Solution: The bitwise OR, bitwise AND, and bitwise XOR of these strings are obtained by taking the OR, AND, and XOR of the corresponding bits, respectively. This gives us

\[
\begin{array}{c}
01 & 1011 & 0110 \\
11 & 0001 & 1101 \\
11 & 1011 & 1111 & \text{bitwise OR} \\
01 & 0001 & 0100 & \text{bitwise AND} \\
10 & 1010 & 1011 & \text{bitwise XOR}
\end{array}
\]

Exercises

1. Which of these sentences are propositions? What are the truth values of those that are propositions?
   a) Boston is the capital of Massachusetts.
   b) Miami is the capital of Florida.
   c) \(2 + 3 = 5\).
   d) \(5 + 7 = 10\).
   e) \(x + 2 = 11\).
   f) Answer this question.

2. Which of these are propositions? What are the truth values of those that are propositions?
   a) Do not pass go.
   b) What time is it?
   c) There are no black flies in Maine.
   d) \(4 + x = 5\).
   e) The moon is made of green cheese.
   f) \(2^n \geq 100\).

3. What is the negation of each of these propositions?
   a) Today is Thursday.

4. Let \(p\) and \(q\) be the propositions
   
   \(p: I\) bought a lottery ticket this week.
   \(q: I\) won the million dollar jackpot on Friday.

   Express each of these propositions as an English sentence.
   a) \(\neg p\)
   b) \(p \lor q\)
   c) \(p \rightarrow q\)
   d) \(p \land q\)
   e) \(p \leftrightarrow q\)
   f) \(\neg p \rightarrow \neg q\)
   g) \(\neg p \land \neg q\)
   h) \(\neg p \lor (p \land q)\)

5. Let \(p\) and \(q\) be the propositions “Swimming at the New Jersey shore is allowed” and “Sharks have been spotted near the shore,” respectively. Express each of these compound propositions as an English sentence.
   a) \(\neg q\)
   b) \(p \land q\)
   c) \(\neg p \lor q\)
   d) \(p \rightarrow \neg q\)
   e) \(\neg q \rightarrow p\)
   f) \(\neg p \land \neg q\)
   g) \(p \leftrightarrow \neg q\)
   h) \(\neg p \land (p \lor \neg q)\)

---

Links

JOHN WILDER TUKEY (1915–2000)  Tukey, born in New Bedford, Massachusetts, was an only child. His parents, both teachers, decided home schooling would best develop his potential. His formal education began at Brown University, where he studied mathematics and chemistry. He received a master’s degree in chemistry from Brown and continued his studies at Princeton University, changing his field of study from chemistry to mathematics. He received his Ph.D. from Princeton in 1939 for work in topology, when he was appointed an instructor in mathematics at Princeton. With the start of World War II, he joined the Fire Control Research Office, where he began working in statistics. Tukey found statistical research to his liking and impressed several leading statisticians with his skills. In 1945, at the conclusion of the war, Tukey returned to the mathematics department at Princeton as a professor of statistics, and he also took a position at AT&T Bell Laboratories. Tukey founded the Statistics Department at Princeton in 1966 and was its first chairman. Tukey made significant contributions to many areas of statistics, including the analysis of variance, the estimation of spectra of time series, inferences about the values of a set of parameters from a single experiment, and the philosophy of statistics. However, he is best known for his invention, with J. W. Cooley, of the fast Fourier transform. In addition to his contributions to statistics, Tukey was noted as a skilled wordsmith; he is credited with coining the terms bit and software.

Tukey contributed his insight and expertise by serving on the President’s Science Advisory Committee. He chaired several important committees dealing with the environment, education, and chemicals and health. He also served on committees working on nuclear disarmament. Tukey received many awards, including the National Medal of Science.

HISTORICAL NOTE  There were several other suggested words for a binary digit, including binit and bigit, that never were widely accepted. The adoption of the word bit may be due to its meaning as a common English word. For an account of Tukey’s coining of the word bit, see the April 1984 issue of Annals of the History of Computing.
6. Let $p$ and $q$ be the propositions “The election is decided” and “The votes have been counted,” respectively. Express each of these compound propositions as an English sentence.

$$
\begin{align*}
  a) & \quad \neg p \\
  b) & \quad p \lor q \\
  c) & \quad p \land q \\
  d) & \quad q \rightarrow p \\
  e) & \quad \neg q \rightarrow \neg p \\
  f) & \quad p \leftrightarrow q \\
  g) & \quad p \lor (\neg p \land q)
\end{align*}
$$

7. Let $p$ and $q$ be the propositions

$p$ : It is below freezing.
$q$ : It is snowing.

Write these propositions using $p$ and $q$ and logical connectives.

$$
\begin{align*}
  a) & \quad \text{It is below freezing and snowing.} \\
  b) & \quad \text{It is below freezing but not snowing.} \\
  c) & \quad \text{It is not below freezing and it is not snowing.} \\
  d) & \quad \text{It is either snowing or below freezing (or both).} \\
  e) & \quad \text{If it is below freezing, it is also snowing.} \\
  f) & \quad \text{It is either below freezing or it is snowing, but it is not snowing if it is below freezing.} \\
  g) & \quad \text{That it is below freezing is necessary and sufficient for it to be snowing.}
\end{align*}
$$

8. Let $p$, $q$, and $r$ be the propositions

$p$ : You have the flu.
$q$ : You miss the final examination.
$r$ : You pass the course.

Express each of these propositions as an English sentence.

$$
\begin{align*}
  a) & \quad p \rightarrow q \\
  b) & \quad \neg q \leftrightarrow r \\
  c) & \quad q \rightarrow \neg r \\
  d) & \quad p \lor q \lor r \\
  e) & \quad (p \rightarrow \neg r) \lor (q \rightarrow \neg r) \\
  f) & \quad (p \land q) \lor (\neg q \land r)
\end{align*}
$$

9. Let $p$ and $q$ be the propositions

$p$ : You drive over 65 miles per hour.
$q$ : You get a speeding ticket.

Write these propositions using $p$ and $q$ and logical connectives.

$$
\begin{align*}
  a) & \quad \text{You do not drive over 65 miles per hour.} \\
  b) & \quad \text{You drive over 65 miles per hour, but you do not get a speeding ticket.} \\
  c) & \quad \text{You will get a speeding ticket if you drive over 65 miles per hour.} \\
  d) & \quad \text{If you do not drive over 65 miles per hour, then you will not get a speeding ticket.} \\
  e) & \quad \text{Driving over 65 miles per hour is sufficient for getting a speeding ticket.} \\
  f) & \quad \text{You get a speeding ticket, but you do not drive over 65 miles per hour.} \\
  g) & \quad \text{Whenever you get a speeding ticket, you are driving over 65 miles per hour.}
\end{align*}
$$

10. Let $p$, $q$, and $r$ be the propositions

$p$ : You get an $A$ on the final exam.
$q$ : You do every exercise in this book.
$r$ : You get an $A$ in this class.

Write these propositions using $p$, $q$, and $r$ and logical connectives.

$$
\begin{align*}
  a) & \quad \text{You get an $A$ in this class, but you do not do every exercise in this book.} \\
  b) & \quad \text{You get an $A$ on the final, you do every exercise in this book, and you get an $A$ in this class.} \\
  c) & \quad \text{To get an $A$ in this class, it is necessary for you to get an $A$ on the final.} \\
  d) & \quad \text{You get an $A$ on the final, but you don’t do every exercise in this book; nevertheless, you get an $A$ in this class.} \\
  e) & \quad \text{Getting an $A$ on the final and doing every exercise in this book is sufficient for getting an $A$ in this class.} \\
  f) & \quad \text{You will get an $A$ in this class if and only if you either do every exercise in this book or you get an $A$ on the final.}
\end{align*}
$$

11. Let $p$, $q$, and $r$ be the propositions

$p$ : Grizzly bears have been seen in the area.
$q$ : Hiking is safe on the trail.
$r$ : Berries are ripe along the trail.

Write these propositions using $p$, $q$, and $r$ and logical connectives.

$$
\begin{align*}
  a) & \quad \text{Berries are ripe along the trail, but grizzly bears have not been seen in the area.} \\
  b) & \quad \text{Grizzly bears have not been seen in the area and hiking on the trail is safe, but berries are ripe along the trail.} \\
  c) & \quad \text{If berries are ripe along the trail, hiking is safe if and only if grizzly bears have not been seen in the area.} \\
  d) & \quad \text{It is not safe to hike on the trail, but grizzly bears have not been seen in the area and the berries along the trail are ripe.} \\
  e) & \quad \text{For hiking on the trail to be safe, it is necessary but not sufficient that berries not be ripe along the trail and for grizzly bears not to have been seen in the area.} \\
  f) & \quad \text{Hiking is not safe on the trail whenever grizzly bears have been seen in the area and berries are ripe along the trail.}
\end{align*}
$$

12. Determine whether these biconditionals are true or false.

$$
\begin{align*}
  a) & \quad 2 + 2 = 4 \text{ if and only if } 1 + 1 = 2. \\
  b) & \quad 1 + 1 = 2 \text{ if and only if } 2 + 3 = 4. \\
  c) & \quad 1 + 1 = 3 \text{ if and only if } \text{monkeys can fly.} \\
  d) & \quad 0 > 1 \text{ if and only if } 2 > 1.
\end{align*}
$$

13. Determine whether each of these conditional statements is true or false.

$$
\begin{align*}
  a) & \quad \text{If } 1 + 1 = 2, \text{ then } 2 + 2 = 5. \\
  b) & \quad \text{If } 1 + 1 = 3, \text{ then } 2 + 2 = 4. \\
  c) & \quad \text{If } 1 + 1 = 3, \text{ then } 2 + 2 = 5. \\
  d) & \quad \text{If } \text{monkeys can fly, then } 1 + 1 = 3.
\end{align*}
$$

14. Determine whether each of these conditional statements is true or false.

$$
\begin{align*}
  a) & \quad \text{If } 1 + 1 = 3, \text{ then unicorns exists.} \\
  b) & \quad \text{If } 1 + 1 = 3, \text{ then dogs can fly.} \\
  c) & \quad \text{If } 1 + 1 = 2, \text{ then dogs can fly.} \\
  d) & \quad \text{If } 2 + 2 = 4, \text{ then } 1 + 2 = 3.
\end{align*}
$$
15. For each of these sentences, determine whether an inclusive or or an exclusive or is intended. Explain your answer.
   a) Coffee or tea comes with dinner.
   b) A password must have at least three digits or be at least eight characters long.
   c) The prerequisite for the course is a course in number theory or a course in cryptography.
   d) You can pay using U.S. dollars or euros.

16. For each of these sentences, determine whether an inclusive or or an exclusive or is intended. Explain your answer.
   a) Experience with C++ or Java is required.
   b) Lunch includes soup or salad.
   c) To enter the country you need a passport or a voter registration card.
   d) Publish or perish.

17. For each of these sentences, state what the sentence means if the or is an inclusive or (that is, a disjunction) versus an exclusive or. Which of these meanings of or do you think is intended?
   a) To take discrete mathematics, you must have taken calculus or a course in computer science.
   b) When you buy a new car from Acme Motor Company, you get $2000 back in cash or a 2% car loan.
   c) Dinner for two includes three items from column A or three items from column B.
   d) School is closed if more than 2 feet of snow falls or if the wind chill is below -100.

18. Write each of these statements in the form "if \( p \) then \( q \)" in English. [Hint: Refer to the list of common ways to express conditional statements provided in this section.]
   a) It is necessary to wash the boss' s car to get promoted.
   b) A sufficient condition for the warranty to be good is that you have the only winning ticket.
   c) It rains if it is a weekend day, and it is a weekend day if the or is an inclusive or (that is, a disjunction) versus an exclusive or.

19. Write each of these statements in the form "if \( p \) then \( q \)" in English. [Hint: Refer to the list of common ways to express conditional statements.]
   a) It is necessary to wash the boss's car to get promoted.
   b) When you buy a new car from Acme Motor Company, you get $2000 back in cash or a 2% car loan.
   c) Dinner for two includes three items from column A or three items from column B.
   d) School is closed if more than 2 feet of snow falls or if the wind chill is below -100.

20. Write each of these statements in the form "if \( p \), then \( q \)" in English. [Hint: Refer to the list of common ways to express conditional statements provided in this section.]
   a) I will remember to send you the address only if you send me an e-mail message.
   b) To be a citizen of this country, it is sufficient that you were born in the United States.
   c) If you keep your textbook, it will be a useful reference in your future courses.
   d) The Red Wings will win the Stanley Cup if their goalie plays well.
   e) That you get the job implies that you had the best credentials.
   f) The beach erodes whenever there is a storm.
   g) It is necessary to have a valid password to log on to the server.
   h) You will reach the summit unless you begin your climb too late.

21. Write each of these propositions in the form "\( p \) if and only if \( q \)" in English.
   a) If it is hot outside you buy an ice cream cone, and if you buy an ice cream cone it is hot outside.
   b) To win the contest it is necessary and sufficient that you have the only winning ticket.
   c) You get promoted only if you have connections, and you have connections only if you get promoted.
   d) If you watch television your mind will decay, and conversely.
   e) The trains run late on exactly those days when I take it.

22. Write each of these propositions in the form "\( p \) if and only if \( q \)" in English.
   a) If you get an A in this course, it is necessary and sufficient that you learn how to solve discrete mathematics problems.
   b) If you read the newspaper every day, you will be informed, and conversely.
   c) It rains if it is a weekend day, and it is a weekend day if it rains.
   d) You can see the wizard only if the wizard is not in, and the wizard is not in only if you can see him.

23. State the converse, contrapositive, and inverse of each of these conditional statements.
   a) If it snows today, I will ski tomorrow.
   b) I come to class whenever there is going to be a quiz.
   c) A positive integer is a prime only if it has no divisors other than 1 and itself.

24. State the converse, contrapositive, and inverse of each of these conditional statements.
   a) If it snows tonight, then I will stay at home.
   b) I go to the beach whenever it is a sunny summer day.
   c) When I stay up late, it is necessary that I sleep until noon.

25. How many rows appear in a truth table for each of these compound propositions?
a) \( p \rightarrow \neg p \)
b) \((p \lor \neg r) \land (q \lor \neg s)\)
c) \(q \lor p \lor \neg s \lor \neg r \lor \neg u \lor u\)
d) \((p \land r \land t) \leftrightarrow (q \land t)\)

26. How many rows appear in a truth table for each of these compound propositions?

a) \((q \rightarrow \neg p) \lor (\neg p \rightarrow \neg q)\)
b) \((p \lor \neg t) \land (p \lor \neg s)\)
c) \((p \rightarrow r) \lor (\neg s \rightarrow \neg t) \lor (\neg u \rightarrow v)\)
d) \((p \land r \land s) \lor (q \land t) \lor (r \land t)\)

27. Construct a truth table for each of these compound propositions.

a) \( p \land \neg p \)
b) \( p \lor \neg p \)
c) \((p \rightarrow q) \land \neg q \)
d) \((p \land q) \lor (p \lor q)\)
e) \((p \rightarrow q) \leftrightarrow (q \rightarrow r)\)
f) \((p \leftrightarrow q) \leftrightarrow (p \leftrightarrow \neg q)\)

28. Construct a truth table for each of these compound propositions.

a) \( p \rightarrow \neg p \)
b) \( p \leftrightarrow \neg p \)
c) \((p \lor q) \land (p \lor \neg q)\)
d) \((p \lor q) \land (p \land q)\)
e) \((p \lor q) \leftrightarrow (p \land q)\)
f) \((p \leftrightarrow q) \leftrightarrow (p \leftrightarrow \neg q)\)

29. Construct a truth table for each of these compound propositions.

a) \((p \lor q) \rightarrow (p \lor \neg q)\)
b) \((p \land q) \rightarrow (p \land q)\)
c) \((p \lor q) \land (p \land q)\)
d) \((p \land q) \lor (p \lor q)\)
e) \((p \leftrightarrow q) \land (\neg p \leftrightarrow q)\)
f) \((p \land q) \leftrightarrow (p \land \neg q)\)

30. Construct a truth table for each of these compound propositions.

a) \( p \land p \)
b) \( p \land \neg p \)
c) \((p \lor q) \land (p \lor \neg q)\)
d) \((p \lor q) \land (p \land \neg q)\)
e) \((p \lor q) \land (p \land \neg q)\)
f) \((p \land q) \land (p \land \neg q)\)

31. Construct a truth table for each of these compound propositions.

a) \( p \rightarrow \neg q \)
b) \( \neg p \leftrightarrow q \)
c) \((p \lor q) \lor (\neg p \lor q)\)
d) \((p \lor q) \lor (\neg p \lor q)\)
e) \((p \lor q) \lor (\neg p \lor q)\)
f) \((p \lor q) \lor (\neg p \lor q)\)

32. Construct a truth table for each of these compound propositions.

a) \((p \lor q) \lor r \)
b) \((p \lor q) \land r \)
c) \((p \land q) \lor r \)
d) \((p \land q) \lor r \)
e) \((p \land q) \lor r \)
f) \((p \land q) \lor r \)

33. Construct a truth table for each of these compound propositions.

a) \( p \rightarrow (\neg q \lor r) \)
b) \( \neg p \rightarrow (q \rightarrow r) \)
c) \((p \rightarrow q) \lor (\neg p \rightarrow r) \)
d) \((p \lor q) \lor (\neg p \lor r) \)
e) \((p \land q) \lor (\neg q \lor r) \)
f) \((\neg p \land q) \lor (q \lor r) \)

34. Construct a truth table for \((p \rightarrow q) \rightarrow r \rightarrow s\).

35. Construct a truth table for \((p \rightarrow q) \leftrightarrow (r \rightarrow s)\).

36. What is the value of \(x\) after each of these statements is encountered in a computer program, if \(x = 1\) before the statement is reached?

a) \(1 + 2 = 3\) then \(x := x + 1\)
b) \(1 + 1 = 3\) \(OR\) \((2 + 2 = 3)\) then \(x := x + 1\)
c) \((2 + 3 = 5)\) \(AND\) \((3 + 4 = 7)\) then \(x := x + 1\)
d) \((1 + 1 = 2)\) \(XOR\) \((1 + 2 = 3)\) then \(x := x + 1\)
e) \(x < 2\) then \(x := x + 1\)

37. Find the bitwise \(OR\), bitwise \(AND\), and bitwise \(XOR\) of each of these pairs of bit strings.

a) \(1011\)
b) \(1111\)
c) \(0011\)
d) \(1111\)

38. Evaluate each of these expressions.

a) \(1 000 \land (0 101 1 \lor 1 1011)\)
b) \((0 1111 \land 1 0101) \lor 0 1000\)
c) \((0 1010 \oplus 1 1011) \oplus 0 1000\)
d) \((1 1011 \lor 0 1010) \land (1 0001 \lor 1 1011)\)

Fuzzy logic is used in artificial intelligence. In fuzzy logic, a proposition has a truth value that is a number between 0 and 1, inclusive. A proposition with a truth value of 0 is false and one with a truth value of 1 is true. Truth values that are between 0 and 1 indicate varying degrees of truth. For instance, the truth value 0.8 can be assigned to the statement "Fred is happy," because Fred is happy most of the time, and the truth value 0.4 can be assigned to the statement "John is happy," because John is happy slightly less than half the time.

39. The truth value of the negation of a proposition in fuzzy logic is 1 minus the truth value of the proposition. What are the truth values of the statements "Fred is not happy" and "John is not happy"?

40. The truth value of the conjunction of two propositions in fuzzy logic is the minimum of the truth values of the two propositions. What are the truth values of the statements "Fred and John are happy" and "Neither Fred nor John is happy"?

41. The truth value of the disjunction of two propositions in fuzzy logic is the maximum of the truth values of the two propositions. What are the truth values of the statements "Fred is happy, or John is happy" and "Fred is not happy, or John is not happy"?

*42. Is the assertion "This statement is false" a proposition?

*43. The \(n\)th statement in a list of 100 statements is "Exactly \(n\) of the statements in this list are false."

a) What conclusions can you draw from these statements?

b) Answer part (a) if the \(n\)th statement is "At least \(n\) of the statements in this list are false."

c) Answer part (b) assuming that the list contains 99 statements.

44. An ancient Sicilian legend says that the barber in a remote town who can be reached only by traveling a dangerous mountain road shaves those people, and only those
people, who do not shave themselves. Can there be such a barber?

45. Each inhabitant of a remote village always tells the truth or always lies. A villager will only give a “Yes” or a “No” response to a question a tourist asks. Suppose you are a tourist visiting this area and come to a fork in the road. One branch leads to the ruins you want to visit; the other branch leads deep into the jungle. A villager is standing at the fork in the road. What one question can you ask the villager to determine which branch to take?

46. An explorer is captured by a group of cannibals. There are two types of cannibals—those who always tell the truth and those who always lie. The cannibals will barbecue the explorer unless he can determine whether a particular cannibal always lies or always tells the truth. He is allowed to ask the cannibal exactly one question.

a) Explain why the question “Are you a liar?” does not work.

b) Find a question that the explorer can use to determine whether the cannibal always lies or always tells the truth.

47. Express these system specifications using the propositions

p “The message is scanned for viruses” and q “The message was sent from an unknown system” together with logical connectives.

a) “The message is scanned for viruses whenever the message was sent from an unknown system.”

b) “The message was sent from an unknown system but it was not scanned for viruses.”

c) “It is necessary to scan the message for viruses whenever it was sent from an unknown system.”

d) “When a message is not sent from an unknown system it is not scanned for viruses.”

48. Express these system specifications using the propositions

p “The user enters a valid password,” q “Access is granted,” and r “The user has paid the subscription fee” and logical connectives.

a) “The user has paid the subscription fee, but does not enter a valid password.”

b) “Access is granted whenever the user has paid the subscription fee and enters a valid password.”

c) “Access is denied if the user has not paid the subscription fee.”

d) “If the user has not entered a valid password but has paid the subscription fee, then access is granted.”

49. Are these system specifications consistent? “The system is in multiuser state if and only if it is operating normally. If the system is operating normally, the kernel is functioning. The kernel is not functioning or the system is in interrupt mode. If the system is not in multiuser state, then it is in interrupt mode. The system is not in interrupt mode.”

50. Are these system specifications consistent? “Whenever the system software is being upgraded, users cannot access the file system. If users can access the file system, then they can save new files. If users cannot save new files, then the system software is not being upgraded.”

51. Are these system specifications consistent? “The router can send packets to the edge system only if it supports the new address space. For the router to support the new address space it is necessary that the latest software release be installed. The router can send packets to the edge system if the latest software release is installed. The router does not support the new address space.”

52. Are these system specifications consistent? “If the file system is not locked, then new messages will be queued. If the file system is not locked, then the system is functioning normally, and conversely. If new messages are not queued, then they will be sent to the message buffer. If the file system is not locked, then new messages will be sent to the message buffer. New messages will not be sent to the message buffer.”

53. What Boolean search would you use to look for Web pages about beaches in New Jersey? What if you wanted to find Web pages about beaches on the isle of Jersey (in the English Channel)?

54. What Boolean search would you use to look for Web pages about hiking in West Virginia? What if you wanted to find Web pages about hiking in Virginia, but not in West Virginia?

Exercises 55–59 relate to inhabitants of the island of knights and knaves created by Smullyan, where knights always tell the truth and knaves always lie. You encounter two people, A and B. Determine, if possible, what A and B are if they address you in the ways described. If you cannot determine what these two people are, can you draw any conclusions?

55. A says “At least one of us is a knave” and B says nothing.

56. A says “The two of us are both knights” and B says “A is a knave.”

57. A says “I am a knave or B is a knight” and B says nothing.

58. Both A and B say “I am a knight.”

59. A says “We are both knaves” and B says nothing.

Exercises 60–65 are puzzles that can be solved by translating statements into logical expressions and reasoning from these expressions using truth tables.

60. The police have three suspects for the murder of Mr. Cooper: Mr. Smith, Mr. Jones, and Mr. Williams. Smith, Jones, and Williams each declare that they did not kill Cooper. Smith also states that Cooper was a friend of Jones and that Williams disliked him. Jones also states that he did not know Cooper and that he was out of town the day Cooper was killed. Williams also states that he saw both Smith and Jones with Cooper the day of the killing and that either Smith or Jones must have killed him. Can you determine who the murderer was if

a) one of the three men is guilty, the two innocent men are telling the truth, but the statements of the guilty man may or may not be true?

b) innocent men do not lie?
61. Steve would like to determine the relative salaries of three coworkers using two facts. First, he knows that if Fred is not the highest paid of the three, then Janice is. Second, he knows that if Janice is not the lowest paid, then Maggie is paid the most. Is it possible to determine the relative salaries of Fred, Maggie, and Janice from what Steve knows? If so, who is paid the most and who the least? Explain your reasoning.

62. Five friends have access to a chat room. Is it possible to determine who is chatting if the following information is known? Either Kevin or Heather, or both, are chatting. Either Randy or Vijay, but not both, are chatting. If Abby is chatting, so is Randy. Vijay and Kevin are either both chatting or neither is. If Heather is chatting, then so are Abby and Kevin. Explain your reasoning.

63. A detective has interviewed four witnesses to a crime. From the stories of the witnesses the detective has concluded that if the butler is telling the truth then so is the cook; the cook and the gardener cannot both be telling the truth; the gardener and the handyman are not both lying; and if the handyman is telling the truth then the cook is lying. For each of the four witnesses, can the detective determine whether that person is telling the truth or lying? Explain your reasoning.

64. Four friends have been identified as suspects for an unauthorized access into a computer system. They have made statements to the investigating authorities. Alice said “Carlos did it.” John said “I did not do it.” Carlos said “Diana did it.” Diana said “Carlos lied when he said that I did it.”

a) If the authorities also know that exactly one of the four suspects is telling the truth, who did it? Explain your reasoning.

b) If the authorities also know that exactly one is lying, who did it? Explain your reasoning.

*65. Solve this famous logic puzzle, attributed to Albert Einstein, and known as the zebra puzzle. Five men with different nationalities and with different jobs live in consecutive houses on a street. These houses are painted different colors. The men have different pets and have different favorite drinks. Determine who owns a zebra and whose favorite drink is mineral water (which is one of the favorite drinks) given these clues: The Englishman lives in the red house. The Spaniard owns a dog. The Japanese man is a painter. The Italian drinks tea. The Norwegian lives in the first house on the left. The green house is immediately to the right of the white one. The photographer breeds snails. The diplomat lives in the yellow house. Milk is drunk in the middle house. The owner of the green house drinks coffee. The Norwegian’s house is next to the blue one. The violinist drinks orange juice. The fox is in a house next to that of the physician. The horse is in a house next to that of the diplomat. [Hint: Make a table where the rows represent the men and columns represent the color of their houses, their jobs, their pets, and their favorite drinks and use logical reasoning to determine the correct entries in the table.]

1.2 Propositional Equivalences

Introduction

An important type of step used in a mathematical argument is the replacement of a statement with another statement with the same truth value. Because of this, methods that produce propositions with the same truth value as a given compound proposition are used extensively in the construction of mathematical arguments. Note that we will use the term “compound proposition” to refer to an expression formed from propositional variables using logical operators, such as $p \land q$.

We begin our discussion with a classification of compound propositions according to their possible truth values.

**DEFINITION 1** A compound proposition that is always true, no matter what the truth values of the propositions that occur in it, is called a tautology. A compound proposition that is always false is called a contradiction. A compound proposition that is neither a tautology nor a contradiction is called a contingency.

Tautologies and contradictions are often important in mathematical reasoning. Example 1 illustrates these types of compound propositions.
Exercises

1. Use truth tables to verify these equivalences.
   a) \( p \land T \equiv p \)  
   b) \( p \lor F \equiv p \)  
   c) \( p \land F \equiv F \)  
   d) \( p \lor T \equiv T \)  
   e) \( p \lor p \equiv p \)  
   f) \( p \land p \equiv p \)  

2. Show that \( \neg(\neg p) \) and \( p \) are logically equivalent.

3. Use truth tables to verify the commutative laws
   a) \( p \lor q \equiv q \lor p \)  
   b) \( p \land q \equiv q \land p \)  

4. Use truth tables to verify the associative laws
   a) \( (p \lor q) \lor r \equiv p \lor (q \lor r) \)  
   b) \( (p \land q) \land r \equiv p \land (q \land r) \)  

5. Use a truth table to verify the distributive law
   \( p \land (q \lor r) \equiv (p \land q) \lor (p \land r) \).

6. Use a truth table to verify the first De Morgan law
   \( \neg(p \land q) \equiv \neg p \lor \neg q \)  

7. Use De Morgan's laws to find the negation of each of the following statements.
   a) Jan is rich and happy.
   b) Carlos will bicycle or run tomorrow.
   c) Mei walks or takes the bus to class.
   d) Ibrahim is smart and hard working.

