\{v_5, v_3\}$ todos son puentes.

8. a. Tres componentes están conectados.



9. a. No. Este grafo tiene dos vértices de grado impar, mientras que todos los vértices de un grafo con un bucle de Euler tienen grado par.

12. Un bucle de Euler es $e_4e_5e_6e_3e_2e_7e_8e_1$.

14. Un bucle de Euler es *iabihbchgcdgfdefi*.

19. Existe una trayectoria de Euler porque grad(u) y grad(w) son impares, todos los otros vértices tienen grados pares positivos y el grafo es conexo. Una trayectoria de Euler es $uv_1v_0v_7uv_2v_3v_4v_2v_6v_4wv_5v_6w$.

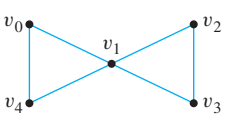
23. $v_0v_7v_1v_2v_3v_4v_5v_6v_0$

25. *Sugerencia:* vea la solución del ejemplo 10.2.8

26. Aquí está una sucesión de un razonamiento que podría emplear: sea G el grafo dado y suponga que G tiene un bucle hamiltoniano. Entonces G tiene un subgrafo H que satisface las condiciones de la 1) a la 4) de la proposición 10.2.6. El grado de b en G es 4 y cada vértice en H tiene grado 2, entonces los dos extremos que inciden en b se deben eliminar de G para crear H. El extremo $\{a, b\}$ no se puede eliminar porque el hacerlo daría como resultado que el vértice d tendría grado menor que 2 en H. Un razonamiento similar muestra que el extremo $\{b, c\}$ no se puede remover. Así que los extremos $\{b, i\}$ y $\{b, e\}$ deben eliminarse de G para crear H. Como el vértice e debe tener grado 2 en H y como el extremo $\{b, e\}$ no está en H, entonces $\{e, d\}$ y $\{e, f\}$ deben estar en H. Similarmente, los vértices c y g deben tener grado 2 en H, los extremos $\{c, d\}$ y $\{g, d\}$ también deben estar en H. Pero entonces tres extremos que inciden en d, a saber $\{e, d\}$,$\{c, d\}$ y $\{g, d\}$ deben estar en H, lo que contradice el hecho de que el vértice d debe tener grado 2 en H.

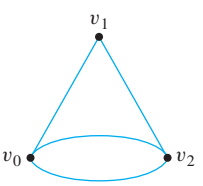
28. *Sugerencia:* este grafo no tiene un bucle hamiltoniano.

32. *Respuesta parcial:*



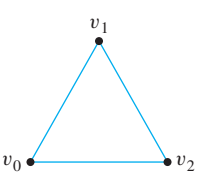
Este grafo tiene el bucle de Euler $v_0v_1v_2v_3v_1v_4v_0$ pero no tiene bucle hamiltoniano.

33. *Respuesta parcial:*



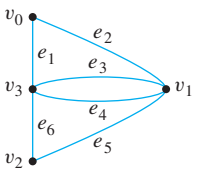
Este grafo tiene el bucle hamiltoniano $v_0v_1v_2v_0$ pero no tiene bucle de Euler.

34. *Respuesta parcial:*



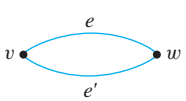
El camino $v_0v_1v_2v_0$ es un bucle de Euler y también hamiltoniano para este grafo.

35. *Respuesta parcial:*

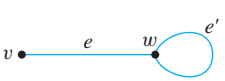


Este grafo tiene el bucle de Euler $e_1e_2e_3e_4e_5e_6$ y el bucle hamiltoniano $v_0v_1v_2v_3v_0$. No coinciden entre sí.

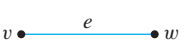
37. **a.** *Demostración:* Suponga que G es un grafo y W es un camino en G que contiene un extremo repetido e. Sean v y w los puntos extremos de e. En el caso $v = w$, entonces v es un vértice repetido de W. En el caso $v \neq w$, entonces debe ocurrir una de las siguientes situaciones: 1) W contiene dos copias de vew o de wev (por ejemplo, W podría contener una sección de la forma $vewe'vew$, como se muestra a continuación); 2) W contiene secciones separadas de la forma vew y wev (por ejemplo, W podría tener una sección de la forma $vewe'ev$, como se muestra a continuación); o 3) W contiene una sección de la forma $vewev$ o de la forma $wevew$ (como se muestra a continuación). En los casos 1) y 2), v y w están repetidos. En todos los casos, hay al menos un vértice en el que W está repetido.



1



2

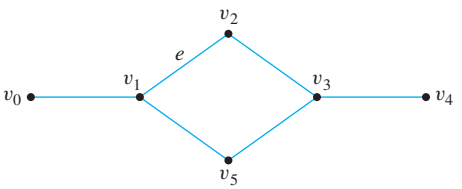


3

38. *Demostración:* Suponga que G es un grafo conexo, v y u son vértices particulares, pero arbitrariamente elegidos, de G. *[Debemos demostrar que u y v pueden ser conectados por una trayectoria.]* Como G está conectada, existe un camino de v a w. Si el camino contiene un vértice repetido, entonces borre la parte del camino de la primera ocurrencia del vértice a su próxima ocurrencia. (Por ejemplo, en el camino $ve_1v_2e_5v_7e_6v_2e_3w$, el vértice v_2 ocurre dos veces. Borrando la parte del camino de una ocurrencia a la próxima se obtiene $ve_1v_2e_3w$.) Si el camino resultante contiene un vértice repetido, entonces realice otra vez el proceso anterior de borrado. Vuelva a comprobar si hay un vértice repetido. Continúe de esta manera hasta que todos los vértices repetidos hayan sido borrados. (Esto ocurrirá eventualmente, porque es finito el número de vértices). El camino resultante conecta a v con w pero con ningún vértice repetido. Por el ejercicio 37(b), tampoco tiene algún extremo repetido. Así esta es una trayectoria de v a w.

40. El grafo de la derecha contiene un bucle, cualquier extremo se puede eliminar sin desconectar el grafo.

Por ejemplo, si se quita el extremo e, entonces se puede usar el siguiente camino para ir de v_1 a v_2: $v_1v_5v_3v_2$.



42. *Sugerencia:* Vea la respuesta al ejercicio 40 y use el hecho de que todos los grafos tienen un número finito de extremos.

44. *Demostración:* Sea G un grafo conexo y C un bucle en G. Sea G' el subgrafo obtenido al quitar todos los extremos de C de G y también cualquier vértice que se convierta en aislado cuando los extremos de C son eliminados. *[Debemos demostrar que existe un vértice v tal que v está en C y G'.]* Tome cualquier vértice v de C y cualquier vértice w de G'. Como G es conexa, existe una trayectoria de v a w (por el lema 10.2.1(a)):

$$\underset{\text{en } C}{v} = v_0e_1\underset{\text{en } C}{v_1}e_2v_2 \ldots v_{i-1}e_i\underset{\text{en } C}{v_i}e_{i+1}\underset{\text{no en } C}{v_{i+1}} \ldots v_{n-1}e_n\underset{\text{en } G'}{v_n} = w.$$

Sea i el mayor subíndice tal que v_i esté en C. Si $i = n$, entonces $v_n = w$ está en C y también en G' y listo. Si $i < n$, entonces v_i está en C y v_{i+1} no está en C. Esto implica que e_{i+1} no está en C (porque si estuviera, ambos puntos extremos estarían en C por definición de bucle). Así que cuando G' se forma por eliminación de los extremos y los vértices aislados resultantes de G, entonces e_{i+1} no es removido. Eso significa que v_i no se convierte en un vértice aislado, por lo que v_i no es removido. Por tanto, v_i está en G'. En consecuencia, v_i está en C y G' *[que era lo que se quería demostrar]*.

45. *Demostración:* Suponga que G es un grafo con un bucle de Euler. Si G sólo tiene un vértice, entonces G está automáticamente conexa. Si v y w son vértices arbitrarios de G, entonces v y w aparecen, cada una, al menos una vez en el bucle de Euler (porque un bucle de Euler contiene a cada vértice del grafo). La sección del bucle entre la primera ocurrencia de v o w y la primera ocurrencia de la otra es un camino de uno de los dos vértices al otro.

Sección 10.3

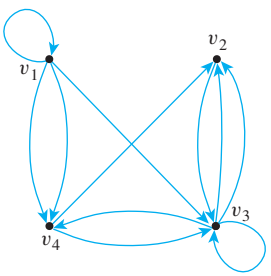
1. **a.** Al igualar las correspondientes entradas se muestra que

$$\begin{aligned} a + b &= 1, \\ a - c &= 0, \\ c &= -1, \\ b - a &= 3. \end{aligned}$$

Así $a - c = a - (-1) = 0$, Por tanto $a = -1$. En consecuencia, $a + b = (-1) + b = 1$, entonces $b = 2$. La última ecuación debe comprobarse para estar seguro de que la respuesta es consistente: $b - a = 2 - (-1) = 3$, lo que concuerda.

2. a.
$$\begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \end{array}\begin{array}{c} \begin{array}{ccc} v_1 & v_2 & v_3 \end{array} \\ \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \end{array}$$

3. a.

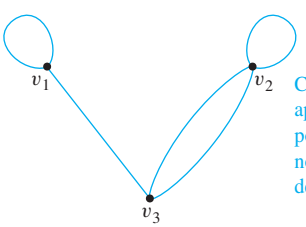


Cualquier etiqueta se puede aplicar a los extremos porque la matriz adyacente no determina las etiquetas de extremos.

4. a.
$$\begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \end{array}\begin{array}{c} \begin{array}{cccc} v_1 & v_2 & v_3 & v_4 \end{array} \\ \begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 2 & 0 \\ 1 & 2 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix} \end{array}$$

c.
$$\begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \end{array}\begin{array}{c} \begin{array}{cccc} v_1 & v_2 & v_3 & v_4 \end{array} \\ \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix} \end{array}$$

5. a.



Cualquier etiqueta se puede aplicar a los extremos porque la matriz adyacente no determina las etiquetas de los extremos.

6. a. El grafo es conexo.

8. a. $2 \cdot 1 + (-1) \cdot 3 = -1$

9. a. $\begin{bmatrix} 3 & -3 & 12 \\ 1 & -5 & 2 \end{bmatrix}$

10. a. ningún producto (A tiene tres columnas y B tiene dos renglones).

b. $BA = \begin{bmatrix} -2 & -2 & 2 \\ 1 & -5 & 2 \end{bmatrix}$ **f.** $B^2 = \begin{bmatrix} 4 & 0 \\ 1 & 9 \end{bmatrix}$

i. $AC = \begin{bmatrix} 2 & -1 \\ -5 & -2 \end{bmatrix}$

12. Uno de muchos posibles ejemplos es $A = B = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}$.

14. *Sugerencia:* Si las entradas de la matriz identidad $m \times m$ son denotadas por δ_{ik}, entonces $\delta_{ik} = \begin{cases} 0 & \text{si } i \neq k \\ 1 & \text{si } i = k \end{cases}$. La ij-ésima entrada de $\mathbf{IA}$ es $\sum_{k=1}^{m} \delta_{ik} A_{kj}$.

15. *Demostración:* Suponga que $\mathbf{A}$ es una matriz simétrica $m \times m$. Entonces para todos los enteros i y j con $1 \leq i, j \leq m$,

$$(A^2)_{ij} = \sum_{k=1}^{m} A_{ik} A_{kj} \quad \text{y} \quad (A^2)_{ji} = \sum_{k=1}^{m} A_{jk} A_{ki}.$$

Como $\mathbf{A}$ es simétrica, $A_{ik} = A_{ki}$ y $A_{kj} = A_{jk}$ para toda i, j y k y así $A_{ik}A_{kj} = A_{jk}A_{ki}$ *[por la ley conmutativa de la multiplicación de números reales]*. Entonces $(A^2)_{ij} = (A^2)_{ji}$ para todos los enteros i y j con $1 \leq i, j \leq m$.

17. *Demostración (por inducción matemática):* Aceptemos que la propiedad $P(n)$ sea la ecuación $\mathbf{A}^n\mathbf{A} = \mathbf{A}\mathbf{A}^n$.

Demostración de que P(1) es verdadera:

Debemos demostrar que $\mathbf{A}^1\mathbf{A} = \mathbf{A}\mathbf{A}^1$. Pero esto es verdadero porque $\mathbf{A}^1 = \mathbf{A}$ y $\mathbf{A}\mathbf{A} = \mathbf{A}\mathbf{A}$.

Demostración de que para todos los enteros $k \geq 1$, si $P(k)$ es verdadero, entonces $P(k+1)$ también es verdadero:

Sea k cualquier entero tal que $k \geq 1$ y suponga que $\mathbf{A}^k\mathbf{A} = \mathbf{A}\mathbf{A}^k$. *[Esto es la hipótesis de inducción.]* Debemos demostrar que $\mathbf{A}^{k+1}\mathbf{A} = \mathbf{A}\mathbf{A}^{k+1}$. Pero

$$\begin{aligned} \mathbf{A}^{k+1}\mathbf{A} &= (\mathbf{A}\mathbf{A}^k)\mathbf{A} && \text{por definición de potencia matricial} \\ &= \mathbf{A}(\mathbf{A}^k\mathbf{A}) && \text{por el ejercicio 16} \\ &= \mathbf{A}(\mathbf{A}\mathbf{A}^k) && \text{por hipótesis de inducción} \\ &= \mathbf{A}\mathbf{A}^{k+1} && \text{por definición de potencia matricial.} \end{aligned}$$

19. a.
$$A^2 = \begin{bmatrix} 1 & 1 & 2 \\ 1 & 0 & 1 \\ 2 & 1 & 0 \end{bmatrix}\begin{bmatrix} 1 & 1 & 2 \\ 1 & 0 & 1 \\ 2 & 1 & 0 \end{bmatrix} = \begin{bmatrix} 6 & 3 & 3 \\ 3 & 2 & 2 \\ 3 & 2 & 5 \end{bmatrix}$$
$$A^3 = \begin{bmatrix} 1 & 1 & 2 \\ 1 & 0 & 1 \\ 2 & 1 & 0 \end{bmatrix}\begin{bmatrix} 6 & 3 & 3 \\ 3 & 2 & 2 \\ 3 & 2 & 5 \end{bmatrix} = \begin{bmatrix} 15 & 9 & 15 \\ 9 & 5 & 8 \\ 15 & 8 & 8 \end{bmatrix}$$

20. a. 2 puesto que $(A^2)_{23} = 2$
b. 3 puesto que $(A^2)_{34} = 3$
c. 6 puesto que $(A^3)_{14} = 6$
d. 17 puesto que $(A^3)_{23} = 17$

22. b. *Sugerencia:* Si G es bipartita, entonces sus vértices se pueden particionar en dos conjuntos V_1 y V_2, tal que no hay vértices en V_1 que entre sí estén conectados por un extremo y no existen vértices en V_2 que entre sí se conecten mediante un extremo. En V_1 marque los vértices como $v_1, v_2, \ldots, v_k$ y en V_2 quedan marcados como $v_{k+1}, v_{k+2}, \ldots, v_n$. Ahora veamos en la matriz de G formada de acuerdo al etiquetado de vértices dado.

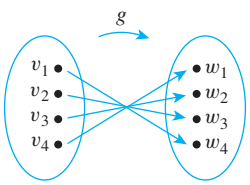
23. b. *Sugerencia:* Consideremos la entrada ij de

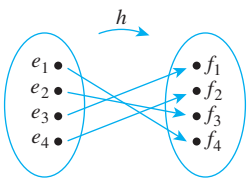
$$\mathbf{A} + \mathbf{A}^2 + \mathbf{A}^3 + \ldots + \mathbf{A}^n.$$

Si G es conexo, entonces dados los vértices v_i y v_j, existe un camino conectando a v_i y a v_j. Si este camino tiene longitud k, entonces por el teorema 10.3.2, la entrada ij de $\mathbf{A}^k$ no es igual a 0. Use los hechos de que todas las entradas de cada potencia de $\mathbf{A}$ son no-negativos y una suma de números no-negativos es positiva si al menos uno de los números es positivo.

Sección 10.4

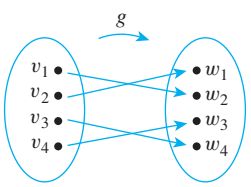
1. Los grafos son isomorfos. Una forma de definir isomorfismo es como sigue:





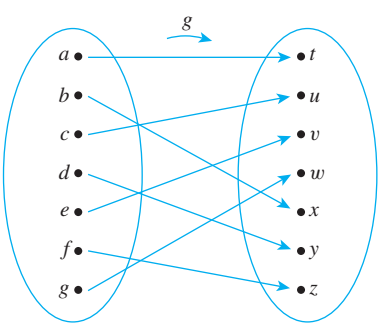
2. Los grafos no son isomorfos. G tiene cinco vértices y G' tiene seis.

6. Los grafos son isomorfos. Un isomorfismo es el siguiente:

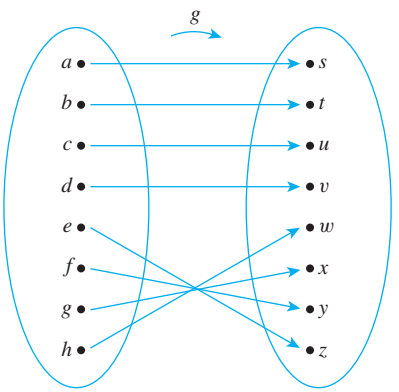


8. Los grafos no son isomorfos. G tiene un bucle simple de longitud 3; G' no.

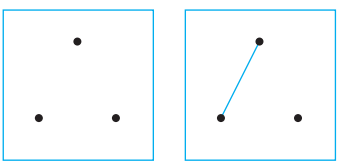
10. Los grafos son isomorfos. Una manera de definir isomorfismo es como sigue:

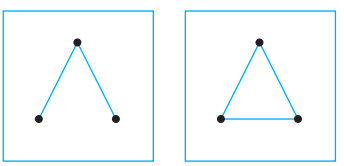


12. a. Esos grafos son isomorfos. El siguiente es un isomorfismo:

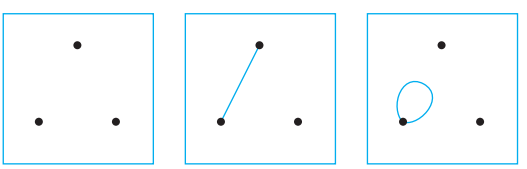


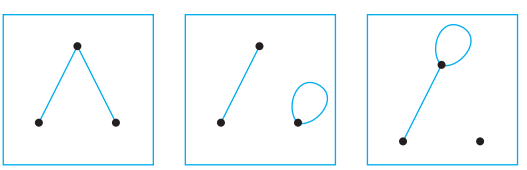
14.

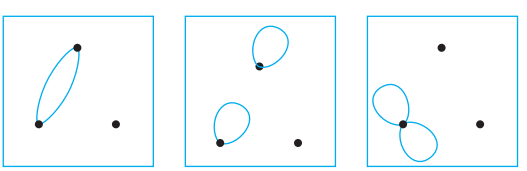




16.

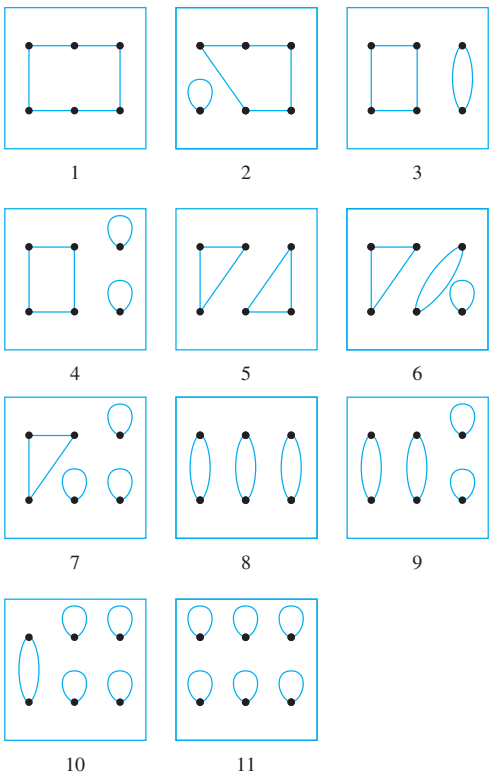






18. *Sugerencia:* Existen 20.

19.



21. *Demostración:* Suponga que G y G' son grafos isomorfos y G tiene n vértices, en donde n es un entero no-negativo. *[Debemos demostrar que G' tiene n vértices.]* Por definición de isomorfismo de grafos, hay una correspondencia uno a uno g: $V(G) \to V(G')$ enviando vértices de G a vértices de G'. Como V $G)$ es un conjunto finito y g es una correspondencia uno a uno, entonces el número de vértices en $V(G')$ es igual al número de vértices en $V(G)$. Así que G' tiene n vértices *[que era lo que se quería demostrar]*.

23. *Demostración:* Suponga que G y G' son grafos isomorfos y G tiene un bucle C de longitud k, en donde k es un entero no-negativo. Aceptemos que C sea $v_0e_1v_1e_2 \ldots e_kv_k$ $(= v_0)$. Por definición de isomorfismo en grafos, existen correspondencias uno a uno g: $V(G) \to V(G')$ y h: $E(G) \to E(G')$ que conservan las funciones extremo-puntos finales en el sentido de que para toda v en $V(G)$ y e en $E(G)$, v es un punto final de $e \Leftrightarrow g(v)$ es un punto extremo de $h(e)$. Aceptemos que C' sea $g(v_0)h(e_1)g(v_1)$ $h(e_2)\ldots$ $h(e_k)g(v_k)(= g(v_0))$. Entonces C' es un bucle de longitud k en G'. La razón es que 1) porque g y h preservan las funciones de extremo-puntos finales, para toda $i = 0, 1,\ldots, k-1$ se tiene que $g(v_i)$ y $g(v_{i+1})$ están incidiendo sobre $h(e_{i+1})$ tal que C' es un camino de $g(v_0)$ a $g(v_0)$ y 2) como C es un bucle, entonces $e_1, e_2,\ldots,e_k$ son distintos y como h es una correspondencia uno a uno, $h(e_1)$, $h(e_2),\ldots$, $h(e_k)$ también son distintos, lo que implica que C' tiene k extremos diferentes. Por tanto, G' tiene un bucle C de longitud k.