8. Use De Morgan's laws to find the negation of each of the following statements.
   a) Kwame will take a job in industry or go to graduate school.
   b) Yoshiko knows Java and calculus.
   c) James is young and strong.
   d) Rita will move to Oregon or Washington.

9. Show that each of these conditional statements is a tautology by using truth tables.
   a) \( (p \land q) \rightarrow p \)  
   b) \( p \rightarrow (p \lor q) \)  
   c) \( \neg p \rightarrow (p \lor q) \)  
   d) \( (p \land q) \rightarrow (p \rightarrow q) \)  
   e) \( \neg(p \rightarrow q) \rightarrow p \)  
   f) \( \neg(p \rightarrow q) \rightarrow \neg q \)  

10. Show that each of these conditional statements is a tautology by using truth tables.
    a) \( [(\neg p \land (p \lor q)) \rightarrow q \)  
    b) \( [(p \rightarrow q) \land (q \rightarrow r)] \rightarrow (p \rightarrow r) \)  
    c) \( [p \land (p \rightarrow q)] \rightarrow q \)  
    d) \( [(p \lor q) \land (p \rightarrow r) \land (q \rightarrow r)] \rightarrow r \)  

11. Show that each conditional statement in Exercise 9 is a tautology without using truth tables.

12. Show that each conditional statement in Exercise 10 is a tautology without using truth tables.

13. Use truth tables to verify the absorption laws.
    a) \( p \lor (p \land q) \equiv p \)  
    b) \( p \land (p \lor q) \equiv p \)  

14. Determine whether \( (\neg p \land (p \rightarrow q)) \rightarrow \neg q \)  
    is a tautology.

15. Determine whether \( (\neg q \land (p \rightarrow q)) \rightarrow \neg p \)  
    is a tautology.

Each of Exercises 16–28 asks you to show that two compound propositions are logically equivalent. To do this, either show that both sides are true, or that both sides are false, for exactly the same combinations of truth values of the propositional variables in these expressions (whichever is easier).

16. Show that \( p \leftrightarrow q \)  
    and \( (p \land q) \lor (\neg p \land \neg q) \)  
    are equivalent.

17. Show that \( \neg(p \leftrightarrow q) \)  
    and \( p \leftrightarrow \neg q \)  
    are logically equivalent.

---

**HENRY MAURICE SHEFFER (1883–1964)**

Henry Maurice Sheffer, born to Jewish parents in the western Ukraine, emigrated to the United States in 1892 with his parents and six siblings. He studied at the Boston Latin School before entering Harvard, where he completed his undergraduate degree in 1905, his master's in 1907, and his Ph.D. in philosophy in 1908. After holding a postdoctoral position at Harvard, Sheffer traveled to Europe on a fellowship. Upon returning to the United States, he became an academic nomad, spending one year each at the University of Washington, Cornell, the University of Minnesota, the University of Missouri, and City College in New York. In 1916 he returned to Harvard as a faculty member in the philosophy department. He remained at Harvard until his retirement in 1952.

Sheffer introduced what is now known as the Sheffer stroke in 1913; it became well known only after its use in the 1925 edition of Whitehead and Russell's *Principia Mathematica*. In this same edition Russell wrote that Sheffer had invented a powerful method that could be used to simplify the *Principia*. Because of this comment, Sheffer was something of a mystery man to logicians, especially because Sheffer, who published little in his career, never published the details of this method, only describing it in mimeographed notes and in a brief published abstract.

Sheffer was a dedicated teacher of mathematical logic. He liked his classes to be small and did not like auditors. When strangers appeared in his classroom, Sheffer would order them to leave, even his colleagues or distinguished guests visiting Harvard. Sheffer was barely five feet tall; he was noted for his wit and vigor, as well as for his nervousness and irritability. Although widely liked, he was quite lonely. He is noted for a quip he spoke at his retirement: "Old professors never die, they just become emeriti." Sheffer is also credited with coining the term "Boolean algebra" (the subject of Chapter 11 of this text). Sheffer was briefly married and lived most of his later life in small rooms at a hotel packed with his logic books and vast files of slips of paper he used to jot down his ideas. Unfortunately, Sheffer suffered from severe depression during the last two decades of his life.
18. Show that \( p \rightarrow q \) and \( \neg q \rightarrow \neg p \) are logically equivalent.
19. Show that \( \neg p \leftrightarrow q \) and \( p \leftrightarrow \neg q \) are logically equivalent.
20. Show that \( \neg (p \oplus q) \) and \( p \leftrightarrow q \) are logically equivalent.
21. Show that \( \neg (p \leftrightarrow q) \) and \( \neg p \leftrightarrow q \) are logically equivalent.
22. Show that \((p \rightarrow q) \land (p \rightarrow r)\) and \( p \rightarrow (q \land r) \) are logically equivalent.
23. Show that \((p \rightarrow r) \land (q \rightarrow r)\) and \( (p \lor q) \rightarrow r \) are logically equivalent.
24. Show that \((p \rightarrow q) \lor (p \rightarrow r)\) and \( p \rightarrow (q \lor r) \) are logically equivalent.
25. Show that \((p \rightarrow r) \lor (q \rightarrow r)\) and \( (p \land q) \rightarrow r \) are logically equivalent.
26. Show that \( \neg p \rightarrow (q \rightarrow r) \) and \( q \rightarrow (p \lor r) \) are logically equivalent.
27. Show that \( p \leftrightarrow q \) and \( (p \rightarrow q) \land (q \rightarrow p) \) are logically equivalent.
28. Show that \( p \leftrightarrow q \) and \( \neg p \leftrightarrow \neg q \) are logically equivalent.
29. Show that \((p \rightarrow q) \land (q \rightarrow r) \rightarrow (p \rightarrow r)\) is a tautology.
30. Show that \((p \lor q) \land (\neg p \lor r) \rightarrow (q \lor r)\) is a tautology.
31. Show that \((p \rightarrow q) \rightarrow r\) and \( p \rightarrow (q \rightarrow r)\) are not equivalent.
32. Show that \((p \land q) \rightarrow r\) and \( (p \rightarrow r) \land (q \rightarrow r)\) are not equivalent.
33. Show that \((p \rightarrow q) \rightarrow (r \rightarrow s)\) and \( (p \rightarrow r) \rightarrow (q \rightarrow s)\) are not logically equivalent.

The dual of a compound proposition that contains only the logical operators \( \lor \), \( \land \), and \( \neg \) is the compound proposition obtained by replacing each \( \land \) by \( \lor \), each \( \lor \) by \( \land \), each \( \top \) by \( \bot \), and each \( \bot \) by \( \top \). The dual of \( s \) is denoted by \( s^* \).

34. Find the dual of each of these compound propositions.
   a) \( p \lor \neg q \)
   b) \( p \neg (q \lor (r \land \top)) \)
   c) \( (p \land \neg q) \lor (q \lor F) \)

35. Find the dual of each of these compound propositions.
   a) \( p \land \neg q \land \neg r \)
   b) \( (p \land q \land r) \lor s \)
   c) \( (p \lor F) \land (q \lor T) \)

36. When does \( s^* = s \), where \( s \) is a compound proposition?
37. Show that \( (s^*)^* = s \) when \( s \) is a compound proposition.
38. Show that the logical equivalences in Table 6, except for the double negation law, come in pairs, where each pair contains compound propositions that are duals of each other.

**39. Why are the duals of two equivalent compound propositions also equivalent, where these compound propositions contain only the operators \( \land \), \( \lor \), and \( \neg \)?

40. Find a compound proposition involving the propositional variables \( p \), \( q \), and \( r \) that is true when \( p \) and \( q \) are true and \( r \) is false, but is false otherwise. [Hint: Use a conjunction of each propositional variable or its negation.]
41. Find a compound proposition involving the propositional variables \( p \), \( q \), and \( r \) that is true when exactly two of \( p \), \( q \), and \( r \) are true and is false otherwise. [Hint: Form a disjunction of conjunctions. Include a conjunction for each combination of values for which the propositional variable is true. Each conjunction should include each of the three propositional variables or their negations.]

42. Suppose that a truth table in \( n \) propositional variables is specified. Show that a compound proposition with this truth table can be formed by taking the disjunction of conjunctions of the variables or their negations, with one conjunction included for each combination of values for which the compound proposition is true. The resulting compound proposition is said to be in disjunctive normal form.

A collection of logical operators is called functionally complete if every compound proposition is logically equivalent to a compound proposition involving only these logical operators.

43. Show that \( \neg \), \( \land \), and \( \lor \) form a functionally complete collection of logical operators. [Hint: Use the fact that every compound proposition is logically equivalent to one in disjunctive normal form, as shown in Exercise 42.]
44. Show that \( \neg \) and \( \land \) form a functionally complete collection of logical operators. [Hint: First use a De Morgan law to show that \( p \lor q \) is equivalent to \( \neg (\neg p \land \neg q) \).]
45. Show that \( \neg \) and \( \lor \) form a functionally complete collection of logical operators.

The following exercises involve the logical operators \( \text{NAND} \) and \( \text{NOR} \). The proposition \( p \text{ NAND} q \) is true when either \( p \) or \( q \), or both, are false; and it is false when both \( p \) and \( q \) are true. The proposition \( p \text{ NOR} q \) is true when both \( p \) and \( q \) are false, and it is false otherwise. The propositions \( p \text{ NAND} q \) and \( p \text{ NOR} q \) are denoted by \( p \downarrow q \) and \( p \downarrow q \), respectively. (The operators \( \downarrow \) and \( \downarrow \) are called the Sheffer stroke and the Peirce arrow after H. M. Sheffer and C. S. Peirce, respectively.)

46. Construct a truth table for the logical operator \( \text{NAND} \).
47. Show that \( p \downarrow q \) is logically equivalent to \( \neg (p \land q) \).
48. Construct a truth table for the logical operator \( \text{NOR} \).
49. Show that \( p \downarrow q \) is logically equivalent to \( \neg (p \lor q) \).
50. In this exercise we will show that \( \{\downarrow\} \) is a functionally complete collection of logical operators.
   a) Show that \( p \downarrow p \) is logically equivalent to \( \neg p \).
   b) Show that \( (p \downarrow q) \downarrow (p \downarrow q) \) is logically equivalent to \( p \lor q \).
   c) Conclude from parts (a) and (b), and Exercise 49, that \( \{\downarrow\} \) is a functionally complete collection of logical operators.

51. Find a compound proposition logically equivalent to \( p \rightarrow q \) using only the logical operator \( \downarrow \).
52. Show that \( \{\downarrow\} \) is a functionally complete collection of logical operators.
53. Show that \( p \downarrow q \) and \( q \downarrow p \) are equivalent.
54. Show that \( p \downarrow (q \lor r) \) and \( (p \downarrow q) \downarrow r \) are not equivalent, so that the logical operator \( \downarrow \) is not associative.

**55. How many different truth tables of compound propositions are there that involve the propositional variables \( p \) and \( q \)?
56. Show that if \( p, q, \) and \( r \) are compound propositions such that \( p \) and \( q \) are logically equivalent and \( q \) and \( r \) are logically equivalent, then \( p \) and \( r \) are logically equivalent.

57. The following sentence is taken from the specification of a telephone system: “If the directory database is opened, then the monitor is put in a closed state, if the system is not in its initial state.” This specification is hard to understand because it involves two conditional statements. Find an equivalent, easier-to-understand specification that involves disjunctions and negations but not conditional statements.

58. How many of the disjunctions \( p \lor \neg q, \neg p \lor q, q \lor r, \) and \( \neg q \lor \neg r \) can be made simultaneously true by an assignment of truth values to \( p, q, \) and \( r \)?

59. How many of the disjunctions \( p \lor \neg q \lor s, \neg p \lor \neg r \lor s, \neg p \lor \neg r \lor \neg s, \neg p \lor q \lor \neg s, q \lor r \lor \neg s, q \lor r \lor \neg s, \), and \( p \lor r \lor \neg s \) can be made simultaneously true by an assignment of truth values to \( p, q, r, \) and \( s \)?

A compound proposition is **satisfiable** if there is an assignment of truth values to the variables in the compound proposition that makes the statement form true.

60. Which of these compound propositions are satisfiable?

\[
\begin{align*}
\text{a)} & \quad (p \lor q \lor \neg r) \land (p \lor \neg q \lor \neg s) \land (p \lor \neg r \lor \neg s) \land \\
& \quad (\neg p \lor \neg q \lor \neg s) \land (p \lor q \lor \neg s) \\
\text{b)} & \quad (\neg p \lor \neg q \lor \neg r) \land (\neg p \lor q \lor \neg s) \land (p \lor \neg q \lor \neg s) \land \\
& \quad (p \lor \neg r \lor \neg s) \land (p \lor \neg r \lor \neg s) \\
\text{c)} & \quad (p \lor q \lor r) \land (p \lor \neg q \lor \neg s) \land (q \lor \neg r \lor s) \land \\
& \quad (\neg p \lor r \lor s) \land (\neg p \lor q \lor \neg s) \land (p \lor \neg q \lor \neg r) \land \\
& \quad (\neg p \lor \neg q \lor \neg s) \land (\neg p \lor \neg r \lor \neg s)
\end{align*}
\]

61. Explain how an algorithm for determining whether a compound proposition is satisfiable can be used to determine whether a compound proposition is a tautology.

**Hint:** Look at \( \neg p \), where \( p \) is the compound proposition that is being examined.

### 1.3 Predicates and Quantifiers

**Introduction**

Propositional logic, studied in Sections 1.1 and 1.2, cannot adequately express the meaning of statements in mathematics and in natural language. For example, suppose that we know that

“Every computer connected to the university network is functioning properly.”

No rules of propositional logic allow us to conclude the truth of the statement

“MATH3 is functioning properly,”

where MATH3 is one of the computers connected to the university network. Likewise, we cannot use the rules of propositional logic to conclude from the statement

“CS2 is under attack by an intruder,”

where CS2 is a computer on the university network, to conclude the truth of

“There is a computer on the university network that is under attack by an intruder.”

In this section we will introduce a more powerful type of logic called **predicate logic**. We will see how predicate logic can be used to express the meaning of a wide range of statements in mathematics and computer science in ways that permit us to reason and explore relationships between objects. To understand predicate logic, we first need to introduce the concept of a predicate. Afterward, we will introduce the notion of quantifiers, which enable us reason with statements that assert that a certain property holds for all objects of a certain type and with statements that assert the existence of an object with a particular property.
A new predicate \( teaches(p, s) \), representing that professor \( p \) teaches student \( s \), can be defined using the Prolog rule

\[
\text{teaches}(P, S) :\text{-- instructor}(P, C), \text{enrolled}(S, C)
\]

which means that \( teaches(p, s) \) is true if there exists a class \( c \) such that professor \( p \) is the instructor of class \( c \) and student \( s \) is enrolled in class \( c \). (Note that a comma is used to represent a conjunction of predicates in Prolog. Similarly, a semicolon is used to represent a disjunction of predicates.)

Prolog answers queries using the facts and rules it is given. For example, using the facts and rules listed, the query

\[
?\text{enrolled}(\text{kevin}, \text{math273})
\]

produces the response

\text{yes}

because the fact \( \text{enrolled} \) (kevin, math273) was provided as input. The query

\[
?\text{enrolled}(X, \text{math273})
\]

produces the response

\text{kevin}
\text{kiko}

To produce this response, Prolog determines all possible values of \( X \) for which \( \text{enrolled}(X, \text{math273}) \) has been included as a Prolog fact. Similarly, to find all the professors who are instructors in classes being taken by Juana, we use the query

\[
?\text{teaches}(X, \text{juana})
\]

This query returns

\text{patel}
\text{grossman}

Exercises

1. Let \( P(x) \) denote the statement "\( x \leq 4 \)." What are the truth values?
   a) \( P(0) \)  
   b) \( P(4) \)  
   c) \( P(6) \)

2. Let \( P(x) \) be the statement "the word \( x \) contains the letter \( \text{a} \)." What are the truth values?
   a) \( P(\text{orange}) \)  
   b) \( P(\text{lemon}) \)  
   c) \( P(\text{true}) \)  
   d) \( P(\text{false}) \)

3. Let \( Q(x, y) \) denote the statement "\( x \) is the capital of \( y \)." What are these truth values?
   a) \( Q(\text{Denver, Colorado}) \)  
   b) \( Q(\text{Detroit, Michigan}) \)  
   c) \( Q(\text{Massachusetts, Boston}) \)  
   d) \( Q(\text{New York, New York}) \)

4. State the value of \( x \) after the statement \( \text{if } P(x) \text{ then } x := 1 \) is executed, where \( P(x) \) is the statement "\( x > 1 \)," if the value of \( x \) when this statement is reached is
   a) \( x = 0 \)  
   b) \( x = 1 \)  
   c) \( x = 2 \)

5. Let \( P(x) \) be the statement "\( x \) spends more than five hours every weekday in class," where the domain for \( x \) consists of all students. Express each of these quantifications in English.
6. Let \( N(x) \) be the statement “\( x \) has visited North Dakota,” where the domain consists of the students in your school. Express each of these quantifications in English.

a) \( \exists x \, N(x) \)  
b) \( \forall x \, N(x) \)  
c) \( \exists x \, \neg N(x) \)  
d) \( \forall x \, \neg N(x) \)

7. Translate these statements into English, where \( C(x) \) is “\( x \) is a comedian” and \( F(x) \) is “\( x \) is funny” and the domain consists of all people.

a) \( \forall x \, (C(x) \rightarrow F(x)) \)  
b) \( \forall x \, (C(x) \land F(x)) \)  
c) \( \exists x \, \neg (C(x) \rightarrow F(x)) \)  
d) \( \exists x \, (C(x) \land \neg F(x)) \)

8. Translate these statements into English, where \( R(x) \) is “\( x \) is a rabbit” and \( H(x) \) is “\( x \) hops” and the domain consists of all animals.

a) \( \forall x \, (R(x) \land H(x)) \)  
b) \( \forall x \, (R(x) \land \neg H(x)) \)  
c) \( \exists x \, (\neg R(x) \land H(x)) \)  
d) \( \exists x \, (\neg R(x) \land \neg H(x)) \)

9. Let \( P(x) \) be the statement “\( x \) can speak Russian” and let \( Q(x) \) be the statement “\( x \) knows the computer language C++.” Express each of these sentences in terms of \( P(x), Q(x) \), quantifiers, and logical connectives. The domain for quantifiers consists of all students at your school.

a) There is a student at your school who can speak Russian and who knows C++.
   b) There is a student at your school who can speak Russian but who doesn’t know C++.
   c) Every student at your school either can speak Russian or knows C++.
   d) No student at your school can speak Russian or knows C++.

10. Let \( C(x) \) be the statement “\( x \) has a cat,” let \( D(x) \) be the statement “\( x \) has a dog,” and let \( F(x) \) be the statement “\( x \) has a ferret.” Express each of these statements in terms of \( C(x), D(x), F(x) \), quantifiers, and logical connectives. Let the domain consist of all students in your class.

a) A student in your class has a cat, a dog, and a ferret.
   b) All students in your class have a cat, a dog, or a ferret.
   c) Some student in your class has a cat and a ferret, but not a dog.
   d) No student in your class has a cat, a dog, and a ferret.
   e) For each of the three animals, cats, dogs, and ferrets, there is a student in your class who has one of these animals as a pet.

11. Let \( P(x) \) be the statement “\( x = x^2 \).” If the domain consists of the integers, what are the truth values?

a) \( P(0) \)  
b) \( P(1) \)  
c) \( P(2) \)  
d) \( P(-1) \)  
e) \( \exists x \, P(x) \)  
f) \( \forall x \, P(x) \)

12. Let \( Q(x) \) be the statement “\( x + 1 > 2x \).” If the domain consists of all integers, what are these truth values?

a) \( Q(0) \)  
b) \( Q(-1) \)  
c) \( Q(1) \)  
d) \( \exists x \, Q(x) \)  
e) \( \forall x \, Q(x) \)  
f) \( \exists x \, \neg Q(x) \)  
g) \( \forall x \, \neg Q(x) \)

13. Determine the truth value of each of these statements if the domain consists of all integers.

a) \( \forall n(n + 1 > n) \)  
b) \( \exists n(2n = 3n) \)  
c) \( \exists n(n = -n) \)  
d) \( \forall n(n^2 \geq n) \)

14. Determine the truth value of each of these statements if the domain consists of all real numbers.

a) \( \exists x(x^2 = -1) \)  
b) \( \exists x(x^4 < x^2) \)  
c) \( \forall x((-x)^2 = x^2) \)  
d) \( \forall x(2x > x) \)

15. Determine the truth value of each of these statements if the domain for all variables consists of all integers.

a) \( \forall n(n^2 \geq 0) \)  
b) \( \exists n(n^2 = 2) \)  
c) \( \forall n(n^2 \geq n) \)  
d) \( \exists n(n^2 < 0) \)

16. Determine the truth value of each of these statements if the domain for each variable consists of all real numbers.

a) \( \exists x(x^2 = 2) \)  
b) \( \exists x(x^2 = -1) \)  
c) \( \forall x(x^2 + 2 \geq 1) \)  
d) \( \forall x(x^2 \neq x) \)

17. Suppose that the domain of the propositional function \( P(x) \) consists of the integers 0, 1, 2, 3, and 4. Write out each of these propositions using disjunctions, conjunctions, and negations.

a) \( \exists x \, P(x) \)  
b) \( \forall x \, P(x) \)  
c) \( \exists x \, \neg P(x) \)  
d) \( \forall x \, \neg P(x) \)  
e) \( \neg \exists x \, P(x) \)  
f) \( \neg \forall x \, P(x) \)

18. Suppose that the domain of the propositional function \( P(x) \) consists of the integers -2, -1, 0, 1, and 2. Write out each of these propositions using disjunctions, conjunctions, and negations.

a) \( \exists x \, P(x) \)  
b) \( \forall x \, P(x) \)  
c) \( \exists x \, \neg P(x) \)  
d) \( \forall x \, \neg P(x) \)  
e) \( \neg \exists x \, P(x) \)  
f) \( \neg \forall x \, P(x) \)

19. Suppose that the domain of the propositional function \( P(x) \) consists of the integers 1, 2, 3, 4, and 5. Express these statements without using quantifiers, instead using only negations, disjunctions, and conjunctions.

a) \( \exists x \, P(x) \)  
b) \( \forall x \, P(x) \)  
c) \( \neg \exists x \, P(x) \)  
d) \( \neg \forall x \, P(x) \)  
e) \( \forall x \, (x \neq 3) \rightarrow P(x) \)  
f) \( \exists x \, \neg P(x) \)

20. Suppose that the domain of the propositional function \( P(x) \) consists of -5, -3, -1, 1, 3, and 5. Express these statements without using quantifiers, instead using only negations, disjunctions, and conjunctions.

a) \( \exists x \, P(x) \)  
b) \( \forall x \, P(x) \)  
c) \( \neg \exists x \, P(x) \)  
d) \( \neg \forall x \, P(x) \)  
e) \( \forall x \, ((x \neq 3) \rightarrow P(x)) \land \exists x \, \neg P(x) \)

21. For each of these statements find a domain for which the statement is true and a domain for which the statement is false.

a) Everyone is studying discrete mathematics.
   b) Everyone is older than 21 years.
   c) Every two people have the same mother.
   d) No two different people have the same grandmother.

22. For each of these statements find a domain for which the statement is true and a domain for which the statement is false.

a) Everyone speaks Hindi.
   b) There is someone older than 21 years.
23. Translate in two ways each of these statements into logical expressions using predicates, quantifiers, and logical connectives. First, let the domain consist of the students in your class and second, let it consist of all people.
   a) Someone in your class can speak Hindi.
   b) Everyone in your class is friendly.
   c) There is a person in your class who was not born in California.
   d) A student in your class has been in a movie.
   e) No student in your class has taken a course in logic programming.

24. Translate in two ways each of these statements into logical expressions using predicates, quantifiers, and logical connectives. First, let the domain consist of the students in your class and second, let it consist of all people.
   a) Everyone in your class has a cellular phone.
   b) Somebody in your class has seen a foreign movie.
   c) There is a person in your class who cannot swim.
   d) All students in your class can solve quadratic equations.
   e) Some student in your class does not want to be rich.

25. Translate each of these statements into logical expressions using predicates, quantifiers, and logical connectives.
   a) No one is perfect.
   b) Not everyone is perfect.
   c) All your friends are perfect.
   d) At least one of your friends is perfect.
   e) Everyone is your friend and is perfect.
   f) Not everybody is your friend or someone is not perfect.

26. Translate each of these statements into logical expressions in three different ways by varying the domain and by using predicates with one and with two variables.
   a) Someone in your school has visited Uzbekistan.
   b) Everyone in your class has studied calculus and C++.
   c) No one in your school owns both a bicycle and a motorcycle.
   d) There is a person in your school who is not happy.
   e) Everyone in your school was born in the twentieth century.

27. Translate each of these statements into logical expressions in three different ways by varying the domain and by using predicates with one and with two variables.
   a) A student in your school has lived in Vietnam.
   b) There is a student in your school who cannot speak Hindi.
   c) A student in your school knows Java, Prolog, and C++.
   d) Everyone in your class enjoys Thai food.
   e) Someone in your class does not play hockey.

28. Translate each of these statements into logical expressions using predicates, quantifiers, and logical connectives.
   a) Something is not in the correct place.
   b) All tools are in the correct place and are in excellent condition.
   c) Everything is in the correct place and in excellent condition.
   d) Nothing is in the correct place and is in excellent condition.
   e) One of your tools is not in the correct place, but it is in excellent condition.

29. Express each of these statements using logical operators, predicates, and quantifiers.
   a) Some propositions are tautologies.
   b) The negation of a contradiction is a tautology.
   c) The disjunction of two contingencies can be a tautology.
   d) The conjunction of two tautologies is a tautology.

30. Suppose the domain of the propositional function \( P(x, y) \) consists of pairs \( x \) and \( y \), where \( x = 1, 2, 3 \) and \( y = 1, 2, 3 \). Write out these propositions using disjunctions and conjunctions.
   a) \( \exists x \ P(x, 3) \)
   b) \( \forall y \ P(1, y) \)
   c) \( \exists y \neg P(2, y) \)
   d) \( \forall x \neg P(x, 2) \)

31. Suppose that the domain of \( Q(x, y, z) \) consists of triples \( x, y, z \), where \( x = 0, 1 \), or \( y = 0 \) or \( 1 \), and \( z = 0 \) or \( 1 \). Write out these propositions using disjunctions and conjunctions.
   a) \( \forall y \ Q(0, y, 0) \)
   b) \( \exists x \ Q(x, 1, 1) \)
   c) \( \exists z \neg Q(0, 0, z) \)
   d) \( \exists x \neg Q(x, 0, 1) \)

32. Express each of these statements using quantifiers. Then form the negation of the statement so that no negation is to the left of a quantifier. Next, express the negation in simple English. (Do not simply use the words "It is not the case that.")
   a) All dogs have fleas.
   b) There is a horse that can add.
   c) Every koala can climb.
   d) No monkey can speak French.
   e) There exists a pig that can swim and catch fish.

33. Express each of these statements using quantifiers. Then form the negation of the statement, so that no negation is to the left of a quantifier. Next, express the negation in simple English. (Do not simply use the words "It is not the case that.")
   a) Some old dogs can learn new tricks.
   b) No rabbit knows calculus.
   c) Every bird can fly.
   d) There is no dog that can talk.
   e) There is no one in this class who knows French and Russian.

34. Express the negation of these propositions using quantifiers, and then express the negation in English.
   a) Some drivers do not obey the speed limit.
   b) All Swedish movies are serious.
   c) No one can keep a secret.
   d) There is someone in this class who does not have a good attitude.
35. Find a counterexample, if possible, to these universally quantified statements, where the domain for all variables consists of all integers.
   a) $\forall x(x^2 \geq x)$
   b) $\forall x(x > 0 \lor x < 0)$
   c) $\forall x(x = 1)$

36. Find a counterexample, if possible, to these universally quantified statements, where the domain for all variables consists of all real numbers.
   a) $\forall x(x^2 \neq x)$
   b) $\forall x(x^2 \neq 2)$
   c) $\forall x(|x| > 0)$

37. Express each of these statements using predicates and quantifiers.
   a) A passenger on an airline qualifies as an elite flyer if the passenger flies more than 25,000 miles in a year or takes more than 25 flights during that year.
   b) A man qualifies for the marathon if his best previous time is less than 3 hours and a woman qualifies for the marathon if her best previous time is less than 3.5 hours.
   c) A student must take at least 60 course hours, or at least 45 course hours and write a master’s thesis, and receive a grade no lower than a B in all required courses, to receive a master’s degree.
   d) There is a student who has taken more than 21 credit hours in a semester and received all A’s.

Exercises 38–42 deal with the translation between system specification and logical expressions involving quantifiers.

38. Translate these system specifications into English where the predicate $S(x, y)$ is “$x$ is in state $y$” and where the domain for $x$ and $y$ consists of all systems and all possible states, respectively.
   a) $\exists x S(x, \text{open})$
   b) $\exists x S(x, \text{malfunctioning}) \lor S(x, \text{diagnostic})$
   c) $\exists x S(x, \text{open}) \lor \exists x S(x, \text{diagnostic})$
   d) $\exists x \neg S(x, \text{available})$
   e) $\forall x \neg S(x, \text{working})$

39. Translate these specifications into English where $F(p)$ is “Printer $p$ is out of service,” $B(p)$ is “Printer $p$ is busy,” $L(j)$ is “Print job $j$ is lost,” and $Q(j)$ is “Print job $j$ is queued.”
   a) $\exists p (F(p) \land B(p)) \implies \exists j L(j)$
   b) $\forall p B(p) \implies \exists j Q(j)$
   c) $\exists j (Q(j) \land L(j)) \implies \exists p F(p)$
   d) $(\forall p B(p) \land \forall j Q(j)) \implies \exists j L(j)$

40. Express each of these system specifications using predicates, quantifiers, and logical connectives.
   a) When there is less than 30 megabytes free on the hard disk, a warning message is sent to all users.
   b) No directories in the file system can be opened and no files can be closed when system errors have been detected.
   c) The file system cannot be backed up if there is a user currently logged on.
   d) Video on demand can be delivered when there are at least 8 megabytes of memory available and the connection speed is at least 56 kilobits per second.

41. Express each of these system specifications using predicates, quantifiers, and logical connectives.
   a) At least one mail message, among the nonempty set of messages, can be saved if there is a disk with more than 10 kilobytes of free space.
   b) Whenever there is an active alert, all queued messages are transmitted.
   c) The diagnostic monitor tracks the status of all systems except the main console.
   d) Each participant on the conference call whom the host of the call did not put on a special list was billed.

42. Express each of these system specifications using predicates, quantifiers, and logical connectives.
   a) Every user has access to an electronic mailbox.
   b) The system mailbox can be accessed by everyone in the group if the file system is locked.
   c) The firewall is in a diagnostic state only if the proxy server is in a diagnostic state.
   d) At least one router is functioning normally if the throughput is between 100,000 bps and 500,000 bps and the proxy server is not in diagnostic mode.

43. Determine whether $\forall x (P(x) \rightarrow Q(x))$ and $\forall x P(x)$ are logically equivalent. Justify your answer.

44. Determine whether $\forall x (P(x) \leftrightarrow Q(x))$ and $\forall x P(x) \leftrightarrow \forall x Q(x)$ are logically equivalent. Justify your answer.

45. Show that $\exists x (P(x) \lor Q(x))$ and $\exists x P(x) \lor \exists x Q(x)$ are logically equivalent.

Exercises 46–49 establish rules for null quantification that we can use when a quantified variable does not appear in part of a statement.

46. Establish these logical equivalences, where $x$ does not occur as a free variable in $A$. Assume that the domain is nonempty.
   a) $(\forall x P(x)) \land A \equiv \forall x (P(x) \land A)$
   b) $(\exists x P(x)) \lor A \equiv \exists x (P(x) \lor A)$

47. Establish these logical equivalences, where $x$ does not occur as a free variable in $A$. Assume that the domain is nonempty.
   a) $(\forall x P(x)) \land A \equiv \forall x (P(x) \land A)$
   b) $(\exists x P(x)) \lor A \equiv \exists x (P(x) \land A)$

48. Establish these logical equivalences, where $x$ does not occur as a free variable in $A$. Assume that the domain is nonempty.
   a) $\forall x (A \rightarrow P(x)) \equiv A \rightarrow \forall x P(x)$
   b) $\exists x (A \rightarrow P(x)) \equiv A \rightarrow \exists x P(x)$

49. Establish these logical equivalences, where $x$ does not occur as a free variable in $A$. Assume that the domain is nonempty.
   a) $\forall x (P(x) \rightarrow A) \equiv \exists x P(x) \rightarrow A$
   b) $\exists x (P(x) \rightarrow A) \equiv \forall x P(x) \rightarrow A$
50. Show that \( \forall x P(x) \lor \forall x Q(x) \) and \( \forall x (P(x) \lor Q(x)) \) are not logically equivalent.

51. Show that \( \exists x P(x) \land \exists x Q(x) \) and \( \exists x (P(x) \land Q(x)) \) are not logically equivalent.

52. As mentioned in the text, the notation \( \exists! x P(x) \) denotes "There exists a unique \( x \) such that \( P(x) \) is true."

If the domain consists of all integers, what are the truth values of these statements?

a) \( \exists! x (x > 1) \)

b) \( \exists! x (x^2 = 1) \)

c) \( \exists! x (x + 3 = 2x) \)

d) \( \exists! x (x = x + 1) \)

53. What are the truth values of these statements?

a) \( \exists x P(x) \rightarrow \forall x P(x) \)

b) \( \forall x P(x) \rightarrow \exists x P(x) \)

c) \( \exists x \neg P(x) \rightarrow \neg \forall x P(x) \)

54. Write out \( \exists x P(x) \), where the domain consists of the integers 1, 2, and 3, in terms of negations, conjunctions, and disjunctions.

55. Given the Prolog facts in Example 28, what would Prolog return when given these queries?

a) \?instructor(chan,math273)

b) \?instructor(patel,cs301)

c) \?enrolled(X,cs301)

d) \?enrolled(kiko,Y)

e) \?teaches(grossman,Y)

56. Given the Prolog facts in Example 28, what would Prolog return when given these queries?

a) \?enrolled(kevin,ee222)

b) \?enrolled(kiko,math273)

c) \?instructor(grossman,X)

d) \?instructor(X,cs301)

e) \?teaches(X,kevin)

57. Suppose that Prolog facts are used to define the predicates \( \text{mother}(M, Y) \) and \( \text{father}(F, X) \), which represent that \( M \) is the mother of \( Y \) and \( F \) is the father of \( X \), respectively. Give a Prolog rule to define the predicate \( \text{sibling}(X, Y) \), which represents that \( X \) and \( Y \) are siblings (that is, have the same mother and the same father).

58. Suppose that Prolog facts are used to define the predicates \( \text{mother}(M, Y) \) and \( \text{father}(F, X) \), which represent that \( M \) is the mother of \( Y \) and \( F \) is the father of \( X \), respectively. Give a Prolog rule to define the predicate \( \text{grandfather}(X, Y) \), which represents that \( X \) is the grandfather of \( Y \). [Hint: You can write a disjunction in Prolog either by using a semicolon to separate predicates or by putting these predicates on separate lines.]

Exercises 59–62 are based on questions found in the book Symbolic Logic by Lewis Carroll.

59. Let \( P(x), Q(x), \) and \( R(x) \) be the statements "\( x \) is a professor," "\( x \) is ignorant," and "\( x \) is vain," respectively. Express each of these statements using quantifiers, logical connectives; and \( P(x), Q(x), \) and \( R(x) \), where the domain consists of all people.

a) No professors are ignorant.

b) All ignorant people are vain.

c) No professors are ignorant.

d) Does (c) follow from (a) and (b)?

60. Let \( P(x), Q(x), \) and \( R(x) \) be the statements "\( x \) is a clear explanation," "\( x \) is satisfactory," and "\( x \) is an excuse," respectively. Suppose that the domain for \( x \) consists of all English text. Express each of these statements using quantifiers, logical connectives, and \( P(x), Q(x), \) and \( R(x) \).

a) All clear explanations are satisfactory.

b) Some excuses are unsatisfactory.

* c) Some excuses are not clear explanations.

*d) Does (c) follow from (a) and (b)?

61. Let \( P(x), Q(x), \) and \( R(x) \), and \( S(x) \) be the statements "\( x \) is a baby," "\( x \) is logical," "\( x \) is able to manage a crocodile," and "\( x \) is despised," respectively. Suppose that the domain consists of all people. Express each of these statements using quantifiers; logical connectives; and \( P(x), Q(x), R(x), \) and \( S(x) \).

a) Babies are illogical.

b) Nobody is despised who can manage a crocodile.

c) Illogical persons are despised.

d) Babies cannot manage crocodiles.

*e) Does (d) follow from (a), (b), and (c)? If not, is there a correct conclusion?

62. Let \( P(x), Q(x), R(x), \) and \( S(x) \) be the statements "\( x \) is a duck," "\( x \) is one of my poultry," "\( x \) is an officer," and "\( x \) is willing to waltz," respectively. Express each of these statements using quantifiers; logical connectives; and \( P(x), Q(x), R(x), \) and \( S(x) \).

a) No ducks are willing to waltz.

b) No officers ever decline to waltz.

c) All my poultry are ducks.

d) My poultry are not officers.

*e) Does (d) follow from (a), (b), and (c)? If not, is there a correct conclusion?

1.4 Nested Quantifiers

Introduction

In Section 1.3 we defined the existential and universal quantifiers and showed how they can be used to represent mathematical statements. We also explained how they can be used to translate...
Successively applying the rules for negating quantified expressions, we construct this sequence of equivalent statements

\[ \neg \forall \varepsilon > 0 \exists \delta > 0 \forall x (0 < |x - a| < \delta \rightarrow |f(x) - L| < \varepsilon) \]

\[ \equiv \exists \varepsilon > 0 \neg \exists \delta > 0 \forall x (0 < |x - a| < \delta \rightarrow |f(x) - L| < \varepsilon) \]

\[ \equiv \exists \varepsilon > 0 \forall \delta > 0 \neg \forall x (0 < |x - a| < \delta \rightarrow |f(x) - L| < \varepsilon) \]

\[ \equiv \exists \varepsilon > 0 \forall \delta > 0 \exists x (0 < |x - a| < \delta \rightarrow |f(x) - L| < \varepsilon) \]

\[ \equiv \exists \varepsilon > 0 \forall \delta > 0 \exists x (0 < |x - a| < \delta \land |f(x) - L| \geq \varepsilon). \]

In the last step we used the equivalence \( \neg(p \rightarrow q) \equiv p \land \neg q \), which follows from the fifth equivalence in Table 7 of Section 1.2.

Because the statement “\( \lim_{x \to a} f(x) \) does not exist” means for all real numbers \( L \), \( \lim_{x \to a} f(x) \neq L \), this can be expressed as

\[ \forall L \exists \varepsilon > 0 \forall \delta > 0 \exists x (0 < |x - a| < \delta \land |f(x) - L| \geq \varepsilon). \]

This last statement says that for every real number \( L \) there is a real number \( \varepsilon > 0 \) such that for every real number \( \delta > 0 \), there exists a real number \( x \) such that \( 0 < |x - a| < \delta \) and \( |f(x) - L| \geq \varepsilon \).

Exercises

1. Translate these statements into English, where the domain for each variable consists of all real numbers.
   a) \( \forall x \exists y (x < y) \)
   b) \( \forall x \forall y ((x \geq 0) \land (y \geq 0)) \rightarrow (xy \geq 0) \)
   c) \( \forall x \forall y \exists z (xy = z) \)

2. Translate these statements into English, where the domain for each variable consists of all real numbers.
   a) \( \exists x \forall y (xy = y) \)
   b) \( \forall x \forall y (((x \geq 0) \land (y < 0)) \rightarrow (x - y > 0)) \)
   c) \( \forall x \forall y \exists z (x = y + z) \)

3. Let \( Q(x, y) \) be the statement “\( x \) has sent an e-mail message to \( y \),” where the domain for both \( x \) and \( y \) consists of all students in your class. Express each of these quantifications in English.
   a) \( \exists x \exists y Q(x, y) \)
   b) \( \exists x \forall y Q(x, y) \)
   c) \( \forall x \exists y Q(x, y) \)
   d) \( \exists y \forall x Q(x, y) \)

4. Let \( P(x, y) \) be the statement “\( x \) has taken class \( y \),” where the domain for \( x \) consists of all students in your class and for \( y \) consists of all computer science courses at your school. Express each of these quantifications in English.
   a) \( \exists x \exists y P(x, y) \)
   b) \( \exists x \forall y P(x, y) \)
   c) \( \forall x \exists y P(x, y) \)
   d) \( \exists y \forall x P(x, y) \)
   e) \( \forall y \exists x P(x, y) \)
   f) \( \forall x \forall y P(x, y) \)

5. Let \( W(x, y) \) mean that student \( x \) has visited website \( y \), where the domain for \( x \) consists of all students in your school and the domain for \( y \) consists of all websites. Express each of these statements by a simple English sentence.
   a) \( W(\text{Sarah Smith, www.att.com}) \)
   b) \( \exists x W(x, \text{www.imdb.org}) \)
   c) \( \exists y W(\text{Jose Orez, y}) \)
   d) \( \exists y W(\text{Ashok Puri, y}) \land W(\text{Cindy Yoon, y}) \)
   e) \( \exists y \forall z (y \neq (\text{David Belcher}) \land (W(\text{David Belcher, z}) \rightarrow W(y, z))) \)
   f) \( \exists x \exists y \forall z (x \neq y) \land (W(x, z) \leftrightarrow W(y, z)) \)

6. Let \( C(x, y) \) mean that student \( x \) is enrolled in class \( y \), where the domain for \( x \) consists of all students in your school and the domain for \( y \) consists of all classes being given at your school. Express each of these statements by a simple English sentence.
   a) \( C(\text{Randy Goldberg, CS 252}) \)
   b) \( \exists x C(x, \text{Math 695}) \)
   c) \( \exists y C(\text{Carol Sitea, y}) \)
   d) \( \exists x (C(x, \text{Math 222}) \land C(x, \text{CS 252})) \)
   e) \( \exists x \exists y \forall z (x \neq y) \land (C(x, z) \rightarrow C(y, z)) \)
   f) \( \exists x \exists y \forall z (x \neq y) \land (C(x, z) \leftrightarrow C(y, z)) \)

7. Let \( T(x, y) \) mean that student \( x \) likes cuisine \( y \), where the domain for \( x \) consists of all students at your school and the domain for \( y \) consists of all cuisines. Express each of these statements by a simple English sentence.
   a) \( \neg T(\text{Abdallah Hussein, Japanese}) \)
   b) \( \exists x T(x, \text{Korean}) \land \forall x T(x, \text{Mexican}) \)
c) \( \exists y (T(\text{Monique Arsenault}, y) \lor T(\text{Jay Johnson}, y)) \)

d) \( \forall x \forall z \exists y ((x \neq z) \rightarrow \neg (T(x, y) \land T(z, y))) \)

e) \( \exists x \exists y (T(x, y) \leftrightarrow T(z, y)) \)

f) \( \forall x \forall z \exists y (T(x, y) \leftrightarrow T(z, y)) \)

8. Let \( Q(x, y) \) be the statement “student \( x \) has been a contestant on quiz show \( y \).” Express each of these sentences in terms of \( Q(x, y) \), quantifiers, and logical connectives, where the domain for \( x \) consists of all students at your school and for \( y \) consists of all quiz shows on television.

a) There is a student at your school who has been a contestant on a television quiz show.

b) No student at your school has ever been a contestant on a television quiz show.

c) There is a student at your school who has been a contestant on Jeopardy and on Wheel of Fortune.

d) Every television quiz show has had a student from your school as a contestant.

e) At least two students from your school have been contestants on Jeopardy.

9. Let \( L(x, y) \) be the statement “\( x \) loves \( y \),” where the domain for both \( x \) and \( y \) consists of all people in the world. Use quantifiers to express each of these statements.

a) Everybody loves Jerry.

b) Everybody loves somebody.

c) There is somebody whom everybody loves.

d) Nobody loves everybody.

e) There is somebody whom Lydia does not love.

f) There is somebody whom no one loves.

g) There is exactly one person whom everybody loves.

h) There are exactly two people whom Lynn loves.

i) Everyone loves himself or herself.

j) There is someone who loves no one besides himself or herself.

10. Let \( F(x, y) \) be the statement “\( x \) can fool \( y \),” where the domain consists of all people in the world. Use quantifiers to express each of these statements.

a) Everybody can fool Fred.

b) Evelyn can fool everybody.

c) Everybody can fool somebody.

d) There is no one who can fool everybody.

e) Everyone can be fooled by somebody.

f) No one can fool both Fred and Jerry.

g) Nancy can fool exactly two people.

h) There is exactly one person whom everybody can fool.

i) No one can fool himself or herself.

j) There is someone who can fool exactly one person besides himself or herself.

11. Let \( S(x) \) be the predicate “\( x \) is a student,” \( F(x) \) the predicate “\( x \) is a faculty member,” and \( A(x, y) \) the predicate “\( x \) has asked \( y \) a question,” where the domain consists of all people associated with your school. Use quantifiers to express each of these statements.

a) Lois has asked Professor Michaels a question.

b) Every student has asked Professor Gross a question.

c) Every faculty member has either asked Professor Miller a question or been asked a question by Professor Miller.

d) Some student has not asked any faculty member a question.

e) There is a faculty member who has never been asked a question by a student.

f) Some student has asked every faculty member a question.

g) There is a faculty member who has asked every other faculty member a question.

h) Some student has never been asked a question by a faculty member.

12. Let \( I(x) \) be the statement “\( x \) has an Internet connection” and \( C(x, y) \) be the statement “\( x \) and \( y \) have chatted over the Internet,” where the domain for the variables \( x \) and \( y \) consists of all students in your class. Use quantifiers to express each of these statements.

a) Jerry does not have an Internet connection.

b) Rachel has not chatted over the Internet with Chelsea.

c) Jan and Sharon have never chatted over the Internet.

d) No one in the class has chatted with Bob.

e) Sanjay has chatted with everyone except Joseph.

f) Someone in your class does not have an Internet connection.

g) Not everyone in your class has an Internet connection.

h) Exactly one student in your class has an Internet connection.

i) Everyone except one student in your class has an Internet connection.

j) Everyone in your class with an Internet connection has chatted over the Internet with at least one other student in your class.

k) Someone in your class has an Internet connection but has not chatted with anyone else in your class.

l) There are two students in your class who have not chatted with each other over the Internet.

m) There is a student in your class who has chatted with everyone in your class over the Internet.

n) There are at least two students in your class who have not chatted with the same person in your class.

o) There are two students in the class who between them have chatted with everyone else in the class.

13. Let \( M(x, y) \) be “\( x \) has sent \( y \) an e-mail message” and \( T(x, y) \) be “\( x \) has telephoned \( y \),” where the domain consists of all students in your class. Use quantifiers to express each of these statements. (Assume that all e-mail messages that were sent are received, which is not the way things often work.)

a) Chou has never sent an e-mail message to Koko.

b) Arlene has never sent an e-mail message to or telephoned Sarah.

c) Jose has never received an e-mail message from Deborah.

d) Every student in your class has sent an e-mail message to Ken.
15. Use quantifiers and predicates with more than one variable to express these statements.
   a) Every student in the class has telephoned Nina.
   b) Everyone in your class has either telephoned Avi or sent him an e-mail message.
   c) There is a student in your class who has sent everyone else in your class an e-mail message.
   d) There is someone in your class who has either sent an e-mail message or telephoned everyone else in your class.
   e) There are two different students in your class who have sent each other e-mail messages.
   f) There is a student who has sent himself or herself an e-mail message.
   g) There is a student in your class who has not received an e-mail message from anyone else in the class and who has not been called by any other student in the class.
   h) Every student in the class has either received an e-mail message or received a telephone call from another student in the class.
   i) There are at least two students in your class such that one student has sent the other e-mail and the second student has telephoned the first student.
   j) There are two different students in your class who between them have sent an e-mail message to or telephoned everyone else in the class.

16. A discrete mathematics class contains 1 mathematics major who is a freshman, 12 mathematics majors who are sophomores, 15 computer science majors who are sophomores, 2 mathematics majors who are juniors, 2 computer science majors who are juniors, and 1 computer science major who is a senior. Express each of these statements in terms of quantifiers and then determine its truth value.
   a) There is a student in the class who is a junior.
   b) Every student in the class is a computer science major.
   c) There is a student in the class who is neither a mathematics major nor a junior.
   d) Every student in the class is either a sophomore or a computer science major.
   e) There is a major such that there is a student in the class in every year of study with that major.

17. Express each of these system specifications using predicates, quantifiers, and logical connectives, if necessary.
   a) Every user has access to exactly one mailbox.
   b) There is a process that continues to run during all error conditions only if the kernel is working correctly.
   c) All users on the campus network can access all websites whose URL has a .edu extension.
   d) There are exactly two systems that monitor every remote server.

18. Express each of these system specifications using predicates, quantifiers, and logical connectives, if necessary.
   a) At least one console must be accessible during every fault condition.
   b) The e-mail address of every user can be retrieved whenever the archive contains at least one message sent by every user on the system.
   c) For every security breach there is at least one mechanism that can detect that breach if and only if there is a process that has not been compromised.
   d) There are at least two paths connecting every two distinct endpoints on the network.
   e) No one knows the password of every user on the system except for the system administrator, who knows all passwords.

19. Express each of these statements using mathematical and logical operators, predicates, and quantifiers, where the domain consists of all integers.
   a) The sum of two negative integers is negative.
   b) The difference of two positive integers is not necessarily positive.
   c) The sum of the squares of two integers is greater than or equal to the square of their sum.
   d) The absolute value of the product of two integers is the product of their absolute values.

20. Express each of these statements using predicates, quantifiers, logical connectives, and mathematical operators where the domain consists of all integers.
   a) The product of two negative integers is positive.
   b) The average of two positive integers is positive.
c) The difference of two negative integers is not necessarily negative.
d) The absolute value of the sum of two integers does not exceed the sum of the absolute values of these integers.

21. Use predicates, quantifiers, logical connectives, and mathematical operators to express the statement that every positive integer is the sum of the squares of four integers.

22. Use predicates, quantifiers, logical connectives, and mathematical operators to express the statement that there is a positive integer that is not the sum of three squares.

23. Express each of these mathematical statements using predicates, quantifiers, logical connectives, and mathematical operators.
a) The product of two negative real numbers is positive.
b) The difference of a real number and itself is zero.
c) Every positive real number has exactly two square roots.
d) A negative real number does not have a square root that is a real number.

24. Translate each of these nested quantifications into an English statement that expresses a mathematical fact. The domain in each case consists of all real numbers.

\[
\begin{align*}
& \exists x \forall y (xy = y) \\
& \forall x \forall y ((x \geq 0) \land (y < 0)) \rightarrow (x - y > 0) \\
& \exists x \exists y (((x \leq 0) \land (y \leq 0)) \land (x - y > 0)) \\
& \forall x \forall y (x \neq 0) \land (y \neq 0) \land (xy \neq 0)
\end{align*}
\]

25. Translate each of these nested quantifications into an English statement that expresses a mathematical fact. The domain in each case consists of all real numbers.

\[
\begin{align*}
& \exists x \forall y (xy = y) \\
& \forall x \forall y ((x < 0) \land (y < 0)) \rightarrow (xy > 0) \\
& \exists x \exists y ((x^2 > y) \land (x < y)) \\
& \forall x \forall y (x + y = z)
\end{align*}
\]

26. Let \( Q(x, y) \) be the statement \( \text{“} x + y = x - y \text{”} \). If the domain for both variables consists of all integers, what are the truth values?

\[
\begin{align*}
& Q(1, 1) \quad \text{b) } Q(2, 0) \\
& \exists x Q(x, y) \quad \text{d) } \exists x Q(x, y) \\
& \exists x Q(x, y) \quad \text{e) } \forall x Q(x, y) \\
& \forall x \forall y Q(x, y) \quad \text{g) } \forall x \exists y Q(x, y) \\
& \forall x \exists y Q(x, y) \quad \text{i) } \forall x \forall y Q(x, y)
\end{align*}
\]

27. Determine the truth value of each of these statements if the domain for all variables consists of all integers.

\[
\begin{align*}
& \forall m \exists n (n^2 < m) \\
& \exists m \forall n (n < m^2) \\
& \forall n \exists m (n + m = 0) \\
& \exists m \forall n (nm = m) \\
& \exists n \exists m (n^2 + m^2 = 5) \\
& \forall n \forall m \exists p (p = (m + n)/2)
\end{align*}
\]

28. Determine the truth value of each of these statements if the domain of each variable consists of all real numbers.

\[
\begin{align*}
& \forall x \exists y (x^2 = y) \\
& \forall x \exists y (x^2 = y^2)
\end{align*}
\]
simple English. (Do not simply use the words “It is not the case that.”)

a) No one has lost more than one thousand dollars playing the lottery.
b) There is a student in this class who has chatted with exactly one other student.
c) No student in this class has sent e-mail to exactly two other students in this class.
d) Some student has solved every exercise in this book.
e) No student has solved at least one exercise in every section of this book.

37. Express each of these statements using quantifiers. Then form the negation of the statement so that no negation is to the left of a quantifier. Next, express the negation in simple English. (Do not simply use the words “It is not the case that.”)

a) Every student in this class has taken exactly two mathematics classes at this school.
b) Someone has visited every country in the world except Libya.
c) No one has climbed every mountain in the Himalayas.
d) Every movie actor has either been in a movie with Kevin Bacon or has been in a movie with someone who has been in a movie with Kevin Bacon.

38. Express the negations of these propositions using quantifiers, and in English.

a) Every student in this class likes mathematics.
b) There is a student in this class who has never seen a computer.
c) There is a student in this class who has taken every mathematics course offered at this school.
d) There is a student in this class who has been in at least one room of every building on campus.

39. Find a counterexample, if possible, to these universally quantified statements, where the domain for all variables consists of all integers.

a) \( \forall x \forall y (x^2 = y^2 \rightarrow x = y) \)
b) \( \forall x \exists y (y^2 = x) \)
c) \( \forall x \forall y (xy \geq x) \)

40. Find a counterexample, if possible, to these universally quantified statements, where the domain for all variables consists of all integers.

a) \( \forall x \exists y (x = 1/y) \)
b) \( \forall x \exists y (y^2 - x < 100) \)
c) \( \forall x \forall y (x^2 \neq y^3) \)

41. Use quantifiers to express the associative law for multiplication of real numbers.

42. Use quantifiers to express the distributive laws of multiplication over addition for real numbers.

43. Use quantifiers and logical connectives to express the fact that every linear polynomial (that is, polynomial of degree 1) with real coefficients and where the coefficient of \( x \) is nonzero, has exactly one real root.

44. Use quantifiers and logical connectives to express the fact that a quadratic polynomial with real number coefficients has at most two real roots.

45. Determine the truth value of the statement \( \forall x \exists y (xy = 1) \) if the domain for the variables consists of

a) the nonzero real numbers.
b) the nonzero integers.
c) the positive real numbers.

46. Determine the truth value of the statement \( \exists x \forall y (x^2 \leq y^2) \) if the domain for the variables consists of

a) the positive real numbers.
b) the integers.
c) the nonzero real numbers.

47. Show that the two statements \( \neg \exists x \forall y P(x, y) \) and \( \forall x \exists y -P(x, y) \), where both quantifiers over the first variable in \( P(x, y) \) have the same domain, and both quantifiers over the second variable in \( P(x, y) \) have the same domain, are logically equivalent.

48. Show that \( \forall x P(x) \lor \forall x Q(x) \) and \( \forall x \forall y (P(x) \lor Q(y)) \), where all quantifiers have the same nonempty domain, are logically equivalent. (The new variable \( y \) is used to combine the quantifications correctly.)

49. a) Show that \( \forall x P(x) \land \exists x Q(x) \) is logically equivalent to \( \forall x \exists y (P(x) \land Q(y)) \), where all quantifiers have the same nonempty domain.
b) Show that \( \forall x P(x) \lor \exists x Q(x) \) is equivalent to \( \forall x \exists y (P(x) \lor Q(y)) \), where all quantifiers have the same nonempty domain.

A statement is in **prenex normal form (PNF)** if and only if it is of the form

\[ Q_1 x_1 Q_2 x_2 \cdots Q_k x_k P(x_1, x_2, \ldots, x_k), \]

where each \( Q_i, i = 1, 2, \ldots, k \), is either the existential quantifier or the universal quantifier, and \( P(x_1, \ldots, x_k) \) is a predicate involving no quantifiers. For example, \( \exists x \forall y (P(x, y) \land Q(y)) \) is in prenex normal form, whereas \( \exists x P(x) \lor \forall x Q(x) \) is not (because the quantifiers do not all occur first).