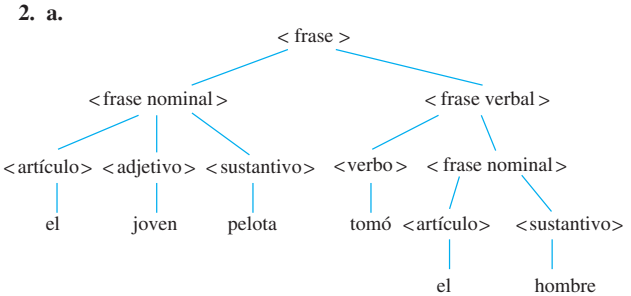
25. *Sugerencia:* Suponga que G y G' son isomorfos y G tiene m vértices de grado k; llamémosles $v_1, v_2,\ldots, v_m$. Como G y G' son isomorfos, existen correspondencias uno a uno g: $V(G) \to V(G')$ y h: $E(G) \to E(G')$. Demuestre que $g(v_1)$, $g(v_2),\ldots, g(v_m)$ son m vértices distintos de G' y cada uno tiene grado k.

27. *Sugerencia:* Suponga que G y G' son isomorfos y G está conexa. Para demostrar que G' está conexa, acepte que w y x son cualesquiera dos vértices de G'. Demuestre que existe un camino conectando a w con x, encontrando un camino que conecte los correspondientes vértices en G.

Sección 10.5

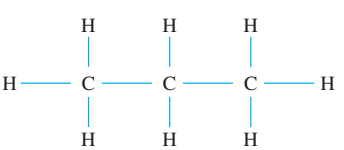
1. a. Matemáticas 110

2. a.



3. *Sugerencia:* La respuesta es $2n - 2$. Para obtener este resultado, use la relación entre el grado total de un grafo y el número de extremos del grafo.

4. a.



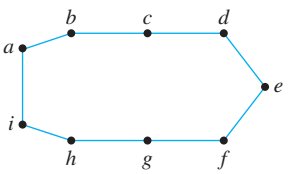
d. *Sugerencia:* Cada átomo de carbono en G está ligado a otros cuatro átomos en G, porque de otra manera un átomo de hidrógeno adicional estaría ligado a éste y esto estaría en contradicción con la suposición de que G tiene el número máximo de átomos de hidrógeno para sus átomos de carbono. También cada átomo de hidrógeno está ligado a exactamente un átomo de carbono en G, porque sino G no estaría conectada.

5. *Sugerencia:* Revise el algoritmo dado en la demostración del lema 10.5.1 para rastrear cuál vértice y extremo fueron seleccionados en el paso 1 (por, digamos, marcándolos como v_0 y e_0). Entonces, después de que se encuentra un vértice de grado 1, retorne a v_0 y busque otro vértice de grado 1 moviéndose sobre la trayectoria partiendo de v_0 iniciando con e_0.

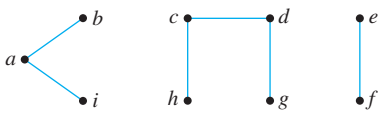
7. a. Vértices internos: v_2, v_3, v_4, v_6
Vértices terminales: v_1, v_5, v_7

8. Cualquier árbol con nueve vértices tiene ocho extremos, no nueve. Así que no existe un árbol con nueve vértices y nueve extremos.

9. Dicho grafo es

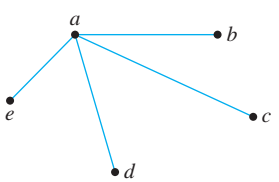


10. Dicho grafo es



11. No existe un árbol con seis vértices y un grado total de 14. Cualquier árbol con seis vértices tiene cinco extremos y así (por el teorema 10.1.1) un grado total de 10, no de 14.

12. Se muestra uno de esos árboles



13. No existe dicho grafo. Por el teorema 10.5.4, un grafo conexo con seis vértices y cinco extremos es un árbol. Entonces ese grafo no puede tener un bucle no-trivial.

14.

22. Sí. Como el grafo es conexo y tiene 12 vértices y 11 extremos, entonces es un árbol debido al teorema 10.5.4. Del lema 10.5.1 se tiene que ésta tiene un vértice de grado 1.

25. Supongamos que fuera un grafo conexo con ocho vértices y seis extremos. Puede ocurrir que el grafo mismo sea un árbol o los extremos podrían eliminarse de sus bucles para obtener un árbol. En cualquier caso, sería un árbol con ocho vértices y seis o menos extremos. Por el teorema 10.5.2, un árbol con ocho vértices tiene siete extremos, pero no seis o menos. Esta contradicción muestra que la suposición es falsa, así que no existe un grafo conexo con ocho vértices y seis extremos.

26. *Sugerencia:* vea la respuesta al ejercicio 25.

27. Sí. Suponga que G es un grafo libre de bucles con diez vértices y nueve extremos. Sean $G_1, G_2, \ldots, G_k$ componentes que estén conectados de G *[Para demostrar que G es conexo, probaremos que* $k = 1$.*]* Cada G_i es un árbol porque cada G_i está conectada y libre de bucles. Para cada $i = 1, 2, \ldots, k$, aceptemos que G_i tenga n_i vértices. Observe que G tiene un total de diez vértices

$$n_1 + n_2 + \cdots + n_k = 10.$$

Por el teorema 10.5.2,

G_1 tiene $n_1 - 1$ extremos,
G_2 tiene $n_2 - 1$ extremos,
$\vdots$
G_k tiene $n_k - 1$ extremos.

Así el número de extremos de G es igual a

$$(n_i - 1) + (n_2 - 1) + \cdots + (n_k - 1)$$
$$= (n_1 + n_2 + \cdots + n_k) - \underbrace{(1 + 1 + \cdots + 1)}_{k \text{ 1's}}$$
$$= 10 - k.$$

Pero se ha dado que G tiene nueve extremos. Entonces $10 - k = 9$, de donde $k = 1$. Por tanto, G sólo tiene una componente conectada, G_1, en consecuencia, G es conexo.

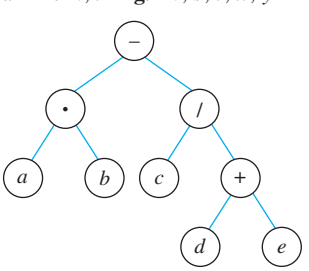
28. *Sugerencia:* vea la respuesta al ejercicio 27.

31. b. *Sugerencia:* existen seis.

Sección 10.6

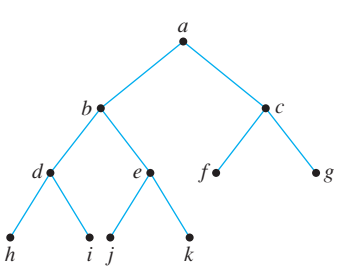
1. a. 3 **b.** 0 **c.** 5 **d.** u, v
e. d **f.** k, l **g.** m, s, t, x, y

3. a.



Los ejercicios 4 y del 8 al 10 tienen otras respuestas además de las que aquí se muestran.

4.

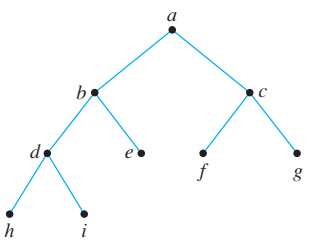


5. No existe un árbol binario completo con las propiedades dadas porque cualquier árbol binario completo con cinco vértices internos tiene seis vértices terminales, no siete.

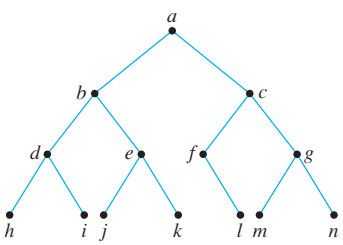
6. Cualquier árbol binario completo con cuatro vértices internos tiene cinco vértices terminales para un total de nueve, no siete, vértices. Entonces no existe un árbol binario completo con las propiedades dadas.

7. No hay un árbol binario completo con 12 vértices porque cualquier árbol binario completo tiene $2k + 1$ vértices, en donde k es el número de vértices internos. Pero $2k + 1$ siempre es impar y 12 es par.

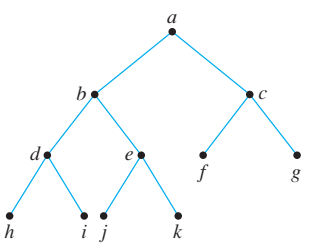
8.



9.



10.

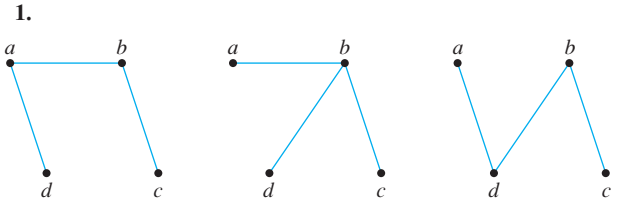


11. No existe un árbol binario que tenga altura 3 y nueve vértices terminales porque cualquier árbol binario de altura 3 tiene a lo más $2^3 = 8$ vértices terminales.

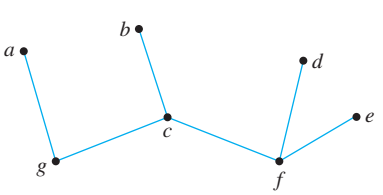
20. a. Altura de un árbol $\geq \log_2 25 \cong 4.6$. La altura de cualquier árbol es un entero, entonces la altura debe ser al menos 5.

Sección 10.7

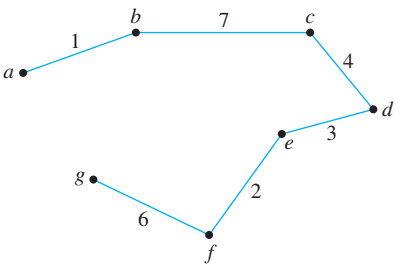
1.



3. Uno de muchos árboles extendidos es como sigue:



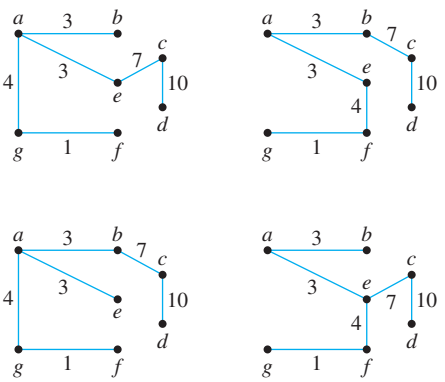
5. Árbol extendido mínimo



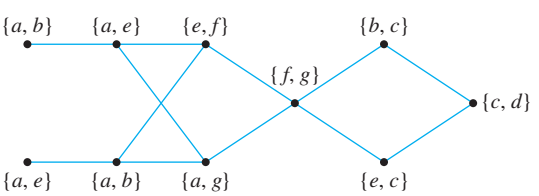
Orden de suma de los extremos:
$\{a, b\}, \{e, f\}, \{e, d\}, \{d, c\}, \{g, f\}, \{b, c\}$

7. Árbol extendido mínimo: como en el ejercicio 5.
Orden de suma de los extremos:
$\{a, \mathrm{b}\}, \{b, c\}, \{c, d\}, \{d, e\}, \{e, f\}, \{f, g\}$

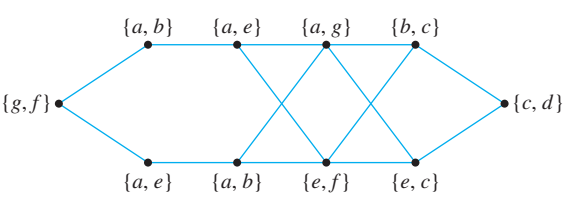
9. Hay cuatro árboles extendidos mínimos:



Cuando se utiliza el algoritmo de Prim, los extremos se suman en cualquiera de los órdenes obtenidos siguiendo una de las ocho trayectorias de izquierda a derecha a través del diagrama que se muestra a continuación.



Cuando se emplea el algoritmo de Kruskal, los extremos se suman en cualquiera de los órdenes obtenidos siguiendo una de las ocho trayectorias de izquierda a derecha en el diagrama que se muestra a continuación.



12. Sean N = Nashville, S = St. Louis, Lv = Louisville, Ch = Chicago, Cn = Cincinnati, D = Detroit, Mw = Milwaukee y Mn = Minneapolis.

Paso	$V(T)$	$E(T)$	F
0	$\{N\}$	$\emptyset$	$\{N\}$
1	$\{N\}$	$\emptyset$	$\{Lv, Mn\}$
2	$\{N, Lv\}$	$\{\{N, Lv\}\}$	$\{Mn, S, Cn, Ch, D, Mw\}$
3	$\{N, Lv, Cn\}$	$\{\{N, Lv\}, \{Lv, Ci\}\}$	$\{Mn, S, Ch, D, Mw\}$
4	$\{N, Lv, Cn, S\}$	$\{\{N, Lv\}, \{Lv, Ci\}, \{Lv, S\}\}$	$\{Mn, Ch, D, Mw\}$
5	$\{N, Lv, Cn, S, Ch\}$	$\{\{N, Lv\}, \{Lv, Ci\}, \{Lv, S\}, \{Lv, Ch\}\}$	$\{Mn, D, Mw\}$
6	$\{N, Lv, Cn, S, Ch, D\}$	$\{\{N, Lv\}, \{Lv, Ci\}, \{Lv, S\}, \{Lv, Ch\}\{Lv, D\}\}$	$\{Mn, Mw\}$
7	$\{N, Lv, Cn, S, Ch, D, Mw\}$	$\{\{N, Lv\}, \{Lv, Ci\}, \{Lv, S\}, \{Lv, Ch\}\{Lv, D\}, \{Ch, Mw\}\}$	$\{Mn\}$
8	$\{N, Lv, Cn, S, Ch, D, Mw, Mn\}$		

Paso	$L(N)$	$L(S)$	$L(Lv)$	$L(Cn)$	$L(Ch)$	$L(D)$	$L(Mw)$	$L(Mn)$
0	**0**	∞	∞	∞	∞	∞	∞	∞
1	0	∞	**151**	∞	∞	∞	∞	695
2	0	393	151	**234**	420	457	499	695
3	0	**393**	151	234	420	457	499	695
4	0	393	151	234	**420**	457	499	695
5	0	393	151	234	420	**457**	494	695
6	0	393	151	234	420	457	**494**	695
7	0	393	151	234	420	457	494	**695**

Así la trayectoria más corta de Nashville a Minneapolis tiene longitud $L(Mn) = 695$ millas.

13.

Paso	$V(T)$	$E(T)$	F	$L(a)$	$L(b)$	$L(c)$	$L(d)$	$L(e)$	$L(z)$
0	$\{a\}$	$\emptyset$	$\{a\}$	**0**	∞	∞	∞	∞	∞
1	$\{a\}$	$\emptyset$	$\{b, d\}$	0	2	∞	**1**	∞	∞
2	$\{a, d\}$	$\{\{a, d\}\}$	$\{b, c, e\}$	0	**2**	6	1	11	∞
3	$\{a, b, d\}$	$\{\{a, d\}, \{a, b\}\}$	$\{c, e\}$	0	2	**5**	1	6	∞
4	$\{a, b, c, d\}$	$\{\{a, d\}, \{a, b\}, \{b, c\}\}$	$\{e, z\}$	0	2	5	1	**6**	13
5	$\{a, b, c, d, e\}$	$\{\{a, d\}, \{a, b\}, \{b, c\}, \{c, e\}\}$	$\{z\}$	0	2	5	1	6	**8**
6	$\{a, b, c, d, e, z\}$	$\{\{a, d\}, \{a, b\}, \{b, c\}, \{c, e\}, \{e, z\}\}$							

Entonces la trayectoria más corta de a a z tiene longitud $L(z) = 8$.

18. b. *Demostración:* Suponga que no. Aceptemos que para algún árbol T, u y v son vértices distintos de T y P_1 y P_2 son dos trayectorias distintas uniendo a u con v. *[Debemos deducir una contradicción. De hecho, probaremos que T contiene un bucle.]* Dejemos que P_1 sea denotada por $u = v_0, v_1, v_2, \ldots, v_m = v$ y que P_2 sea representada por $u = w_0, w_1, w_2, \ldots, w_n = v$. P_1 y P_2 son distintos y T no tiene extremos paralelos, entonces en algún punto la secuencia de vértices en P_1 debe alejarse de la secuencia de vértices en P_2. Sea i el mínimo entero tal que $v_i \neq w_i$. Entonces $v_{i-1} = w_{i-1}$. Aceptemos que j y k sean los mínimos enteros mayores que i tal que $v_j = w_k$. (Existen tales enteros porque $v_m = w_n$). Por tanto

$$v_{i-1}v_i v_{i+1} \ldots v_j (= w_k) w_{k-1} \ldots w_i w_{i-1} (= v_{i-1})$$

es un bucle en T. La existencia de tal bucle contradice el hecho de que T es un árbol. Así que la suposición debe ser falsa. Es decir, dado cualquier árbol con vértices u y v, existe una única trayectoria que une a u con w.

20. *Demostración:* Suponga que G es un grafo conexo, T es un subgrafo de G libre de bucles y si cualquier extremo e de G que no esté en T se agrega a T, entonces el grafo resultante contiene un bucle. Acepte que T no es un árbol extendido para G. *[Debemos obtener una contradicción.]*

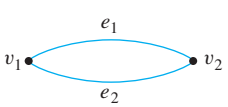
Caso 1 (T no está conectada): En este caso hay vértices u y v en T tales que no existe una trayectoria en T que una a u con v. G está conectada, entonces hay un camino en G de u a v, así que, por el lema 10.2.1, existe una trayectoria en G de u a v. Dejemos que $e_1, e_2, \ldots, e_k$ sean los extremos de esta trayectoria que no están en T. Cuando esos extremos se agregan a T, el resultado es un grafo T' en la que u y v están conectados por una trayectoria. Además, por hipótesis, cada uno de los lados e_i, crea un bucle

cuando se agregan a T. Ahora en T' eliminemos esos extremos uno por uno. Por el mismo argumento empleado en la prueba del lema 10.5.3, esa eliminación deja a u y v conectados porque cada e_i es un extremo de un bucle cuando se agregan a T. Así que, después de que todos los e_i se han eliminado, u y v permanecen conectados. Pero esto contradice el hecho de que en T no existe camino de u a v.

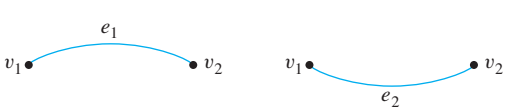
Caso 2 (T es conexo): En este caso, como T no es un árbol extendido y está libre de bucles, entonces existe un vértice v en G tal que v no está en T. *[Porque si T estuviera conectada, libre de bucles y que contiene cada vértice de G, entonces T sería un árbol extendido para G.]* G es conexo, Por tanto v está aislado. Entonces existe un extremo e en G con v como punto final. Dejemos que T' sea el grafo obtenido de T agregando a e y a v. *[Observe que e no estaba en T porque si así fuera, entonces su punto final v también estaría en T, lo que no es verdadero.]* Entonces T' contiene un bucle porque, por hipótesis, la suma de cualquier extremo a T crea un bucle. T' también está conectada porque T lo está y porque cuando e se agrega a T, e se convierte en parte de un bucle en T'. La eliminación de un extremo en un bucle no desconecta una gráfica, así si e es borrado de T' el resultado es un grafo conexo. Pero el grafo resultante contiene a v, lo que significa que existe un extremo en T conectando a v con otro vértice en T. Esto implica que v está en T *[porque ambos puntos finales de un extremo en un grafo deben ser parte del conjunto de vértices del grafo]*, lo que contradice el hecho de que v no está en T.

Así, en cualquier caso, la suposición de que T no es árbol extendido conduce a una contradicción. Por tanto la suposición es falsa y T es un árbol extendido de G.

21. a. No. *Contraejemplo:* Sea G el siguiente grafo



Entonces G tiene los árboles extendidos que se muestran a continuación.



Esos árboles no tienen extremos en común.

22. *Sugerencia:* Suponga que e está contenido en cada árbol extendido de G y que el grafo obtenido al eliminar e en G está conectada. Dejemos que G' sea el subgrafo de G obtenido al eliminar e y que T' sea un árbol extendido para G'. ¿Cómo está relacionado T' con G'?

24. *Demostración:* Suponga que $w(e') > w(e)$. Forme un nuevo grafo T' sumando e a T y borrando e'. Por el ejercicio 20, la suma de un extremo a un árbol extendido crea un bucle y por el lema 10.5.3, la eliminación de un extremo en un bucle no desconecta a un grafo. En consecuencia, T' también es un árbol extendido para G. Aún más, $w(T') < w(T)$ porque $w(T') = w(T) - w(e') + w(e) = w(T) - (w(e') - w(e)) < w(T)$ *[porque $w(e') > w(e)$, lo que implica que $w(e') - w(e) > 0$]*. Pero esto contradice el hecho de que T es un árbol extendido mínimo para G. Así que la suposición es falsa y entonces $w(e') \leq w(e)$.

25. *Sugerencia:* Suponga que e es un extremo que tiene el más pequeño peso que cualquier otro extremo en G y acepte que T es un árbol extendido mínimo para G que no contiene a e. Crear un nuevo árbol extendido T' agregando e a T y eliminando al otro extremo de T (¿cuál?). Entonces $w(T') < w(T)$.