Every statement formed from propositional variables, predicates, \( T \), and \( F \) using logical connectives and quantifiers is equivalent to a statement in prenex normal form. Exercise 51 asks for a proof of this fact.

50. Put these statements in prenex normal form. [Hint: Use logical equivalence from Tables 6 and 7 in Section 1.2, Table 2 in Section 1.3, Example 19 in Section 1.3, Exercises 45 and 46 in Section 1.3, and Exercises 48 and 49 in this section.]

a) \( \exists x P(x) \lor \exists x Q(x) \lor A \), where \( A \) is a proposition not involving any quantifiers.
b) \( \neg (\forall x P(x) \lor \forall x Q(x)) \)
c) \( \exists x P(x) \rightarrow \exists x Q(x) \)

51. Show how to transform an arbitrary statement to a statement in prenex normal form that is equivalent to the given statement.

52. Express the quantification \( \exists! x P(x) \), introduced on page 38, using universal quantifications, existential quantifications, and logical operators.
Solution: Let \( P(n) \) denote \( "n > 4" \) and \( Q(n) \) denote \( "n^2 < 2^n\)." The statement "For all positive integers \( n \), if \( n \) is greater than 4, then \( n^2 \) is less than \( 2^n\)" can be represented by \( \forall n (P(n) \to Q(n)) \), where the domain consists of all positive integers. We are assuming that \( \forall n (P(n) \to Q(n)) \) is true. Note that \( P(100) \) is true because \( 100 > 4 \). It follows by universal modus ponens that \( Q(n) \) is true, namely that \( 100^2 < 2^{100} \).

Another useful combination of a rule of inference from propositional logic and a rule of inference for quantified statements is \textbf{universal modus tollens}. Universal modus tollens combines universal instantiation and modus tollens and can be expressed in the following way:

\[
\begin{align*}
\forall x (P(x) & \to Q(x)) \\
\neg Q(a) & \text{, where } a \text{ is a particular element in the domain} \\
\therefore \neg P(a)
\end{align*}
\]

We leave the verification of universal modus tollens to the reader (see Exercise 25). Exercise 26 develops additional combinations of rules of inference in propositional logic and quantified statements.

**Exercises**

1. Find the argument form for the following argument and determine whether it is valid. Can we conclude that the conclusion is true if the premises are true?
   
   - If Socrates is human, then Socrates is mortal. 
   - Socrates is human. 
   
   \therefore Socrates is mortal.

2. Find the argument form for the following argument and determine whether it is valid. Can we conclude that the conclusion is true if the premises are true?
   
   - If George does not have eight legs, then he is not an insect. 
   - George is an insect. 
   
   \therefore George has eight legs.

3. What rule of inference is used in each of these arguments?
   
   a) Alice is a mathematics major. Therefore, Alice is either a mathematics major or a computer science major. 
   b) Jerry is a mathematics major and a computer science major. Therefore, Jerry is a mathematics major. 
   c) If it is rainy, then the pool will be closed. It is rainy. Therefore, the pool is closed. 
   d) If it snows today, the university will close. The university is not closed today. Therefore, it did not snow today. 
   e) If I go swimming, then I will stay in the sun too long. If I stay in the sun too long, then I will sunburn. Therefore, if I go swimming, then I will sunburn.

4. What rule of inference is used in each of these arguments?
   
   a) Kangaroos live in Australia and are marsupials. Therefore, kangaroos are marsupials. 
   b) It is either hotter than 100 degrees today or the pollution is dangerous. It is less than 100 degrees outside today. Therefore, the pollution is dangerous. 
   c) Linda is an excellent swimmer. If Linda is an excellent swimmer, then she can work as a lifeguard. Therefore, Linda can work as a lifeguard. 
   d) Steve will work at a computer company this summer. Therefore, this summer Steve will work at a computer company or he will be a beach bum. 
   e) If I work all night on this homework, then I can answer all the exercises. If I answer all the exercises, I will understand the material. Therefore, if I work all night on this homework, then I will understand the material.

5. Use rules of inference to show that the hypotheses "Randy works hard," "If Randy works hard, then he is a dull boy," and "If Randy is a dull boy, then he will not get the job" imply the conclusion "Randy will not get the job."

6. Use rules of inference to show that the hypotheses "If it does not rain or if it is not foggy, then the sailing race will be held and the lifesaving demonstration will go on," "If the sailing race is held, then the trophy will be awarded," and "The trophy was not awarded" imply the conclusion "It rained."

7. What rules of inference are used in this famous argument? "All men are mortal. Socrates is a man. Therefore, Socrates is mortal."

8. What rules of inference are used in this argument? "No man is an island. Manhattan is an island. Therefore, Manhattan is not a man."
9. For each of these sets of premises, what relevant conclusion or conclusions can be drawn? Explain the rules of inference used to obtain each conclusion from the premises.
   a) “If I take the day off, it either rains or snows.” “I took Tuesday off or I took Thursday off.” “It was sunny on Tuesday.” “It did not snow on Thursday.”
   b) “If I eat spicy foods, then I have strange dreams.” “I have strange dreams if there is thunder while I sleep.” “I did not have strange dreams.”
   c) “I am either clever or lucky.” “I am not lucky.” “If I am lucky, then I will win the lottery.”
   d) “Every computer science major has a personal computer.” “Ralph does not have a personal computer.” “Ann has a personal computer.”
   e) “What is good for corporations is good for the United States.” “What is good for the United States is good for you.” “What is good for corporations is for you to buy lots of stuff.”
   f) “All rodents gnaw their food.” “Mice are rodents.” “Rabbits do not gnaw their food.” “Bats are not rodents.”

10. For each of these sets of premises, what relevant conclusion or conclusions can be drawn? Explain the rules of inference used to obtain each conclusion from the premises.
   a) “If I play hockey, then I am sore the next day.” “I use the whirlpool if I am sore.” “I did not use the whirlpool.”
   b) “If I work, it is either sunny or partly sunny.” “I worked Monday or I worked last Friday.” “It was not sunny on Tuesday.” “It was not partly sunny on Friday.”
   c) “All insects have six legs.” “Dragonflies are insects.” “Spiders do not have six legs.” “Spiders eat dragonflies.”
   d) “Every student has an Internet account.” “Homer does not have an Internet account.” “Maggie has an Internet account.”
   e) “All foods that are healthy to eat do not taste good.” “Tofu is healthy to eat.” “You only eat what tastes good.” “You do not eat tofu.” “Cheeseburgers are not healthy to eat.”
   f) “I am either dreaming or hallucinating.” “I am not dreaming.” “If I am hallucinating, I see elephants running down the road.”

11. Show that the argument form with premises $P_1$, $P_2$, ..., $P_n$ and conclusion $q \rightarrow r$ is valid if the argument form with premises $P_1$, $P_2$, ..., $P_n$, $q$, and conclusion $r$ is valid.

12. Show that the argument form with premises $(P \land t) \rightarrow (r \lor s)$, $q \rightarrow (u \land t)$, $u \rightarrow p$, and $\neg s$ and conclusion $q \rightarrow r$ is valid by first using Exercise 11 and then using rules of inference from Table 1.

13. For each of these arguments, explain which rules of inference are used for each step.
   a) “Doug, a student in this class, knows how to write programs in JAVA. Everyone who knows how to write programs in JAVA can get a high-paying job. Therefore, someone in this class can get a high-paying job.”
   b) “Somebody in this class enjoys whale watching. Every person who enjoys whale watching cares about ocean pollution. Therefore, there is a person in this class who cares about ocean pollution.”
   c) “Each of the 93 students in this class owns a personal computer. Everyone who owns a personal computer can use a word processing program. Therefore, Zeke, a student in this class, can use a word processing program.”
   d) “Everyone in New Jersey lives within 50 miles of the ocean. Someone in New Jersey has never seen the ocean. Therefore, someone who lives within 50 miles of the ocean has never seen the ocean.”

14. For each of these arguments, explain which rules of inference are used for each step.
   a) “Linda, a student in this class, owns a red convertible. Everyone who owns a red convertible has gotten at least one speeding ticket. Therefore, someone in this class has gotten a speeding ticket.”
   b) “Each of five roommates, Melissa, Aaron, Ralph, Veneesha, and Keeshawn, has taken a course in discrete mathematics. Every student who has taken a course in discrete mathematics can take a course in algorithms. Therefore, all five roommates can take a course in algorithms next year.”
   c) “All movies produced by John Sayles are wonderful. John Sayles produced a movie about coal miners. Therefore, there is a wonderful movie about coal miners.”
   d) “There is someone in this class who has been to France. Everyone who goes to France visits the Louvre. Therefore, someone in this class has visited the Louvre.”

15. For each of these arguments determine whether the argument is correct or incorrect and explain why.
   a) All students in this class understand logic. Xavier is a student in this class. Therefore, Xavier understands logic.
   b) Every computer science major takes discrete mathematics. Natasha is taking discrete mathematics. Therefore, Natasha is a computer science major.
   c) All parrots like fruit. My pet bird is not a parrot. Therefore, my pet bird does not like fruit.
   d) Everyone who eats granola every day is healthy. Linda is not healthy. Therefore, Linda does not eat granola every day.

16. For each of these arguments determine whether the argument is correct or incorrect and explain why.
   a) Everyone enrolled in the university has lived in a dormitory. Mia has never lived in a dormitory. Therefore, Mia is not enrolled in the university.
   b) A convertible car is fun to drive. Isaac’s car is not a convertible. Therefore, Isaac’s car is not fun to drive.
   c) Quincy likes all action movies. Quincy likes the movie *Eight Men Out*. Therefore, *Eight Men Out* is an action movie.
17. What is wrong with this argument? Let \( H(x) \) be “\( x \) is happy.” Given the premise \( \exists x H(x) \), we conclude that \( H(Lola) \). Therefore, Lola is happy.

18. What is wrong with this argument? Let \( S(x,y) \) be “\( x \) is shorter than \( y \).” Given the premise \( \exists x S(x, \text{Max}) \), it follows that \( S(\text{Max}, \text{Max}) \). Then by existential generalization it follows that \( \exists x S(x,x) \), so that someone is shorter than himself.

19. Determine whether each of these arguments is valid. If an argument is correct, what rule of inference is being used? If it is not, what logical error occurs?
   a) If \( n \) is a real number such that \( n > 1 \), then \( n^2 > 1 \).
      Suppose that \( n^2 > 1 \). Then \( n > 1 \).
   b) If \( n \) is a real number with \( n > 3 \), then \( n^2 > 9 \).
      Suppose that \( n^2 > 9 \).
   c) If \( n \) is a real number with \( n > 2 \), then \( n^2 > 4 \).
      Suppose that \( n > 2 \).

20. Determine whether these are valid arguments.
   a) If \( x \) is a positive real number, then \( x^2 \) is a positive real number.
      Therefore, if \( a^2 \) is positive, where \( a \) is a real number, then \( a \) is a positive real number.
   b) If \( x^2 \neq 0 \), where \( x \) is a real number, then \( x \neq 0 \).
      Let \( a \) be a real number with \( a^2 \neq 0 \); then \( a \neq 0 \).

21. Which rules of inference are used to establish the conclusion of Lewis Carroll’s argument described in Example 26 of Section 1.3?

22. Which rules of inference are used to establish the conclusion of Lewis Carroll’s argument described in Example 27 of Section 1.3?

23. Identify the error or errors in this argument that supposedly shows that if \( \exists x P(x) \wedge \exists x Q(x) \) is true then \( \exists x(P(x) \wedge Q(x)) \) is true.
   1. \( \exists x P(x) \wedge \exists x Q(x) \)  Premise
   2. \( \exists x P(x) \)  Simplification from (1)
   3. \( P(c) \)  Existential instantiation from (2)
   4. \( \exists x Q(x) \)  Simplification from (1)
   5. \( Q(c) \)  Existential instantiation from (2)
   6. \( P(c) \wedge Q(c) \)  Conjunction from (3) and (5)
   7. \( \exists x(P(x) \wedge Q(x)) \)  Existential generalization

24. Identify the error or errors in this argument that supposedly shows that if \( \forall x (P(x) \vee Q(x)) \) is true then \( \forall x P(x) \vee \forall x Q(x) \) is true.
   1. \( \forall x (P(x) \vee Q(x)) \)  Premise
   2. \( P(c) \vee Q(c) \)  Universal instantiation from (1)
   3. \( P(c) \)  Simplification from (2)
   4. \( \exists x P(x) \)  Universal generalization from (3)
   5. \( Q(c) \)  Simplification from (2)
   6. \( \exists x Q(x) \)  Universal generalization from (5)
   7. \( \forall x(P(x) \vee \exists x Q(x)) \)  Conjunction from (4) and (6)

25. Justify the rule of universal modus tollens by showing that the premises \( \forall x (P(x) \rightarrow Q(x)) \) and \( \neg Q(a) \) for a particular element \( a \) in the domain, imply \( \neg P(a) \).

26. Justify the rule of **universal transitivity**, which states that if \( \forall x (P(x) \rightarrow Q(x)) \) and \( \forall x (Q(x) \rightarrow R(x)) \) are true, then \( \forall x (P(x) \rightarrow R(x)) \) is true, where the domains of all quantifiers are the same.

27. Use rules of inference to show that if \( \forall x (P(x) \rightarrow (Q(x) \wedge S(x))) \) and \( \forall x (P(x) \wedge R(x)) \) are true, then \( \forall x (R(x) \wedge S(x)) \) is true.

28. Use rules of inference to show that if \( \forall x (P(x) \vee Q(x)) \) and \( \forall x (\neg P(x) \vee Q(x)) \rightarrow R(x) \) are true, then \( \forall x (\neg R(x) \rightarrow P(x)) \) is also true, where the domains of all quantifiers are the same.

29. Use rules of inference to show that if \( \forall x (P(x) \vee Q(x)) \), \( \forall x (\neg Q(x) \vee S(x)) \), \( \forall x (R(x) \rightarrow \neg S(x)) \), and \( \exists x \neg P(x) \) are true, then \( \exists x \neg R(x) \) is true.

30. Use resolution to show the hypotheses “Allen is a bad boy or Hillary is a good girl” and “Allen is a good boy or David is happy” imply the conclusion “Hillary is a good girl or David is happy.”

31. Use resolution to show that the hypotheses “It is not raining or Yvette has her umbrella,” “Yvette does not have her umbrella or she does not get wet,” and “It is raining or Yvette does not get wet” imply that “Yvette does not get wet.”

32. Show that the equivalence \( p \wedge \neg p \equiv \text{F} \) can be derived using resolution together with the fact that a conditional statement with a false hypothesis is true. [Hint: Let \( q = r = \text{F} \) in resolution.]

33. Use resolution to show that the compound proposition \( (p \vee q) \wedge (\neg p \vee q) \wedge (p \vee \neg q) \wedge (\neg p \vee \neg q) \) is not satisfiable.

*34. The Logic Problem, taken from WFF’N PROOF, The Game of Logic, has these two assumptions:
   1. “Logic is difficult or not many students like logic.”
   2. “If mathematics is easy, then logic is not difficult.”
   By translating these assumptions into statements involving propositional variables and logical connectives, determine whether each of the following are valid conclusions of these assumptions:
   a) That mathematics is not easy, if many students like logic.
   b) That not many students like logic, if mathematics is not easy.
   c) That mathematics is not easy or logic is difficult.
   d) That logic is not difficult or mathematics is not easy.
   e) That if not many students like logic, then either mathematics is not easy or logic is difficult.

*35. Determine whether this argument, taken from Kalish and Montague, is valid.
   If Superman were able and willing to prevent evil, he would do so. If Superman were unable to prevent evil, he would be impotent; if he were unwilling to prevent evil, he would be malevolent. Superman does not prevent evil. If Superman exists, he is neither impotent nor malevolent. Therefore, Superman does not exist.
Chapter 4, including mathematical induction, which can be used to prove results that hold for all positive integers. In Chapter 5 we will introduce the notion of combinatorial proofs.

In this section we introduced several methods for proving theorems of the form \( \forall x (P(x) \rightarrow Q(x)) \), including direct proofs and proofs by contraposition. There are many theorems of this type whose proofs are easy to construct by directly working through the hypotheses and definitions of the terms of the theorem. However, it is often difficult to prove a theorem without resorting to a clever use of a proof by contraposition or a proof by contradiction, or some other proof technique. In Section 1.7 we will address proof strategy. We will describe various approaches that can be used to find proofs when straightforward approaches do not work. Constructing proofs is an art that can be learned only through experience, including writing proofs, having your proofs critiqued, and reading and analyzing other proofs.

### Exercises

1. Use a direct proof to show that the sum of two odd integers is even.
2. Use a direct proof to show that the sum of two even integers is even.
3. Show that the square of an even number is an even number using a direct proof.
4. Show that the additive inverse, or negative, of an even number is an even number using a direct proof.
5. Prove that if \( m + n \) and \( n + p \) are even integers, where \( m, n, \) and \( p \) are integers, then \( m + p \) is even. What kind of proof did you use?
6. Use a direct proof to show that the product of two odd numbers is odd.
7. Use a direct proof to show that every odd integer is the difference of two squares.
8. Prove that if \( n \) is a perfect square, then \( n + 2 \) is not a perfect square.
9. Use a proof by contradiction to prove that the sum of an irrational number and a rational number is irrational.
10. Use a direct proof to show that the product of two rational numbers is rational.
11. Prove or disprove that the product of two irrational numbers is irrational.
12. Prove or disprove that the product of a nonzero rational number and an irrational number is irrational.
13. Prove that if \( x \) is irrational, then \( 1/x \) is irrational.
14. Prove that if \( x \) is rational and \( x \neq 0 \), then \( 1/x \) is rational.
15. Use a proof by contraposition to show that if \( x + y \geq 2 \), where \( x \) and \( y \) are real numbers, then \( x \geq 1 \) or \( y \geq 1 \).
16. Prove that if \( m \) and \( n \) are integers and \( mn \) is even, then \( m \) is even or \( n \) is even.
17. Show that if \( n \) is an integer and \( n^3 + 5 \) is odd, then \( n \) is even using
   a) a proof by contraposition.
   b) a proof by contradiction.
18. Prove that if \( n \) is an integer and \( 3n + 2 \) is even, then \( n \) is even using
   a) a proof by contraposition.
   b) a proof by contradiction.
19. Prove the proposition \( P(0) \), where \( P(n) \) is the proposition “If \( n \) is a positive integer greater than 1, then \( n^2 > n \).” What kind of proof did you use?
20. Prove the proposition \( P(1) \), where \( P(n) \) is the proposition “If \( n \) is a positive integer, then \( n^2 \geq n \).” What kind of proof did you use?
21. Let \( P(n) \) be the proposition “If \( a \) and \( b \) are positive real numbers, then \((a + b)^n \geq a^n + b^n\).” Prove that \( P(1) \) is true. What kind of proof did you use?
22. Show that if you pick three socks from a drawer containing just blue socks and black socks, you must get either a pair of blue socks or a pair of black socks.
23. Show that at least 10 of any 64 days chosen must fall on the same day of the week.
24. Show that at least 3 of any 25 days chosen must fall in the same month of the year.
25. Use a proof by contradiction to show that there is no rational number \( r \) for which \( r^3 + r + 1 = 0 \). [Hint: Assume that \( r = a/b \) is a root, where \( a \) and \( b \) are integers and \( a/b \) is in lowest terms. Obtain an equation involving integers by multiplying by \( b^3 \). Then look at whether \( a \) and \( b \) are each odd or even.]
26. Prove that if \( n \) is a positive integer, then \( n \) is even if and only if \( 7n + 4 \) is even.
27. Prove that if \( n \) is a positive integer, then \( n \) is odd if and only if \( 5n + 6 \) is odd.
28. Prove that \( m^2 = n^2 \) if and only if \( m = n \) or \( m = -n \).
29. Prove or disprove that if \( m \) and \( n \) are integers such that \( mn = 1 \), then either \( m = 1 \) and \( n = 1 \), or else \( m = -1 \) and \( n = -1 \).
30. Show that these three statements are equivalent, where \( a \) and \( b \) are real numbers: (i) \( a \) is less than \( b \), (ii) the average of \( a \) and \( b \) is greater than \( a \), and (iii) the average of \( a \) and \( b \) is less than \( b \).
31. Show that these statements about the integer \( x \) are equivalent: (i) \( 3x + 2 \) is even, (ii) \( x + 5 \) is odd, (iii) \( x^2 \) is even.
32. Show that these statements about the real number $x$ are equivalent: (i) $x$ is rational, (ii) $x/2$ is rational, and (iii) $3x - 1$ is rational.

33. Show that these statements about the real number $x$ are equivalent: (i) $x$ is irrational, (ii) $3x + 2$ is irrational, (iii) $x/2$ is irrational.

34. Is this reasoning for finding the solutions of the equation $\sqrt{2x^2 - 1} = x$ correct? (1) $\sqrt{2x^2 - 1} = x$ is given; (2) $2x^2 - 1 = x^2$, obtained by squaring both sides of (1); (3) $x^2 - 1 = 0$, obtained by subtracting $x^2$ from both sides of (2); (4) $(x - 1)(x + 1) = 0$, obtained by factoring the left-hand side of $x^2 - 1$; (5) $x = 1$ or $x = -1$, which follows because $ab = 0$ implies that $a = 0$ or $b = 0$.

35. Are these steps for finding the solutions of $\sqrt[3]{x + 3} = 3 - x$ correct? (1) $\sqrt[3]{x + 3} = 3 - x$ is given; (2) $x + 3 = x^2 - 6x + 9$, obtained by squaring both sides of (1); (3) $0 = x^2 - 7x + 6$, obtained by subtracting $x + 3$ from both sides of (2); (4) $0 = (x - 1)(x - 6)$, obtained by factoring the right-hand side of (3); (5) $x = 1$ or $x = 6$, which follows from (4) because $ab = 0$ implies that $a = 0$ or $b = 0$.

36. Show that the propositions $p_1, p_2, p_3,$ and $p_4$ can be shown to be equivalent by giving that $p_1 \iff p_4, p_2 \iff p_3,$ and $p_1 \iff p_3$.

37. Show that the propositions $p_1, p_2, p_3, p_4,$ and $p_5$ can be shown to be equivalent by giving that the conditional statements $p_1 \rightarrow p_4, p_3 \rightarrow p_1, p_4 \rightarrow p_2, p_2 \rightarrow p_3,$ and $p_5 \rightarrow p_3$ are true.

38. Find a counterexample to the statement that every positive integer can be written as the sum of the squares of three integers.

39. Prove that at least one of the real numbers $a_1, a_2, \ldots, a_n$ is greater than or equal to the average of these numbers. What kind of proof did you use?

40. Use Exercise 39 to show that if the first 10 positive integers are placed around a circle, in any order, there exist three integers in consecutive locations around the circle that have a sum greater than or equal to 17.

41. Prove that if $n$ is an integer, these four statements are equivalent: (i) $n$ is even, (ii) $n + 1$ is odd, (iii) $3n + 1$ is odd, (iv) $3n$ is even.

42. Prove that these four statements about the integer $n$ are equivalent: (i) $n^2$ is odd, (ii) $1 - n$ is even, (iii) $n^3$ is odd, (iv) $n^2 + 1$ is even.

### 1.7 Proof Methods and Strategy

#### Introduction

In Section 1.6 we introduced a variety of different methods of proof and illustrated how each method is used. In this section we continue this effort. We will introduce several other important proof methods, including proofs where we consider different cases separately and proofs where we prove the existence of objects with desired properties.

In Section 1.6 we only briefly discussed the strategy behind constructing proofs. This strategy includes selecting a proof method and then successfully constructing an argument step by step, based on this method. In this section, after we have developed a wider arsenal of proof methods, we will study some additional aspects of the art and science of proofs. We will provide advice on how to find a proof of a theorem. We will describe some tricks of the trade, including how proofs can be found by working backward and by adapting existing proofs.

When mathematicians work, they formulate conjectures and attempt to prove or disprove them. We will briefly describe this process here by proving results about tiling checkerboards with dominoes and other types of pieces. Looking at tilings of this kind, we will be able to quickly formulate conjectures and prove theorems without first developing a theory.

We will conclude the section by discussing the role of open questions. In particular, we will discuss some interesting problems either that have been solved after remaining open for hundreds of years or that still remain open.

#### Exhaustive Proof and Proof by Cases

Sometimes we cannot prove a theorem using a single argument that holds for all possible cases. We now introduce a method that can be used to prove a theorem, by considering different cases
The $3x + 1$ conjecture has an interesting history and has attracted the attention of mathematicians since the 1950s. The conjecture has been raised many times and goes by many other names, including the Collatz problem, Hasse's algorithm, Ulam's problem, the Syracuse problem, and Kakutani's problem. Many mathematicians have been diverted from their work to spend time attacking this conjecture. This led to the joke that this problem was part of a conspiracy to slow down American mathematical research. See the article by Jeffrey Lagarias [La85] for a fascinating discussion of this problem and the results that have been found by mathematicians attacking it.

In Chapter 3 we will describe additional open questions about prime numbers. Students already familiar with the basic notions about primes might want to explore Section 3.4, where these open questions are discussed. We will mention other important open questions throughout the book.

### Additional Proof Methods

In this chapter we introduced the basic methods used in proofs. We also described how to leverage these methods to prove a variety of results. We will use these proof methods in Chapters 2 and 3 to prove results about sets, functions, algorithms, and number theory. Among the theorems we will prove is the famous halting theorem which states that there is a problem that cannot be solved using any procedure. However, there are many important proof methods besides those we have covered. We will introduce some of these methods later in this book. In particular, in Section 4.1 we will discuss mathematical induction, which is an extremely useful method for proving statements of the form $\forall n P(n)$, where the domain consists of all positive integers. In Section 4.3 we will introduce structural induction, which can be used to prove results about recursively defined sets. We will use the Cantor diagonalization method, which can be used to prove results about the size of infinite sets, in Section 2.4. In Chapter 5 we will introduce the notion of combinatorial proofs, which can be used to prove results by counting arguments. The reader should note that entire books have been devoted to the activities discussed in this section, including many excellent works by George Pólya ([Po61], [Po71], [Po90]).

Finally, note that we have not given a procedure that can be used for proving theorems in mathematics. It is a deep theorem of mathematical logic that there is no such procedure.

### Exercises

1. Prove that $n^2 + 1 \geq 2^n$ when $n$ is a positive integer with $1 \leq n \leq 4$.
2. Prove that there are no positive perfect cubes less 1000 that are the sum of the cubes of two positive integers.
3. Prove that if $x$ and $y$ are real numbers, then $\max(x, y) + \min(x, y) = x + y$. [Hint: Use a proof by cases, with the two cases corresponding to $x \geq y$ and $x < y$, respectively.]
4. Use a proof by cases to show that $\min(a, \min(b, c)) = \min(\min(a, b), c)$ whenever $a$, $b$, and $c$ are real numbers.
5. Prove the triangle inequality, which states that if $x$ and $y$ are real numbers, then $|x| + |y| \geq |x + y|$ (where $|x|$ represents the absolute value of $x$, which equals $x$ if $x \geq 0$ and equals $-x$ if $x < 0$).
6. Prove that there is a positive integer that equals the sum of the positive integers not exceeding it. Is your proof constructive or nonconstructive?
7. Prove that there are 100 consecutive positive integers that are not perfect squares. Is your proof constructive or nonconstructive?
8. Prove that either $2 \cdot 10^{500} + 15$ or $2 \cdot 10^{500} + 16$ is not a perfect square. Is your proof constructive or nonconstructive?
9. Prove that there exists a pair of consecutive integers such that one of these integers is a perfect square and the other is a perfect cube.
10. Show that the product of two of the numbers $65^{1000} - 8^{2001} + 3177$, $79^{1212} - 9^{2399} + 2^{2001}$, and $24^{4493} - 58^{192} +$
1. Prove or disprove that there is a rational number $x$ and an irrational number $y$ such that $x^2 + y^2$ is irrational.

2. Prove or disprove that if $a$ and $b$ are rational numbers, then $a^b$ is also rational.

3. Show that each of these statements can be used to express the fact that there is a unique element $x$ such that $P(x)$ is true. [Note that we can also write this statement as $\exists x P(x).$

   a) $\exists x \forall y (P(y) \leftrightarrow x = y)$
   b) $\exists x \forall y (P(x) \land P(y) \rightarrow x = y)$
   c) $\exists x (P(x) \land \forall y (P(y) \rightarrow x = y))$

4. Show that if $a$, $b$, and $c$ are real numbers and $a \neq 0$, then there is a unique solution of the equation $ax + b = c$.