26. Sí. *Demostración por contradicción:* Suponga que G es un grafo pesado en la que todos los pesos de todos los extremos son distintos y también acepte que G tiene dos diferentes árboles extendidos mínimos T_1 y T_2. Sea e el extremo del mínimo peso que está en uno de los árboles pero no en el otro. Sin pérdida de generalidad, podemos decir que e está en T_1. Agregamos e a T_2 para obtener un grafo G'. Por el ejercicio 19, G' contiene un bucle no-trivial. Al menos otro extremo f de este bucle no está en T_1 porque si no T_1 contendría al bucle completo lo que sería una contradicción para el hecho de que T_1 es un árbol. Ahora f tiene un peso mayor que e porque todos los extremos tienen distintos pesos, f está en T_2 pero no en T_1 y e es el extremo de mínimo peso que está en uno de los árboles pero no en el otro. Elimine f de G' para obtener un árbol T_3. Entonces $w(T_3) < w(T_2)$ porque T_3 es igual que T_2 excepto que contiene a e en lugar de f y $w(e) < w(f)$. En consecuencia, T_3 es un árbol extendido para G de menor peso que T_2. Esto contradice la suposición de que T_2 es un árbol extendido mínimo para G. Así G no puede tener más de un árbol extendido mínimo.

28. La salida será un "bosque extendido mínimo" para el grafo. Y en su contenido estará un árbol extendido mínimo para cada componente conectada del grafo de entrada.

Sección 11.1

1. a. $f(0)$ es positiva.

b. $f(x) = 0$ cuando $x = -2$ y $x = 3$ (aproximadamente)

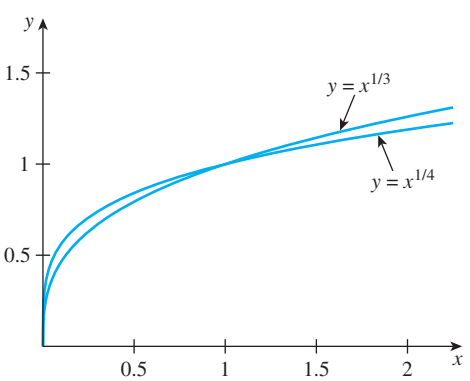
c. $x_1 = -1$ y $x_2 = 2$ (aproximadamente)

d. $x = 1$ o $x = -\frac{1}{2}$ (aproximadamente)

e. crece

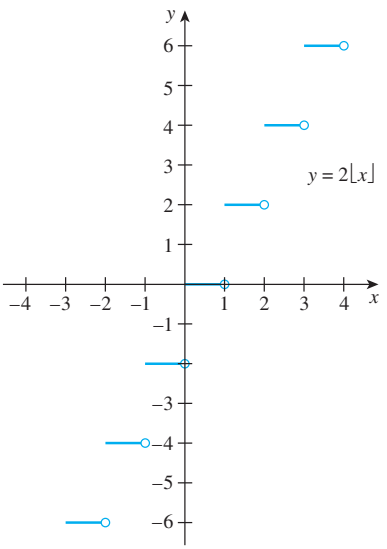
f. decrece

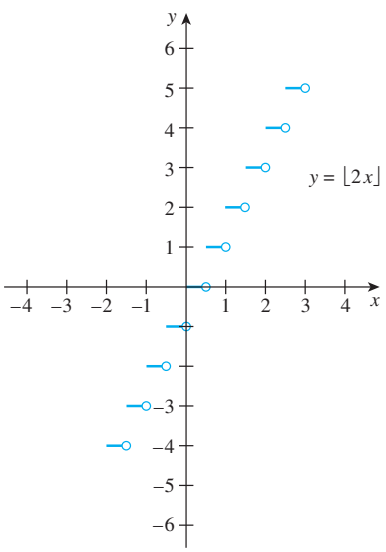
3.



Cuando $0 < x < 1$, $x^{1/3} < x^{1/4}$. Cuando $x > 1$, $x^{1/3} > x^{1/4}$.

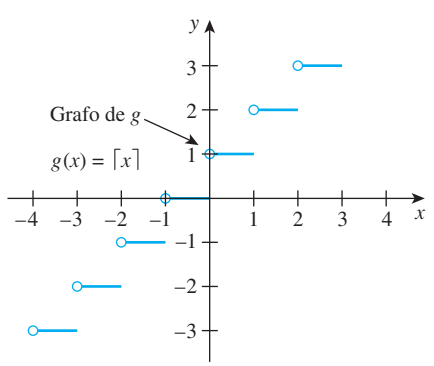
5.





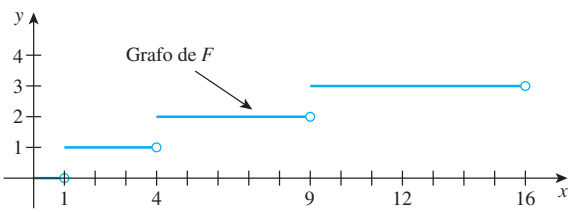
Los grafos muestran que $2[x] \neq [2x]$ para muchos valores de x.

6.



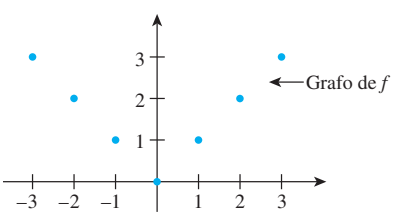
8.

x	$F(x) = \lfloor x^{1/2} \rfloor$
0	0
$\frac{1}{2}$	0
1	1
2	1
3	1
4	2



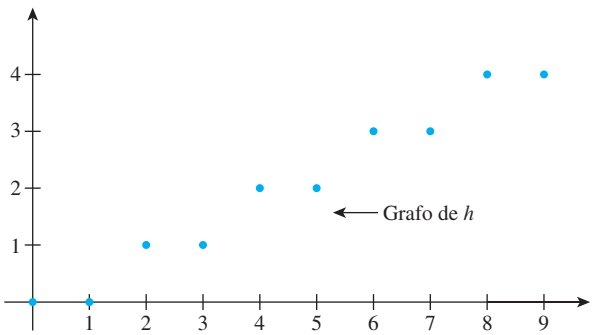
10.

n	$f(n) = \lvert n \rvert$
0	0
1	1
2	2
3	3
−1	1
−2	2
−3	3



12.

n	$h(n) = \left\lfloor \frac{n}{2} \right\rfloor$
0	0
1	0
2	1
3	1
4	2
5	2
6	3
7	3
8	4
9	4



14. f es creciente en los intervalos

$\{x \in \mathbf{R} \mid -3 < x < -2\}$ y

$\{x \in \mathbf{R} \mid 0 < x < 2.5\}$ y f es decreciente en

$\{x \in \mathbf{R} \mid -2 < x < 0\}$ y $\{x \in \mathbf{R} \mid 2.5 < x < 4\}$ (aproximadamente).

15. *Demostración:* Suponga que x_1 y x_2 son números reales dados, pero arbitrariamente elegidos, tales que $x_1 < x_2$. *[Debemos demostrar que* $f(x_1) < f(x_2)$*.]* Como

$$x_1 < x_2$$

entonces $$2x_1 < 2x_2$$

y $$2x_1 - 3 < 2x_2 - 3$$

por las propiedades básicas de las desigualdades. Pero entonces, por definición de f,

$$f(x_1) < f(x_2)$$

[que era lo que se quería demostrar]. Por tanto, f es creciente sobre todo el conjunto de números reales.

17. a. *Demostración:* Suponga que x_1 y x_2 son números reales con $x_1 < x_2 < 0$. *[Debemos demostrar que* $h(x_1) > h(x_2)$*.]* Multiplicamos ambos lados de $x_1 < x_2$ por x_1 para obtener $(x_1)^2 > x_1x_2$ *[por T23 del apéndice A porque* $x_1 < 0$*]* y multiplicamos ambos lados de $x_1 < x_2$ por x_2 para obtener $x_1x_2 > (x_2)^2$ *[por T23 del apéndice A porque* $x_2 < 0$*]*. Por transitividad de orden *[apéndice A, T18]* $(x_2)^2 < (x_1)^2$ y así, por definición de h, $h(x_2) < h(x_1)$.

18. a. *Preliminares:* Si x_1 y x_2 son positivos, entonces por las reglas para manejar desigualdades (vea el apéndice A),

$$\frac{x_1 - 1}{x_1} < \frac{x_2 - 1}{x_2} \Rightarrow x_2(x_1 - 1) < x_1(x_2 - 1)$$

al multiplicar ambos lados por x_1x_2 (que es positivo)

$$\Rightarrow x_1x_2 - x_2 < x_1x_2 - x_1$$

al realizar la multiplicación,

$$\Rightarrow -x_2 < -x_1$$

al restar x_1x_2 en ambos lados

$$\Rightarrow x_2 > x_1$$

al multiplicar por -1.

¿Son reversibles todos estos pasos? ¡Sí!

Demostración: Suponga que x_1 y x_2 son números reales positivos con $x_1 < x_2$. *[Debemos demostrar que* $k(x_1) < k(x_2)$*.]* Entonces

$x_1 < x_2$

$\Rightarrow -x_2 < -x_1$ multiplicando por -1

$\Rightarrow x_1x_2 - x_2 < x_1x_2 - x_1$ sumando x_1x_2 en ambos lados

$\Rightarrow x_2(x_1 - 1) < x_1(x_2 - 1)$ factorizando ambos lados

$\Rightarrow \dfrac{x_1 - 1}{x_1} < \dfrac{x_2 - 1}{x_2}$ dividiendo ambos ladosentre el número positivo x_1x_2

$\Rightarrow k(x_1) < k(x_2)$ por definición de k.

[Que era lo que se quería demostrar.]

19. *Demostración:* Suponga $f: \mathbf{R} \to \mathbf{R}$ creciente. *[Debemos demostrar que f es inyectiva. En otras palabras, debemos demostrar que para todos los números reales* x_1 *y* x_2*, si* $x_1 \neq x_2$ *entonces* $f(x_1) \neq f(x_2)$*.]* Suponga que x_1 y x_2 son números reales con $x_1 \neq x_2$. Por la ley de tricotomía *[apéndice A, T17]* $x_1 < x_2$, o $x_1 > x_2$. En el caso $x_1 < x_2$, como f es creciente, $f(x_1) < f(x_2)$ y así $f(x_1) \neq f(x_2)$. Similarmente, cuando $x_1 > x_2$, entonces $f(x_1) > f(x_2)$ y por tanto $f(x_1) \neq f(x_2)$. Así en cualquier caso, $f(x_1) \neq f(x_2)$ *[que era lo que se quería demostrar]*.

21. a. *Demostración:* Suponga que u y v son números reales no-negativos con $u < v$. *[Debemos demostrar que* $f(u) < f(v)$*.]* Observe que $v = u + h$ para algún número real positivo h. Sustituyendo y por el teorema binomial,

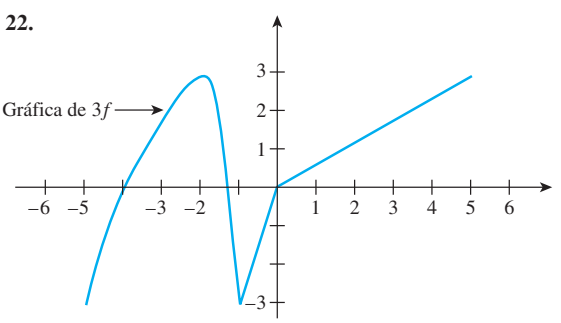
$$\begin{aligned} v^m &= (u + h)^m \\ &= u^m + \left[\binom{m}{1}u^{m-1}h + \binom{m}{2}u^{m-2}h^2 + \cdots \right. \\ &\qquad \left. + \binom{m}{m-1}uh^{m-1} + h^m\right]. \end{aligned}$$

La suma entre corchetes es positiva porque $u \geq 0$ y $h > 0$ y una suma de términos no-negativos que incluye al menos un término positivo es positiva. Entonces

$$v^m = u^m + \text{un número positivo,}$$

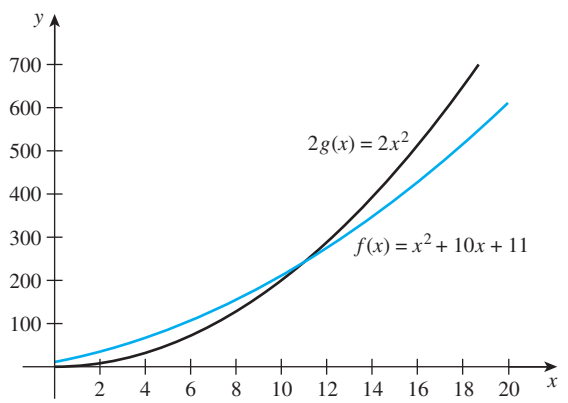
y así $f(u) = u^m < v^m = f(v)$ *[que era lo que se quería demostrar]*.

22.



24. *Demostración:* Suponga que f es una función valuada en los reales, de una variable real y es decreciente sobre un conjunto S y M es cualquier número real positivo. *[Debemos demostrar que Mf es decreciente en S. En otras palabras, debemos demostrar que para todo x_1 y x_2 en S, si $x_1 < x_2$ entonces $(Mf)(x_1) > (Mf)(x_2)$.]* Suponga que x_1 y x_2 están en S con $x_1 < x_2$. Como f es decreciente en S, entonces $f(x_1) > f(x_2)$ y al ser M positivo resulta que $Mf(x_1) > Mf(x_2)$ *[porque cuando ambos lados de una desigualdad se multiplican por un número positivo, la dirección de la desigualdad queda inalterada]*. Por definición de Mf se tiene que $(Mf)(x_1) > (Mf)(x_2)$ *[que era lo que se quería demostrar]*.

27. Para encontrar la respuesta algebraicamente, resuelva para x la ecuación $2x^2 = x^2 + 10x + 11$. Restando x^2 en ambos lados se obtiene $x^2 - 10x - 11 = 0$ y ya sea factorizando $x^2 - 10x - 11 = (x - 11)(x + 1)$ o empleando la fórmula cuadrática da $x = 11$ (porque $x > 0$). Obtenga una respuesta aproximada con una calculadora graficadora, dibuje $f(x) = x^2 + 10x + 11$ y $2g(x) = 2x^2$ para $x > 0$, como se muestra en la figura y encuentre que $2g(x) > f(x)$ cuando $x > 11$ (aproximadamente). Puede tener solamente una respuesta aproximada mediante la calculadora porque ésta maneja valores sólo hasta determinada exactitud de un número finito de lugares decimales.



Sección 11.2

1. a. $\forall$ números reales positivos a y A, existe $x > a$ tal que $A \mid g(x) \mid > \mid f(x) \mid$

b. No importa qué números reales positivos a y A pudieran ser elegidos, siempre es posible encontrar un número x mayor que a con la propiedad $A \mid g(x) \mid > \mid f(x) \mid$.

4. $5x^8 - 9x^7 + 2x^5 + 3x - 1$ es $O(x^8)$

5. $\dfrac{(x^2 - 1)(12x + 25)}{3x^2 + 4}$ es $\Theta(x)$

6. $\dfrac{(x^2 - 7)^2(10x^{1/2} + 3)}{x + 1}$ es $\Omega(x^{7/2})$

10. *Demostración:* Suponga que f y g son funciones valuadas en los reales, de una variable real, que están definidas sobre el mismo conjunto de números reales no-negativos y acepte que $g(x)$ es $O(f(x))$. Por definición de la O-notación, existen números reales positivos b y B tales que $\mid g(x) \mid \leq B \mid f(x) \mid$ para todos los números reales $x > b$. Divida ambos lados de la desigualdad por B para obtener $\frac{1}{B}\mid g(x)\mid \leq \mid f(x)\mid$. Sean $A = \frac{1}{B}$ y $a = b$. Entonces $A \mid g(x) \mid \leq \mid f(x) \mid$ para todos los números reales $x > a$ y así, por definición de la Ω-notación, $f(x)$ es $\Omega(g(x))$.

12. *Demostración:* Suponga que f, g, h y k son funciones valuadas en los reales, de una variable real, definidas sobre el mismo conjunto D de números reales no-negativos y acepte que $f(x)$ es $O(h(x))$ y $g(x)$ es $O(k(x))$. Por definición de la O-notación, existen números reales positivos b_1, B_1, b_2 y B_2, tales que $\mid f(x) \mid \leq B_1 \mid h(x) \mid$ para todos los números reales $x > b_1$ y $\mid g(x) \mid \leq B_2 \mid k(x) \mid$ para todos los números reales $x > b_2$. Para cada x en D, definimos $G(x) =$ máx($\mid h(x) \mid$, $\mid k(x) \mid$) y sea $b =$ máx(b_1, b_2) con $B = B_1 + B_2$. Observe que la desigualdad del triángulo para el valor absoluto (teorema 4.4.6) implica que

$$|f(x) + g(x)| \leq |f(x)| + |g(x)|$$

para todos los números x en D. Suponga que $x > b$. Entonces como b es mayor que b_1 y b_2,

$$|f(x)| \leq B_1|h(x)| \quad \text{y} \quad |g(x)| \leq B_2|h(x)|,$$

así, sumando las desigualdades (apéndice A, T26), obtenemos

$$|f(x)| + |g(x)| \leq B_1|h(x)| + B_2|k(x)|.$$

Entonces, por la ley transitiva para desigualdades (apéndice A, T18),

$$|f(x) + g(x)| \leq B_1|h(x)| + B_2|k(x)|.$$

Ahora bien, como cada valor de $G(x) = \mid G(x) \mid$ es mayor o igual que $\mid h(x) \mid$ y $\mid k(x) \mid$,

$$B_1|h(x)| + B_2|k(x)| \leq B_1|G(x)| + B_2|G(x)| \leq (B_1 + B_2)|G(x)|.$$

Así que, otra vez por transitividad y $B = B_1 + B_2$,

$|f(x) + g(x)| \leq B|G(x)|$ para todos los números reales $x > b$.

Por tanto, por definición de la O-notación, $f(x) + g(x)$ es $O(G(x))$.

14. *Inicio de demostración:* Suponga que f, g, h y k son funciones valuadas en los reales, de una variable real, definidas sobre el mismo conjunto D de números reales no-negativos y acepte que $f(x)$ es $O(h(x))$ y $g(x)$ es $O(k(x))$. Por definición de la O-notación, existen números reales positivos b_1, B_1, b_2 y B_2 tales que $\mid f(x) \mid \leq B_1 \mid h(x) \mid$ para todos los números reales $x > b_1$ y $\mid g(x) \mid \leq B_2 \mid k(x) \mid$ para todos los números reales $x > b_2$. Sean $B = B_1B_2$ y $b =$ máx(b_1, b_2).

15. b. *Sugerencia:* Por las leyes de los exponentes, $x^{n-m} = \dfrac{x^n}{x^m}$. Así si $x^{n-m} > 1$, entonces $n\,\dfrac{x^n}{x^m} > 1$.

16. a. Para todos los números reales $x > 1$, $x^2 + 15x + 4 \geq 0$ porque todos los términos son no-negativos. Sumando x^2 en ambos miembros se obtiene $2x^2 + 15x + 4 \geq x^2$. Por la no-negatividad de todos los términos cuando $x > 1$, los signos de valor absoluto se pueden agregar en ambos lados de la desigualdad. Así $\mid x^2 \mid \leq \mid 2x^2 + 15x + 4 \mid$ para todos los números reales $x > 1$.

b. Para todos los números reales $x > 1$,

$$|2x^2 + 15x + 4| = 2x^2 + 15x + 4 \quad \text{porque } 2x^2 + 15x + 4 \text{ es positivo (porque } x > 1)$$
$$\Rightarrow |2x^2 + 15x + 4| \le 2x^2 + 15x^2 + 4x^2 \quad \text{porque } x > 1, \text{ entonces } x < x^2 \text{ y } 1 < x^2$$
$$\Rightarrow |2x^2 + 15x + 4| \le 21x^2 \quad \text{porque } 2 + 15 + 4 = 21$$
$$\Rightarrow |2x^2 + 15x + 4| \le 21|x^2| \quad \text{porque } x^2 \text{ es positiva.}$$

c. Sean $A = 1$ y $a = 1$. Entonces por el inciso *a*), $A\,|\,x^2\,| \le |\,2x^2 + 15x + 4\,|$ para todos los números reales $x > a$ y así, por definición de la Ω-notación, $2x^2 + 15x + 4$ es $\Omega(x^2)$. Sea $B = 21$ y $b = 1$. Entonces, por el inciso *b*), $|\,2x^2 + 15x + 4\,| \le B\,|\,x^2\,|$ para todo número real $x > b$ y así, por definición de O-notación, $2x^2 + 15x + 4$ es $O(x^2)$.

d. Sean $k = 1$, $A = 1$ y $B = 21$. Por los incisos *a*) y *b*), para todos los números reales $x > k$,

$$A|x^2| \le |2x^2 + 15x + 4| \le B|x^2|$$

y así, por definición de Θ-notación, $2x^2 + 15x + 4$ es $\Theta(x^2)$. En otras palabras, $2x^2 + 15x + 4$ tiene orden x^2. (Alternativamente, podría usarse el teorema 11.2.1(1) para obtener este resultado.)

18. Primero observe que para todos los números reales $x > 1$, $4x^3 + 65x + 30 \ge 0$ porque todos los términos son no-negativos. Sumando x^3 en ambos lados da $5x^3 + 65x + 30 \ge x^3$. Por la no-negatividad de los términos cuando $x > 1$, los signos de valor absoluto pueden agregarse en ambos lados de la desigualdad para obtener $|\,x^3\,| \le |\,5x^3 + 65x + 30\,|$ para todos los números reales $x > 1$. Sean $a = 1$ y $A = 1$. Entonces $A\,|\,x^3\,| \le |\,5x^3 + 65x + 30\,|$ (*) para todos los números reales $x > a$.

Segundo, observe que cuando $x > 1$,

$$|5x^3 + 65x + 30| \le 5x^3 + 65x + 30 \quad \text{porque todos los términos son positivos debido a que } x > 1.$$
$$\Rightarrow |5x^3 + 65x + 30| \le 5x^3 = 65x^3 + 30x^3 \quad \text{porque como } x > 1, \text{ entonces } 65x \le 65x^3 \text{ y } 30 \le 30x^3$$
$$\Rightarrow |5x^3 + 65x + 30| \le 100x^3 \quad \text{porque } 5 + 65 + 30 = 100$$
$$\Rightarrow |5x^3 + 65x + 30| \le 100|x^3| \quad \text{porque } x^3 \text{ es positivo ya que } x > 1.$$

Sean $b = 1$ y $B = 100$. Entonces $|\,5x^3 + 65x + 30\,| \le B\,|\,x^3\,|$ (**) para todos los números reales $x > b$.

Sea $k = \text{máx}(a, b)$. Juntando las desigualdades (*) y (**) se obtiene para todos los números reales $x > k$,

$$A\,|\,x^3\,| \le |\,5x^3 + 65x + 30\,| \le B\,|\,x^3\,|.$$

Así que, por definición de la Θ-notación, $5x^3 + 65x + 30$ es $\Theta(x^3)$; en otras palabras, $5x^3 + 65x + 30$ tiene orden x^3.

20. a. Por definición de techo, para cualquier número real x, $\lceil x^2 \rceil$ es el entero n tal que $n - 1 < x^2 \le n$ y así, sustituyendo, $x^2 \le \lceil x^2 \rceil$. Como $x > 1$, entonces son positivos ambos lados de la desigualdad, así $|x^2| \le \big|\lceil x^2 \rceil\big|$.

b. Como en el inciso *a*), $\lceil x^2 \rceil$ es un entero n tal que $n - 1 < x^2 \le n$. Sumando 1 en todas las partes de esta desigualdad se obtiene $n < x^2 + 1 \le n + 1$, así $\lceil x^2 \rceil < x^2 + 1$. Por tanto, si x es cualquier número real x con $x > 1$, entonces

$$\big|\lceil x^2 \rceil\big| \le \lceil x^2 \rceil \quad \text{porque } \lceil x^2 \rceil \text{ es positivo}$$
$$\Rightarrow \big|\lceil x^2 \rceil\big| \le x^2 + 1 \quad \text{por el argumento de arriba}$$
$$\Rightarrow \big|\lceil x^2 \rceil\big| \le x^2 + x^2 \quad \text{porque } 1 < x^2 \text{ ya que } x > 1$$
$$\Rightarrow \big|\lceil x^2 \rceil\big| \le 2x^2$$
$$\Rightarrow \big|\lceil x^2 \rceil\big| \le 2\,|x^2| \quad \text{porque } x^2 \text{ es positivo.}$$

c. Sean $A = 1$ y $a = 1$. Entonces, por el inciso *a*), $|x^2| \le A|\lceil x^2 \rceil|$ para todos los números reales $x > a$ y así, por definición de la Ω-notación, $\lceil x^2 \rceil$ es $\Omega(x^2)$.

Sean $B = 2$ y $b = 1$. Entonces, por el inciso *b*), $|x^2| \le B\,\big|\lceil x^2 \rceil\big|$ para todos los números reales $x > b$ y así, por definición de la O-notación, $\lceil x^2 \rceil$ es $O(x^2)$.

d. Concluimos que $\lceil x^2 \rceil$ es $\Theta(x^2)$ por el inciso *c*) y el teorema 11.2.1(1). Alternativamente, podemos emplear los resultados de los incisos *a*) y *b*), dejando que $k = \text{máx}(a, b)$, para obtener el resultado de que para todos los números reales $x > k$,

$$A\,|x^2| \le \big|\lceil x^2 \rceil\big| \le B\,|x^2|$$

y concluir directamente de la definición de la Θ-notación que $\lceil x^2 \rceil$ es $\Theta(x^2)$.

22. a. Para todos los números reales > 1,

$$|7x^4 - 95x^3 + 3| \le |7x^4| + |95x^3| + |3| \quad \text{por la desigualdad del triángulo}$$
$$\Rightarrow |7x^4 - 95x^3 + 3| \le 7x^4 + 95x^3 + 3 \quad \text{porque todos los términos son positivos ya que } x > 1$$
$$\Rightarrow |7x^4 - 95x^3 + 3| \le 7x^4 + 95x^4 + 3x^4 \quad \text{porque } x > 1 \text{ implica que } x^3 \le x^4 \text{ y } 1 \le x^4$$
$$\Rightarrow |7x^4 - 95x^3 + 3| \le 105|x^4| \quad \text{porque } 7 + 95 + 3 = 105 \text{ y } x^4 > 0.$$

b. $7x^4 - 95x^3 + 3$ es $O(x^4)$

25. *Sugerencia:* Use un argumento por contradicción similar al empleado en el ejemplo 11.2.8.

26. *Demostración:* Suponga que $a_0, a_1, a_2, \ldots, a_n$ son números reales con $a_n \ne 0$. Por la desigualdad del triángulo generalizada,

$$|a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0| \le |a_n x^n| + |a_{n-1}x^{n-1}| + \cdots + |a_1 x| + |a_0|,$$

y como el valor absoluto de un producto es el producto de los valores absolutos (ejercicio 44, sección 4.4)

$$|a_n x^n| + |a_{n-1}x^{n-1}| + \cdots + |a_1 x| + |a_0| \le |a_n||x^n| + |a_{n-1}||x^{n-1}| + \cdots + |a_1||x| + |a_0|.$$

Además, cuando $x > 1$, la propiedad (11.2.1) implica que

$$x^n \le x^n, \quad x^{n-1} \le x^n, \ldots, x^2 \le x^n, \quad x \le x^n, \quad 1 \le x^n$$

y también $x^n = |x^n|$ porque $x > 1$. Así

$$\begin{aligned}|a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0| &\le |a_n||x^n| + |a_{n-1}||x^n| + \cdots + |a_1||x^n| + |a_0||x^n| \\ &\le (|a_n| + |a_{n-1}| + \cdots + |a_1| + |a_0|)|x^n|.\end{aligned}$$

Sean $b = 1$ y $B = |a_n| + |a_{n-1}| + \cdots + |a_1| + |a_0|$. Entonces para todos los números reales $x > b$,

$$|a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0| \le B|x^n|$$

y así, por definición de la O-notación,

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \text{ is } O(x^n).$$

28. Sea $a = \left(\frac{95+3}{7}\right)\cdot 2 = 28$ y sea $A = \frac{7}{2}$. Si $x > a$, entonces

$$\begin{aligned}
& x \ge \left(\frac{95+3}{7}\right)\cdot 2 \\
\Rightarrow \quad & x \ge \frac{95}{7}\cdot 2 + \frac{3}{7}\cdot 2 \\
\Rightarrow \quad & x \ge \frac{95}{7}\cdot 2 + \frac{3}{7}\cdot 2\frac{1}{x^3} \\
& \qquad \text{porque } \tfrac{1}{x^3} < 1 \text{ ya que } x > 28 \\
\Rightarrow \quad & \frac{7}{2}x^4 \ge 95x^3 + 3 \\
& \qquad \text{multiplicando ambos lados por } \tfrac{7x^3}{2} \\
\Rightarrow \quad & \left(7 - \frac{7}{2}\right)x^4 \ge 95x^3 - 3 \\
& \qquad \text{porque } 95x^3 + 3 \ge 95x^3 - 3 \\
& \qquad \text{y } \ 7 - \tfrac{7}{2} = \tfrac{7}{2} \\
\Rightarrow \quad & 7x^4 - \frac{7}{2}x^4 \ge 95x^3 - 3 \\
& \qquad \text{efectuando la multiplicación,} \\
\Rightarrow \quad & 7x^4 - 95x^3 + 3 \ge \frac{7}{2}x^4 \\
& \qquad \text{sumando } \tfrac{7}{2}x^4 - 95x^3 + 3 \\
& \qquad \text{en ambos lados} \\
\Rightarrow \quad & 7x^4 - 95x^3 + 3 \ge Ax^4 \\
& \qquad \text{porque } \ A = \tfrac{7}{2} \\
\Rightarrow \quad & |7x^4 - 95x^3 + 3| \ge A|x^4| \\
& \qquad \text{porque ambos lados son no-negativos.}
\end{aligned}$$

Así que, por definición de la Ω-notación, $7x^4 - 95x^3 + 3$ es $\Omega(x^4)$.

31. Por el ejercicio 22, $7x^4 - 95x^3 + 3$ es $O(x^4)$ y por el ejercicio 28, $7x^4 - 95x^3 + 3$ es $\Omega(x^4)$. Así, por el teorema 11.2.1(1), $7x^4 - 95x^3 + 3$ es $\Theta(x^4)$.

34. $\frac{x+1)(x-2)}{4} = \frac{x^2-x-2}{4} = \frac{1}{4}x^2 - \frac{1}{4}x - \frac{1}{2}$ es $\Theta(x^2)$

por el teorema sobre órdenes polinomiales.

37. $\frac{n(n+1)(2n+1)}{6} = \frac{2n^3+3n^2+n}{6} = \frac{1}{3}n^3 + \frac{1}{2}n^2 + \frac{1}{6}n$,

que es $\Theta(n^3)$ por el teorema sobre órdenes polinomiales.

40. Por el ejercicio 10 de la sección 5.2, $1^2 + 2^2 + 3^2 + \ldots + n^2 = \frac{n(n+1)(2n+1)}{6}$ y, por el ejercicio 37 anterior $\frac{n(n+1)(2n+1)}{6}$ es $\Theta(n^3)$. Así $1^2 + 2^2 + 3^2 + \cdots + n^2$ es $\Theta(n^3)$.

42. Por el teorema 5.2.2, $2 + 4 + 6 + \cdots + 2n = 2\left(\frac{n(n+1)}{2}\right) = n^2 + n$ y por el teorema sobre órdenes polinomiales, $n^2 + n$ es $\Theta(n^2)$. Así $2 + 4 + 6 + \cdots + 2n$ es $\Theta(n^2)$.

44. Por cálculo directo o por el teorema 5.1.1, $\sum_{i=1}^{n}(4i - 9) = 4\sum_{i=1}^{n} i - \sum_{i=1}^{n} 9 = 4\left(\frac{n(n+1)}{2}\right) - 9n$. La última igualdad es válida porque del teorema 5.2.2 y el hecho de que $\sum_{i=1}^{n} 9 = 9 + 9 + \cdots + 9$ (sumandos n) $= 9n$.

Entonces $4\left(\frac{n(n+1)}{2}\right) - 9n = 2n^2 + 2n - 9n = 2n^2 - 7n$ y así $\sum_{i=1}^{n}(4i - 9) = 2n^2 - 7n$. Pero $2n^2 - 7n$ es $\Theta(n^2)$ por el teorema sobre órdenes polinomiales. Así $\sum_{i=1}^{n}(4i - 9)$ es $\Theta(n^2)$.

46. *Sugerencia:* Use el resultado del ejercicio 13 de la sección 5.2

48. *Sugerencias:*

a. $$\frac{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0}{a_n x^n}$$
$$= 1 + \frac{a_{n-1}}{a_n}\cdot\frac{1}{x} + \frac{a_{n-2}}{a_n}\cdot\frac{1}{x^2} + \cdots + \frac{a_1}{a_n}\cdot\frac{1}{x^{n-1}} + \frac{a_0}{a_n}\cdot\frac{1}{x^n}.$$

b. $\lim_{n\to\infty} f(x) = L$ significa que dado cualquier número real $\varepsilon > 0$, existe un número real $M > 0$ tal que $L - \varepsilon < f(x) < L + \varepsilon$ para todos los números $x > M$. Aplique la definición de límite al resultado del inciso *a*), usando $\varepsilon = \frac{1}{2}$.

49. **a.** Sean f, g y h funciones de $\mathbf{R}$ a $\mathbf{R}$ y suponga que $f(x)$ es $O(h(x))$ y $g(x)$ es $O(h(x))$. Entonces existen números reales b_1, b_2, B_1 y B_2 tales que $|f(x)| \le B_1|h(x)|$ para todo $x > b_1$ y $|g(x)| \le B_2|h(x)|$ para todo $x > b_2$. Sea $B = B_1 + B_2$, con b el mayor de b_1 y b_2. Entonces, para todo $x > b$,

$$\begin{aligned}
& |f(x) + g(x)| < |f(x)| + |g(x)| \\
& \qquad \text{por la desigualdad del triángulo} \\
\Rightarrow \quad & |f(x) + g(x)| \le B_1|h(x)| + B_2|h(x)| \\
& \qquad \text{por hipótesis} \\
\Rightarrow \quad & |f(x) + g(x)| \le (B_1 + B_2)|h(x)| \\
& \qquad \text{por álgebra} \\
\Rightarrow \quad & |f(x) + g(x)| \le B|h(x)| \quad \text{porque } \ B = B_1 + B_2.
\end{aligned}$$

Así que, por definición de la O-notación $f(x) + g(x)$ es $O(h(x))$.

Así que, por definición de la O-notación, $f(x) + g(x)$ es $O(h(x))$.

b. Por el ejercicio 15, para toda $x > 1$, $x^2 < x^4$. Así que $|x^2| \le 1\cdot|x^4|$ para toda $x > 1$. Entonces, por definición de la O-notación, x^2 es $O(x^4)$. También, $|x^4| \le 1\cdot|x^4|$ para toda x y así x^4 es $O(x^4)$. Del inciso *a*) se tiene que $x^2 + x^4$ es $O(x^4)$.

50. **d.** *Sugerencia:* Si p, q y s son enteros positivos, r es un entero no-negativo y $\frac{p}{q} > \frac{r}{s}$, entonces $ps > qr$ y así $ps - qr > 0$.

Además, $\frac{x^{p/q}}{x^{r/s}} = x^{(p/q - r/s)} = x^{(pq-rs)/qs}$. Aplique el inciso *c*) a $x^{1/qs}$ y use el hecho de que $ps - qr$ es un entero y $ps - qr > 0$ para hacer uso del resultado del ejercicio 15.

51. Por el inciso *a*) del ejercicio 50, para toda $x > 1$, $x \le x^{4/3}$ y $1 = x^0 \le x^{4/3}$. Así que, por definición de la O-notación (ya que todas las expresiones son positivas), x es $O(x^{4/3})$ y 1 es $O(x^{4/3})$. También, por el ejercicio 13, $x^{4/3}$ es $O(x^{4/3})$. Por el inciso *c*) del ejercicio 49, entonces, $-15x = (-15)x$ es $O(x^{4/3})$ y $7 = 7 \cdot 1$ es $O(x^{4/3})$. Se tiene, por el inciso *a*) del ejercicio 49 (aplicado dos veces), que $4x^{4/3} - 15x + 7 = 4x^{4/3} + (-15x) + 7$ es $O(x^{4/3})$.

53. *Sugerencia:* La demostración es similar a la solución en el ejemplo 11.2.8. (Elegir un número real x tal que $x > B^{1/(r-s)}$ $x > 1$ y $x \ge b$).

54. $f(x) = \dfrac{\sqrt{x}(3x+5)}{2x+1} = \dfrac{3x^{3/2} + 5x^{1/2}}{2x+1}$. El numerador de $f(x)$ es una suma de potencias racionales con la potencia más alta $3/2$ y el denominador es una suma de potencias racionales con la potencia más alta 1. Como $3/2 - 1 = 1/2$, el teorema 11.2.4 implica que $f(x)$ es $\Theta(x^{1/2})$.

57. **a.** *Demostración (por inducción matemática):* Dejemos que la propiedad $P(n)$ sea la desigualdad

$$\sqrt{1} + \sqrt{2} + \sqrt{3} + \cdots + \sqrt{n} \le n^{3/2}.$$

Demostración de que P(1) es verdadero:

Cuando $n = 1$, el lado izquierdo de la desigualdad es 1 y el lado derecho es $1^{3/2}$, que también es 1. Así $P(1)$ es verdadero.

Demostración de que para todos los enteros k ≥ 1, si P(k) es verdadero, entonces P(k + 1) también es verdadero:

Sea k un entero con $k \ge 1$ y supongamos

$$\sqrt{1} + \sqrt{2} + \sqrt{3} + \cdots + \sqrt{k} \le k^{3/2}.$$

[Hipótesis de inducción.]

Debemos demostrar que

$$\sqrt{1} + \sqrt{2} + \sqrt{3} + \cdots + \sqrt{k+1} \le (k+1)^{3/2}.$$

Pero

$$\begin{aligned}
&\sqrt{1} + \sqrt{2} + \sqrt{3} + \cdots + \sqrt{k+1} \\
&\quad = \sqrt{1} + \sqrt{2} + \sqrt{3} + \cdots + \sqrt{k} + \sqrt{k+1} \\
&\qquad \text{haciendo explícito el penúltimo término} \\
\Rightarrow\ &\sqrt{1} + \sqrt{2} + \sqrt{3} + \cdots + \sqrt{k+1} \le k^{3)2} + \sqrt{k+1} \\
&\qquad \text{por la hipótesis de inducción} \\
\Rightarrow\ &\sqrt{1} + \sqrt{2} + \sqrt{3} + \cdots + \sqrt{k+1} \le k\sqrt{k} + \sqrt{k+1} \\
&\qquad \text{porque } k^{3/2} = k\sqrt{k} \\
\Rightarrow\ &\sqrt{1} + \sqrt{2} + \sqrt{3} + \cdots + \sqrt{k+1} \\
&\qquad \le k\sqrt{k+1} + \sqrt{k+1} \\
&\qquad \text{porque } \sqrt{k} < \sqrt{k+1} \\
\Rightarrow\ &\sqrt{1} + \sqrt{2} + \sqrt{3} + \cdots + \sqrt{k+1} \le (k+1)\sqrt{k+1} \\
&\qquad \text{factorizando } \sqrt{k+1} \\
\Rightarrow\ &\sqrt{1} + \sqrt{2} + \sqrt{3} + \cdots + \sqrt{k+1} \le (k+1)^{3/2}.
\end{aligned}$$

[Que era lo que se quería demostrar.]

b. *Sugerencia:* Cuando $k \ge 1$, $k^2 \ge k^2 - 1$. Use el hecho de que $k^2 - 1 = (k-1)(k+1)$ y divida ambos lados entre $k(k-1)$ para obtener $\frac{k}{k-1} \ge \frac{k+1}{k}$. Pero $\frac{k+1}{k} \ge 1$ y cualquier número mayor o igual que 1 es mayor o igual que su propia raíz cuadrada. Así $\frac{k}{k-1} \ge \frac{k+1}{k} \ge \sqrt{\frac{k+1}{k}} = \frac{\sqrt{k+1}}{\sqrt{k}}$. Entonces $k\sqrt{k} \ge (k-1)\sqrt{k+1} = (k+1-2)\sqrt{k+1} = (k+1)\sqrt{k+1} - 2\sqrt{k+1}$ y en consecuencia $k\sqrt{k} + 2\sqrt{k+1} \ge (k+1)\sqrt{k+1}$.

c. $\sqrt{1} + \sqrt{2} + \sqrt{3} + \cdots + \sqrt{n}$ es $\Theta(x^{3/2})$.

59. *Demostración:* Suponga que $f(x)$ es $O(g(x))$. Por definición de la O-notación, $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 0$. Por definición de límite, esto implica que dado cualquier número real $\varepsilon > 0$, existe un número real x_0 tal que $\left| \frac{f(x)}{g(x)} - 0 \right| < \varepsilon$ para toda $x > x_0$. Sea $b = \text{máx}(x_0, 1)$. Entonces $|f(x)| \le \varepsilon\ |g(x)|$ para toda $x > b$. Elija $\varepsilon = 1$ y haga $B = 1$. Así, existe un número real b tal que $|f(x)| \le B\ |g(x)|$ para toda $x > b$. Por tanto, por definición de la O-notación, $f(x)$ es $O(g(x))$.

Sección 11.3

1. **a.** $\log_2(200) = \dfrac{\ln 200}{\ln 2} \cong 7.6$ nanosegundos $=$ 0.0000000076 segundos.

d. $200^2 = 40\,000$ nanosegundos $= 0.00004$ segundos

e. $200^8 = 2.56 \times 10^{18}$ nanosegundos $\cong$ $\dfrac{2.56 \times 10^{18}}{10^9 \cdot 60 \cdot 60 \cdot 24 \cdot (365.25)}$ años $\cong 81.1215$ años

[porque hay 10^9 nanosegundos en un segundo, 60 segundos en un minuto, 60 minutos en una hora, 24 horas en un día y aproximadamente 365.25 días en un año en promedio].

2. **a.** Cuando el tamaño de la entrada se incrementa de m a $2m$, el número de operaciones aumenta de cm^2 a $c(2m)^2 = 4cm^2$.

b. Del inciso *a*), el número de operaciones se incrementa por un factor de $(4cm^2)/cm^2 = 4$.

c. Cuando el tamaño de la entrada se incrementa en un factor de 10 (de m a $10m$), entonces el número de operaciones aumenta por un factor de $(c(10m)^2)/(cm^2) = (100cm^2)/cm^2 = 100$.

4. **a.** El algoritmo A tiene orden n^2 y el orden del algoritmo B es $n^{3/2}$.

b. El algoritmo A es más eficiente que el algoritmo B cuando $2n^2 < 80\ n^{3/2}$. Esto ocurre exactamente cuándo

$$n^2 < 40n^{3/2} \Leftrightarrow \frac{n^2}{n^{3/2}} < 40 \Leftrightarrow n^{1/2} < 40 \Leftrightarrow n < 40^2.$$

Así, el algoritmo A es más eficiente que el algoritmo B cuando $n < 1\,600$.

c. El algoritmo B es al menos 100 veces más eficiente que el algoritmo A para valores de n con $100(80n^{3/2}) \le 2n^2$. Esto

sucede exactamente cuando $8\,000n^{3/2} \le 2n^2 \Leftrightarrow 4\,000 \le \dfrac{n^2}{n^{3)2}}$ $\Leftrightarrow 4\,000 \le \sqrt{n} \Leftrightarrow 16\,000\,000 \le n$. Así, el algoritmo B es al menos 100 veces más eficiente que el algoritmo A cuando $n \ge 16\,000\,000$.