5. Suppose that $a$ and $b$ are odd integers with $a \neq b$. Show that there is a unique integer $c$ such that $|a - c| = |b - c|$.

6. Show that if $r$ is an irrational number, there is a unique integer $n$ such that the distance between $r$ and $n$ is less than $1/2$.

7. Show that if $n$ is an odd integer, then there is a unique integer $k$ such that $n$ is the sum of $k - 2$ and $k + 3$.

8. Prove that given a real number $x$ there exist unique numbers $n$ and $\varepsilon$ such that $x = n + \varepsilon$, $n$ is an integer, and $0 \leq \varepsilon < 1$.

9. Prove that given a real number $x$ there exist unique numbers $n$ and $\varepsilon$ such that $x = n - \varepsilon$, $n$ is an integer, and $0 \leq \varepsilon < 1$.

10. Use forward reasoning to show that if $x$ is a nonzero real number, then $x^2 + 1/x^2 \geq 2$. [Hint: Start with the inequality $(x - 1/x)^2 \geq 0$ which holds for all nonzero real numbers $x$.]

11. The harmonic mean of two real numbers $x$ and $y$ equals $2xy/(x + y)$. By computing the harmonic and geometric means of different pairs of positive real numbers, formulate a conjecture about their relative sizes and prove your conjecture.

12. The quadratic mean of two real numbers $x$ and $y$ equals $\sqrt{(x^2 + y^2)/2}$. By computing the arithmetic and quadratic means of different pairs of positive real numbers, formulate a conjecture about their relative sizes and prove your conjecture.

13. Write the numbers $1, 2, \ldots, 2n$ on a blackboard, where $n$ is an odd integer. Pick any two of the numbers, $j$ and $k$, write $|j - k|$ on the board and erase $j$ and $k$. Continue this process until only one integer is written on the board. Prove that this integer must be odd.

14. Suppose that five ones and four zeros are arranged around a circle. Between any two equal bits you insert a $0$ and between any two unequal bits you insert a $1$ to produce nine new bits. Then you erase the nine original bits. Show that when you iterate this procedure, you can never get nine zeros. [Hint: Work backward, assuming that you did end up with nine zeros.]

15. Formulate a conjecture about the decimal digits that appear as the final decimal digit of the fourth power of an integer. Prove your conjecture using a proof by cases.

16. Formulate a conjecture about the final two decimal digits of the square of an integer. Prove your conjecture using a proof by cases.

17. Prove that there is no positive integer $n$ such that $n^2 + n^3 = 100$.

18. Prove that there are no solutions in integers $x$ and $y$ to the equation $x^2 + 5y^2 = 14$.

19. Prove that there are infinitely many solutions in positive integers $x$ and $y$ to the equation $x^4 + y^4 = 625$.

20. Prove that there are infinitely many solutions in positive integers $x$, $y$, and $z$ to the equation $x^2 + y^2 = z^2$. [Hint: Let $x = m^2 - n^2$, $y = 2mn$, and $z = m^2 + n^2$, where $m$ and $n$ are integers.]

21. Adapt the proof in Example 4 in Section 1.6 to prove that if $n = abc$, where $a$, $b$, and $c$ are positive integers, then $a \leq \sqrt[3]{n}, b \leq \sqrt[3]{n}$, or $c \leq \sqrt[3]{n}$.

22. Prove that $\sqrt[3]{2}$ is irrational.

23. Prove that between every two rational numbers there is an irrational number.

24. Prove that between every rational number and every irrational number there is an irrational number.

25. Let $S = x_1 y_1 + x_2 y_2 + \cdots + x_n y_n$, where $x_1, x_2, \ldots, x_n$ and $y_1, y_2, \ldots, y_n$ are orderings of two different sequences of positive real numbers, each containing $n$ elements.

   a) Show that $S$ takes its maximum value over all orderings of the two sequences when both sequences are sorted (so that the elements in each sequence are in nondecreasing order).
   b) Show that $S$ takes its minimum value over all orderings of the two sequences when one sequence is sorted into nondecreasing order and the other is sorted into nonincreasing order.

26. Prove or disprove that if you have an 8-gallon jug of water and two empty jugs with capacities of 5 gallons and 3 gallons, respectively, then you can measure 4 gallons by successively pouring some or all of the water in a jug into another jug.

27. Verify the $3x + 1$ conjecture for these integers.
   a) 6 b) 7 c) 17 d) 21

28. Verify the $3x + 1$ conjecture for these integers.
   a) 16 b) 11 c) 35 d) 113

29. Prove or disprove that you can use dominoes to tile the standard checkerboard with two adjacent corners removed (that is, corners that are not opposite).

30. Prove or disprove that you can use dominoes to tile the standard checkerboard with all four corners removed.

31. Prove that you can use dominoes to tile a rectangular checkerboard with an even number of squares.

32. Prove or disprove that you can use dominoes to tile a $5 \times 5$ checkerboard with three corners removed.
43. Use a proof by exhaustion to show that a tiling using dominoes of a 4 x 4 checkerboard with opposite corners removed does not exist. [Hint: First show that you can assume that the squares in the upper left and lower right corners are removed. Number the squares of the original checkerboard from 1 to 16, starting in the first row, moving right in this row, then starting in the left-most square in the second row and moving right, and so on. Remove squares 1 and 16. To begin the proof, note that square 2 is covered either by a domino laid horizontally, which covers squares 2 and 3, or vertically, which covers squares 2 and 6. Consider each of these cases separately, and work through all the subcases that arise.]

*44. Prove that when a white square and a black square are removed from an 8 x 8 checkerboard (colored as in the text) you can tile the remaining squares of the checkerboard using dominoes. [Hint: Show that when one black and one white square are removed, each part of the partition of the remaining cells formed by inserting the barriers shown in the figure can be covered by dominoes.]

45. Show that by removing two white squares and two black squares from an 8 x 8 checkerboard (colored as in the text) you can make it impossible to tile the remaining squares using dominoes.

*46. Find all squares, if they exist, on an 8 x 8 checkerboard so that the board obtained by removing one of these square can be tiled using straight triominoes. [Hint: First use arguments based on coloring and rotations to eliminate as many squares as possible from consideration.]

*47. a) Draw each of the five different tetrominoes, where a tetromino is a polyomino consisting of four squares.
   b) For each of the five different tetrominoes, prove or disprove that you can tile a standard checkerboard using these tetrominoes.

*48. Prove or disprove that you can tile a 10 x 10 checkerboard using straight tetrominoes.

---

Key Terms and Results

**TERMS**

- **proposition**: a statement that is true or false
- **propositional variable**: a variable that represents a proposition
- **truth value**: true or false
- **¬ p (negation of p)**: the proposition with truth value opposite to the truth value of p
- **logical operators**: operators used to combine propositions
- **compound proposition**: a proposition constructed by combining propositions using logical operators
- **truth table**: a table displaying the truth values of propositions p ∨ q (disjunction of p and q): the proposition “p or q,” which is true if and only if at least one of p and q is true
- **p ∧ q (conjunction of p and q)**: the proposition “p and q” which is true if and only if both p and q are true
- **p ⊕ q (exclusive or of p and q)**: the proposition “p XOR q” which is true when exactly one of p and q is true
- **p → q (implies q)**: the proposition “if p, then q,” which is false if and only if p is true and q is false
- **converse of p → q**: the conditional statement q → p
- **contrapositive of p → q**: the conditional statement ¬q → ¬p
- **¬ p → ¬q**: the conditional statement ¬p → ¬q
- **p ↔ q (biconditional)**: the proposition “p if and only if q,” which is true if and only if p and q have the same truth value
- **bit**: either a 0 or a 1
- **Boolean variable**: a variable that has a value of 0 or 1
- **bit operation**: an operation on a bit or bits
- **bit string**: a list of bits
- **bitwise operations**: operations on bit strings that operate on each bit in one string and the corresponding bit in the other string
- **tautology**: a compound proposition that is always true
- **contradiction**: a compound proposition that is always false
- **contingency**: a compound proposition that is sometimes true and sometimes false
- **consistent compound propositions**: compound propositions for which there is an assignment of truth values to the variables that makes all these propositions true
- **logically equivalent compound propositions**: compound propositions that always have the same truth values
b) Describe the different ways to show that two compound propositions are logically equivalent.

c) Show in at least two different ways that the compound propositions \( \neg p \lor (r \rightarrow \neg q) \) and \( \neg p \lor \neg q \lor \neg r \) are equivalent.

5. (Depends on the Exercise Set in Section 1.2)

a) Given a truth table, explain how to use disjunctive normal form to construct a compound proposition with this truth table.

b) Explain why part (a) shows that the operators \( \land, \lor, \neg \) are functionally complete.

c) Is there an operator such that the set containing just this operator is functionally complete?

6. What are the universal and existential quantifications of a predicate \( P(x) \)? What are their negations?

7. a) What is the difference between the quantification \( \exists x \forall y P(x, y) \) and \( \forall y \exists x P(x, y) \), where \( P(x, y) \) is a predicate?

b) Give an example of a predicate \( P(x, y) \) such that \( \exists x \forall y P(x, y) \) and \( \forall y \exists x P(x, y) \) have different truth values.

8. Describe what is meant by a valid argument in propositional logic and show that the argument “If the earth is flat, then you can sail off the edge of the earth,” “You cannot sail off the edge of the earth,” therefore, “The earth is not flat” is a valid argument.

9. Use rules of inference to show that if the premises “All zebras have stripes” and “Mark is a zebra” are true, then the conclusion “Mark has stripes” is true.

10. a) Describe what is meant by a direct proof, a proof by contraposition, and a proof by contradiction of a conditional statement \( p \rightarrow q \).

b) Give a direct proof, a proof by contraposition and a proof by contradiction of the statement: “If \( n \) is even, then \( n + 4 \) is even.”

11. a) Describe a way to prove the biconditional \( p \leftrightarrow q \).

b) Prove the statement: “The integer \( 3n + 2 \) is odd if and only if the integer \( 9n + 5 \) is even, where \( n \) is an integer.”

12. To prove that the statements \( p_1, p_2, p_3, \) and \( p_4 \) are equivalent, is it sufficient to show that the conditional statements \( p_4 \rightarrow p_2, p_3 \rightarrow p_1, \) and \( p_1 \rightarrow p_2 \) are valid? If not, provide another set of conditional statements that can be used to show that the four statements are equivalent.

13. a) Suppose that a statement of the form \( \forall x P(x) \) is false. How can this be proved?

b) Show that the statement “For every positive integer \( n, n^2 \geq 2n \)” is false.

14. What is the difference between a constructive and nonconstructive existence proof? Give an example of each.

15. What are the elements of a proof that there is a unique element \( x \) such that \( P(x) \), where \( P(x) \) is a propositional function?

16. Explain how a proof by cases can be used to prove a result about absolute values, such as the fact that \( |xy| = |x||y| \) for all real numbers \( x \) and \( y \).

---

### Supplementary Exercises

1. Let \( p \) be the proposition “I will do every exercise in this book” and \( q \) be the proposition “I will get an “A” in this course.” Express each of these as a combination of \( p \) and \( q \).

a) I will get an “A” in this course only if I do every exercise in this book.

b) I will get an “A” in this course and I will do every exercise in this book.

c) Either I will not get an “A” in this course or I will not do every exercise in this book.

d) For me to get an “A” in this course it is necessary and sufficient that I do every exercise in this book.

2. Find the truth table of the compound proposition \( (p \lor q) \rightarrow (p \land \neg r) \).

3. Show that these compound propositions are tautologies.

a) \( (\neg q \land (p \rightarrow q)) \rightarrow \neg p \)

b) \( ((p \lor q) \land \neg p) \rightarrow q \)

4. Give the converse, the contrapositive, and the inverse of these conditional statements.

a) If it rains today, then I will drive to work.

b) If \( |x| = x \), then \( x \geq 0 \).

c) If \( n \) is greater than 3, then \( n^2 \) is greater than 9.

5. Given a conditional statement \( p \rightarrow q \), find the converse of its inverse, the converse of its converse, and the converse of its contrapositive.

6. Given a conditional statement \( p \rightarrow q \), find the inverse of its inverse, the inverse of its converse, and the inverse of its contrapositive.

7. Find a compound proposition involving the propositional variables \( p, q, r, \) and \( s \) that is true when exactly three of these propositional variables are true and is false otherwise.

8. Show that these statements are inconsistent: “If Sergei takes the job offer then he will get a signing bonus.” “If Sergei takes the job offer, then he will receive a higher salary.” “If Sergei gets a signing bonus, then he will not receive a higher salary.” “Sergei takes the job offer.”

9. Show that these statements are inconsistent: “If Miranda does not take a course in discrete mathematics, then she will not graduate.” “If Miranda does not graduate, then she is not qualified for the job.” “If Miranda reads this book, then she is qualified for the job.” “Miranda does not take a course in discrete mathematics but she reads this book.”
10. Suppose that you meet three people, A, B, and C, on the island of knights and knaves described in Example 18 in Section 1.1. What are A, B, and C if A says “I am a knave and B is a knight” and B says “Exactly one of the three of us is a knight”?

11. (Adapted from [Sm78]) Suppose that on an island there are three types of people, knights, knaves, and normals. Knights always tell the truth, knaves always lie, and normals sometimes lie and sometimes tell the truth. Detectives questioned three inhabitants of the island—Amy, Brenda, and Claire—as part of the investigation of a crime. The detectives knew that one of the three committed the crime, but not which one. They also knew that the criminal was a knight, and that the other two were not. Additionally, the detectives recorded these statements: Amy: “I am innocent.” Brenda: “What Amy says is true.” Claire: “Brenda is not a normal.” After analyzing their information, the detectives positively identified the guilty party. Who was it?

12. Show that if \( S \) is a proposition, where \( S \) is the conditional statement “If \( S \) is true, then unicorns live,” then “Unicorns live” is true. Show that it follows that \( S \) cannot be a proposition. (This paradox is known as Löb’s paradox.)

13. Show that the argument with premises “The tooth fairy is a real person” and “The truth fairy is not a real person” and conclusion “You can find gold at the end of the rainbow” is a valid argument. Does this show that the conclusion is true?

14. Let \( P(x) \) be the statement “student \( x \) knows calculus” and let \( Q(y) \) be the statement “class \( y \) contains a student who knows calculus.” Express each of these as quantifications of \( P(x) \) and \( Q(y) \).
   a) Some students know calculus.
   b) Not every student knows calculus.
   c) Every class has a student in it who knows calculus.
   d) Every student in every class knows calculus.
   e) There is at least one class with no students who know calculus.

15. Let \( P(m, n) \) be the statement “\( m \) divides \( n \),” where the domain for both variables consists of all positive integers. (By “\( m \) divides \( n \)” we mean that \( n = km \) for some integer \( k \).) Determine the truth values of each of these statements.
   a) \( P(4, 5) \)
   b) \( P(2, 4) \)
   c) \( \forall m \forall n P(m, n) \)
   d) \( \exists m \forall n P(m, n) \)
   e) \( \exists n \forall m P(m, n) \)
   f) \( \forall n P(1, n) \)

16. Find a domain for the quantifiers in \( \exists x \exists y (x \neq y \land \forall z ((z \neq x) \land (z \neq y)) \) such that this statement is true.
   17. Find a domain for the quantifiers in \( \exists x \exists y (x \neq y \land \forall z ((z = x) \lor (z = y)) \) such that this statement is false.

18. Use existential and universal quantifiers to express the statement “No one has more than three grandmothers” using the propositional function \( G(x, y) \), which represents “\( x \) is the grandmother of \( y \).

19. Use existential and universal quantifiers to express the statement “Everyone has exactly two biological parents” using the propositional function \( P(x, y) \), which represents “\( x \) is the biological parent of \( y \).

20. The quantifier \( \exists_n \) denotes “there exists exactly \( n \)” so that \( \exists_n P(x) \) means there exist exactly \( n \) values in the domain such that \( P(x) \) is true. Determine the true value of these statement where the domain consists of all real numbers.
   a) \( \exists_0 x (x^2 = -1) \)
   b) \( \exists_1 x (|x| = 0) \)
   c) \( \exists_2 x (x^2 = 2) \)
   d) \( \exists_3 x (x = |x|) \)

21. Express each of these statements using existential and universal quantifiers and propositional logic where \( \exists_n \) is defined in Exercise 20.
   a) \( \exists_0 P(x) \)
   b) \( \exists_1 P(x) \)
   c) \( \exists_2 P(x) \)
   d) \( \exists_3 P(x) \)

22. Let \( P(x, y) \) be a propositional function. Show that \( \exists x \forall y P(x, y) \rightarrow \forall y \exists x P(x, y) \) is a tautology.

23. Let \( P(x) \) and \( Q(x) \) be propositional functions. Show that \( \exists x (P(x) \rightarrow Q(x)) \) and \( \forall x P(x) \rightarrow \exists x Q(x) \) always have the same truth value.

24. If \( \forall y \exists x P(x, y) \) is true, does it necessarily follow that \( \exists x \forall y P(x, y) \) is true?

25. If \( \forall x \exists y P(x, y) \) is true, does it necessarily follow that \( \exists y \forall x P(x, y) \) is true?

26. Find the negations of these statements.
   a) If it snows today, then I will go skiing tomorrow.
   b) Every person in this class understands mathematical induction.
   c) Some students in this class do not like discrete mathematics.
   d) In every mathematics class there is some student who falls asleep during lectures.

27. Express this statement using quantifiers: “Every student in this class takes some course in every department in the school of mathematical sciences.”

28. Express this statement using quantifiers: “There is a building on the campus of some college in the United States in which every room is painted white.”

29. Express the statement “There is exactly one student in this class who has taken exactly one mathematics class at this school” using the uniqueness quantifier. Then express this statement using quantifiers, without using the uniqueness quantifier.

30. Describe a rule of inference that can be used to prove that there are exactly two elements \( x \) and \( y \) in a domain such that \( P(x) \) and \( P(y) \) are true. Express this rule of inference as a statement in English.

31. Use rules of inference to show that if the premises \( \forall x (P(x) \rightarrow Q(x)) \), \( \forall x (Q(x) \rightarrow R(x)) \), and \( \neg R(a) \), where \( a \) is in the domain, are true, then the conclusion \( \neg P(a) \) is true.
32. Prove that if $x^3$ is irrational, then $x$ is irrational.
33. Prove that if $x$ is irrational and $x \geq 0$, then $\sqrt{x}$ is irrational.
34. Prove that given a nonnegative integer $n$, there is a unique nonnegative integer $m$ such that $m^2 \leq n < (m + 1)^2$.
35. Prove that there exists an integer $m$ such that $m^2 > 10^{1000}$. Is your proof constructive or nonconstructive?
36. Prove that there is a positive integer that can be written as the sum of squares of positive integers in two different ways. (Use a computer or calculator to speed up your work.)

Computer Projects

Write programs with the specified input and output.

1. Given the truth values of the propositions $p$ and $q$, find the truth values of the conjunction, disjunction, exclusive or, conditional statement, and biconditional of these propositions.
2. Given two bit strings of length $n$, find the bitwise AND, bitwise OR, and bitwise XOR of these strings.
3. Given the truth values of the propositions $p$ and $q$ in fuzzy logic, find the truth value of the disjunction and the conjunction of $p$ and $q$ (see Exercises 40 and 41 of Section 1.1).
*4. Given positive integers $m$ and $n$, interactively play the game of Chomp.
*5. Given a portion of a checkerboard, look for tilings of this checkerboard with various types of polyominoes, including dominoes, the two types of triominoes, and larger polyominoes.

Computations and Explorations

Use a computational program or programs you have written to do these exercises.

1. Look for positive integers that are not the sum of the cubes of nine different positive integers.
2. Look for positive integers greater than 79 that are not the sum of the fourth powers of 18 positive integers.
3. Find as many positive integers as you can that can be written as the sum of cubes of positive integers, in two different ways, sharing this property with 1729.
*4. Try to find winning strategies for the game of Chomp for different initial configurations of cookies.
*5. Look for tilings of checkerboards and parts of checkerboards with polyominoes.

Writing Projects

Respond to these with essays using outside sources.

1. Discuss logical paradoxes, including the paradox of Epimenides the Cretan, Jourdain's card paradox, and the barber paradox, and how they are resolved.
2. Describe how fuzzy logic is being applied to practical applications. Consult one or more of the recent books on fuzzy logic written for general audiences.
3. Describe the basic rules of WFF'N PROOF, The Game of Modern Logic, developed by Layman Allen. Give examples of some of the games included in WFF'N PROOF.
4. Read some of the writings of Lewis Carroll on symbolic logic. Describe in detail some of the models he used to represent logical arguments and the rules of inference he used in these arguments.
5. Extend the discussion of Prolog given in Section 1.3, explaining in more depth how Prolog employs resolution.
6. Discuss some of the techniques used in computational logic, including Skolem's rule.
7. “Automated theorem proving” is the task of using computers to mechanically prove theorems. Discuss the goals...
Example 29 illustrates that the factorial function grows extremely rapidly as \( n \) grows. The rapid growth of the factorial function is made clearer by Stirling's formula, a result from higher mathematics that tell us that \( n! \sim \sqrt{2\pi n}(n/e)^n \). Here, we have used the notation \( f(n) \sim g(n) \), which means that the ratio \( f(n)/g(n) \) approaches 1 as \( n \) grows without bound (that is, \( \lim_{n \to \infty} f(n)/g(n) = 1 \)). The symbol \( \sim \) is read "is asymptotic to." Stirling's formula is named after James Stirling, a Scottish mathematician of the eighteenth century.

**Exercises**

1. Why is \( f \) not a function from \( \mathbb{R} \) to \( \mathbb{R} \) if
   a) \( f(x) = 1/x \)?
   b) \( f(x) = \sqrt{x} \)?
   c) \( f(x) = \pm \sqrt{x^2 + 1} \)?

2. Determine whether \( f \) is a function from \( \mathbb{Z} \) to \( \mathbb{R} \) if
   a) \( f(n) = \pm n \).
   b) \( f(n) = \sqrt{n^2 + 1} \).
   c) \( f(n) = 1/(n^2 - 4) \).

3. Determine whether \( f \) is a function from the set of all bit strings to the set of integers if
   a) \( f(S) \) is the position of a 0 bit in \( S \).
   b) \( f(S) \) is the number of 1 bits in \( S \).
   c) \( f(S) \) is the smallest integer \( i \) such that the \( i \)th bit of \( S \) is 1 and \( f(S) = 0 \) when \( S \) is the empty string, the string with no bits.

4. Find the domain and range of these functions. Note that in each case, to find the domain, determine the set of elements assigned values by the function.
   a) the function that assigns to each nonnegative integer its last digit
   b) the function that assigns the next largest integer to a positive integer
   c) the function that assigns to a bit string the number of one bits in the string
   d) the function that assigns to a bit string the number of bits in the string

5. Find the domain and range of these functions. Note that in each case, to find the domain, determine the set of elements assigned values by the function.
   a) the function that assigns to each bit string the number of ones minus the number of zeros in that string
   b) the function that assigns to each bit string twice the number of zeros in that string
   c) the function that assigns the number of bits left over when a bit string is split into bytes (which are blocks of 8 bits)
   d) the function that assigns to each positive integer the largest perfect square not exceeding this integer

6. Find the domain and range of these functions.
   a) the function that assigns to each pair of positive integers the first integer of the pair
   b) the function that assigns to each positive integer its largest decimal digit
   c) the function that assigns to a bit string the number of ones minus the number of zeros in the string
   d) the function that assigns to each positive integer the largest integer not exceeding the square root of the integer
   e) the function that assigns to a bit string the longest string of ones in the string

7. Find the domain and range of these functions.
   a) the function that assigns to each pair of positive integers the maximum of these two integers
   b) the function that assigns to each positive integer the number of the digits 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 that do not appear as decimal digits of the integer
   c) the function that assigns to a bit string the number of times the block 11 appears
   d) the function that assigns to a bit string the numerical position of the first 1 in the string and that assigns the value 0 to a bit string consisting of all 0s

8. Find these values.
   a) \([1.1] \)
   b) \([-0.1]\)
   c) \([2.99]\)
   d) \([-2.99]\)
   e) \([0.5 + 0.5, 2]\)
   f) \([0.5 + 0.5, 0.5]\)

9. Find these values.
   a) \([0.5, 0.5]\)
   b) \([7, 7]\)
   c) \([-3.1]\)
   d) \([-3.1]\)
   e) \([3]\)
   f) \([-1]\)
   g) \([0.5 + 0.5, 0.5]\)
   h) \([0.5 + 0.5, 0.5]\)

10. Determine whether each of these functions from \([a, b, c, d]\) to itself is one-to-one.
    a) \( f(a) = b, f(b) = c, f(c) = d, f(d) = a \)
    b) \( f(a) = b, f(b) = c, f(c) = d, f(d) = c \)
    c) \( f(a) = a, f(b) = b, f(c) = c, f(d) = d \)

11. Which functions in Exercise 10 are onto?

12. Determine whether each of these functions from \( \mathbb{Z} \) to \( \mathbb{Z} \) is one-to-one.
    a) \( f(n) = n - 1 \)
    b) \( f(n) = n^2 + 1 \)
    c) \( f(n) = n^3 \)
    d) \( f(n) = [n/2] \)

13. Which functions in Exercise 12 are onto?

14. Determine whether \( f: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \) is onto if
    a) \( f(m, n) = 2m - n \)
    b) \( f(m, n) = m^2 - n^2 \).
c) \( f(m, n) = m + n + 1 \).

d) \( f(m, n) = |m| - |n| \).

e) \( f(m, n) = m^2 - 4 \).

15. Determine whether the function \( f: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z} \) is onto if
   a) \( f(m, n) = m + n \).
   b) \( f(m, n) = m^2 + n^2 \).
   c) \( f(m, n) = m \).
   d) \( f(m, n) = |n| \).
   e) \( f(m, n) = m - n \).

16. Give an example of a function from \( \mathbb{N} \) to \( \mathbb{N} \) that is
   a) one-to-one but not onto.
   b) onto but not one-to-one.
   c) both onto and one-to-one (but different from the identity function).
   d) neither one-to-one nor onto.

17. Give an explicit formula for a function from the set of integers to the set of positive integers that is
   a) one-to-one, but not onto.
   b) onto, but not one-to-one.
   c) one-to-one and onto.
   d) neither one-to-one nor onto.

18. Determine whether each of these functions is a bijection from \( \mathbb{R} \) to \( \mathbb{R} \).
   a) \( f(x) = -3x + 4 \).
   b) \( f(x) = -3x^2 + 7 \).
   c) \( f(x) = (x + 1)/(x + 2) \).
   d) \( f(x) = x^5 + 1 \).

19. Determine whether each of these functions is a bijection from \( \mathbb{R} \) to \( \mathbb{R} \).
   a) \( f(x) = 2x + 1 \).
   b) \( f(x) = x^2 + 1 \).
   c) \( f(x) = x^3 \).
   d) \( f(x) = (x^2 + 1)/(x^2 + 2) \).

20. Let \( f: \mathbb{R} \rightarrow \mathbb{R} \) and let \( f(x) > 0 \) for all \( x \in \mathbb{R} \). Show that \( f(x) \) is strictly increasing if and only if the function \( g(x) = 1/f(x) \) is strictly decreasing.

21. Let \( f: \mathbb{R} \rightarrow \mathbb{R} \) and let \( f(x) > 0 \). Show that \( f(x) \) is strictly increasing if and only if the function \( g(x) = 1/f(x) \) is strictly increasing.

22. Give an example of an increasing function with the set of real numbers as its domain and codomain that is not one-to-one.

23. Give an example of a decreasing function with the set of real numbers as its domain and codomain that is not one-to-one.

24. Show that the function \( f(x) = e^x \) from the set of real number to the set of real numbers is not invertible, but if the codomain is restricted to the set of positive real numbers, the resulting function is invertible.

25. Show that the function \( f(x) = |x| \) from the set of real numbers to the set of nonnegative real numbers is not invertible, but if the domain is restricted to the set of nonnegative real numbers, the resulting function is invertible.

26. Let \( S = \{-1, 0, 2, 4, 7\} \). Find \( f(S) \) if
   a) \( f(x) = 1 \).
   b) \( f(x) = 2x + 1 \).
   c) \( f(x) = [x/5] \).
   d) \( f(x) = [(x^2 + 1)/3] \).

27. Let \( f(x) = [x^2/3] \). Find \( f(S) \) if
   a) \( S = \{-2, -1, 0, 1, 2, 3\} \).
   b) \( S = \{0, 1, 2, 3, 4, 5\} \).
   c) \( S = \{1, 5, 7, 11\} \).
   d) \( S = \{2, 6, 10, 14\} \).

28. Let \( f(x) = 2x \). What is
   a) \( f(\mathbb{Z}) \)?
   b) \( f(\mathbb{N}) \)?
   c) \( f(\mathbb{R}) \)?

29. Suppose that \( g \) is a function from \( A \) to \( B \) and \( f \) is a function from \( B \) to \( C \).
   a) Show that if both \( f \) and \( g \) are one-to-one functions, then \( f \circ g \) is also one-to-one.
   b) Show that if both \( f \) and \( g \) are onto functions, then \( f \circ g \) is also onto.

30. If \( f \) and \( f \circ g \) are one-to-one, does it follow that \( g \) is one-to-one? Justify your answer.

31. If \( f \) and \( f \circ g \) are onto, does it follow that \( g \) is onto? Justify your answer.

32. Find \( f \circ g \) and \( g \circ f \), where \( f(x) = x^2 + 1 \) and \( g(x) = x + 2 \), are functions from \( \mathbb{R} \) to \( \mathbb{R} \).

33. Find \( f + g \) and \( fg \) for the functions \( f \) and \( g \) given in Exercise 32.

34. Let \( f(x) = ax + b \) and \( g(x) = cx + d \), where \( a, b, c, \) and \( d \) are constants. Determine for which constants \( a, b, c, \) and \( d \) it is true that \( f \circ g = g \circ f \).

35. Show that the function \( f(x) = ax + b \) from \( \mathbb{R} \) to \( \mathbb{R} \) is invertible, where \( a \) and \( b \) are constants, with \( a \neq 0 \), and find the inverse of \( f \).

36. Let \( f \) be a function from the set \( A \) to the set \( B \). Let \( S \) and \( T \) be subsets of \( A \). Show that
   a) \( f(S \cup T) = f(S) \cup f(T) \).
   b) \( f(S \cap T) \subseteq f(S) \cap f(T) \).

37. Give an example to show that the inclusion in part (b) in Exercise 36 may be proper.

Let \( f \) be a function from the set \( A \) to the set \( B \). Let \( S \) be a subset of \( B \). We define the inverse image of \( S \) to be the subset of \( A \) whose elements are precisely all pre-images of all elements of \( S \). We denote the inverse image of \( S \) by \( f^{-1}(S) \), so \( f^{-1}(S) = \{a \in A \mid f(a) \in S\} \). (Beware: The notation \( f^{-1} \) is used in two different ways. Do not confuse the notation introduced here with the notation \( f^{-1}(x) \) for the value at \( y \) of the inverse of the invertible function \( f \). Notice also that \( f^{-1}(S) \), the inverse image of the set \( S \), makes sense for all functions \( f \), not just invertible functions.)

38. Let \( f \) be the function from \( \mathbb{R} \) to \( \mathbb{R} \) defined by \( f(x) = x^2 \). Find
   a) \( f^{-1}([1]) \).
   b) \( f^{-1}((0 < x < 1)) \).
   c) \( f^{-1}((x > 4)) \).

39. Let \( g(x) = |x| \). Find
   a) \( g^{-1}([-1]) \).
   b) \( g^{-1}([-1, 0, 1]) \).
   c) \( g^{-1}([0 < x < 1]) \).
40. Let \( f \) be a function from \( A \) to \( B \). Let \( S \) and \( T \) be subsets of \( B \). Show that
   \[ f^{-1}(S \cup T) = f^{-1}(S) \cup f^{-1}(T). \]
   \[ f^{-1}(S \cap T) = f^{-1}(S) \cap f^{-1}(T). \]

41. Let \( f \) be a function from \( A \) to \( B \). Let \( S \) be a subset of \( B \). Show that
   \[ f^{-1}(\overline{S}) = \overline{f^{-1}(S)}. \]

42. Show that \( \lfloor x + \frac{1}{2} \rfloor \) is the closest integer to the number \( x \), except when \( x \) is midway between two integers, when it is the larger of these two integers.

43. Show that \( \lfloor x - \frac{1}{2} \rfloor \) is the closest integer to the number \( x \), except when \( x \) is midway between two integers, when it is the smaller of these two integers.

44. Show that if \( x \) is a real number, then \( \lfloor x \rfloor - \lfloor x \rfloor = 1 \) if \( x \) is not an integer and \( \lfloor x \rfloor - \lfloor x \rfloor = 0 \) if \( x \) is an integer.

45. Show that if \( x \) is a real number, then \( x - 1 < \lfloor x \rfloor \leq x \leq x + 1 \).

46. Show that if \( x \) is a real number and \( m \) is an integer, then
   \( \lfloor x + m \rfloor = \lfloor x \rfloor + m \).

47. Show that if \( x \) is a real number and \( n \) is an integer, then
   \( a) \ x < n \) if and only if \( \lfloor x \rfloor < n \).
   \( b) \ n < x \) if and only if \( n < \lfloor x \rfloor \).

48. Show that if \( x \) is a real number and \( n \) is an integer, then
   \( a) \ x \leq n \) if and only if \( \lfloor x \rfloor \leq n \).
   \( b) \ n \leq x \) if and only if \( n \leq \lfloor x \rfloor \).

49. Prove that if \( n \) is an integer, then \( \lfloor n/2 \rfloor = n/2 \) if \( n \) is even and \( (n-1)/2 \) if \( n \) is odd.

50. Prove that if \( x \) is a real number, then \( \lceil -x \rceil = -\lfloor x \rfloor \) and \( \lfloor -x \rfloor = -\lceil x \rceil \).

51. The function INT is found on some calculators, where INT\( (x) = \lfloor x \rfloor \) when \( x \) is a nonnegative real number and \( \text{INT}(x) = \lfloor x \rfloor \) when \( x \) is a negative real number. Show that this INT function satisfies the identity \( \text{INT}(-x) = -\text{INT}(x) \).

52. Let \( a \) and \( b \) be real numbers with \( a < b \). Use the floor and/or ceiling functions to express the number of integers \( n \) that satisfy the inequality \( a \leq n \leq b \).

53. Let \( a \) and \( b \) be real numbers with \( a < b \). Use the floor and/or ceiling functions to express the number of integers \( n \) that satisfy the inequality \( a < n < b \).

54. How many bytes are required to encode \( n \) bits of data where \( n \) equals
   \( a) \ 4? \)
   \( b) \ 10? \)
   \( c) \ 500? \)
   \( d) \ 3000? \)

55. How many bytes are required to encode \( n \) bits of data where \( n \) equals
   \( a) \ 7? \)
   \( b) \ 17? \)
   \( c) \ 1001? \)
   \( d) \ 28,800? \)

56. How many ATM cells (described in Example 26) can be transmitted in 10 seconds over a link operating at the following rates?
   \( a) \ 128 \) kilobits per second (1 kilobit = 1000 bits)
   \( b) \ 300 \) kilobits per second
   \( c) \ 1 \) megabit per second (1 megabit = 1,000,000 bits)

57. Data are transmitted over a particular Ethernet network in blocks of 1500 octets (blocks of 8 bits). How many blocks are required to transmit the following amounts of data over this Ethernet network? (Note that a byte is a synonym for an octet, a kilobyte is 1000 bytes, and a megabyte is 1,000,000 bytes.)
   \( a) \ 150 \) kilobytes of data
   \( b) \ 384 \) kilobytes of data
   \( c) \ 1.544 \) megabytes of data
   \( d) \ 45.3 \) megabytes of data

58. Draw the graph of the function \( f(n) = 1 - n^2 \) from \( \mathbb{Z} \) to \( \mathbb{Z} \).

59. Draw the graph of the function \( f(x) = \lfloor 2x \rfloor \) from \( \mathbb{R} \) to \( \mathbb{R} \).

60. Draw the graph of the function \( f(x) = \lfloor x/2 \rfloor \) from \( \mathbb{R} \) to \( \mathbb{R} \).

61. Draw the graph of the function \( f(x) = \lfloor x \rfloor + \lfloor x/2 \rfloor \) from \( \mathbb{R} \) to \( \mathbb{R} \).

62. Draw the graph of the function \( f(x) = \lfloor x \rfloor + \lfloor x/2 \rfloor \) from \( \mathbb{R} \) to \( \mathbb{R} \).

63. Draw graphs of each of these functions.
   \( a) \ f(x) = \lfloor x + \frac{1}{2} \rfloor \)
   \( b) \ f(x) = \lfloor 2x + 1 \rfloor \)
   \( c) \ f(x) = \lfloor x/3 \rfloor \)
   \( d) \ f(x) = \lfloor 1/x \rfloor \)
   \( e) \ f(x) = \lfloor x - 2 \rfloor + \lfloor x + 2 \rfloor \)
   \( f) \ f(x) = \lfloor 2x \rfloor \lfloor x/2 \rfloor \)
   \( g) \ f(x) = \lfloor x - \frac{1}{2} \rfloor + \frac{1}{2} \)

64. Draw graphs of each of these functions.
   \( a) \ f(x) = \lfloor 3x - 2 \rfloor \)
   \( b) \ f(x) = \lfloor 0.2x \rfloor \)
   \( c) \ f(x) = \lfloor -1/x \rfloor \)
   \( d) \ f(x) = \lfloor x^2 \rfloor \)
   \( e) \ f(x) = \lfloor x/2 \rfloor \lfloor x/2 \rfloor \)
   \( f) \ f(x) = \lfloor x/2 \rfloor + \lfloor x/2 \rfloor \)
   \( g) \ f(x) = \lfloor 2 \lfloor x/2 \rfloor + \frac{1}{2} \rfloor \)

65. Find the inverse function of \( f(x) = x^3 + 1 \).

66. Suppose that \( f \) is an invertible function from \( Y \) to \( Z \) and \( g \) is an invertible function from \( X \) to \( Y \). Show that the inverse of the composition \( f \circ g \) is given by \( (f \circ g)^{-1} = g^{-1} \circ f^{-1} \).

67. Let \( S \) be a subset of a universal set \( U \). The characteristic function \( f_S \) of \( S \) is the function from \( U \) to the set \( \{0, 1\} \) such that \( f_S(x) = 1 \) if \( x \) belongs to \( S \) and \( f_S(x) = 0 \) if \( x \) does not belong to \( S \). Let \( A \) and \( B \) be sets. Show that for all \( x \),
   \[ f_{A \cup B}(x) = f_A(x) \cdot f_B(x) \]
   \[ f_{A \cup B}(x) = f_A(x) + f_B(x) - f_A(x) \cdot f_B(x) \]
   \[ f_{A}(x) = 1 - f_A(x) \]
   \[ f_{A\oplus B}(x) = f_A(x) + f_B(x) - 2f_A(x)f_B(x) \]

68. Suppose that \( f \) is a function from \( A \) to \( B \), where \( A \) and \( B \) are finite sets with \( |A| = |B| \). Show that \( f \) is one-to-one if and only if it is onto.

69. Prove or disprove each of these statements about the floor and ceiling functions.
   \( a) \ \lfloor x \rfloor = \lfloor x \rfloor \) for all real numbers \( x \).
   \( b) \ \lfloor 2x \rfloor = 2\lfloor x \rfloor \) whenever \( x \) is a real number.
   \( c) \ \lfloor x \rfloor + \lfloor y \rfloor = \lfloor x + y \rfloor \) or \( 1 \) whenever \( x \) and \( y \) are real numbers.
d) \([xy] = [x][y]\) for all real numbers \(x\) and \(y\).
e) \(\left\lceil \frac{x}{2} \rightceil = \left\lceil \frac{x + 1}{2} \right\rceil\) for all real numbers \(x\).

70. Prove or disprove each of these statements about the floor and ceiling functions.
   a) \([x]\) \(=\) \([x]\) for all real numbers \(x\).
   b) \([x + y]\) \(=\) \([x]\) + \([y]\) for all real numbers \(x\) and \(y\).
   c) \([\lfloor x/2 \rfloor/2]\) \(=\) \([x/4]\) for all real numbers \(x\).
   d) \([\sqrt{x}]\) \(=\) \([\sqrt{x}]\) for all positive real numbers \(x\).
   e) \([x] + [y] + [x + y] \leq [2x] + [2y]\) for all real numbers \(x\) and \(y\).

71. Prove that if \(x\) is a positive real number, then
   a) \([\sqrt{x}]\) \(=\) \([\sqrt{x}]\).
   b) \([\sqrt{x}]\) \(=\) \([\sqrt{x}]\).

72. Let \(x\) be a real number. Show that \([3x]\) \(=\) \([x]\) + \([x + \frac{1}{3}]\) + \([x + \frac{2}{3}]\).

A program designed to evaluate a function may not produce the correct value of the function for all elements in the domain of this function. For example, a program may not produce a correct value because evaluating the function may lead to an infinite loop or an overflow. Similarly, in abstract mathematics, we often want to discuss functions that are defined only for a subset of the real numbers, such as \(1/\sqrt{x}\), \(\sqrt{x}\), and \(\arcsin(x)\).

Also, we may want to use such notions as the "youngest child" function, which is undefined for a couple having no children, or the "time of sunrise," which is undefined for some days above the Arctic Circle.

To study such situations, we use the concept of a partial function. A partial function \(f\) from a set \(A\) to a set \(B\) is an assignment to each element \(a\) in a subset of \(A\), called the domain of definition of \(f\), of a unique element \(b\) in \(B\). The sets \(A\) and \(B\) are called the domain and codomain of \(f\), respectively. We say that \(f\) is undefined for elements in \(A\) that are not in the domain of definition of \(f\). We write \(f: A \rightarrow B\) to denote that \(f\) is a partial function from \(A\) to \(B\). (This is the same notation as is used for functions. The context in which the notation is used determines whether \(f\) is a partial function or a total function.) When the domain of definition of \(f\) equals \(A\), we say that \(f\) is a total function.

73. For each of these partial functions, determine its domain, codomain, domain of definition, and the set of values for which it is undefined. Also, determine whether it is a total function.
   a) \(f: \mathbb{Z} \rightarrow \mathbb{R}\), \(f(n) = 1/n\)
   b) \(f: \mathbb{Z} \rightarrow \mathbb{Z}\), \(f(n) = [n/2]\)
   c) \(f: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Q}\), \(f(m, n) = m/n\)
   d) \(f: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}\), \(f(m, n) = mn\)
   e) \(f: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}\), \(f(m, n) = m - n\) if \(m > n\)

74. a) Show that a partial function from \(A\) to \(B\) can be viewed as a function \(f^*\) from \(A\) to \(B \cup \{u\}\), where \(u\) is not an element of \(B\) and

\[ f^*(a) = \begin{cases} f(a) & \text{if } a \text{ belongs to the domain of definition of } f \\ u & \text{if } f \text{ is undefined at } a. \end{cases} \]

b) Using the construction in (a), find the function \(f^*\) corresponding to each partial function in Exercise 73.

75. a) Show that if a set \(S\) has cardinality \(m\), where \(m\) is a positive integer, then there is a one-to-one correspondence between \(S\) and the set \([1, 2, \ldots, m]\).
   b) Show that if \(S\) and \(T\) are two sets each with \(m\) elements, where \(m\) is a positive integer, then there is a one-to-one correspondence between \(S\) and \(T\).

*76. Show that a set \(S\) is infinite if and only if there is a proper subset \(A\) of \(S\) such that there is a one-to-one correspondence between \(A\) and \(S\).

*77. Show that the polynomial function \(f: \mathbb{Z}^+ \times \mathbb{Z}^+ \rightarrow \mathbb{Z}^+\) with \(f(m, n) = (m + n - 2)(m + n - 1)/2 + m\) is one-to-one and onto.

*78. Show that when you substitute \((3n + 1)^2\) for each occurrence of \(n\) and \((3m + 1)^2\) for each occurrence of \(m\) in the right-hand side of the formula for the function \(f(m, n)\) in Exercise 77, you obtain a one-to-one polynomial function \(\mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}\). It is an open question whether there is a one-to-one polynomial function \(\mathbb{Q} \times \mathbb{Q} \rightarrow \mathbb{Q}\).

2.4 Sequences and Summations

Introduction

Sequences are ordered lists of elements. Sequences are used in discrete mathematics in many ways. They can be used to represent solutions to certain counting problems, as we will see in Chapter 7. They are also an important data structure in computer science. This section contains a review of the notation used to represent sequences and sums of terms of sequences.

When the elements of an infinite set can be listed, the set is called countable. We will conclude this section with a discussion of both countable and uncountable sets. We will prove that the set of rational numbers is countable, but the set of real numbers is not.
Review Questions

1. Explain what it means for one set to be a subset of another set. How do you prove that one set is a subset of another set?
2. What is the empty set? Show that the empty set is a subset of every set.
3. a) Define $|S|$, the cardinality of the set $S$.
   b) Give a formula for $|A \cup B|$, where $A$ and $B$ are sets.
4. a) Define the power set of a set $S$.
   b) When is the empty set in the power set of a set $S$?
   c) How many elements does the power set of a set $S$ with $n$ elements have?
5. a) Define the union, intersection, difference, and symmetric difference of two sets.
   b) What are the union, intersection, difference, and symmetric difference of the set of positive integers and the set of odd integers?
6. a) Explain what it means for two sets to be equal.
   b) Describe as many of the ways as you can to show that two sets are equal.
   c) Show in at least two different ways that the sets $A - (B \cap C)$ and $(A - B) \cup (A - C)$ are equal.
7. Explain the relationship between logical equivalences and set identities.
8. a) Define the domain, codomain, and the range of a function.
   b) Let $f(n)$ be the function from the set of integers to the set of integers such that $f(n) = n^2 + 1$. What are the domain, codomain, and range of this function?
9. a) Define what it means for a function from the set of positive integers to the set of positive integers to be one-to-one.
   b) Define what it means for a function from the set of positive integers to the set of positive integers to be onto.
   c) Give an example of a function from the set of positive integers to the set of positive integers that is both one-to-one and onto.
   d) Give an example of a function from the set of positive integers to the set of positive integers that is one-to-one but not onto.
   e) Give an example of a function from the set of positive integers to the set of positive integers that is not one-to-one but is onto.
   f) Give an example of a function from the set of positive integers to the set of positive integers that is neither one-to-one nor onto.
10. a) Define the inverse of a function.
    b) When does a function have an inverse?
    c) Does the function $f(n) = 10 - n$ from the set of integers to the set of integers have an inverse? If so, what is it?
11. a) Define the floor and ceiling functions from the set of real numbers to the set of integers.
    b) For which real numbers $x$ is it true that $\lfloor x \rfloor = \lceil x \rceil$?
12. Conjecture a formula for the terms of the sequence that begins 8, 14, 32, 86, 248 and find the next three terms of your sequence.
13. What is the sum of the terms of the geometric progression $a + ar + \ldots + ar^n$ when $r \neq 1$?
14. Show that the set of odd integers is countable.
15. Give an example of an uncountable set.

Supplementary Exercises

1. Let $A$ be the set of English words that contain the letter $x$, and let $B$ be the set of English words that contain the letter $q$. Express each of these sets as a combination of $A$ and $B$.
   a) The set of English words that do not contain the letter $x$.
   b) The set of English words that contain both an $x$ and a $q$.
   c) The set of English words that contain an $x$ but not a $q$.
   d) The set of English words that do not contain either an $x$ or a $q$.
   e) The set of English words that contain an $x$ or a $q$, but not both.
2. Show that if $A$ is a subset of $B$, then the power set of $A$ is a subset of the power set of $B$.
3. Suppose that $A$ and $B$ are sets such that the power set of $A$ is a subset of the power set of $B$. Does it follow that $A$ is a subset of $B$?
4. Let $E$ denote the set of even integers and $O$ denote the set of odd integers. As usual, let $Z$ denote the set of all integers. Determine each of these sets.
   a) $E \cup O$
   b) $E \cap O$
   c) $Z - E$
   d) $Z - O$
5. Show that if $A$ and $B$ are sets, then $A - (A - B) = A \cap B$.
6. Let $A$ and $B$ be sets. Show that $A \subseteq B$ if and only if $A \cap B = A$.
7. Let $A$, $B$, and $C$ be sets. Show that $(A - B) - C$ is not necessarily equal to $A - (B - C)$.
8. Suppose that $A$, $B$, and $C$ are sets. Prove or disprove that $(A - B) - C = (A - C) - B$.
9. Suppose that $A$, $B$, $C$, and $D$ are sets. Prove or disprove that $(A - B) - (C - D) = (A - C) - (B - D)$.
10. Show that if $A$ and $B$ are finite sets, then $|A \cap B| \leq |A \cup B|$. Determine when this relationship is an equality.
11. Let $A$ and $B$ be sets in a finite universal set $U$. List the following in order of increasing size.
   a) $|A|, |A \cup B|, |A \cap B|, |U|, |\emptyset|$
   b) $|A - B|, |A \oplus B|, |A| + |B|, |A \cup B|, |\emptyset|$

12. Let $A$ and $B$ be subsets of the finite universal set $U$. Show that $|\overline{A \cap B}| = |U| - |A| - |B| + |A \cap B|$.

13. Let $f$ and $g$ be functions from $\{1, 2, 3, 4\}$ to $\{a, b, c, d\}$ and from $\{a, b, c, d\}$ to $\{1, 2, 3, 4\}$, respectively, such that $f(1) = d$, $f(2) = c$, $f(3) = a$, and $f(4) = b$, and $g(a) = 2$, $g(b) = 1$, $g(c) = 3$, and $g(d) = 2$.
   a) Is $f$ one-to-one? Is $g$ one-to-one?
   b) Is $f$ onto? Is $g$ onto?
   c) Does either $f$ or $g$ have an inverse? If so, find this inverse.

14. Let $f$ be a one-to-one function from the set $A$ to the set $B$. Let $S$ and $T$ be subsets of $A$. Show that $f(S \cap T) = f(S) \cap f(T)$.

15. Give an example to show that the equality in Exercise 14 may not hold if $f$ is not one-to-one.

Suppose that $f$ is a function from $A$ to $B$. We define the function $S_f$ from $P(A)$ to $P(B)$ by the rule $S_f(X) = f(X)$ for each subset $X$ of $A$. Similarly, we define the function $S_{f^{-1}}$ from $P(B)$ to $P(A)$ by the rule $S_{f^{-1}}(Y) = f^{-1}(Y)$ for each subset $Y$ of $B$. Here, we are using Definition 4, and the definition of the inverse image of a set found in the preamble to Exercise 38, both in Section 2.3.

*16. a) Prove that if $f$ is a one-to-one function from $A$ to $B$, then $S_f$ is a one-to-one function from $P(A)$ to $P(B)$.
   b) Prove that if $f$ is an onto function from $A$ to $B$, then $S_f$ is an onto function from $P(A)$ to $P(B)$.
   c) Prove that if $f$ is an onto function from $A$ to $B$, then $S_{f^{-1}}$ is a one-to-one function from $P(B)$ to $P(A)$.
   d) Prove that if $f$ is a one-to-one function from $A$ to $B$, then $S_{f^{-1}}$ is an onto function from $P(B)$ to $P(A)$.
   e) Use parts (a) through (d) to conclude that if $f$ is a one-to-one correspondence from $A$ to $B$, then $S_f$ is a one-to-one correspondence from $P(A)$ to $P(B)$ and $S_{f^{-1}}$ is a one-to-one correspondence from $P(B)$ to $P(A)$.

17. Prove that if $f$ and $g$ are functions from $A$ to $B$ and $S_f = S_g$ (using the definition in the preamble to Exercise 16), then $f(x) = g(x)$ for all $x \in A$.

18. Show that if $n$ is an integer, then $n = \lfloor n/2 \rfloor + \lfloor n/2 \rfloor$.

19. For which real numbers $x$ and $y$ is it true that $[x + y] = [x] + [y]$?

20. For which real numbers $x$ and $y$ is it true that $\lceil x + y \rceil = \lceil x \rceil + \lceil y \rceil$?

21. For which real numbers $x$ and $y$ is it true that $\lfloor x + y \rfloor = \lfloor x \rfloor + \lfloor y \rfloor$?

22. Prove that $\lfloor n/2 \rfloor \lceil n/2 \rceil = \lfloor n^2/4 \rfloor$ for all integers $n$.

23. Prove that if $m$ is an integer, then $\lfloor x \rfloor + \lfloor m - x \rfloor = m - 1$, unless $x$ is an integer, in which case, it equals $m$.

24. Prove that if $x$ is a real number, then $\lfloor x/2 \rfloor = \lfloor x/4 \rfloor$.

25. Prove that if $n$ is an odd integer, then $\lfloor n^2/4 \rfloor = (n^2 + 3)/4$.

26. Prove that if $m$ and $n$ are positive integers and $x$ is a real number, then

$$\left\lfloor \frac{x + n}{m} \right\rfloor = \left\lfloor \frac{x}{m} + \frac{n}{m} \right\rfloor.$$

*27. Prove that if $m$ is a positive integer and $x$ is a real number, then

$$\lfloor mx \rfloor = \left\lfloor x + \frac{1}{m} \right\rfloor + \left\lfloor x + \frac{2}{m} \right\rfloor + \cdots + \left\lfloor x + \frac{m - 1}{m} \right\rfloor.$$

*28. We define the Ulam numbers by setting $u_1 = 1$ and $u_2 = 2$. Furthermore, after determining whether the integers less than $n$ are Ulam numbers, we set $n$ equal to the next Ulam number if it can be written uniquely as the sum of two different Ulam numbers. Note that $u_3 = 3$, $u_4 = 4$, $u_5 = 6$, and $u_6 = 8$.
   a) Find the first 20 Ulam numbers.
   b) Prove that there are infinitely many Ulam numbers.

29. Determine the value of $\prod_{k=1}^{100} \frac{k+1}{k}$. (The notation used here for products is defined in the preamble to Exercise 27 in Section 2.4.)

*30. Determine a rule for generating the terms of the sequence that begins $1, 3, 4, 8, 15, 27, 50, 92, \ldots$, and find the next four terms of the sequence.

*31. Determine a rule for generating the terms of the sequence that begins $2, 3, 3, 5, 10, 13, 39, 43, 172, 177, 885, 891, \ldots$, and find the next four terms of the sequence.

*32. Prove that if $A$ and $B$ are countable sets, then $A \times B$ is also a countable set.

**Computer Projects**

**Write programs with the specified input and output.**

1. Given subsets $A$ and $B$ of a set with $n$ elements, use bit strings to find $A', A \cup B, A \cap B, A - B$, and $A \oplus B$.

2. Given multisets $A$ and $B$ from the same universal set, find $A \cup B, A \cap B, A - B$, and $A + B$ (see preamble to Exercise 59 of Section 2.2).
### Exercises

In Exercises 1–14, to establish a big-\(O\) relationship, find witnesses \(C\) and \(k\) such that \(|f(x)| \leq C|g(x)|\) whenever \(x > k\).

1. Determine whether each of these functions is \(O(x)\).
   a) \(f(x) = 10\)  
   b) \(f(x) = 3x + 7\)  
   c) \(f(x) = x^2 + x + 1\)  
   d) \(f(x) = 5 \log x\)  
   e) \(f(x) = |x|\)  
   f) \(f(x) = |x/2|\)

2. Determine whether each of these functions is \(O(x^2)\).
   a) \(f(x) = 17x + 11\)  
   b) \(f(x) = x^2 + 1000\)  
   c) \(f(x) = x \log x\)  
   d) \(f(x) = x^4/2\)  
   e) \(f(x) = 2^x\)  
   f) \(f(x) = [x] \cdot [x]\)

3. Use the definition of “\(f(x) = O(g(x))\)” to show that \(x^4 + 9x^3 + 4x + 7\) is \(O(x^4)\).
4. Use the definition of “\(f(x) = O(g(x))\)” to show that \(2^x + 17\) is \(O(3^x)\).
5. Show that \((x^2 + 1)/(x + 1) = O(x)\).
6. Show that \((x^3 + 2x)/(2x + 1) = O(x^2)\).