6. a. Hay dos multiplicaciones, una suma y una resta para cada iteración del bucle, así que existen cuatro veces más operaciones como iteraciones del bucle. El bucle es iterado $(n-1)-3+1 = n-3$ veces (porque el número de iteraciones es igual al índice superior menos el inferior más 1). Entonces el número total de operaciones es $4(n-3) = 4n-12$.

b. Por el teorema sobre órdenes polinomiales, $4n-12$ es $\Theta(n)$, así el segmento del algoritmo tiene orden n.

8. a. Existe una diferencia para cada iteración del bucle y hay $\lfloor n/2 \rfloor$ iteraciones del bucle.

b. $$\lfloor n/2 \rfloor = \begin{cases} n/2 & \text{si } n \text{ es par} \\ (n-1)/2 & \text{si } n \text{ es impar} \end{cases}$$

es $\Theta(n)$ por el teorema sobre órdenes polinomiales, así el segmento del algoritmo tiene orden n.

9. a. Para cada iteración del bucle interno, hay dos multiplicaciones y una suma. Existen $2n$ iteraciones del bucle interior para cada iteración del bucle externo. Por tanto, el número de iteraciones del bucle interno es $2n \cdot n = 2n^2$. Se tiene que el número total de operaciones elementales que debe ser realizado cuando se ejecuta el algoritmo es $3 \cdot 2n^2 = 6n^2$.

b. Como $6n^2$ es $\Theta(n^2)$(por el teorema sobre órdenes polinomiales), el segmento del algoritmo tiene orden n^2.

11. a. Hay una suma para cada iteración del bucle interior. El número de iteraciones en el bucle interno se puede deducir de la tabla a la derecha, que muestra los valores de k y j para que se ejecute el bucle interno.

Entonces el número total de iteraciones del bucle interno es

$$2+3+\cdots+n = (1+2+3+\cdots+n) - 1$$
$$= \frac{n(n+1)}{2} - 1 = \frac{1}{2}n^2 + \frac{1}{2}n - 1$$

(por el teorema 5.2.2). Como se realiza una operación para cada iteración del bucle interior, por tanto, el número total de operaciones es $\frac{1}{2}n^2 + \frac{1}{2}n - 1$.

b. Por el teorema sobre órdenes polinomiales, $\frac{1}{2}n^2 + \frac{1}{2}n - 1$ es $\Theta(n^2)$ y así el segmento del algoritmo tiene orden n^2.

k	1		2			3				...	$n-1$				
j	1	2	1	2	3	1	2	3	4	...	1	2	3	...	n
	2		3			4					n				

14. a. Existe una suma para cada iteración del bucle interior y hay una suma adicional y una multiplicación para cada iteración del bucle exterior. El número de iteraciones en el bucle interno se puede deducir de la siguiente tabla, que muestra los valores de i y j para que se ejecute el bucle interior.

i	1	2		3			⋯	n				
j	1	1	2	1	2	3	⋯	1	2	3	⋯	n
	1		2			3					n	

Así el número total de iteraciones del bucle interno es

$$1+2+3+\cdots+n = (1+2+3+\cdots+n)$$
$$= \frac{n(n+1)}{2} = \frac{1}{2}n^2 + \frac{1}{2}n$$

(por el teorema 5.2.2). Se realiza una suma en cada iteración del bucle interior, entonces el número de operaciones efectuadas cuando se ejecuta el bucle interno es $\frac{1}{2}n^2 + \frac{1}{2}$. Ahora dos operaciones adicionales se realizan cada vez que se ejecuta el bucle externo y como éste se ejecuta n veces, da $2n$ operaciones adicionales. Por tanto, el número total de operaciones es

$$\frac{1}{2}n^2 + \frac{1}{2}n + 2n = \frac{1}{2}n^2 + \frac{5}{2}n.$$

b. Por el teorema sobre órdenes polinomiales, $\frac{1}{2}n^2 + \frac{5}{2}n$ es $\Theta(n^2)$ y así el segmento del algoritmo tiene orden n^2.

17. a. Hay dos diferencias y una multiplicación por cada iteración del bucle interno.

Si n es impar, el número de iteraciones del bucle interior se puede deducir de la siguiente tabla, que indica los valores de i y j para que se ejecute el bucle.

i	1	2	3		4		5			6			...	$n-1$		...		n		...	
$\left\lfloor \frac{i+1}{2} \right\rfloor$	1	1	2		2		3			3			...	$\frac{n-1}{2}$		...		$\frac{n+1}{2}$		...	
j	1	1	1	2	1	2	1	2	3	1	2	3	...	1	2	⋯	$\frac{n-1}{2}$	1	2	...	$\frac{n+1}{2}$
	1	1	2		2		3			3				$\frac{n-1}{2}$				$\frac{n+1}{2}$			

Así el número de iteraciones del bucle interno es

$$\begin{aligned}
&1+1+2+2+\cdots+\frac{n-1}{2}+\frac{n-1}{2}+\frac{n+1}{2}\\
&\quad=2\cdot\left(1+2+3+\cdots+\frac{n-1}{2}\right)+\frac{n+1}{2}\\
&\quad=2\cdot\frac{\frac{n-1}{2}\left(\frac{n-1}{2}+1\right)}{2}+\frac{n+1}{2}\\
&\qquad\qquad\text{por el teorema 5.2.2.}\\
&\quad=\frac{n^2-2n+1}{4}+\frac{n-1}{2}+\frac{n+1}{2}\\
&\quad=\frac{1}{4}n^2+\frac{1}{2}n+\frac{1}{4}.
\end{aligned}$$

Mediante un razonamiento similar, si n es par, entonces el número de iteraciones del bucle interior es

$$\begin{aligned}
&1+1+2+2+3+3+\cdots+\frac{n}{2}+\frac{n}{2}\\
&\quad=2\cdot\left(1+2+3+\cdots+\frac{n}{2}\right)\\
&\quad=2\cdot\left(\frac{\frac{n}{2}\left(\frac{n}{2}+1\right)}{2}\right)\qquad\text{por el teorema 5.2.2.}\\
&\quad=\frac{n^2}{4}+\frac{n}{2}.
\end{aligned}$$

Tres operaciones se realizan para cada iteración del bucle interno, entonces la respuesta es $3\left(\frac{n^2}{4}+\frac{n}{2}\right)$ cuando n es par y $3\left(\frac{1}{4}n^2+\frac{1}{2}n+\frac{1}{4}\right)$ cuando n es impar.

b. Porque $3\left(\frac{n^2}{4}+\frac{n}{2}\right)$ es $\Theta(n^2)$ y $3\left(\frac{1}{4}n^2+\frac{1}{2}n+\frac{1}{4}\right)$ también es $\Theta(n^2)$ (por el teorema sobre órdenes polinomiales), este segmento del algoritmo tiene orden n^2.

19. *Sugerencia:* vea la sección 9.6 para un análisis de cómo contar el número de iteraciones del bucle más interno.

22.

	$a[1]$	$a[2]$	$a[3]$	$a[4]$	$a[5]$
Orden inicial	6	2	1	8	4
Resultado del paso 1	2	6	1	8	4
Resultado del paso 2	1	2	6	8	4
Resultado del paso 3	1	2	6	8	4
Orden final	1	2	4	6	8

22.

n	5											
***a*[1]**	6		2				1					
***a*[2]**	2	6				2						
***a*[3]**	1				6						4	
***a*[4]**	8							8			6	
***a*[5]**	4									8		
k	2			3			4		5			6
x	2			1			8		4			
j	1	0		2	1	0	3		4	3	2	

24. Hay 14 comparaciones. Cada iteración del bucle implica dos comparaciones, una para demostrar si $j \neq 0$ y la otra en el enunciado **if** para comparar x y $a[j]$. Cuando $k = 2$, el bucle se ejecuta una vez, da dos comparaciones; cuando $k = 3$, se ejecuta dos veces, da 4 comparaciones, cuando $k = 4$, se ejecuta una vez, da 2 comparaciones y cuando $k = 5$, se ejecuta tres veces, da 6 comparaciones. Así el total es $2 + 4 + 2 + 6 = 14$ comparaciones.

27. *Sugerencia:* La respuesta a la parte (a) es $E_n = 3 + 4 + \ldots + (n + 1)$, que es igual a $(1 + 2 + 3 + \cdots + (n + 1)) - (1 + 2)$.

28. El renglón superior de la tabla que se muestra a continuación presenta los valores iniciales del arreglo y el renglón inferior indica los valores finales. El resultado para cada valor de k se muestra en un renglón separado.

$a[1]$	$a[2]$	$a[3]$	$a[4]$	$a[5]$
5	3	4	6	2
2	3	4	6	5
2	3	4	6	5
2	3	4	6	5
2	3	4	5	6

30.

n	5													
***a*[1]**	5					2								
***a*[2]**	3													
***a*[3]**	4													
***a*[4]**	6												5	
***a*[5]**	2					5							6	
k	1						2			3		4		5
ÍndiceDeMin	1	2			5		2			3		4	5	
i	2	3	4	5			3	4	5	4	5	5		
temp					5								6	

32. Hay una comparación para cada combinación de valores de k e i: a saber, $4 + 3 + 2 + 1 = 10$.

35. **b.** $n - 3 + 1 = n - 2$. **d.** *Sugerencia:* La respuesta es n^2.

36.

n	3									
***a*[0]**	2									
***a*[1]**	1									
***a*[2]**	−1									
***a*[3]**	3									
x	2									
valor polinomio	2		4			0				24
i	1		2			3				
term	1	2	−1	−2	−4	3	6	12	24	
j	1		1	2		1	2	3		

38. Número de multiplicaciones

$$= \text{número de iteraciones del bucle interno}$$
$$= 1 + 2 + 3 + \ldots + n$$
$$= \frac{n(n+1)}{2} \qquad \text{por el teorema 5.2.2}$$

Número de sumas

$$= \text{número de iteraciones del bucle externo}$$
$$= n$$

Así el número total de multiplicaciones y sumas es

$$\frac{n(n+1)}{2} + n = \frac{1}{2}n^2 + \frac{3}{2}n.$$

40.

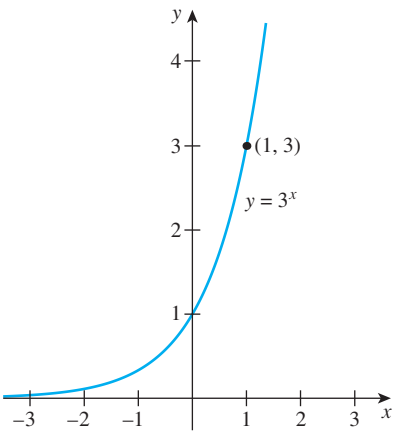
n	3			
***a*[0]**	2			
***a*[1]**	1			
***a*[2]**	−1			
***a*[3]**	3			
x	2			
valor polinomio	3	5	11	24
i	1	2	3	

42. *Sugerencia:* La respuesta es $t_n = 2n$.

Sección 11.4

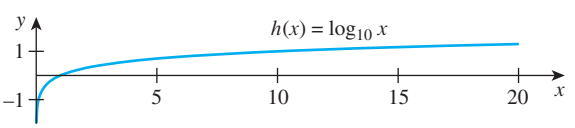
1.

x	$f(x) = 3^x$
0	$3^0 = 1$
1	$3^1 = 3$
2	$3^2 = 9$
−1	$3^{-1} = 1/3$
−2	$3^{-2} = 1/9$
1/2	$3^{1/2} \cong 1.7$
−(1/2)	$3^{-(1/2)} \cong 0.6$



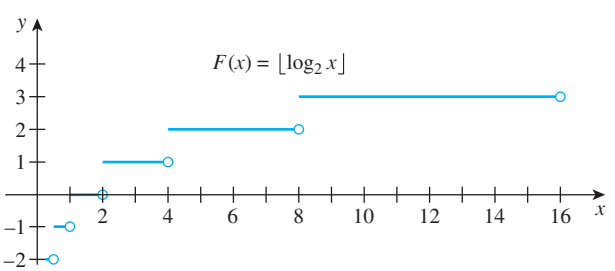
3.

x	$h(x) = \log_{10} x$
1	0
10	1
100	2
1) 10	−1
1) 100	−2



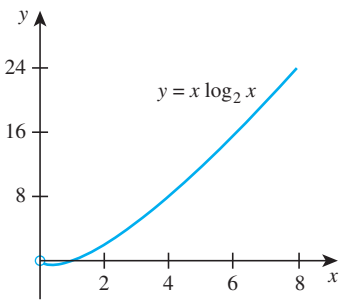
5.

x	$\lfloor \log_2 x \rfloor$
$1 \le x < 2$	0
$2 \le x < 4$	1
$4 \le x < 8$	2
$8 \le x < 16$	3
$1)2 \le x < 1$	−1
$1)4 \le x < 1)2$	−2



7.

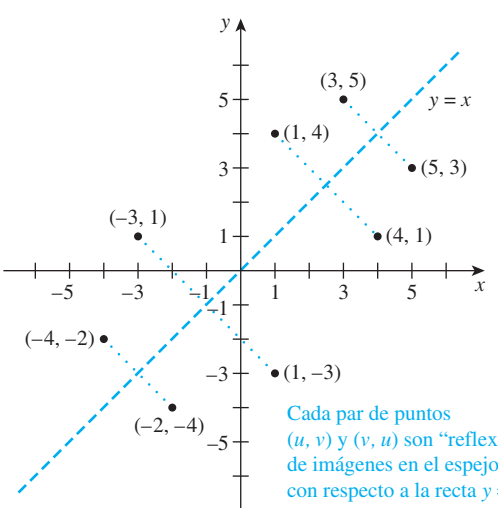
x	$x \log_2 x$
1	$1 \cdot 0 = 0$
2	$2 \cdot 1 = 2$
4	$4 \cdot 2 = 8$
8	$8 \cdot 3 = 24$
1/8	$(1/8) \cdot (-3) = -3/8$
1/4	$(1/4) \cdot (-2) = -1/2$
3/8	$(3/8) \cdot (\log_2(3/8)) \cong -0.53$



9. La distancia arriba del eje es $(2^{64}\text{unidades}) \cdot \left(\frac{1}{4}\frac{\text{pulgada}}{\text{unidad}}\right) = \frac{2^{64}}{4}$ pulgadas $= \frac{2^{64}}{4 \cdot 12 \cdot 5280}$ millas $\cong$ 72 785 448 520 000 millas. La razón de la altura del punto a la distancia promedio de la Tierra al Sol es aproximadamente 72785448520000/93000000 $\cong$ 782 639. (Si efectúa el cálculo empleando unidades métricas y la aproximación 0.635 cm $\cong$ 1/4 pulgada, la razón da aproximadamente 780 912.)

10.b. Por definición de logaritmo, $\log_b x$ es el exponente al cual debemos elevar b para obtener x. Así cuando b se eleva a este exponente, se obtiene x. Es decir, $b^{\log_b x} = x$.

11. b.



Cada par de puntos (u, v) y (v, u) son "reflexiones de imágenes en el espejo" con respecto a la recta $y = x$.

13. *Sugerencias:* (1) $\lfloor \log_{10} x \rfloor = m$, (2) vea el ejemplo 11.4.1.

15. No. *Contraejemplo:* Sea $n = 2$. Entonces $\lceil \log_2(n-1) \rceil = \lceil \log_2 1 \rceil = \lceil 0 \rceil = 0$, mientras que $\lceil \log_2 n \rceil = \lceil \log_2 2 \rceil = \lceil 1 \rceil = 1$.

16. *Sugerencia:* El enunciado es verdadero.

18. $\lfloor \log_2 148206 \rfloor + 1 = 18$

21. a.
$$a_2 = a_{\lfloor 2/2 \rfloor} + 2 = a_1 + 2 = 1 + 2$$
$$a_3 = a_{\lfloor 3/2 \rfloor} + 2 = a_1 + 2 = 1 + 2$$
$$a_4 = a_{\lfloor 4/2 \rfloor} + 2 = a_2 + 2 = (1 + 2) + 2 = 1 + 2 \cdot 2$$
$$a_5 = a_{\lfloor 5/2 \rfloor} + 2 = a_2 + 2 = (1 + 2) + 2 = 1 + 2 \cdot 2$$
$$a_6 = a_{\lfloor 6/2 \rfloor} + 2 = a_3 + 2 = (1 + 2) + 2 = 1 + 2 \cdot 2$$
$$a_7 = a_{\lfloor 7/2 \rfloor} + 2 = a_3 + 2 = (1 + 2) + 2 = 1 + 2 \cdot 2$$
$$a_8 = a_{\lfloor 8/2 \rfloor} + 2 = a_4 + 2 = (1 + 2 \cdot 2) + 2 = 1 + 3 \cdot 2$$
$$a_9 = a_{\lfloor 9/2 \rfloor} + 2 = a_4 + 2 = (1 + 2 \cdot 2) + 2 = 1 + 3 \cdot 2$$
$$\vdots$$
$$a_{15} = a_{\lfloor 15/2 \rfloor} + 2 = a_7 + 2 = (1 + 2 \cdot 2) + 2 = 1 + 3 \cdot 2$$
$$a_{16} = a_{\lfloor 16/2 \rfloor} + 2 = a_8 + 2 = (1 + 3 \cdot 2) + 2 = 1 + 4 \cdot 2$$
$$\vdots$$

Conjetura:

$$a_n = 1 + 2\lfloor \log_2 n \rfloor$$

b. *Demostración:* Suponga que la sucesión $a_1, a_2, a_3, \ldots$ está definida recursivamente como sigue: $a_1 = 1$ y $a_k = a_{\lfloor k/2 \rfloor} + 2$ para todos los enteros $k \geq 2$. Demostraremos por inducción matemática fuerte que la siguiente propiedad, $P(n)$, es verdadera para todos los enteros $n \geq 2$: $a_n = 1 + 2[\log n]$.

Demostración de que P(1) es verdadera: $P(1)$ es la ecuación $1 + 2[\log_2 1] = 1 + 2.0 = 1$, que es el valor de a_1.

Demostración de que para cualquier entero k ≥ 1, si P(i) es verdadera para todos los enteros i de 1 a k, entonces P(k + 1) también es verdadera:
Sea k cualquier entero con $k \geq 1$ y suponga $a_i = 1 + 2[\log_2 i]$ para todos los enteros i de 1 a k. *[Esto es la hipótesis de inducción.]* Debemos demostrar que $a_{k+1} = 1 + 2\,[\log_2(k + 1)]$.

Caso 1 (k es impar): En este caso $k + 1$ es par y

$$a_{k+1} = a_{\lfloor (k+1)/2 \rfloor} + 2$$
por la definición recursiva de $a_1, a_2, a_3, \ldots$
$$= a_{(k+1)/2} + 2$$
porque k + 1 es par (teorema 4.5.2)

$$= 1 + 2\lfloor \log_2((k+1)/2) \rfloor + 2$$
por la hipótesis de inducción
$$= 3 + 2\lfloor \log_2(k+1) - \log_2 2 \rfloor$$
por el teorema 7.2.1(b)
$$= 3 + 2\lfloor \log_2(k+1) - 1 \rfloor$$
porque $\log_2 2 = 1$
$$= 3 + 2(\lfloor \log_2(k+1) \rfloor - 1)$$
porque para todos los número reales x, $\lfloor x - 1 \rfloor = \lfloor x \rfloor - 1$
por el ejercicio 15, sección 4.5
$$= 1 + 2\lfloor \log_2(k+1) \rfloor$$
por álgebra.

Caso 2 (k es par): En este caso $k + 1$ es impar y

$$a_{k+1} = a_{\lfloor (k+1)/2 \rfloor} + 2$$
por la definición recursiva de $a_1, a_2, a_3, \cdots$
$$= a_{k/2} + 2$$
por el teorema 4.5.2 ya que k + 1 es impar,
$$= 1 + 2\lfloor \log_2(k/2) \rfloor + 2$$
por la hipótesis de inducción
$$= 3 + 2\lfloor \log_2 k - \log_2 2 \rfloor$$
por el teorema 7.2.1(b)
$$= 3 + 2\lfloor \log_2 k - 1 \rfloor$$
porque $\log_2 2 = 1$
$$= 3 + 2(\lfloor \log_2 k \rfloor - 1)$$
porque para todos los números reales x, $\lfloor x - 1 \rfloor = \lfloor x \rfloor - 1$ por el ejercicio 15, sección 4.5,
$$= 1 + 2\lfloor \log_2 k \rfloor$$
por álgebra
$$= 1 + 2\lfloor \log_2(k+1) \rfloor$$
por la propiedad 11.4.3

Entonces, en cualquier caso, $a_{k+1} = 1 + 2\,[\log_2(k+1)]$ *[que era lo que se quería demostrar]*.

23. *Sugerencia:* Cuando $k \geq 2$, entonces $k^2 \geq 2k$ y así $k \leq \frac{k^2}{2}$. Así $\frac{k^2}{2} + k \leq \frac{k^2}{2} + \frac{k^2}{2} = k^2$. También cuando $k \geq 2$, entonces $k^2 > 1$, en consecuencia $\frac{1}{2} < \frac{k^2}{2}$. Por tanto, $\frac{k^2}{2} + \frac{1}{2} < \frac{k^2}{2} + \frac{k^2}{2} = k^2$.

24. *Sugerencia:* Aquí está el argumento para el paso inductivo en el caso donde k es impar y $k + 1$ es par.

$$c_{k+1} = 2c_{\lfloor (k+1)/2 \rfloor} + (k+1)$$
por la definición recursiva de $c_1, c_2, c_3, \cdots$
$$\Rightarrow \quad c_{k+1} = c_{(k+1)/2} + (k+1)$$
por el teorema 4.5.2 ya que $k + 1$ es par
$$\Rightarrow \quad \leq 2\left\lfloor \tfrac{k+1}{2} \log_2 \left(\tfrac{k+1}{2} \right) \right\rfloor + (k+1)$$
por la hipótesis de inducción
$$\Rightarrow \quad \leq (k+1)(\log_2(k+1) - \log_2 2) + (k+1)$$
por álgebra y por el teorema 7.2.1(b)
$$\Rightarrow \quad \leq (k+1)(\log_2(k+1) - 1) + (k+1)$$
porque $\log_2 2 = 1$
$$\Rightarrow \quad \leq (k+1)(\log_2(k+1))$$
por álgebra

25. *Solución 1:* Una manera de resolver este problema es comparar valores para $\log_2 x$ y $x^{1/10}$ para valores grandes de x convenientemente seleccionados. Por ejemplo, si se emplean potencias de 10, se obtienen los siguientes resultados $\log_2(10^{10}) = 10 \log_2 10 \cong 33.2$ y $(10^{10})^{1/10} = 10^{10 \cdot (1/10)} = 10^1 = 10$. Así el valor $x = 10^{10}$ no funciona.