7. Find the least integer \(n\) such that \(f(x) = O(x^n)\) for each of these functions.
   a) \(f(x) = 2x^2 + x^3 \log x\)  
   b) \(f(x) = 3x^3 + (\log x)^4\)  
   c) \(f(x) = (x^4 + x^2 + 1)/(x^3 + 1)\)  
   d) \(f(x) = (x^4 + 5 \log x)/(x^4 + 1)\)

8. Find the least integer \(n\) such that \(f(x) = O(x^n)\) for each of these functions.
   a) \(f(x) = 2x^2 + x^3 \log x\)  
   b) \(f(x) = 3x^3 + (\log x)^4\)  
   c) \(f(x) = (x^4 + x^2 + 1)/(x^3 + 1)\)  
   d) \(f(x) = (x^4 + 5 \log x)/(x^4 + 1)\)

9. Show that \(x^2 + 4x + 17\) is \(O(x^3)\) but that \(x^3\) is not \(O(x^2 + 4x + 17)\).
10. Show that \(x^3\) is \(O(x^4)\) but that \(x^4\) is not \(O(x^3)\).
11. Show that \(3x^4 + 1 = O(x^4/2)\) and \(x^4/2 = O(3x^4 + 1)\).
12. Show that \(x \log x = O(x^2)\) but that \(x^2\) is not \(O(x \log x)\).
13. Show that \(2^n = O(3^n)\) but that \(3^n\) is not \(O(2^n)\).
14. Is it true that \(x^3 = O(g(x))\) if \(g\) is the given function? [For example, if \(g(x) = x + 1\), this question asks whether \(x^3\) is \(O(x + 1)\).]
   a) \(g(x) = x^2\)  
   b) \(g(x) = x^3\)  
   c) \(g(x) = x^2 + x^3\)  
   d) \(g(x) = x^2 + x^4\)  
   e) \(g(x) = 3^x\)  
   f) \(g(x) = x^3/2\)

15. Explain what it means for a function to be \(O(1)\).
16. Show that if \(f(x) = O(x)\), then \(f(x) = O(x^2)\).
17. Suppose that \(f(x), g(x),\) and \(h(x)\) are functions such that \(f(x) = O(g(x))\) and \(g(x) = O(h(x))\). Show that \(f(x) = O(h(x))\).
18. Let \(k\) be a positive integer. Show that \(1^k + 2^k + \cdots + n^k\) is \(O(n^{k+1})\).
19. Give as good a big-\(O\) estimate as possible for each of these functions.
   a) \((n^2 + 8)(n + 1)\)  
   b) \((n \log n + n^2)(n^3 + 2)\)

20. Give a big-\(O\) estimate for each of these functions. For the function \(g\) in your estimate \(f(x) = O(g(x))\), use a simple function \(g\) of smallest order.
   a) \((n^3 + n^2 \log n)(\log n^3 + 1) + (17 \log n + 19)(n^3 + 2)\)  
   b) \((2^n + n^2)(n^3 + 3^n)\)  
   c) \((n^n + n^2 + 5^n)(n + 5^n)\)

21. Give a big-\(O\) estimate for each of these functions. For the function \(g\) in your estimate \(f(x) = O(g(x))\), use a simple function \(g\) of the smallest order.
   a) \(n \log(n^2 + 1) + n^2 \log n\)  
   b) \((n \log n + 1)^2 + (\log n + 1)(n^2 + 1)\)  
   c) \(n^2 + n^2\)

22. For each function in Exercise 1, determine whether that function is \(O(x)\) and whether it is \(\Omega(x)\).
23. For each function in Exercise 2, determine whether that function is \(O(x^2)\) and whether it is \(\Omega(x^2)\).
24. a) Show that \(3x + 7 = \Theta(x)\).
   b) Show that \(2x^2 + x - 7 = \Theta(x^2)\).
   c) Show that \([x + 1/2] = \Theta(x)\).
   d) Show that \(\log(x^2 + 1) = \Theta(\log_2 x)\).
   e) Show that \(\log_{10} x = \Theta(\log x)\).
25. Show that \(f(x) = \Theta(g(x))\) if and only if \(f(x) = O(g(x))\) and \(g(x) = O(f(x))\).
26. Show that if \(f(x)\) and \(g(x)\) are functions from the set of real numbers to the set of real numbers, then \(f(x) = O(g(x))\) if and only if \(g(x) = \Omega(f(x))\).
27. Show that if \(f(x)\) and \(g(x)\) are functions from the set of real numbers to the set of real numbers, then \(f(x) = \Theta(g(x))\) if and only if there are positive constants \(k, C_1,\) and \(C_2\) such that \(C_1 |g(x)| \leq |f(x)| \leq C_2 |g(x)|\) whenever \(x > k\).
28. a) Show that \(3x^2 + x + 1 = \Theta(3x^2)\) by directly finding the constants \(k, C_1,\) and \(C_2\) in Exercise 27.
   b) Express the relationship in part (a) using a picture showing the functions \(3x^2 + x + 1, C'_1 \cdot 3x^2,\) and \(C'_2 \cdot 3x^2\), and the constant \(k\) on the \(x\)-axis, where \(C'_1, C'_2,\) and \(k\) are the constants you found in part (a) to show that \(3x^2 + x + 1 = \Theta(3x^2)\).

29. Express the relationship \(f(x) = \Theta(g(x))\) using a picture. Show the graphs of the functions \(f(x), C'_1 |g(x)|,\) and \(C'_2 |g(x)|\), as well as the constant \(k\) on the \(x\)-axis.
30. Explain what it means for a function to be \(\Omega(1)\).
31. Explain what it means for a function to be \(\Theta(1)\).
32. Give a big-\(O\) estimate of the product of the first \(n\) odd positive integers.
33. Show that if \(f\) and \(g\) are real-valued functions such that \(f(x) = O(g(x))\), then for every positive integer \(k\), \(f^k(x) = O(g^k(x))\). [Note that \(f^k(x) = f(x)^k\).]
34. Show that for all real numbers \(a\) and \(b\) with \(a > 1\) and \(b > 1\), if \(f(x) = O(\log_a x)\), then \(f(x) = O(\log_a x)\).
35. Suppose that \( f(x) = O(g(x)) \) where \( f \) and \( g \) are increasing and unbounded functions. Show that \( \log |f(x)| \) is \( O(\log |g(x)|) \).

36. Suppose that \( f(x) = O(g(x)) \). Does it follow that \( 2f(x) = O(2g(x)) \)?

37. Let \( f_1(x) \) and \( f_2(x) \) be functions from the set of real numbers to the set of positive real numbers. Show that if \( f_1(x) \) and \( f_2(x) \) are both \( \Theta(g(x)) \), where \( g(x) \) is a function from the set of real numbers to the set of positive real numbers, then \( f_1(x) + f_2(x) = \Theta(g(x)) \). Is this still true if \( f_1(x) \) and \( f_2(x) \) can take negative values?

38. Suppose that \( f(x) \), \( g(x) \), and \( h(x) \) are functions such that \( f(x) = \Theta(g(x)) \) and \( g(x) = \Theta(h(x)) \). Show that \( f(x) \) is \( \Theta(h(x)) \).

39. If \( f_1(x) \) and \( f_2(x) \) are functions from the set of positive integers to the set of positive real numbers and \( f_1(x) \) and \( f_2(x) \) are both \( \Theta(g(x)) \), is \( f_1 - f_2(x) \) also \( \Theta(g(x)) \)? Either prove that it is or give a counterexample.

40. Show that if \( f_1(x) \) and \( f_2(x) \) are functions from the set of positive integers to the set of real numbers and \( f_1(x) = \Theta(g_1(x)) \) and \( f_2(x) = \Theta(g_2(x)) \), then \( f_1 + f_2(x) = \Theta(g_1 + g_2(x)) \).

41. Find functions \( f \) and \( g \) from the set of positive integers to the set of positive real numbers such that \( f(n) = n \) and \( g(n) = \Theta(n) \) and \( f(n) \) is not \( O(g(n)) \) and \( g(n) \) is not \( O(f(n)) \) simultaneously.

42. Express the relationship \( f(x) = \Omega(g(x)) \) using a picture. Show the graphs of the functions \( f(x) \) and \( Cg(x) \), as well as the constant \( k \) on the real axis.

43. Show that if \( f_1(x) = \Theta(g_1(x)) \), \( f_2(x) = \Theta(g_2(x)) \), and \( f_2(x) \neq 0 \) and \( g_2(x) \neq 0 \) for all real numbers \( x > 0 \), then \( (f_1/f_2)(x) = \Theta((g_1/g_2)(x)) \).

44. Show that if \( f(x) = a_0 x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \), where \( a_0, a_1, \ldots, a_{n-1}, \) and \( a_n \) are real numbers and \( a_n \neq 0 \), then \( f(x) = O(x^n) \).

Big-O, big-Theta, and big-Omega notation can be extended to functions in more than one variable. For example, the statement \( f(x, y) = \Theta(g(x, y)) \) means that there exist constants \( C, k_1, \) and \( k_2 \) such that \( |f(x, y)| \leq C |g(x, y)| \) whenever \( x > k_1 \) and \( y > k_2 \).

45. Define the statement \( f(x, y) = \Theta(g(x, y)) \).

46. Define the statement \( f(x, y) = \Omega(g(x, y)) \).

47. Show that \( (x^2 + xy + x \log y)^3 \) is \( O(x^6 y^3) \).

48. Show that \( x^5 y^3 + x^4 y^4 + x^3 y^5 \) is \( O(x^5 y^3) \).

49. Show that \( \lfloor xy \rfloor \) is \( O(xy) \).

50. Show that \( \lceil xy \rceil \) is \( \Omega(xy) \).

The following problems deal with another type of asymptotic notation, called little-o notation. Because little-o notation is based on the concept of limits, a knowledge of calculus is needed for these problems. We say that \( f(x) = o(g(x)) \) [read \( f(x) \) is "little-oh" of \( g(x) \)], when

\[
\lim_{x \to \infty} \frac{f(x)}{g(x)} = 0.
\]

51. (Requires calculus) Show that

a) \( x^2 \) is \( o(x^3) \).

b) \( x \log x \) is \( o(x^2) \).

c) \( x^2 \) is \( o(2^x) \).

d) \( x^2 + x + 1 \) is not \( o(x^2) \).

52. (Requires calculus)

a) Show that if \( f(x) \) and \( g(x) \) are functions such that \( f(x) = o(g(x)) \) and \( c \) is a constant, then \( cf(x) = o(g(x)) \), where \( (cf)(x) = cf(x) \).

b) Show that if \( f_1(x), f_2(x), \) and \( g(x) \) are functions such that \( f_1(x) = o(g(x)) \) and \( f_2(x) = o(g(x)) \), then \( (f_1 + f_2)(x) \) is \( o(g(x)) \), where \( (f_1 + f_2)(x) = f_1(x) + f_2(x) \).

53. (Requires calculus) Represent pictorially that \( x \log x \) is \( o(x^2) \) by graphing \( x \log x, x^2, \) and \( x \log x/x^2 \). Explain how this picture shows that \( x \log x \) is \( o(x^2) \).

54. (Requires calculus) Express the relationship \( f(x) = o(g(x)) \) using a picture. Show the graphs of \( f(x), g(x), \) and \( f(x)/g(x) \).

55. (Requires calculus) Suppose that \( f(x) = o(g(x)) \). Does it follow that \( 2f(x) = o(2g(x)) \)?

56. (Requires calculus) Suppose that \( f(x) = o(g(x)) \). Does it follow that \( \log |f(x)| = o(\log |g(x)|) \)?

57. (Requires calculus) The two parts of this exercise describe the relationship between little-o and big-O notation.

a) Show that if \( f(x) \) and \( g(x) \) are functions such that \( f(x) = o(g(x)) \), then \( f(x) = O(g(x)) \).

b) Show that if \( f(x) \) and \( g(x) \) are functions such that \( f(x) = O(g(x)) \), then it does not necessarily follow that \( f(x) = o(g(x)) \).

58. (Requires calculus) Show that if \( f(x) \) is a polynomial of degree \( n \) and \( g(x) \) is a polynomial of degree \( m \) where \( m > n \), then \( f(x) = O(g(x)) \).

59. (Requires calculus) Show that if \( f_1(x) = O(g(x)) \) and \( f_2(x) = o(g(x)) \), then \( f_1(x) + f_2(x) = O(g(x)) \).

60. (Requires calculus) Let \( H_n \) be the \( n \)th harmonic number

\[
H_n = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}.
\]

Show that \( H_n \) is \( O(\log n) \). [Hint: First establish the inequality

\[
\sum_{j=2}^{n} \frac{1}{j} < \int_1^{n} \frac{1}{x} \, dx
\]

by showing that the sum of the areas of the rectangles of height \( 1/j \) with base from \( j - 1 \) to \( j \), for \( j = 2, 3, \ldots, n \), is less than the area under the curve \( y = 1/x \) from 2 to \( n \).]

61. Show that \( n \log n = O(\log n!) \).

62. Determine whether \( \log n! \) is \( \Theta(n \log n) \). Justify your answer.

63. Show that \( \log n! \) is greater than \( (n \log n)/4 \) for \( n > 4 \). [Hint: Begin with the inequality \( n! > n(n - 1) \cdots (n - 2) \cdots [n/2] \).

Let \( f(x) \) and \( g(x) \) be functions from the set of real numbers to the set of real numbers. We say that the functions \( f \) and \( g \) are asymptotic and write \( f(x) \sim g(x) \) if \( \lim_{x \to \infty} f(x)/g(x) = 1 \).

64. (Requires calculus) For each of these pairs of functions, determine whether \( f \) and \( g \) are asymptotic.
3.3 Complexity of Algorithms

Introduction

When does an algorithm provide a satisfactory solution to a problem? First, it must always produce the correct answer. How this can be demonstrated will be discussed in Chapter 4. Second, it should be efficient. The efficiency of algorithms will be discussed in this section.

How can the efficiency of an algorithm be analyzed? One measure of efficiency is the time used by a computer to solve a problem using the algorithm, when input values are of a specified size. A second measure is the amount of computer memory required to implement the algorithm when input values are of a specified size.

Questions such as these involve the computational complexity of the algorithm. An analysis of the time required to solve a problem of a particular size involves the time complexity of the algorithm. An analysis of the computer memory required involves the space complexity of the algorithm. Considerations of the time and space complexity of an algorithm are essential when algorithms are implemented. It is obviously important to know whether an algorithm will produce an answer in a microsecond, a minute, or a billion years. Likewise, the required memory must be available to solve a problem, so that space complexity must be taken into account.

Considerations of space complexity are tied in with the particular data structures used to implement the algorithm. Because data structures are not dealt with in detail in this book, space complexity will not be considered. We will restrict our attention to time complexity.

Time Complexity

The time complexity of an algorithm can be expressed in terms of the number of operations used by the algorithm when the input has a particular size. The operations used to measure time complexity can be the comparison of integers, the addition of integers, the multiplication of integers, the division of integers, or any other basic operation.

Time complexity is described in terms of the number of operations required instead of actual computer time because of the difference in time needed for different computers to perform basic operations. Moreover, it is quite complicated to break all operations down to the basic bit operations that a computer uses. Furthermore, the fastest computers in existence can perform basic bit operations (for instance, adding, multiplying, comparing, or exchanging two bits) in \(10^{-9}\) second (1 nanosecond), but personal computers may require \(10^{-6}\) second (1 microsecond), which is 1000 times as long, to do the same operations.

We illustrate how to analyze the time complexity of an algorithm by considering Algorithm 1 of Section 3.1, which finds the maximum of a finite set of integers.

**Example 1** Describe the time complexity of Algorithm 1 of Section 3.1 for finding the maximum element in a set.

**Solution:** The number of comparisons will be used as the measure of the time complexity of the algorithm, because comparisons are the basic operations used.
required to solve this problem. But, if an algorithm requires 10 billion years to solve a problem, it would be unreasonable to use resources to implement this algorithm. One of the most interesting phenomena of modern technology is the tremendous increase in the speed and memory space of computers. Another important factor that decreases the time needed to solve problems on computers is **parallel processing**, which is the technique of performing sequences of operations simultaneously.

Efficient algorithms, including most algorithms with polynomial time complexity, benefit most from significant technology improvements. However, these technology improvements offer little help in overcoming the complexity of algorithms of exponential or factorial time complexity. Because of the increased speed of computation, increases in computer memory, and the use of algorithms that take advantage of parallel processing, many problems that were considered impossible to solve five years ago are now routinely solved, and certainly five years from now this statement will still be true.

### Exercises

1. How many comparisons are used by the algorithm given in Exercise 16 of Section 3.1 to find the smallest natural number in a sequence of \( n \) natural numbers?

2. Write the algorithm that puts the first four terms of a list of arbitrary length in increasing order. Show that this algorithm has time complexity \( O(1) \) in terms of the number of comparisons used.

3. Suppose that an element is known to be among the first four elements in a list of 32 elements. Would a linear search or a binary search locate this element more rapidly?

4. Determine the number of multiplications used to find \( x^{2^n} \) starting with \( x \) and successively squaring (to find \( x^2, x^4, \) and so on). Is this a more efficient way to find \( x^{2^n} \) than by multiplying \( x \) by itself the appropriate number of times?

5. Give a big-\( O \) estimate for the number of comparisons used by the algorithm that determines the number of 1s in a bit string \( S \) by examining each bit of the string to determine whether it is a 1 bit (see Exercise 25 of Section 3.1).

6. **a)** Show that this algorithm determines the number of 1 bits in the bit string \( S \):

   ```
   procedure bit count (S: bit string)
   count := 0
   while S \neq 0
   begin
   count := count + 1
   S := S \land (S - 1)
   end
   {count is the number of 1s in S}
   ```

   Here \( S - 1 \) is the bit string obtained by changing the rightmost 1 bit of \( S \) to a 0 and all the 0 bits to the right of this to 1s. [Recall that \( S \land (S - 1) \) is the bitwise **AND** of \( S \) and \( S - 1 \).]

   **b)** How many bitwise **AND** operations are needed to find the number of 1 bits in a string \( S \)?

7. The conventional algorithm for evaluating a polynomial \( a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \) at \( x = c \) can be expressed in pseudocode by

   ```
   procedure polynomial(c, a0, a1, \ldots, an: real numbers)
   power := 1
   y := a0
   for i := 1 to n
   begin
   power := power * c
   y := y + ai * power
   \}
   \{y = a_n c^n + a_{n-1} c^{n-1} + \cdots + a_1 c + a_0\}
   ```

   where the final value of \( y \) is the value of the polynomial at \( x = c \).

   **a)** Evaluate \( 3x^2 + x + 1 \) at \( x = 2 \) by working through each step of the algorithm showing the values assigned at each assignment step.

   **b)** Exactly how many multiplications and additions are used to evaluate a polynomial of degree \( n \) at \( x = c \)? (Do not count additions used to increment the loop variable.)

8. There is a more efficient algorithm (in terms of the number of multiplications and additions used) for evaluating polynomials than the conventional algorithm described in the previous exercise. It is called **Horner's method**. This pseudocode shows how to use this method to find the value of \( a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \) at \( x = c \).

   ```
   procedure Horner(c, a0, a1, a2, \ldots, an: real numbers)
   y := a0
   for i := 1 to n
   y := y + ai \ast c + ai
   \{y = a_n c^n + a_{n-1} c^{n-1} + \cdots + a_1 c + a_0\}
   ```

   **a)** Evaluate \( 3x^2 + x + 1 \) at \( x = 2 \) by working through each step of the algorithm showing the values assigned at each assignment step.

   **b)** Exactly how many multiplications and additions are used by this algorithm to evaluate a polynomial of degree \( n \) at \( x = c \)? (Do not count additions used to increment the loop variable.)

9. What is the largest \( n \) for which one can solve in one
10. How much time does an algorithm take to solve a problem of size \( n \) if this algorithm uses \( 2n^2 + 2^n \) bit operations, each requiring \( 10^{-9} \) second, with these values of \( n \)?
   a) 10    b) 20    c) 50    d) 100

11. How much time does an algorithm using \( 2^{50} \) bit operations need if each bit operation takes these amounts of time?
   a) \( 10^{-6} \) second    b) \( 10^{-9} \) second    c) \( 10^{-12} \) second

12. Determine the least number of comparisons, or best-case performance,
   a) required to find the maximum of a sequence of \( n \) integers, using Algorithm 1 of Section 3.1.
   b) used to locate an element in a list of \( n \) terms with a linear search.
   c) used to locate an element in a list of \( n \) terms using a binary search.

13. Analyze the average-case performance of the linear search algorithm, if exactly half the time element \( x \) is not in the list and if \( x \) is in the list it is equally likely to be in any position.

14. An algorithm is called **optimal** for the solution of a problem with respect to a specified operation if there is no algorithm for solving this problem using fewer operations.
   a) Show that Algorithm 1 in Section 3.1 is an optimal algorithm with respect to the number of comparisons of integers. (**Note:** Comparisons used for bookkeeping in the loop are not of concern here.)
   b) Is the linear search algorithm optimal with respect to the number of comparisons of integers (not including comparisons used for bookkeeping in the loop)?

15. Describe the worst-case time complexity, measured in terms of comparisons, of the ternary search algorithm described in Exercise 27 of Section 3.1.

16. Describe the worst-case time complexity, measured in terms of comparisons, of the search algorithm described in Exercise 28 of Section 3.1.

17. Analyze the worst-case time complexity of the algorithm you devised in Exercise 29 of Section 3.1 for locating a mode in a list of nondecreasing integers.

18. Analyze the worst-case time complexity of the algorithm you devised in Exercise 30 of Section 3.1 for locating all modes in a list of nondecreasing integers.

19. Analyze the worst-case time complexity of the algorithm you devised in Exercise 31 of Section 3.1 for finding the first term of a sequence of integers equal to some previous term.

20. Analyze the worst-case time complexity of the algorithm you devised in Exercise 32 of Section 3.1 for finding all terms of a sequence that are greater than the sum of all previous terms.

21. Analyze the worst-case time complexity of the algorithm you devised in Exercise 33 of Section 3.1 for finding the first term of a sequence less than the immediately preceding term.

22. Determine the worst-case complexity in terms of comparisons of the algorithm from Exercise 5 in Section 3.1 for determining whether a string is a palindrome.

23. Determine the worst-case complexity in terms of comparisons of the algorithm from Exercise 9 in Section 3.1 for determining whether a string is a palindrome.

24. How many comparisons does the selection sort (see preamble to Exercise 41 in Section 3.1) use to sort \( n \) items? Use your answer to give a big-O estimate of the complexity of the selection sort in terms of number of comparisons for the selection sort.

25. Find a big-O estimate for the worst-case complexity in terms of number of comparisons used and the number of terms swapped by the binary insertion sort described in the preamble to Exercise 47 in Section 3.1.

26. Show that the greedy algorithm for making change for \( n \) cents using quarters, dimes, nickels, and pennies has \( O(n) \) complexity measured in terms of comparisons needed.

27. Describe how the number of comparisons used in the worst case changes when these algorithms are used to search for an element of a list when the size of the list doubles from \( n \) to \( 2n \), where \( n \) is a positive integer.
   a) linear search
   b) binary search

28. Describe how the number of comparisons used in the worst case changes when the size of the list to be sorted doubles from \( n \) to \( 2n \), where \( n \) is a positive integer when these sorting algorithms are used.
   a) bubble sort
   b) insertion sort
   c) selection sort (described in the preamble to Exercise 41 in Section 3.1)
   d) binary insertion sort (described in the preamble to Exercise 47 in Section 3.1)

### 3.4 The Integers and Division

**Introduction**

The part of mathematics involving the integers and their properties belongs to the branch of mathematics called **number theory**. This section is the beginning of a four-section introduction
Now replace each of these numbers $p$ by $f(p) = (p + 3) \mod 26$. This gives

$$15 7 7 22 \quad 11 16 \quad 18 3 20 13.$$  

Translating this back to letters produces the encrypted message “PHHW BRX LQ WKH SDUN.”

To recover the original message from a secret message encrypted by the Caesar cipher, the function $f^{-1}$, the inverse of $f$, is used. Note that the function $f^{-1}$ sends an integer $p$ from $\{0, 1, 2, \ldots, 25\}$ to $f^{-1}(p) = (p - 3) \mod 26$. In other words, to find the original message, each letter is shifted back three letters in the alphabet, with the first three letters sent to the last three letters of the alphabet. The process of determining the original message from the encrypted message is called **decryption**.

There are various ways to generalize the Caesar cipher. For example, instead of shifting each letter by 3, we can shift each letter by $k$, so that

$$f(p) = (p + k) \mod 26.$$  

Such a cipher is called a **shift cipher**. Note that decryption can be carried out using

$$f^{-1}(p) = (p - k) \mod 26.$$  

Obviously, Caesar’s method and shift ciphers do not provide a high level of security. There are various ways to enhance this method. One approach that slightly enhances the security is to use a function of the form

$$f(p) = (ap + b) \mod 26,$$

where $a$ and $b$ are integers, chosen such that $f$ is a bijection. (Such a mapping is called an **affine transformation**.) This provides a number of possible encryption systems. The use of one of these systems is illustrated in Example 10.

**EXAMPLE 10** What letter replaces the letter $K$ when the function $f(p) = (7p + 3) \mod 26$ is used for encryption?

**Solution:** First, note that 10 represents $K$. Then, using the encryption function specified, it follows that $f(10) = (7 \cdot 10 + 3) \mod 26 = 21$. Because 21 represents $V$, $K$ is replaced by $V$ in the encrypted message.

Caesar’s encryption method, and the generalization of this method, proceed by replacing each letter of the alphabet by another letter in the alphabet. Encryption methods of this kind are vulnerable to attacks based on the frequency of occurrence of letters in the message. More sophisticated encryption methods are based on replacing blocks of letters with other blocks of letters. There are a number of techniques based on modular arithmetic for encrypting blocks of letters. A discussion of these can be found in the suggested readings listed at the end of the book.

**Exercises**

1. Does 17 divide each of these numbers?
   - a) 68
   - b) 84
   - c) 357
   - d) 1001
2. Show that if $a$ is an integer other than 0, then
   - a) $1$ divides $a$. 
   - b) $a$ divides 0.
3. Show that part (ii) of Theorem 1 is true.
4. Show that part (iii) of Theorem 1 is true.
5. Show that if $a \mid b$ and $b \mid a$, where $a$ and $b$ are integers, then $a = b$ or $a = -b$.
6. Show that if $a, b, c,$ and $d$ are integers such that $a \mid c$ and $b \mid d$, then $ab \mid cd$. 
7. Show that if \(a, b,\) and \(c\) are integers with \(c \neq 0,\) such that \(ac \mid bc,\) then \(a \mid b.\)

8. Prove or disprove that if \(a \mid bc,\) where \(a, b,\) and \(c\) are positive integers, then \(a \mid b\) or \(a \mid c.\)

9. What are the quotient and remainder when
   a) \(19\) is divided by \(?\)?
   b) \(-111\) is divided by \(11?\)
   c) \(789\) is divided by \(23?\)
   d) \(1001\) is divided by \(13?\)
   e) \(0\) is divided by \(19?\)
   f) \(3\) is divided by \(5?\)
   g) \(-1\) is divided by \(3?\)
   h) \(4\) is divided by \(1?\)

10. What are the quotient and remainder when
   a) \(44\) is divided by \(8?\)
   b) \(777\) is divided by \(21?\)
   c) \(-123\) is divided by \(19?\)
   d) \(-1\) is divided by \(23?\)
   e) \(-2002\) is divided by \(87?\)
   f) \(0\) is divided by \(17?\)
   g) \(1,234,567\) is divided by \(1001?\)
   h) \(-100\) is divided by \(101?\)

11. Let \(m\) be a positive integer. Show that \(a \equiv b \pmod{m}\) if \(a \mod m = b \mod m.\)

12. Let \(m\) be a positive integer. Show that \(a \mod m = b \mod m\) if \(a = b \pmod{m}.\)

13. Show that if \(n\) and \(k\) are positive integers, then \([n/k] = \lfloor(n-1)/k\rfloor + 1.\)

14. Show that if \(a\) is an integer and \(d\) is a positive integer greater than 1, then the quotient and remainder obtained when \(a\) is divided by \(d\) are \([a/d]\) and \(a-d[a/d]\), respectively.

15. Find a formula for the integer with smallest absolute value that is congruent to an integer \(a\) modulo \(m,\) where \(m\) is a positive integer.