Sin embargo, como $\log_2(10^{20}) = 20 \log_2 \cong 66.4$ y $(10^{20})^{1/10} = 10^{20 \cdot (1/10)} = 10^2 = 100$ y puesto que $66.4 < 100$, entonces el valor $x = 10^{20}$ sí funciona.

Solución 2: Otro enfoque es emplear una graficadora o computadora para realizar gráficas de $y = \log_2 x$ y $y = x^{1/10}$, tomando muy en serio la sugerencia de "pensar en grande" al elegir el tamaño del intervalo para las x. Haga unos pocos intentos y use el zoom para trazar aspectos que hagan cruzar a la gráfica de $y = x^{1/10}$ por arriba de $y = \log_2 x$ alrededor de 4.9155×10^{17}. Así, para valores de x más grandes que éste, $x^{1/10} > \log_2 x$.

27. Al igual que en el ejercicio 25, se puede resolver este problema por exploración numérica o mediante una calculadora graficadora. Por ejemplo, si eleva 1.0001 a sucesivas grandes potencias de 10, puede encontrar la solución $x = 10^6 = 1\,000\,000$. Es decir,
$(1.0001)^{1000000} > 2\,67 \times 10^{43} > 1\,000\,000$.
(Esta es la primera potencia de 10 que funciona.)

Alternativamente, puede emplear una graficadora para trazar las gráficas de $y_1 = (1.0001)^x$ y $y_2 = x$ y observe en dónde la gráfica de y_1 supera a la gráfica de y_2. Necesitará un zoom para obtener cuidadosamente una respuesta exacta. Si emplea este método, encontrará que si $x > 116703$, entonces $(1.0001)^x > x$.

29. $7x^2 + 3x \log_2 x$ es $\Theta(x^2)$.

30. *[Para demostrar que $2x + log_2\, x$ es $\Theta(x)$, debemos encontrar números reales positivos A, B y k tales que $A\,|\,x\,| \leq |\,2x + log_2\, x\,| \leq B\,|\,x\,|$ para toda $x > k$.]* Es claro, de las gráficas de $y = \log_2 x$ y $y = x$, que para toda $x > 0$, $\log_2 x \leq x$. Sumando $2x$ en ambos lados se obtiene $2x + \log_2 x \leq 3x$, o, como todos los términos son positivos

$$|\,2x + \log_2 x\,| \leq 3\,|\,x\,|.$$

También, cuando $x > 1$, entonces $\log_2 x > 0$ y así $0 < x + \log_2 x$. Sumando x en ambos lados se obtiene $x < 2x + \log_2 x$. Entonces cuando $x > 1$,

$$|\,x\,| \leq |\,2x + \log_2 x\,|.$$

Por tanto, sean $k = 1$, $A = 1$ y $B = 3$. Así, para todos los números reales $x > k$,

$$A\,|\,x\,| \leq |\,2x + \log_2 x\,| \leq B\,|\,x\,|$$

En consecuencia, por definición de Θ-notación, $2x + \log_2 x$ es $\Theta(x)$.

32. Para todos los enteros n, $2^n \leq n^2 + 2^n$. También, por la propiedad (11.4.10), existe un número real k tal que $n^2 \leq 2^n$ para toda $n > k$. Sumando 2^n en ambos lados da $n^2 + 2^n \leq 2^n + 2^n = 2 \cdot 2^n$. Como todas las cantidades son no-negativas, podemos escribir

$$|2^n| \leq |n^2 + 2^n| \leq 2 \cdot |2^n| \text{ para todos los enteros } n > k.$$

Sean $A = 1$ y $B = 2$. Entonces

$$A|2^n| \leq |n^2 + 2^n| \leq B|2^n| \text{ para todos los enteros } n > k,$$

así que, por definición de la Θ-notación, $n^2 + 2^n$ es $\Theta(2^n)$.

33. *Sugerencia:* $2^{n+1} = 2.2^n$

34. *Sugerencia:* Use una demostración por contradicción. Inicie suponiendo que hay números reales positivos B y b tales que $4^n < B \cdot 2^n$ para todos los números reales $n > b$ y utilice el hecho de que $\frac{4^n}{2^n} = \left(\frac{4}{2}\right)^n = 2^n$ para obtener una contradicción.

35. Por el teorema 5.2.3, para todos los enteros $n \geq 0$,

$$1 + 2 + 2^2 + \cdots + 2^n = \frac{2^{n+1} - 1}{2 - 1} = 2^{n+1} - 1.$$

También

$$2^{n+1} - 1 \leq 2^{n+1} = 2 \cdot 2^n.$$

Así, por transitividad de orden,

$$1 + 2 + 2^2 + \cdots + 2^n \leq 2 \cdot 2^n. \qquad (*)$$

Aún más, si $n > 0$, entonces

$$2^n \leq 1 + 2 + 2^2 + \cdots + 2^n. \qquad (**)$$

Combinando (*) y (**) se obtiene

$$1 \cdot 2^n \leq 1 + 2 + 2^2 + \cdots + 2^n \leq 2 \cdot 2^n,$$

Y así, porque todas las partes son positivas,

$$1 \cdot |2^n| \leq |1 + 2 + 2^2 + \cdots + 2^n| \leq 2 \cdot |2^n|.$$

Sean $A = 1$, $B = 2$ y $k = 1$. Entonces para todos los enteros $n > k$,

$$A \cdot |2^n| \leq |1 + 2 + 2^2 + \cdots + 2^n| \leq B \cdot |2^n|.$$

Así, por definición de la Θ-notación, $1 + 2 + 2^2 + \cdots + 2^n$ es $\Theta(2^n)$.

36. *Sugerencia:* Esto es similar a la solución para el ejercicio 35. Use el hecho de que $4 + 4^2 + 4^3 + \cdots + 4^n = 4(1 + 4 + 4^2 + 4^3 + \cdots + 4^{n-1})$.

39. Factorice la n para obtener

$$\begin{aligned} n + \frac{n}{2} + \frac{n}{4} + \cdots + \frac{n}{2^n} &= n\left(1 + \frac{1}{2} + \frac{1}{4} + \cdots + \frac{1}{2^n}\right) \\ &= n\left(\frac{\left(\frac{1}{2}\right)^{n+1} - 1}{\frac{1}{2} - 1}\right) \quad \text{por el teorema 5.2.3} \\ &= n\left(\frac{1 - 2^{n+1}}{2^n(1-2)}\right) \quad \text{multiplicando numerador y denominador por } 2^{n+1} \\ &= n\left(\frac{2^{n+1} - 1}{2^n}\right) \\ &= n\left(2 - \frac{1}{2^n}\right) \quad \text{por álgebra.} \end{aligned}$$

Ahora $1 \leq 2 - 1/2^n \leq 2$ cuando $n > 1$. Así

$$1 \cdot n \leq n\left(2 - \frac{1}{2^n}\right) \leq 2 \cdot n,$$

entonces, sustituyendo,

$$1 \cdot n \leq n + \frac{n}{2} + \frac{n}{4} + \cdots + \frac{n}{2^n} \leq 2 \cdot n.$$

Sean $A = 1$, $B = 2$ y $k = 1$. Entonces, como todas las cantidades son positivas, para todos los enteros $n > k$,

$$A \cdot |n| \leq \left|n + \frac{n}{2} + \frac{n}{4} + \cdots + \frac{n}{2^n}\right| \leq B \cdot |n|.$$

Así que, por definición de la Θ-notación, $n + \frac{n}{2} + \frac{n}{4} + \cdots + \frac{n}{2^n}$ es $\Theta(n)$.

43. Si n es cualquier entero con $n \geq 3$, entonces

$$n + \frac{n}{2} + \frac{n}{3} + \cdots + \frac{n}{n} = n\left(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}\right).$$

Por el ejemplo 11.4.7,

$$\ln(n) \leq 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} \leq 2\ln(n).$$

Si $n > 1$, entonces podemos multiplicar por n y usar el hecho de que todas las cantidades son positivas para obtener

$$|n \ln(n)| \leq \left|n + \frac{n}{2} + \frac{n}{3} + \cdots + \frac{n}{n}\right| \leq 2\,|n \ln(n)|.$$

Sean $A = 1$, $B = 2$ y $k = 1$. Entonces para todos los enteros $n > k$,

$$A \cdot |n \ln(n)| \leq \left|n + \frac{n}{2} + \frac{n}{3} + \cdots + \frac{n}{n}\right| \leq B \cdot |n \ln(n)|$$

y así, por definición de la Θ-notación, $n + \frac{n}{2} + \frac{n}{3} + \cdots + \frac{n}{n}$ es $\Theta(n \ln n)$.

46. *Demostración (por inducción matemática):* Aceptemos que la propiedad $P(n)$ sea la desigualdad $n \leq 10^n$.

Demostración de que P(1) es verdadera:

Cuando $n = 1$, la desigualdad es $1 \leq 10$, que es verdadera.

Demostración que para todos los enteros k ≥ 1, si P(k) es verdadera, entonces P(k + 1) también es verdadera.

Sea k cualquier entero con $k \geq 1$ y suponga $k \leq 10^k$. *[Esta es la hipótesis de inducción.]* Debemos demostrar que $k + 1 \leq 10^{k+1}$. Por hipótesis de inducción, $k \leq 10^k$. Sumando 1 en ambos lados se obtiene $k + 1 \leq 10^k + 1$. Pero cuando $10^k + 1 \leq 10^k + 9 \cdot 10^k = 10 \cdot 10^k = 10^{k+1}$. Así, por transitividad de orden, $k + 1 \leq 10^{k+1}$ *[que era lo que se quería demostrar].*

47. *Sugerencia:* Para demostrar el paso inductivo, use el hecho de que si $k > 1$, entonces $k + 1 \leq 2k$. Aplique la función logarítmica de base 2 en ambos lados de esta desigualdad y utilice propiedades de los logaritmos.

48. *Sugerencia:* $\underbrace{2 \cdot 2 \cdot 2 \cdots 2}_{n \text{ factores}} \leq 2 \cdot (2 \cdot 3 \cdot 4 \cdots n) = 2 \cdot n!$

49. **a.** *Demostración:* Suponga que n es una variable que tome valores enteros positivos. Entonces

$$n! = \underbrace{n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 2 \cdot 1}_{n \text{ factores}}$$

$$\leq \underbrace{n \cdot n \cdot n \cdot n \cdot \ldots \cdot n}_{n \text{ factores}} = n^n$$

porque $(n-1) \le n$, $(n-2) \le n, \ldots,$ y $1 \le n$. Sea $B = 1$ y $b = 1$. Se tiene de la desigualdad presentada y del hecho de que $n!$ y n^n para todos los enteros $n > b$. Por tanto, por definición de la O-notación, $n!$ es $O(n^n)$.

c. *Sugerencia:* $(n!)^2 = n! \cdot n! = (1 \cdot 2 \cdot 3 \cdots n)(n \cdot)n - 1(\cdots 3 \cdot 2 \cdot 1) = \left(\prod_{r=1}^{n} r\right)\left(\prod_{r=1}^{n}(n-r+1)\right) = \prod_{r=1}^{n} r(n-r+1)$. Muestre que para todos los enteros $r = 1, 2, \ldots, n$, $nr - n^2 + r \ge n$.

50. a. Sea n un entero positivo. Para cualquier número real $x > 1$, las propiedades de los logaritmos y de los exponentes (vea la sección 7.2) implica que $0 \le \log_2(x) = \log_2((x^{1)n})^n) = n \log_2(x^{1/n}) < nx^{1/n}$ donde la última desigualdad se satisface sustituyendo $x^{1/n}$ en lugar de u en $\log_2 u < u$.

b. Sea $B = n$ y $b = 1$. Entonces $x > x_0$, $|\log_2 x| = \log_2 x \le B \cdot |x^{1)n}|$ y por lo tanto $\log_2 x$ es $O(x^{1/n})$.

52. Sea n un entero positivo y suponga que $x > (2n)^{2n}$. Por las propiedades de los logaritmos,

$$\log_2 x = (2n)\left(\frac{1}{2n}\right)(\log_2 x)$$
$$= (2n)\log_2\left(x^{\frac{1}{2n}}\right) < 2nx^{\frac{1}{2n}} \qquad (*)$$

(donde la última desigualdad vale sustituyendo $x^{\frac{1}{2n}}$ en lugar de u en $\log_2 u < u$). Pero elevando ambos lados de $x > (2n)^{2n}$ a la potencia $1/2$ se obtiene $x^{1/2} > ((2n)^{2n})^{1/2} = (2n)^n$. Cuando se multiplican ambos lados por $x^{1/2}$, el resultado es $x = x^{1/2}x^{1/2} > x^{1/2}(2n)^n = x^{1/2}(2n)^n$, o de un modo más compacto,

$$x^{1/2}(2n)^n < x.$$

Entonces, ya que la función potencia se define por $x \to x^{1/n}$ está creciendo para toda $x > 0$ (vea el ejercicio 21 de la sección 11.1), podemos tomar la raíz enésima en ambos lados de la desigualdad y usando las leyes de los exponentes obtenemos

$$(x^{1/2}(2n)^n)^{1/n} < x^{1/n}$$

O, equivalentemente,

$$2nx^{\frac{1}{2n}} < x^{1/n}. \qquad .(**)$$

Ahora use la transitividad del orden (apéndice A, T18) para combinar (*) y (**) y concluir que $\log_2 x < x^{1/n}$ *[que era lo que se quería demostrar]*.

54. *Demostración (por inducción matemática):* Sea b un número real con $b > 1$ y sea la propiedad $P(n)$ la ecuación

$$\lim_{x\to\infty}\left(\frac{x^n}{b^x}\right) = 0.$$

Demostración de que P(1) es verdadera:

Por la regla de L'Hôpital, $\lim_{x\to\infty}\left(\frac{x^1}{b^x}\right) = \lim_{x\to\infty}\left(\frac{1}{b^x(\ln b)}\right) = 0$. Así $P(1)$ es verdadera.

Demostración que para todos los enteros $k \ge 1$, si $P(k)$ es verdadera, entonces $P(k+1)$ también es verdadera.

Sea k cualquier entero con $k \ge 1$ y suponga que $\lim_{x\to\infty}\left(\frac{x^k}{b^x}\right) = 0$. *[Esta es la hipótesis de inducción.]* Debemos demostrar que $\lim_{x\to\infty}\left(\frac{x^{k+1}}{b^x}\right) = 0$. Pero por la regla de L'Hôpital, $\lim_{x\to\infty}\frac{x^{k+1}}{b^x}$ $= \lim_{x\to\infty}\frac{(k+1)x^k}{(\ln b)b^x} = \frac{(k+1)}{(\ln b)}\lim_{x!\infty}\ \frac{x^k}{b^x} = \frac{(k+1)}{(\ln b)}\cdot 0$ *[por la hipótesis de inducción]* $= 0$. *[Que era lo que se quería demostrar.]*

b. Por el resultado del inciso *a*) y por la definición de límite dado cualquier número real $\varepsilon > 0$, existe un entero N tal que $|\frac{x^n}{b^n} - 0| < \varepsilon$ para toda $x > N$. En este caso tome $\varepsilon = 1$. Se tiene que para toda $x > N$, $|\frac{x^n}{b^x}| = |\frac{x^n}{b^x}| < 1$. Multiplicando ambos lados por $|b^x|$, para obtener $|x^n| < |b^x|$. Sea $B = 1$ y $b = N$. Entonces $|x^n| < B \cdot |b^x|$ para toda $x > b$. Así por definición de la O-notación, x^n es $O(b^x)$.

Sección 11.5

3. $\log_2 1000 = \log_2(10^3) = 3\log_2 10 \cong 3(3.32) \cong 9.96$
$\log_2(1{,}000{,}000) = \log_2(10^6) = 6\log_2 10 \cong 6(3.32)$
$\cong 19.92$
$\log_2(1{,}000{,}000{,}000{,}000) = \log_2(10^{12}) = 12\log_2 10$
$\cong 12(3.32) = 39.84$

2. a. Si $m = 2^k$, donde k es un entero positivo, entonces el algoritmo requiere de $c\lfloor\log_2(2^k)\rfloor = c\lfloor k\rfloor = ck$ operaciones. Si el tamaño de entrada es $m^2 = (2^k)^2 = 2^{2k}$, entonces el número de operaciones requerido es $c\lfloor\log_2(2^{2k})\rfloor = c\lfloor 2k\rfloor = 2(ck)$. Que es el número de operaciones dobles.

b. Como en el inciso *a*), para una entrada de tamaño $m = 2^k$, donde k es un entero positivo, el algoritmo requiere ck operaciones. Si se incrementa el tamaño de entrada a $m^{10} = (2^k)^{10} = 2^{10k}$, entonces el número de operaciones requeridas es $c\lfloor\log_2(2^{10k})\rfloor = c\lfloor 10k\rfloor = 10(ck)$. Así el número de operaciones aumenta en un factor de 10.

c. Cuando el tamaño de entrada aumenta de 2^7 a 2^{28}, el factor con el que el número de operaciones aumenta es $\frac{c\lfloor\log_2(2^{28})\rfloor}{c\lfloor\log_2(2^7)\rfloor} = \frac{28c}{7c} = 4$.

3. Una pequeña exploración numérica puede ayudar para encontrar una ventana inicial para dibujar las gráficas de $y = x$ y de $y = [50\log_2 x]$. Observe que $x = 2^8 = 256$, $\lfloor 50\log_2 x\rfloor = \lfloor 50\log_2(2^8)\rfloor = \lfloor 50\cdot 8\rfloor = \lfloor 400\rfloor = 400 > 256 = x$. Pero cuando $x = 2^9 = 512$, $\lfloor 50\log_2 x\rfloor = \lfloor 50\log_2(2^9)\rfloor = \lfloor 50\cdot 9\rfloor = \lfloor 450\rfloor = 450 < 512 = x$. Así una buena elección de una ventana inicial sería el intervalo de 256 a 512. Dibujando las gráficas , acerque si es necesario y al usar la característica de trazo se encuentra que cuando < 438, $n < \lfloor 50\log_2 n\rfloor$.

5. a.

índice	0			1
inf	1			
superior	10	4	1	
medio		5	2	1

b.

índice	0				
inf	1	6		7	
superior	10		7		6
medio		5	8	6	7

7. a. $superior - inf + 1$

b. *Demostración:* Suponga que *superior* e *inf* son enteros positivos dados tales que $superior - inf + 1$ es un número impar. Entonces, por definición de impar, hay un entero k tal que

$$superior - inf + 1 = 2k + 1$$

Sumando $2 \cdot inf - 1$ a ambos lados se obtiene

$$\begin{aligned} inf + superior &= 2 \cdot inf - 1 + 2k + 1 \\ &= 2(inf + k). \end{aligned}$$

Pero $inf + k$ es un entero. Por lo tanto, por definición de par $inf + superior$.

8.

n	27	13	6	3	1	0

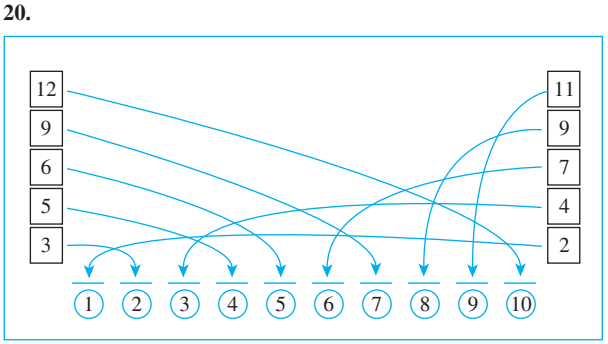
9. Para cada entero positivo, n, $n \; div \; 2 = \lfloor n/2 \rfloor$. Así cuando el segmento del algoritmo se ejecuta para una n particular y el bucle **while** ha iterado una vez, la entrada de la siguiente iteración es $\lfloor n/2 \rfloor$. Se tiene que el número de iteraciones del bucle para n es uno más que el número de iteraciones para $\lfloor n/2 \rfloor$. Esto es $a_n = 1 + a_{\lfloor n/2 \rfloor}$. También $a_1 = 1$.

10. La relación de recurrencia y condición inicial de $a_1, a_2, a_3, \ldots$ deducida en el ejercicio 9 son iguales a aquellas de la sucesión $w_1, w_2, w_3, \ldots$ analizadas en el peor de los casos de la búsqueda del algoritmo binario. Así las fórmulas generales para los dos casos son las mismas. Esto es $a_n = 1 + \lfloor \log_2 n \rfloor$, para todos los enteros $n \geq 1$.

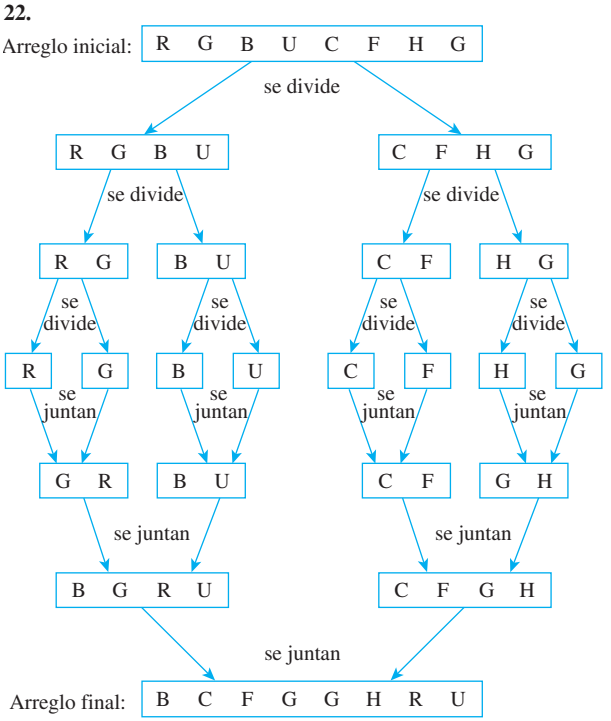
11. En el análisis del algoritmo de la búsqueda binaria, se muestra que $1 + \lfloor \log_2 n \rfloor$ es $\Theta(\log_2 n)$. Así el segmento de algoritmo tiene orden $\log_2 n$.

14. *Sugerencia:* La fórmula es $b_n = 1 + \lfloor \log_3 n \rfloor$.

20.



22.



24. b. Consulte la figura 11.5.3 y observe que cuando k es impar, el subarreglo $a[inf]$, $a[inf + 1]$, …, $a[medio]$ tiene longitud $(k + 1)/2 = \lceil k/2 \rceil$ y que cuando k es par, también tiene longitud $k/2 = \lceil k/2 \rceil$.

25. *Sugerencia:* Los siguientes son los pasos para el inciso *a*) en el caso en que k es impar y $k + 1$ es par:

$$\begin{aligned}
& m_{k+1} = m_{\lfloor (k+1)\ 2 \rfloor} + m_{\lceil (k+1)/2 \rceil} + (k+1) - 1 \\
\Rightarrow\ & m_{k+1} = m_{(k+1)/2} + m_{(k+1)/2} + (k+1) - 1 \\
& \qquad \text{por el teorema 4.5.2 y el ejercicio 19 de la sección 4.5 ya que } k+1 \text{ es par} \\
\Rightarrow\ & m_{k+1} = 2m_{(k+1)/2} + k \\
\Rightarrow\ & m_{k+1} \geq 2 \cdot \left[\tfrac{1}{2} \cdot \left(\tfrac{k+1}{2} \right) \log_2 \left(\tfrac{k+1}{2} \right) \right] + k \\
& \qquad \text{es la hipótesis de inducción} \\
\Rightarrow\ & m_{k+1} \geq \left(\tfrac{k+1}{2} \right) [\log_2 (k+1) - \log_2 2] + k \\
\Rightarrow\ & m_{k+1} \geq \tfrac{1}{2}(k+1)[\log_2 (k+1) - 1] + k \\
\Rightarrow\ & m_{k+1} \geq \tfrac{1}{2}(k+1) \log_2 (k+1) - \left(\tfrac{k+1}{2} \right) + \tfrac{2k}{2} \\
\Rightarrow\ & m_{k+1} \geq \tfrac{1}{2}(k+1) \log_2 (k+1) + \tfrac{k-1}{2} \\
\Rightarrow\ & m_{k+1} \geq \tfrac{1}{2}(k+1) \log_2 (k+1)
\end{aligned}$$

Sección 12.1

1. a. $L_1 = \{\epsilon, x, y, xx, yy, xxx, xyx, yxy, yyy, xxxx, xyyx, yxxy, yyyy\}$

b. $L_2 = \{x, xx, xy, xxx, xxy, xyx, xyy\}$

3. a. $(a + b) \cdot (c + d)$

b. *Respuesta parcial:* $11* = 1 \cdot 1 = 1$, $12* = 1 \cdot 2 = 2$, $21/ = 2/1 = 2$

4. L_1L_2 es el conjunto de todas las cadenas de a y b que comienzan con un a y contienen un número impar de a.

$L_1 \cup L_2$ es el conjunto de todas las cadenas de a y que contienen un número par de a o que comienzan con una a y contienen sólo una a. (Observe que porque o es un número par, tanto e como b están en $L_1 \cup L_2$).

$(L_1 \cup L_2)^*$ es el conjunto de todas las cadenas de a y b. La razón es que a y b están ambas en $L_1 \cup L_2$ y así cada cadena en a y b $(L_1 \cup L_2)^*$.

7. $(a \mid ((b^*)b))((a^*) \mid (ab))$

10. $(ab^* \mid cb^*)(ac \mid bc)$

13.
$$\begin{aligned} L(\epsilon \mid ab) &= L(\epsilon) \cup L(ab) = \{\epsilon\} \cup L(a)L(b) \\ &= \{\epsilon\} \cup \{xy \mid x \in L(a) \text{ y } \ y \in L(b)\} \\ &= \{\epsilon\} \cup \{xy \mid x \in \{a\} \text{ y } \ y \in \{b\}\} \\ &= \{\epsilon\} \cup \{ab\} = \{\epsilon, ab\} \end{aligned}$$

16. Aquí son cinco cadenas de infinitamente muchos: 0101, 1, 01, 10000 y 011100.

19. El idioma está conformado por todas las cadenas de a y b que contiene exactamente tres a y al final una a.

22. *aaaba* está en el lenguaje pero *baabb* no está, porque si una cadena en el lenguaje contiene una b a la derecha de la izquierda más a, entonces debe contener otra a a la derecha de todas las b.

25. Una solución es 0* 10*(0*10*10*)*.

28.
$$\begin{aligned} L((r \mid s)t) &= L(r \mid s)L(t) = (L)r(\cup L)s))L(t) \\ &= \{xy \mid x \in (L(r) \cup L(s)) \text{ y } y \in L(t)\} \\ &= \{xy \mid (x \in L(r) \text{ o } \ x \in L(s)) \text{ y } \ y \in L(t)\} \\ &= \{xy \mid (x \in L(r) \text{ y } \ y \in L(t)) \text{ o } \\ &\qquad (x \in L)s(\text{ y } \ y \in L(t))\} \\ &= \{xy \mid xy \in L(rt) \text{ o } xy \in L(st)\} \\ &= L(rt) \cup L(st) \\ &= L(rt \mid st) \end{aligned}$$

31. $pre[a - z]^+$

34. $[a - z]^*(a \mid e \mid i \mid o \mid u)]a - z]^*$

37. [0 − 9]{3} - {0 − 9]{2} - [0 − 9]{4}

39. $([+ -] \mid \epsilon)[0 - 9]^*(\backslash. \mid \epsilon)[0 - 9]^*$

40. *Sugerencia:* Los años bisiestos desde 1980 a 2079 son 1980, 1984, 1988, 1992, 1996, 2000, 2004, etc.. Observe que el cuarto dígito es 0, 4, o 8 para aquellos cuyo tercer dígito es par y cuyo cuarto dígito es 2 o 6 para aquellos cuyo tercer dígito es impar.

Sección 12.2

1. **a.** \$1 o más depositado

2. **a.** s_0, s_1, s_2 **b.** 0, 1 **c.** s_0 **d.** s_2
e. Anote en la tabla de estado siguiente:

		Entrada	
		0	1
→	s_0	s_1	s_0
Estado	s_1	s_1	s_2
◎	s_2	s_2	s_2

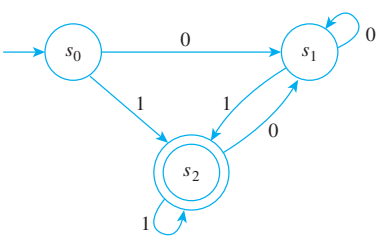
5. **a.** A, B, C, D, E, F **b.** x, y **c.** A **d.** D, E
e. Anote en la tabla de estado siguiente:

		Entrada	
		x	y
→	A	C	B
	B	F	D
Estado	C	E	F
◎	D	F	D
◎	E	E	F
	F	F	F

7. **a.** s_0, s_1, s_2, s_3 **b.** 0, 1 **c.** s_0 **d.** s_0, s_2
e. Anote en la tabla de estado siguiente:

		Entrada	
		0	1
→ ◎	s_0	s_0	s_1
Estado	s_1	s_1	s_2
◎	s_2	s_2	s_3
	s_3	s_3	s_0

8. **a.** s_0, s_1, s_2 **b.** 0, 1 **c.** s_0 **d.** s_2
e.



10. **a.** $N(s_1, 1) = s_2$, $N(s_0, 1) = s_3$
c. $N^*(s_0, 10011) = s_2$, $N^*(s_1, 01001) = s_2$

11. **a.** $N(s_3, 0) = s_4$, $N(s_2, 1) = s_4$
c. $N^*(s_0, 010011) = s_3$, $N^*(s_3, 01101) = s_4$

Observe que existen múltiples respuestas correctas por el inciso *d*) de los ejercicios 12 y 13, el inciso *b*) de los ejercicios del 14 al 19 y para los ejercicios del 20 al 48.

12. **a.** (i) s_2 (ii) s_2 (iii) s_1
b. los de (i) y (ii) pero no (iii).
c. El lenguaje aceptado por este autómata es el conjunto de todas las cadenas de 0 y 1 que contienen al menos un 0 (no necesariamente inmediatamente) seguido por al menos un 1.
d. 1*00*1(0 | 1)*

14. **a.** El lenguaje aceptado por éste autómata es el conjunto de todas las cadenas de 0 y 1 que terminan en 00.
b. (0 | 1)*00

15. **a.** El lenguaje aceptado por este autómata es el conjunto de todas las cadenas de x y y de longitud al menos dos que tienen puras x o puras y.
b. $xxx^* \mid yyy^*$

17. **a.** El lenguaje aceptado por este autómata es el conjunto de todas las cadenas de 0 y 1 con la siguiente propiedad: si n es el número de 1 en la cadena, entonces $n \ mod \ 4 = 0$ o $n \ mod \ 4 = 2$. Esto equivale a decir que n es par.
b. 0* | (0*10*10*)*

18.a. El lenguaje aceptado por este autómata es el conjunto de todas las cadenas de 0 y 1 que terminan en 1.

b. (0 | 1)*1

20. a. Llame al autómata que está construyendo A. Acepte que una cadena de A depende de los valores de tres entradas consecutivas.

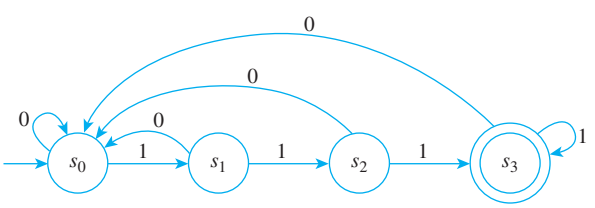
s_0: estado inicial

s_1: indica el estado de que el último carácter que entró era un 1.

s_2: indica el estado de que los dos últimos caracteres que entraron eran 1.

s_3: indica el estado de que los tres últimos caracteres que entraron eran 1, el estado es aceptable

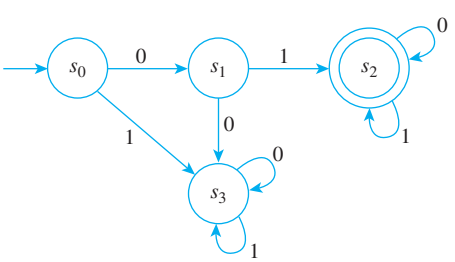
Si un 0 entra en A cuando está en el estado s_0, no hay ningún progreso hacia la realización de una secuencia de tres 1 consecutivos. Así A permanece en el estado s_0. Si un 1 está entrando en A, cuando está en el estado inicial s_0, va al estado s_1, que indica que el último carácter que entró fue un 1. Esto indica que los dos últimos caracteres que entraron eran 1. Pero si se introduce un 0, A regresaría a s_0 porque la espera de una cadena de tres 1 consecutivos debe empezar de nuevo. Cuando A está en estado s_2 y 1 es la entrada, entonces se alcanza una cadena de tres 1 consecutivos, por lo que A irá al estado s_3. Si entra un 0 cuando A está en el estado s_2, entonces la secuencia acumulada de tres 1 que se pierde, por lo que A regresa a s_0. Cuando A está en el estado s_3 y 1 es la entrada, entonces los tres símbolos finales de la cadena de entrada son 1 y así A permanecerá en el estado s_3, entonces A regresaría al estado s_0 para esperar la entrada de más 1. Por lo que el diagrama de transición es el siguiente:



b. (0 | 1)*111

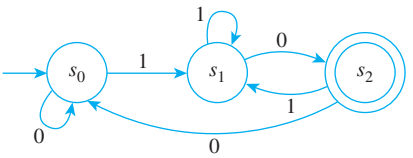
21. *Sugerencia:* Utilice cinco estados: s_0 (el estado inicial), s_1 (el estado que indica que el símbolo anterior que entró fue una a), s_2 (el estado que indica que el símbolo anterior que entró fue una b), s_3 (el estado que indica que los dos símbolos anteriores que entraron eran a) y s_4 (el estado que indica que los dos símbolos anteriores que entraron eran b).

23. a.



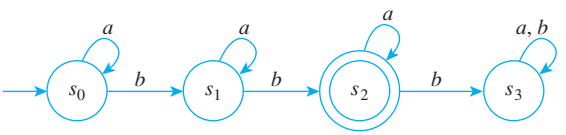
b. 01(0 | 1)*

25. a.



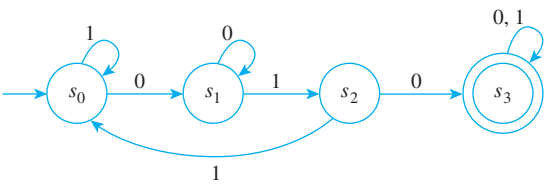
b. (0 | 1)*10

26. a.



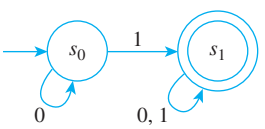
b. *a*ba*ba*

28. a.

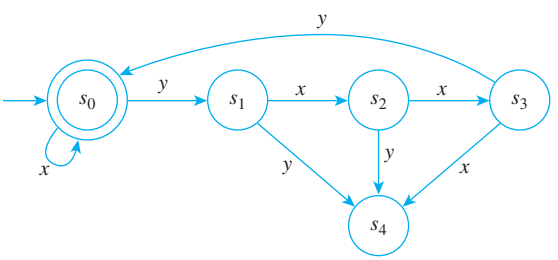


b. (0 | 1)*010(0 | 1)*

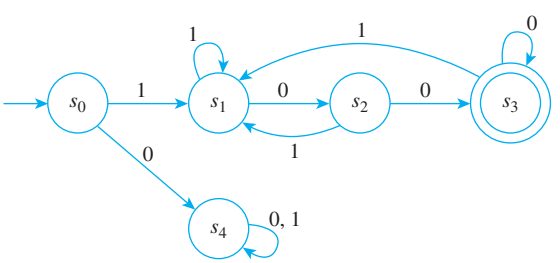
29.



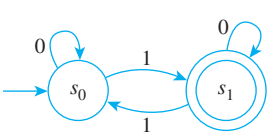
31.



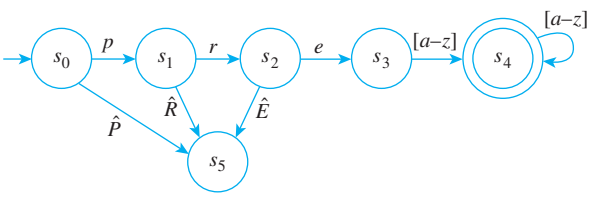
33.



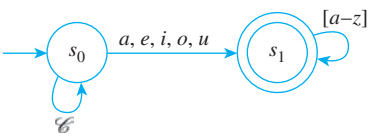
36.



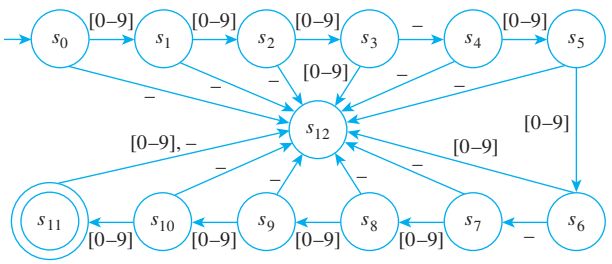
39. Sea que $\hat{P}$ indique una lista de todas las letras de un alfabeto de minúsculas salvo p, $\hat{R}$ denota una lista de todas las letras del alfabeto de minúsculas excepto r y $\hat{E}$ indique una lista de todas las letras de un alfabeto de minúsculas salvo e.



42. Sea que $\mathscr{C}$ denote una lista de todas las consonantes en un alfabeto de minúsculas.



45.



51. *Sugerencia:* Esta demostración es prácticamente idéntica a la del ejemplo 12.2.8. Sólo tome p y q y demuestre que $p > q$. Del hecho de que A acepta $a^p b^p$, se puede deducir que A acepta $a^q b^p$. Ya que $p > q$, esta cadena no está en L.

53. *Sugerencia:* Supongamos que el autómata A tiene N estados. Elija un entero m tal que $(m + 1)^2 - m^2 > N$. Considere cadenas de a de longitud entre m^2 y $(m + 1)^2$.

Ya que hay más cadenas que estados, al menos dos cadenas deben enviar A al mismo estado s_i:

$$\overbrace{\underbrace{aa\ldots a}_{m^2}aa\ldots aaa\ldots aaa\ldots a}^{(m+1)^2}$$

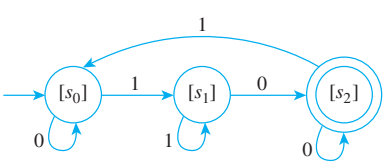
Después de ambas de estas entradas, A está en el estado s_i

Se tiene (eliminando las a que se muestren en color) que el autómata debe aceptar una cadena de forma a^k, donde $m^2 < k < (m + 1)^2$.

Sección 12.3

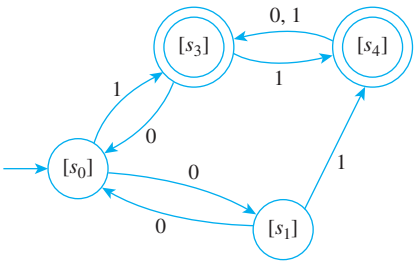
1. a. 0, clases de equivalencia: $\{s_0, s_1, s_3, s_4\}$, $\{s_2, s_5\}$
1, clases de equivalencia: $\{s_0, s_3\}$, $\{s_1, s_4\}$, $\{s_2, s_5\}$
2, clases de equivalencia: $\{s_0, s_3\}$, $\{s_1, s_4\}$, $\{s_2, s_5\}$

b.



4. a. 0, clases de equivalencia: $\{s_0, s_1, s_2\}$, $\{s_3, s_4, s_5\}$
1, clases de equivalencia: $\{s_0, s_1, s_2\}$, $\{s_3, s_5\}$, $\{s_4\}$
2, clases de equivalencia: $\{s_0, s_2\}$, $\{s_1\}$, $\{s_3, s_5\}\{s_4\}$
3, clases de equivalencia: $\{s_0, s_2\}$, $\{s_1\}$, $\{s_3, s_5\}$, $\{s_4\}$

b.

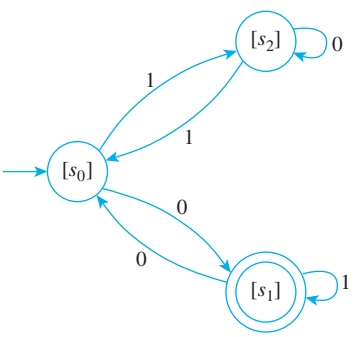


6. a. *Sugerencia:* Las 3, clases de equivalencia son $\{s_0\}$, $\{s_1\}$, $\{s_2\}$, $\{s_3\}$, $\{s_4\}$

7. Sí. para A:

0, clases de equivalencia: $\{s_0, s_2\}$, $\{s_1, s_3\}$
1, clases de equivalencia: $\{s_0\}$, $\{s_2\}$, $\{s_1, s_3\}$
2, clases de equivalencia: $\{s_0\}$, $\{s_2\}$, $\{s_2, s_3\}$

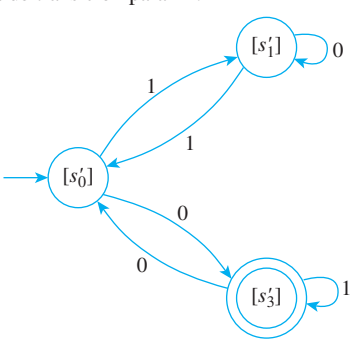
Diagrama de transición para $\overline{A}$:



Para A':

0, clases de equivalencia: $\{s_0', s_1', s_2'\}$, $\{s_3'\}$
1, clases de equivalencia: $\{s_0', s_2'\}$, $\{s_1'\}$, $\{s_3'\}$
2, clases de equivalencia: $\{s_0', s_2'\}$, $\{s_1'\}$, $\{s_3'\}$

Diagrama de transición para $\overline{A'}$:



Excepto por el etiquetado de los estados, los diagramas de la transición para $\overline{A}$ y $\overline{A'}$ son idénticos. Por tanto $\overline{A}$ y $\overline{A'}$ aceptan el mismo lenguaje y por el teorema 12.3.3, A y A' también aceptan el mismo idioma. Por lo tanto A y A' son autómatas equivalentes.

9. Para A:

0, clases de equivalencia: $\{s_1, s_2, s_4, s_5\}, \{s_0, s_3\}$
1, clases de equivalencia: $\{s_1, s_2\}, \{s_4, s_5\}, \{s_0, s_3\}$
2, clases de equivalencia: $\{s_1\}, \{s_2\}, \{s_4, s_5\}, \{s_0, s_3\}$
3, clases de equivalencia: $\{s_1\}, \{s_2\}, \{s_4, s_5\}, \{s_0, s_3\}$

Por lo tanto, los estados de $\overline{A}$ son las 3, clases de equivalencia de A.

Para $\overline{A'}$:

0, clases de equivalencia: $\{s'_2, s'_3, s'_4, s'_5\}, \{s'_0, s'_1\}$
1, clases de equivalencia: $\{s'_2, s'_3, s'_4, s'_5\}, \{s'_0, s'_1\}$

Por lo tanto, los estados de $\overline{A'}$ son la 1-clases de equivalencia de A'.

De acuerdo con el libro, dos autómatas son equivalentes si y sólo si, su autómata cociente es isomorfo, siempre que primero se han eliminado los estados inaccesibles. Ahora A y A' no tienen estados inaccesibles y $\overline{A}$ tiene cuatro estados, mientras que $\overline{A'}$ tiene sólo dos estados. Por lo tanto, A y A' no son equivalentes.

Este resultado también puede obtenerse observando, por ejemplo, que la cadena 11 es aceptada por A' pero no por A.

11. *Respuesta parcial:* Supongamos que A es un autómata de estado finito con el conjunto de estados S y la relación R_* de *-equivalencia de estados. *[Demuestre que R_* es una relación de equivalencia, debemos demostrar que R es reflexiva, simétrica y transitiva.]*

Prueba de que R_* es simétrica:

[Debemos demostrar que para todos los estados s y t, si s R_* t entonces t R_* s.] Suponga que s y t son estados de A tales que $s\ R_*\ t$. [Debemos demostrar que $t\ R_*\ s$.] Ya que $s\ R_*\ t$, entonces para todas las cadenas de entrada w,

$$\begin{bmatrix} N^*(s, w) \text{ es un} \\ \text{estado aceptado} \end{bmatrix} \Leftrightarrow \begin{bmatrix} N^*(t, w) \text{ es un} \\ \text{estado aceptado} \end{bmatrix}$$

donde N^* es la función de estado eventual en A. Pero luego, por la simetría de la relación $\Leftrightarrow$, es cierto que para todas las cadenas de entrada w,

$$\begin{bmatrix} N^*(t, w) \text{ es un} \\ \text{estado aceptado} \end{bmatrix} \Leftrightarrow \begin{bmatrix} N^*(s, w) \text{ es un} \\ \text{estado aceptado} \end{bmatrix}$$

De ahí que $t\ R_*\ s$ *[que era lo que se quería demostrar]*, así R_* es simétrico.

12. La demostración es idéntica a la demostración de propiedad (12.3.1) dado en la solución del ejercicio 11 siempre que aparezca "para todas las cadenas de entrada w" se sustituirá por "para todas las cadenas de entrada w de longitud inferior o igual a k".

13. *Demostración:* Por la propiedad (12.3.2), para cada entero $k \geq 0$, la k-equivalencia es una relación de equivalencia. Pero por el teorema 10.3.4, la distintas clases de equivalencia de una relación de equivalencia forman una partición del conjunto en el que se define la relación. En este caso, la relación se define en los estados del autómata. Así las k-clases de equivalencia forman un partición del conjunto de todos los estados del autómata.

15. *Sugerencia 1:* Suponga que C_k es una k-clase de equivalencia dada pero arbitrariamente elegida. Debe demostrar que existe una $(k-1)$-clase de equivalencia C_{k-1} tal que $C_k \subseteq C_{k-1}$.

Sugerencia 2: si s es cualquier elemento en C_k, s es un estado del autómata. Ahora la $(k-1)$-clase de equivalencia particionan el conjunto de todos los estados del autómata en una unión de subconjuntos mutuamente disjuntos, por lo que $s \in C_{k-1}$ para *alguna* $(k-1)$-clase de equivalencia C_{k-1}.

Sugerencia 3: Demostrar que $C_k \subseteq C_{k-1}$, debe demostrar que para cualquier estado t, si $t \in C_k$, entonces $t \in C_{k-1}$.

17. *Sugerencia:* Si $m < k$, entonces cada cadena de entrada de longitud inferior o igual a m tiene longitud inferior o igual a k.

19. *Sugerencia:* Supongamos que dos estados s y t son equivalentes. Debe demostrar que para cualquier símbolo de entrada m, los siguientes $N(s, m)$ estados y $N(t, m)$ son equivalentes. Para ello, utilice la definición de equivalencia y el hecho de que para cualquier cadena w', símbolo de entrada m y estado s, $N^*(N(s, m), w') = N^*(s, mw')$.

ÍNDICE

CRÉDITOS

Esta página constituye una extensión de la página de derechos de autor. Hemos hecho todo lo posible para localizar a los propietarios de todo el material con derechos de autor y para obtener el permiso de los titulares de éstos. En caso de que surja algún problema en cuanto al uso de cualquier material, estaremos encantados de hacer las correcciones necesarias en futuras ediciones. Se agradece a los siguientes autores, editores y agentes, la autorización para utilizar el material indicado.

Capítulo 1 **10** Problemy monthly, Julio 1959

Capítulo 2 **23** Bettmann/CORBIS; **32** Culver Pictures; **60** Indiana University Archives; **64** MIT Museum; **65** (izquierda) Cortesía de IBM; **65** (derecha) Intel; **69** CORBIS; **74** Harvard University Archives

Capítulo 3 **98** (arriba) Culver Pictures; **98** (abajo) Friedrich Schiller, Universitat Jena; **105** Dominio público; **122** Dominio público; **137** Culver Pictures

Capítulo 4 **160** (arriba) Bettmann/CORBIS; **160** (abajo) Andrew Wiles/Princeton University; **208** Bettmann/CORBIS; **211** (arriba) Cortesía de Ben Joseph Green; **211** (abajo) UCLA; **212** The Art Gallery Collection/Alamy; **214** Hulton Archive/Getty Images; **218** Suleymaniye Kutuphanesi

Capítulo 5 **230** Corbis; **279** The University of Texas en Austin; **280** Cortesía de Christiane Floyd; **282** Cortesía de Tony Hoare; **292** Academie Royale de Belgique; **293** (izquierda) Cortesía de Francis Lucas; **293** (derecha) Cortesía de Paul Stockmeyer; **297** Bettmann/CORBIS; **332** (arriba) Roger Ressmeyer/CORBIS; **332** (abajo) Dominio público

Capítulo 6 **336** David Eugene Smith Colletion, Columbia University; **340** Royal Society of London; **341** Stock Montage; **378** Sylvia Salmi; **379** Dominio público

Capítulo 7 **384** Stock Montage; **390** Cortesía de U.S. Naval Academy; **428** iStockphoto.com/Steven Wynn; **433** (arriba) Dominio público; **433** (abajo) Bettmann/CORBIS

Capítulo 8 **472** Bettmann/CORBIS; **479** Cortesía de Leonard Adleman

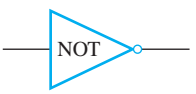
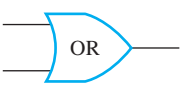
Capítulo 9 **516** Reimpreso con permiso de United Feature Syndicate, Inc.; **520** Bettmann/CORBIS; **593** Hulton-Deutch Collection/CORBIS; **605** Yevgeny Khaldei/CORBIS; 616 Cortesía de Stephen Stigler

Capítulo 10 **630** Wikipedia/Chris 73; **643** (arriba) Merian-Erben; **643** (abajo) Bettmann/CORBIS; **653** Bettmann/CORBIS; **669** David Eugene Smith Collection, Rare Book and Manuscript Library, Columbia University; **685** (arriba) Cortesía de IBM Corporation; **685** (abajo) Cortesía de Peter Naur; **686** Bettmann/CORBIS; **704** Cortesía de Joseph Kruskal; **707** Cortesía de Alcatel-Lucent Technologies

Capítulo 11 **717** Bettmann/CORBIS; **739** Bettmann/CORBIS; **740** Cortesía de Donald Knuth; **752** Bettmann/CORBIS

Capítulo 12 **780** Fotografía de Norman Lenburg, 1979. Cortesía de University of Wisconsin-Madison Archives; **781** University of Wisconsin; **793** (arriba) David Eugene Smith Collection, Rare Book and Manuscript Library, Columbia Universisty; **793** (abajo) Time & Life Pictures/Getty Images

Lista de símbolos

Tema	Símbolo	Significado	Página
Lógica	$\sim p$	no p	25
	$p \wedge q$	p y q	25
	$p \vee q$	p o q	25
	$p \oplus q$ o p XOR q	p o q pero no ambos p y q	28
	$P \equiv Q$	P es lógicamente equivalente a Q	30
	$p \rightarrow q$	si p entonces q	40
	$p \leftrightarrow q$	p si y sólo si q	45
	$\therefore$	por tanto	51
	$P(x)$	predicado en x	97
	$P(x) \Rightarrow Q(x)$	cada elemento en el conjunto verdadero para $P(x)$ está en el conjunto verdadero para $Q(x)$	104
	$P(x) \Leftrightarrow Q(x)$	$P(x)$ y $Q(x)$ tienen conjuntos verdaderos idénticos	104
	$\forall$	para todo	101
	$\exists$	existe	103
Aplicaciones a la lógica		NOT-puerta	67
		AND-puerta	67
		OR-puerta	67
		NAND-puerta	75
		NOR-puerta	75
	$\mid$	trazo de Sheffer	74
	$\downarrow$	flecha de Peirce	74
	n_2	número escrito en notación binaria	78
	n_{10}	número escrito en notación decimal	78
	n_{16}	número escrito en notación hexadecimal	91
Teoría de números y aplicaciones	$d \mid n$	d divide n	170
	$d \nmid n$	d no divide a n	172
	$n \text{ div } d$	el cociente entero de n dividido entre d	181
	$n \bmod d$	el residuo entero de n dividido entre d	181
	$\lfloor x \rfloor$	el piso de x	191
	$\lceil x \rceil$	el techo de x	191
	$\lvert x \rvert$	el valor absoluto de x	187
	mcd(a, b)	el máximo común divisor de a y b	220
	$x := e$	x se le asigna el valor e	214

Tema	Símbolo	Significado	Página
Secuencias	$\ldots$	y así sucesivamente	227
	$\sum_{k=m}^{n} a_k$	la suma de k igual a m a n de a_k	230
	$\prod_{k=m}^{n} a_k$	el producto de k igual a m a n de a_k	223
	$n!$	n factorial	237
Teoría de conjuntos	$a \in A$	a es un elemento de A	7
	$a \notin A$	a no es un elemento de A	7
	$\{a_1, a_2, \ldots, a_n\}$	el conjunto con elementos $a_1, a_2, \ldots, a_n$	7
	$\{x \in D \mid P(x)\}$	el conjunto de todas las x en D para las que $P(x)$ es verdadero	8
	$\mathbf{R}, \mathbf{R}^-, \mathbf{R}^+, \mathbf{R}^{noneg}$	los conjuntos de todos los números reales, números reales negativos, números reales positivos y números reales no negativos	7, 8
	$\mathbf{Z}, \mathbf{Z}^-, \mathbf{Z}^+, \mathbf{Z}^{noneg}$	los conjuntos de todos los enteros, enteros negativos, enteros positivos y enteros no negativos	7, 8
	$\mathbf{Q}, \mathbf{Q}^-, \mathbf{Q}^+, \mathbf{Q}^{noneg}$	los conjuntos de todos los números racionales, números racionales negativos, números racionales positivos y números racionales no negativos	7, 8
	$\mathbf{N}$	el conjunto de los números naturales	8
	$A \subseteq B$	A es subconjunto de B	9
	$A \not\subseteq B$	A no es subconjunto de B	9
	$A = B$	A es igual a B	339
	$A \cup B$	A unión B	341
	$A \cap B$	A intersección B	341
	$B - A$	la diferencia B menos A	341
	A^c	el complemento de A	341
	(x, y)	par ordenado	11
	$(x_1, x_2, \ldots, x_n)$	n-tupla ordenada	346
	$A \times B$	el producto cartesiano de A y B	12
	$A_1 \times A_2 \times \cdots \times A_n$	el producto cartesiano de $A_1, A_2, \ldots, A_n$	347
	$\emptyset$	el conjunto vacío	361
	$\mathscr{P}(A)$	el conjunto de potencias de A	346

Lista de símbolos

Tema	Símbolo	Significado	Página
Conteo y probabilidad	$N(A)$	el número de elementos del conjunto A	518
	$P(A)$	la probabilidad de un conjunto A	518
	$P(n, r)$	el número de r-permutaciones de un conjunto de n elementos	553
	$\binom{n}{r}$	se eligen r de n, el número de r combinaciones de un conjunto de n elementos, el número de subconjuntos de r elementos de un conjunto de n elementos	566
	$[x_{i_1}, x_{i_2}, \ldots, x_{i_r}]$	muticonjunto de tamaño r	584
	$P(A \mid B)$	la probabilidad de A dado B	612
Funciones	$f: X \to Y$	f es una función de X a Y	384
	$f(x)$	el valor de f en x	384
	$x \xrightarrow{f} y$	f manda x a y	384
	$f(A)$	la imagen de A	397
	$f^{-1}(C)$	la imagen inversa de C	397
	I_x	la función identidad en X	387
	b^x	b elevado a la potencia x	405, 406
	$\exp_b(x)$	b elevado a la potencia x	405, 406
	$\log_b(x)$	logaritmo con base b de x	388
	F^{-1}	función inversa de F	411
	$f \circ g$	composición de g y f	417
Eficiencia del algoritmo	$x \cong y$	x es aproximadamente igual a y	237
	$O(f(x))$	O mayúscula de f de x	727
	$\Omega(f(x))$	Omega mayúscula de f de x	727
	$\Theta(f(x))$	Theta mayúscula de f de x	727
Relaciones	$x\,R\,y$	x está relacionado con y a través de R	14
	R^{-1}	la relación inversa de R	444
	$m \equiv n \pmod{d}$	m es congruente a n módulo d	473
	$[a]$	la clase de equivalencia de a	465
	$x \preceq y$	x está relacionado con y a través de la relación de orden parcial $\preceq$	502

Continúa en la primera página de la cubierta trasera

Lista de símbolos

Tema	Símbolo	Significado	Página
Lenguajes formales y autómata de estado finito	Σ	un alfabeto de un lenguaje	780
	ϵ	la cadena nula	529
	Σ^n	el conjunto de todas las cadenas en Σ de longitud n	781
	Σ^*	el conjunto de todas las cadenas en Σ	781
	Σ^+	el conjunto de todas las cadenas en Σ con longitud al menos de 1	781
	LL'	la concatenación de lenguajes L y L'	783
	L^*	la cerradura Kleene de L	783
	(rs), $(r \mid s)$, (r^*)	expresiones regulares	783
	$[x_1 - x_n]$, $[\hat{}x_m - x_n]$	clases de caracteres	787
	$x+$, $x?$, $x\{n\}$, $x\{m, n\}$	notaciones taquigráficas para expresiones regulares	788
	$N\{s, m\}$	el valor de la función siguiente estado para un estado s y símbolo de entrada m	793, 794
	$\rightarrow (s_0)$	estado inicial	793
	$((s_a))$	estado de aceptación	793
	$L(A)$	lenguaje aceptado por A	795
	$N^*(s, w)$	el valor de la función de estado eventual para un estado s y una cadena de entrada w	796, 797
	$s\, R_*\, t$	s y t son $*$-equivalentes	809
	$s\, R_k\, t$	s y t son k-equivalentes	810
	$\overline{A}$	el autómata cociente de A	813
Matrices	$\mathbf{A}$	matriz	661
	$\mathbf{I}$	matriz identidad	669, 670
	$\mathbf{A} + \mathbf{B}$	suma de matrices $\mathbf{A}$ y $\mathbf{B}$	675
	$\mathbf{AB}$	producto de matrices $\mathbf{A}$ y $\mathbf{B}$	666, 667
	$\mathbf{A}^n$	matrices $\mathbf{A}$ a la potencia n	678
Gráficas y árboles	$V(G)$	el conjunto de vértices de una gráfica G	626
	$E(G)$	el conjunto de extremos de una gráfica G	626
	$\{v, w\}$	el extremo que une a v con w en una gráfica simple	632, 633
	K_n	gráfica completa con n vértices	633
	$K_{m,n}$	gráfica bipartita completa de (m, n) vértices	633
	$deg(v)$	grado del vértice v	635
	$v_0e_1v_1e_2 \cdots e_nv_n$	un camino de v_0 a v_n	644
	$w(e)$	el peso del extremo e	704
	$w(G)$	el peso total de la gráfica G	704

Fórmulas de referencia

Tema	Nombre	Fórmula	Página
Lógica	Ley de De Morgan	$\sim(p \wedge q) \equiv \sim p \vee \sim q$	32
	Ley de De Morgan	$\sim(p \vee q) \equiv \sim p \wedge \sim q$	32
	Negación de $\rightarrow$	$\sim(p \rightarrow q) \equiv p \wedge \sim q$	42
	Equivalencia de un condicional y su contrapositivo	$p \rightarrow q \equiv \sim q \rightarrow \sim p$	43
	No equivalencia de un condicional y su converso	$p \rightarrow q \not\equiv q \rightarrow p$	44
	No equivalencia de un condicional y su inverso	$p \rightarrow q \not\equiv \sim p \rightarrow \sim q$	44
	Negación de un enunciado universal	$\sim(\forall x \text{ en } D, Q(x)) \equiv \exists x \text{ en } D \text{ tal que } \sim Q(x)$	109
	Negación de un enunciado existencial	$\sim(\exists x \text{ en } D \text{ tal que } Q(x)) \equiv \forall x \text{ en } D, \sim Q(x)$	109
Sumas	Suma de los primeros n enteros	$1 + 2 + \cdots + n = \dfrac{n(n+1)}{2}$	248
	Suma de las potencias de r	$1 + r + r^2 + \cdots + r^n = \dfrac{r^{n+1} - 1}{r - 1}$	252
Conteo y probabilidad	Probabilidad en el caso de eventos equiprobables	$P(E) = \dfrac{N(E)}{N(S)}$	518
	Número de r-permutaciones de un conjunto con n elementos	$P(n, r) = \dfrac{n!}{(n-r)!}$	533
	Número de elementos en una unión	$N(A \cup B) = N(A) + N(B) - N(A \cap B)$	546
	Número de subconjuntos de tamaño r de un conjunto con n elementos	$\binom{n}{r} = \dfrac{n!}{r!\ n-r)!}$	568
	Fórmula de Pascal	$\binom{n+1}{r} = \binom{n}{r-1} = \binom{n}{r}$	593

Tema	Nombre	Fórmula	Página
Conteo y probabilidad	Teorema del binomio	$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$	598
	Probabilidad del complemento de un evento	$P(A^c) = 1 - P(A)$	543
	Probabilidad de una unión	$P(A \cup B) = P(A) + P(B) - P(A \cap B)$	606
	Probabilidad condicional	$P(A \mid B) = \dfrac{P(A \cap B)}{P(B)}$	612
	Fórmula de Bayes	$P(B_k \mid A) = \dfrac{P(A \mid B_k)P(B_k)}{P(A \mid B_1)P(B_1) + P(A \mid B_2)P(B_2) + \cdots + P(A \mid B_n)P(B_n)}$	616
Leyes de los exponentes		$b^0 = 1$	405
		$b^{-x} = \dfrac{1}{b^x}$	405
		$b^u \cdot b^v = b^{u+v}$	406
		$\dfrac{b^u}{b^v} = b^{u-v}$	406
		$(b^u)^v = b^{u \cdot v}$	406
		$(bc)^u = b^u \cdot c^u$	406
		$b^u = b^v \Rightarrow u = v$	406
Propiedades de los logaritmos		$\log_b x = y \Leftrightarrow b^y = x$	406
		$\log_b(xy) = \log_b(x) + \log_b(y)$	406
		$\log_b(x^a) = a \log_b(x)$	406
		$\log_b\left(\dfrac{x}{y}\right) = \log_b(x) - \log_b(y)$	406
		$\log_c(x) = \dfrac{\log_b(x)}{\log_b(c)}$	406
		$\log_b(u) = \log_b(v) \Rightarrow u = v$	406

Matemáticas discretas con aplicaciones, de Susanna Epp, cuarta edición, ofrece una introducción clara a la matemática discreta. Célebre por su prosa lúcida y accesible, Epp explica conceptos complejos y abstractos con claridad y precisión. Este libro presenta no sólo los temas principales de la matemática discreta, sino también el razonamiento que subyace el pensamiento matemático. Los estudiantes desarrollan la capacidad de pensar en forma abstracta del mismo modo en que ellos estudian las ideas de la lógica y la demostración. Mientras se aprende acerca de conceptos tales como circuitos lógicos y adición de equipo, análisis de algoritmos, pensamiento recursivo, computabilidad, autómatas, criptografía y combinatoria, los estudiantes descubren que las ideas de la matemática discreta subyacen y son esenciales para la ciencia y la tecnología de la era de las computadoras. En general, Epp hace énfasis en el razonamiento y proporciona a los alumnos una base sólida para Ciencias de la computación y cursos de matemáticas de nivel superior.

Características

- Epp enfrenta dificultades inherentes en la lógica de la comprensión y el lenguaje con ejemplos muy concretos y fáciles para conceptualizar, un enfoque que ayuda a los estudiantes con una variedad de fondo a entender el razonamiento matemático básico y permite construir mejores argumentos matemáticos.
- Alrededor de 2500 ejercicios proporcionan una amplia práctica para los estudiantes, con numerosos problemas aplicados, cubriendo una impresionante variedad de aplicaciones.
- Más de 500 ejemplos trabajados en formato de solución del problema. Las demostraciones de soluciones se desarrollan intuitivamente en dos pasos, un debate sobre cómo enfocar la prueba y un resumen de la solución, para permitir a los estudiantes la elección más rápida o más deliberada de las instrucciones dependiendo de qué tan bien entienden el problema.
- Organización flexible, que permiten a los instructores mezclar fácilmente los temas principales y los temas opcionales para adaptarse a una amplia variedad de programas de estudios de los cursos de matemáticas discretas.
- Características, definiciones, teoremas y tipos de ejercicios se definen con claridad y son fácilmente navegables, haciendo el libro una excelente referencia que los estudiantes desean mantener y consultar continuamente para sus cursos posteriores.

CENGAGE Learning™

ISBN-13: 978-607481757-7
ISBN-10: 607481757-X

9 786074 817577

http://latinoamerica.cengage.com