16. Evaluate these quantities.
   a) \(-17 \mod 2\)
   b) \(144 \mod 7\)
   c) \(-101 \mod 13\)
   d) \(199 \mod 19\)

17. Evaluate these quantities.
   a) \(13 \mod 3\)
   b) \(-97 \mod 11\)
   c) \(155 \mod 19\)
   d) \(-221 \mod 23\)

18. List five integers that are congruent to 4 modulo 12.

19. Decide whether each of these integers is congruent to 5 modulo 17.
   a) \(80\)
   b) \(103\)
   c) \(-29\)
   d) \(-122\)

20. Show that if \(a \equiv b \pmod{m}\) and \(c \equiv d \pmod{m},\) where \(a, b, c, d,\) and \(m\) are integers with \(m \geq 2,\) then \(a - c \equiv b - d \pmod{m}.)\)

21. Show that if \(n \mid m,\) where \(n\) and \(m\) are positive integers greater than 1, and if \(a \equiv b \pmod{m},\) where \(a\) and \(b\) are integers, then \(a \equiv b \pmod{n.}\)

22. Show that if \(a, b, c,\) and \(m\) are integers such that \(m \geq 2,\)
   c > 0, and \(a \equiv b \pmod{m},\) then \(ac \equiv bc \pmod{mc).\)

23. Find counterexamples to each of these statements about congruences.
   a) If \(ac \equiv bc \pmod{m},\) where \(a, b, c,\) and \(m\) are integers with \(m \geq 2,\) then \(a \equiv b \pmod{m.}\)
   b) If \(a \equiv b \pmod{m}\) and \(c \equiv d \pmod{m},\) where \(a, b, c,\) and \(d,\) and \(m\) are integers with \(c\) and \(d\) positive and \(m \geq 2,\) then \(a^c \equiv b^d \pmod{m}.)\)

24. Prove that if \(n\) is an odd positive integer, then \(n^2 \equiv 1 \pmod{8).\)

25. Show that if \(a, b, k,\) and \(m\) are integers such that \(k \geq 1, m \geq 2,\) and \(a \equiv b \pmod{m},\) then \(a^k \equiv b^k \pmod{m}\)
   whenever \(k\) is a positive integer.

26. Which memory locations are assigned by the hashing function \(h(k) = k \mod 101\) to the records of insurance company customers with these Social Security numbers?
   a) 104578690
   b) 432222187
   c) 372201919
   d) 501338753

27. A parking lot has 31 visitor spaces, numbered from 0 to 30. Visitors are assigned parking spaces using the hashing function \(h(k) = k \mod 31,\) where \(k\) is the number formed from the first three digits on a visitor’s license plate.
   a) Which spaces are assigned by the hashing function to cars that have these first three digits on their license plates?
      317, 918, 007, 100, 111, 310
   b) Describe a procedure visitors should follow to find a free parking space, when the space they are assigned is occupied.

28. What sequence of pseudorandom numbers is generated using the linear congruential generator \(x_{n+1} = (4x_n + 1) \mod 7\) with seed \(x_0 = 3?\)

29. What sequence of pseudorandom numbers is generated using the pure multiplicative generator \(x_{n+1} = 3x_n \mod 11\) with seed \(x_0 = 2?\)

30. Write an algorithm in pseudocode for generating a sequence of pseudorandom numbers using a linear congruential generator.

31. Encrypt the message “DO NOT PASS GO” by translating the letters into numbers, applying the encryption function given, and then translating the numbers back into letters.
   a) \(f(p) = (p + 3) \mod 26\) (the Caesar cipher)
   b) \(f(p) = (p + 13) \mod 26\)
   c) \(f(p) = (3p + 7) \mod 26\)

32. Decrypt these messages encrypted using the Caesar cipher.
   a) EOXH MHDQV
   b) WHVW WRGDB
   c) HDW GLP VXP

All books are identified by an International Standard Book Number (ISBN), a 10-digit code \(x_1x_2\ldots x_{10}\) assigned by the publisher. (This system will change in 2007 when a new 13-digit code will be introduced.) These 10 digits consist of
blocks identifying the language, the publisher, the number assigned to the book by its publishing company, and finally, a 1-digit check digit that is either a digit or the letter X (used to represent 10). This check digit is selected so that \( \sum_{i=1}^{10} x_i \equiv 0 \pmod{11} \) and is used to detect errors in individual digits and transposition of digits.

33. The first nine digits of the ISBN of the European version of the fifth edition of this book are 0-07-119881. What is the check digit for that book?

34. The ISBN of the fifth edition of *Elementary Number Theory and Its Applications* is 0-32-123Q072, where \( Q \) is a digit. Find the value of \( Q \).

35. Determine whether the check digit of the ISBN for this textbook was computed correctly by the publisher.

### 3.5 Primes and Greatest Common Divisors

#### Introduction

In Section 3.4 we studied the concept of divisibility of integers. One important concept based on divisibility is that of a prime number. A prime is an integer greater than 1 that is divisible only by 1 and by itself. The study of prime numbers goes back to ancient times. Thousands of years ago it was known that there are infinitely many primes. Great mathematicians of the last 400 years have studied primes and have proved many important results about them. However, many old conjectures about primes remain unsettled. Primes have become essential in modern cryptographic systems.

An important theorem, the Fundamental Theorem of Arithmetic, asserts that every positive integer can be written uniquely as the product of prime numbers. The length of time required to factor large integers into their prime factors plays an important role in cryptography.

In this section we will also study the greatest common divisor of two integers, as well as the least common multiple of two integers. We will develop an algorithm for computing greatest common divisors in Section 3.6.

#### Primes

Every positive integer greater than 1 is divisible by at least two integers, because a positive integer is divisible by 1 and by itself. Positive integers that have exactly two different positive integer factors are called primes.

**DEFINITION 1**  
A positive integer \( p \) greater than 1 is called prime if the only positive factors of \( p \) are 1 and \( p \). A positive integer that is greater than 1 and is not prime is called composite.

**Remark:** The integer \( n \) is composite if and only if there exists an integer \( a \) such that \( a \mid n \) and \( 1 < a < n \).

**EXAMPLE 1**  
The integer 7 is prime because its only positive factors are 1 and 7, whereas the integer 9 is composite because it is divisible by 3.

The primes less than 100 are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, and 97. In Section 7.6 we introduce a procedure, known as the sieve of Eratosthenes, that can be used to find all the primes not exceeding an integer \( n \).

The primes are the building blocks of positive integers, as the Fundamental Theorem of Arithmetic shows. The proof will be given in Section 4.2.
DEFINITION 5  The least common multiple of the positive integers \(a\) and \(b\) is the smallest positive integer that is divisible by both \(a\) and \(b\). The least common multiple of \(a\) and \(b\) is denoted by \(\text{lcm}(a, b)\).

The least common multiple exists because the set of integers divisible by both \(a\) and \(b\) is nonempty, and every nonempty set of positive integers has a least element (by the well-ordering property, which will be discussed in Section 4.2). Suppose that the prime factorizations of \(a\) and \(b\) are as before. Then the least common multiple of \(a\) and \(b\) is given by

\[
\text{lcm}(a, b) = p_1^{\max(a_1, b_1)} p_2^{\max(a_2, b_2)} \cdots p_n^{\max(a_n, b_n)}
\]

where \(\max(x, y)\) denotes the maximum of the two numbers \(x\) and \(y\). This formula is valid because a common multiple of \(a\) and \(b\) has at least \(\max(a_i, b_i)\) factors of \(p_i\) in its prime factorization, and the least common multiple has no other prime factors besides those in \(a\) and \(b\).

EXAMPLE 15  What is the least common multiple of \(2^3 3^5 7^2\) and \(2^4 3^3\)?

Solution: We have

\[
\text{lcm}(2^3 3^5 7^2, 2^4 3^3) = 2^{\max(3, 4)} 3^{\max(5, 3)} 7^{\max(2, 0)} = 2^4 3^5 7^2.
\]

Theorem 5 gives the relationship between the greatest common divisor and least common multiple of two integers. It can be proved using the formulae we have derived for these quantities. The proof of this theorem is left as an exercise for the reader.

THEOREM 5  Let \(a\) and \(b\) be positive integers. Then

\[
ab = \gcd(a, b) \cdot \text{lcm}(a, b).
\]

Exercises

1. Determine whether each of these integers is prime.
   a) 21  b) 29  c) 71  d) 97  e) 111  f) 143
2. Determine whether each of these integers is prime.
   a) 19  b) 27  c) 93  d) 101  e) 107  f) 113
3. Find the prime factorization of each of these integers.
   a) 88  b) 126  c) 729  d) 1001  e) 1111  f) 909,090
4. Find the prime factorization of each of these integers.
   a) 39  b) 81  c) 101  d) 143  e) 289  f) 899
5. Find the prime factorization of 10!.
6. How many zeros are there at the end of 100!?
7. Show that \(\log_2 3\) is an irrational number. Recall that an irrational number is a real number \(x\) that cannot be written as the ratio of two integers.
8. Prove that for every positive integer \(n\), there are \(n\) consecutive composite integers. [Hint: Consider the \(n\) consecutive integers starting with \((n + 1)! + 2\).]
9. Prove or disprove that there are three consecutive odd positive integers that are primes, that is, odd primes of the form \(p, p + 2,\) and \(p + 4\).
10. Which positive integers less than 12 are relatively prime to 12?
11. Which positive integers less than 30 are relatively prime to 30?
12. Determine whether the integers in each of these sets are pairwise relatively prime.
   a) 21, 34, 55  b) 14, 17, 85  c) 25, 41, 49, 64  d) 17, 18, 19, 23
13. Determine whether the integers in each of these sets are pairwise relatively prime.
   a) 11, 15, 19
   b) 14, 15, 21
   c) 12, 17, 31, 37
   d) 7, 8, 9, 11

14. We call a positive integer perfect if it equals the sum of its positive divisors other than itself.
   a) Show that 6 and 28 are perfect.
   b) Show that \(2^{p-1}(2^p - 1)\) is a perfect number when \(2^p - 1\) is prime.

15. Show that if \(2^n - 1\) is prime, then \(n\) is prime. [Hint: Use the identity \(2^{ab} - 1 = (2^a - 1) \cdot (2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^a + 1)\).]

16. Determine whether each of these integers is prime, verifying some of Mersenne's claims.
   a) \(2^7 - 1\)
   b) \(2^9 - 1\)
   c) \(2^{11} - 1\)
   d) \(2^{13} - 1\)

The value of the Euler \(\phi\)-function at the positive integer \(n\) is defined to be the number of positive integers less than or equal to \(n\) that are relatively prime to \(n\). (Note: \(\phi\) is the Greek letter phi.)

17. Find
   a) \(\phi(4)\)
   b) \(\phi(10)\)
   c) \(\phi(13)\)

18. Show that \(n\) is prime if and only if \(\phi(n) = n - 1\).

19. What is the value of \(\phi(p^n)\) when \(p\) is prime and \(k\) is a positive integer?

20. What are the greatest common divisors of these pairs of integers?
   a) \(2^2 \cdot 3^2 \cdot 5^2, 2^5 \cdot 3^3 \cdot 5^2\)
   b) \(2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13, 2^{11} \cdot 3^9 \cdot 11 \cdot 17^{14}\)
   c) \(17, 17^{17}\)
   d) \(2^2 \cdot 7, 5^3 \cdot 13\)
   e) \(0, 5\)
   f) \(2 \cdot 3 \cdot 5 \cdot 7, 2 \cdot 3 \cdot 5 \cdot 7\)

21. What are the greatest common divisors of these pairs of integers?
   a) \(3^2 \cdot 5^3 \cdot 7^2, 2^{11} \cdot 3^5 \cdot 5^9\)
   b) \(11 \cdot 13 \cdot 17, 2^9 \cdot 3^7 \cdot 5^3 \cdot 7^3\)
   c) \(23^{31}, 23^{17}\)
   d) \(41 \cdot 43 \cdot 53, 41 \cdot 43 \cdot 53\)
   e) \(3^{13}, 5^{17}, 2^{12} \cdot 7^{21}\)
   f) \(1111, 0\)

22. What is the least common multiple of each pair in Exercise 20?

23. What is the least common multiple of each pair in Exercise 21?

24. Find \(\gcd(1000, 625)\) and \(\text{lcm}(1000, 625)\) and verify that \(\gcd(1000, 625) \cdot \text{lcm}(1000, 625) = 1000 \cdot 625\).

25. Find \(\gcd(92928, 123552)\) and \(\text{lcm}(92928, 123552)\), and verify that \(\gcd(92928, 123552) \cdot \text{lcm}(92928, 123552) = 92928 \cdot 123552\). [Hint: First find the prime factorizations of 92928 and 123552.]

26. If the product of two integers is \(2^7 \cdot 3^8 \cdot 5^2 \cdot 7^{11}\) and their greatest common divisor is \(2^3 \cdot 3^4 \cdot 5\), what is their least common multiple?

27. Show that if \(a\) and \(b\) are positive integers, then \(ab = \gcd(a, b) \cdot \text{lcm}(a, b)\). [Hint: Use the prime factorizations of \(a\) and \(b\) and the formulae for \(\gcd(a, b)\) and \(\text{lcm}(a, b)\) in terms of these factorizations.]

28. Find the smallest positive integer with exactly \(n\) different factors when \(n\) is
   a) 3
   b) 4
   c) 5
   d) 6
   e) 10

29. Can you find a formula or rule for the \(n\)th term of a sequence related to the prime numbers or prime factorizations so that the initial terms of the sequence have these values?
   a) \(0, 1, 1, 0, 1, 0, 1, 0, 1, 0, 1, \ldots\)
   b) \(1, 2, 3, 2, 5, 2, 7, 2, 3, 2, 11, 2, 13, 2, \ldots\)
   c) \(1, 2, 2, 3, 2, 4, 2, 4, 3, 2, 6, 2, 4, \ldots\)
   d) \(1, 1, 1, 0, 1, 1, 0, 1, 1, 0, 1, \ldots\)
   e) \(1, 2, 3, 3, 5, 7, 7, 7, 7, 11, 11, 13, 13, \ldots\)
   f) \(1, 2, 6, 30, 210, 2310, 30030, 510510, 96999690, 223092870, \ldots\)

30. Can you find a formula or rule for the \(n\)th term of a sequence related to the prime numbers or prime factorizations so that the initial terms of the sequence have these values?
   a) \(2, 2, 3, 5, 5, 7, 7, 11, 11, 11, 13, 13, \ldots\)
   b) \(0, 1, 2, 2, 3, 3, 4, 4, 4, 4, 5, 5, 6, 6, \ldots\)
   c) \(1, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 1, 0, 1, \ldots\)
   d) \(1, -1, -1, 0, -1, 1, -1, 0, 1, -1, 1, 0, \ldots\)
   e) \(1, 1, 1, 1, 0, 1, 1, 0, 1, 0, 0, 0, \ldots\)
   f) \(4, 9, 25, 49, 121, 169, 289, 361, 529, 841, 961, 1369, \ldots\)

31. Prove that the product of any three consecutive integers is divisible by 6.

32. Show that if \(a, b,\) and \(m\) are integers such that \(m \geq 2\) and \(a \equiv b \pmod{m}\), then \(\gcd(a, m) = \gcd(b, m)\).

33. Prove or disprove that \(n^2 - 79n + 1601\) is prime whenever \(n\) is a positive integer.

34. Prove or disprove that \(p_1, p_2, \ldots, p_n + 1\) is prime for every positive integer \(n\), where \(p_1, p_2, \ldots, p_n\) are the \(n\) smallest prime numbers.

35. Adapt the proof in the text that there are infinitely many primes to prove that there are infinitely many primes of the form \(4k + 3\), where \(k\) is a nonnegative integer. [Hint: Suppose that there are only finitely many such primes \(q_1, q_2, \ldots, q_n\), and consider the number \(4q_1q_2\cdots q_n - 1\).]

36. Prove that the set of positive rational numbers is countable by setting up a function that assigns to a rational number \(p/q\) with \(\gcd(p, q) = 1\) the base 11 number formed from the decimal representation of \(p\) followed by the base 11 digit \(A\), which corresponds to the decimal number 10, followed by the decimal representation of \(q\).

37. Prove that the set of positive rational numbers is countable by showing that the function \(K\) is a one-to-one correspondence between the set of positive rational numbers and the set of positive integers if \(K(m/n) = p_1^a_1 p_2^a_2 \cdots p_s^a_s q_1^{b_1 - 1} q_2^{b_2 - 1} \cdots q_t^{b_t - 1}\), where \(\gcd(m, n) = 1\) and the prime-power factorizations of \(m\) and \(n\) are \(m = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}\) and \(n = q_1^{b_1} q_2^{b_2} \cdots q_t^{b_t}\).
EXAMPLE 12  Find the greatest common divisor of 414 and 662 using the Euclidean algorithm.

Solution: Successive uses of the division algorithm give:

\[
\begin{align*}
662 &= 414 \cdot 1 + 248 \\
414 &= 248 \cdot 1 + 166 \\
248 &= 166 \cdot 1 + 82 \\
166 &= 82 \cdot 2 + 2 \\
82 &= 2 \cdot 41.
\end{align*}
\]

Hence, \( \gcd(414, 662) = 2 \), because 2 is the last nonzero remainder.

The Euclidean algorithm is expressed in pseudocode in Algorithm 6.

<table>
<thead>
<tr>
<th>ALGORITHM 6  The Euclidean Algorithm.</th>
</tr>
</thead>
<tbody>
<tr>
<td>procedure ( \gcd(a, b: \text{positive integers}) )</td>
</tr>
<tr>
<td>( x := a )</td>
</tr>
<tr>
<td>( y := b )</td>
</tr>
<tr>
<td>while ( y \neq 0 )</td>
</tr>
<tr>
<td>begin</td>
</tr>
<tr>
<td>( r := x \mod y )</td>
</tr>
<tr>
<td>( x := y )</td>
</tr>
<tr>
<td>( y := r )</td>
</tr>
<tr>
<td>end #(\gcd(a, b) \text{ is } x)</td>
</tr>
</tbody>
</table>

In Algorithm 6, the initial values of \( x \) and \( y \) are \( a \) and \( b \), respectively. At each stage of the procedure, \( x \) is replaced by \( y \), and \( y \) is replaced by \( x \mod y \), which is the remainder when \( x \) is divided by \( y \). This process is repeated as long as \( y \neq 0 \). The algorithm terminates when \( y = 0 \), and the value of \( x \) at that point, the last nonzero remainder in the procedure, is the greatest common divisor of \( a \) and \( b \).

We will study the time complexity of the Euclidean algorithm in Section 4.3, where we will show that the number of divisions required to find the greatest common divisor of \( a \) and \( b \), where \( a \geq b \), is \( O(\log b) \).

Exercises

1. Convert these integers from decimal notation to binary notation.
   a) 231  b) 4532  c) 97644
2. Convert these integers from decimal notation to binary notation.
   a) 321  b) 1023  c) 100632
3. Convert these integers from binary notation to decimal notation.
   a) 11111  b) 100000001
   c) 10101 0101  d) 110 1001 0001 0000
4. Convert these integers from binary notation to decimal notation.
   a) 11011  b) 101011 0101
   c) 111011 1110  d) 111 1100 0001 1111
5. Convert these integers from hexadecimal notation to binary notation.
   a) 80E  b) 135AB
   c) ABBA  d) DEFACE
6. Convert \((BADFACED)_{16}\) from its hexadecimal expansion to its binary expansion.
7. Convert \((ABCDEF)_{16}\) from its hexadecimal expansion to its binary expansion. 

8. Convert each of these integers from binary notation to hexadecimal notation. 
   a) \(1111\ 0111\)  
   b) \(1010\ 1010\ 1010\)  
   c) \(111\ 0111\ 0111\ 0111\)

9. Convert \((1011\ 0111\ 1011)_{2}\) from its binary expansion to its hexadecimal expansion. 

10. Convert \((1\ 000\ 0110\ 0011)_{2}\) from its binary expansion to its hexadecimal expansion. 

11. Show that the hexadecimal expansion of a positive integer can be obtained from its binary expansion by grouping together blocks of four binary digits, adding initial digits if necessary, and translating each block of four binary digits into a single hexadecimal digit. 

12. Show that the binary expansion of a positive integer can be obtained from its hexadecimal expansion by translating each hexadecimal digit into a block of four binary digits. 

13. Give a simple procedure for converting from the binary expansion of an integer to its octal expansion. 

14. Give a simple procedure for converting from the octal expansion of an integer to its binary expansion. 

15. Convert \((7345321)_{10}\) to its binary expansion and \((10\ 1011\ 1011)_{2}\) to its octal expansion. 

16. Give a procedure for converting from the hexadecimal expansion of an integer to its octal expansion using binary notation as an intermediate step. 

17. Give a procedure for converting from the octal expansion of an integer to its hexadecimal expansion using binary notation as an intermediate step. 

18. Convert \((12345670)_{8}\) to its hexadecimal expansion and \((ABB093BABA)_{16}\) to its octal expansion. 

19. Use Algorithm 5 to find \(7^{644} \mod 645\). 

20. Use Algorithm 5 to find \(11^{544} \mod 645\). 

21. Use Algorithm 5 to find \(3^{2003} \mod 99\). 

22. Use Algorithm 5 to find \(123^{1001} \mod 101\). 

23. Use the Euclidean algorithm to find 
   a) \(\gcd(12, 18)\)  
   b) \(\gcd(111, 201)\)  
   c) \(\gcd(1001, 1331)\)  
   d) \(\gcd(12345, 54321)\)  
   e) \(\gcd(1000, 5040)\)  
   f) \(\gcd(9888, 6060)\). 

24. Use the Euclidean algorithm to find 
   a) \(\gcd(1, 5)\)  
   b) \(\gcd(100, 101)\)  
   c) \(\gcd(123, 277)\)  
   d) \(\gcd(1529, 14039)\)  
   e) \(\gcd(1529, 14038)\)  
   f) \(\gcd(11111, 111111)\). 

25. How many divisions are required to find \(\gcd(21, 34)\) using the Euclidean algorithm? 

26. How many divisions are required to find \(\gcd(34, 55)\) using the Euclidean algorithm? 

27. Show that every positive integer can be represented uniquely as the sum of distinct powers of 2. [Hint: Consider binary expansions of integers.] 

28. It can be shown that every integer can be uniquely represented in the form 

\[ e_k 3^k + e_{k-1} 3^{k-1} + \cdots + e_1 3 + e_0, \]

where \(e_j = -1, 0, or 1\) for \(j = 0, 1, 2, \ldots, k\). Expansions of this type are called balanced ternary expansions. Find the balanced ternary expansions of 
   a) \(5\)  
   b) \(13\)  
   c) \(37\)  
   d) \(79\). 

29. Show that a positive integer is divisible by 3 if and only if the sum of its decimal digits is divisible by 3. 

30. Show that a positive integer is divisible by 11 if and only if the difference of the sum of its decimal digits in even-numbered positions and the sum of its decimal digits in odd-numbered positions is divisible by 11. 

31. Show that a positive integer is divisible by 3 if and only if the difference of the sum of its binary digits in even-numbered positions and the sum of its binary digits in odd-numbered positions is divisible by 3. 

One's complement representations of integers are used to simplify computer arithmetic. To represent positive and negative integers with absolute value less than \(2^n-1\), a total of \(n\) bits is used. The leftmost bit is used to represent the sign. A 0 bit in this position is used for positive integers, and a 1 bit in this position is used for negative integers. For positive integers, the remaining bits are identical to the binary expansion of the integer. For negative integers, the remaining bits are obtained by first finding the binary expansion of the absolute value of the integer, and then taking the complement of each of these bits, where the complement of a 1 is a 0 and the complement of a 0 is a 1. 

32. Find the one's complement representations, using bit strings of length six, of the following integers. 
   a) \(22\)  
   b) \(31\)  
   c) \(-7\)  
   d) \(-19\). 

33. What integer does each of the following one's complement representations of length five represent? 
   a) \(11001\)  
   b) \(01101\)  
   c) \(10001\)  
   d) \(11111\). 

34. If \(m\) is a positive integer less than \(2^n-1\), how is the one's complement representation of \(-m\) obtained from the one's complement of \(m\), when bit strings of length \(n\) are used? 

35. How is the one's complement representation of the sum of two integers obtained from the one's complement representations of these integers? 

36. How is the one's complement representation of the difference of two integers obtained from the one's complement representations of these integers? 

37. Show that the integer \(m\) with one's complement representation \((a_{n-1}a_{n-2} \ldots a_0a_0)\) can be found using the equation 

\[ m = -a_{n-1}(2^{n-1} - 1) + a_{n-2}2^{n-2} + \cdots + a_1 2 + a_0. \]

Two's complement representations of integers are also used to simplify computer arithmetic and are used more commonly than one's complement representations. To represent an integer \(x\) with \(-2^{n-1} \leq x \leq 2^{n-1} - 1\) for a specified positive integer \(n\), a total of \(n\) bits is used. The leftmost bit is used to represent the sign. A 0 bit in this position is used for positive
integers, and a 1 bit in this position is used for negative integers, just as in one's complement expansions. For a positive integer, the remaining bits are identical to the binary expansion of the integer. For a negative integer, the remaining bits are the bits of the binary expansion of $2^n - |x|$. Two's complement expansions of integers are often used by computers because addition and subtraction of integers can be performed easily using these expansions, where these integers can be either positive or negative.

38. Answer Exercise 32, but this time find the two's complement expansion using bit strings of length six.

39. Answer Exercise 33 if each expansion is a two's complement expansion of length five.

40. Answer Exercise 34 for two's complement expansions.

41. Answer Exercise 35 for two's complement expansions.

42. **Answer Exercise 36 for two's complement expansions.**

43. Show that the integer $m$ with two's complement representation $(a_{n-1}a_{n-2}...a_1a_0)$ can be found using the equation $m = -a_{n-1} \cdot 2^{n-1} + a_{n-2}2^{n-2} + ... + a_1 \cdot 2 + a_0$.

44. **Give a simple algorithm for forming the two's complement representation of an integer from its one's complement representation.**

45. Sometimes integers are encoded by using four-digit binary expansions to represent each decimal digit. This produces the **binary coded decimal** form of the integer. For instance, 791 is encoded in this way by 0111 1001 001. How many bits are required to represent a number with $n$ decimal digits using this type of encoding?

A **Cantor expansion** is a sum of the form

$$a_n n! + a_{n-1} (n-1)! + \cdots + a_2 2! + a_1!,$$

where $a_i$ is an integer with $0 \leq a_i \leq i$ for $i = 1, 2, \ldots, n$.

46. **Find the Cantor expansions of**

   a) 2.  
   b) 7.  
   c) 19.  
   d) 87.  
   e) 1000.  
   f) 1,000,000.

47. **Describe an algorithm that finds the Cantor expansion of an integer.**

48. **Describe an algorithm to add two integers from their Cantor expansions.**

49. **Add (10111)_2 and (11010)_2 by working through each step of the algorithm for addition given in the text.**

50. **Multiply (1110)_2 and (1010)_2 by working through each step of the algorithm for multiplication given in the text.**

51. **Describe an algorithm for finding the difference of two binary expansions.**

52. **Estimate the number of bit operations used to subtract two binary expansions.**

53. **Devise an algorithm that, given the binary expansions of the integers $a$ and $b$, determines whether $a > b$, $a = b$, or $a < b$.**

54. **How many bit operations does the comparison algorithm from Exercise 53 use when the larger of $a$ and $b$ has $n$ bits in its binary expansion?**

55. **Estimate the complexity of Algorithm 1 for finding the base $b$ expansion of an integer $n$ in terms of the number of divisions used.**

56. **Show that Algorithm 5 uses $O((\log m) \log b)$ bit operations to find $b^n \mod m$.**

57. **Show that Algorithm 4 uses $O(q \log a)$ bit operations, assuming that $a > d$.**

### 3.7 Applications of Number Theory

#### Introduction

Number theory has many applications, especially to computer science. In Section 3.4 we described several of these applications, including hashing functions, the generation of pseudorandom numbers, and shift ciphers. This section continues our introduction to number theory, developing some key results and presenting two important applications: a method for performing arithmetic with large integers and a recently invented type of cryptosystem, called a public key system. In such a cryptosystem, we do not have to keep encryption keys secret, because knowledge of an encryption key does not help someone decrypt messages in a realistic amount of time. Privately held decryption keys are used to decrypt messages.

Before developing these applications, we will introduce some key results that play a central role in number theory and its applications. For example, we will show how to solve systems of linear congruences modulo pairwise relatively prime integers using the Chinese Remainder Theorem, and then show how to use this result as a basis for performing arithmetic with large integers. We will introduce Fermat's Little Theorem and the concept of a pseudoprime and will show how to use these concepts to develop a public key cryptosystem.
finding a factorization of \( n \), or that does not also lead to the factorization of \( n \). Factorization is believed to be a difficult problem, as opposed to finding large primes \( p \) and \( q \), which can be done quickly. The most efficient factorization methods known (as of 2005) require billions of years to factor 400-digit integers. Consequently, when \( p \) and \( q \) are 200-digit primes, messages encrypted using \( n = pq \) as the modulus cannot be found in a reasonable time unless the primes \( p \) and \( q \) are known.

Active research is under way to find new ways to efficiently factor integers. Integers that were thought, as recently as several years ago, to be far too large to be factored in a reasonable amount of time can now be factored routinely. Integers with more than 100 digits, as well as some with more than 150 digits, have been factored using team efforts. When new factorization techniques are found, it will be necessary to use larger primes to ensure secrecy of messages. Unfortunately, messages that were considered secure earlier can be saved and subsequently decrypted by unintended recipients when it becomes feasible to factor the \( n = pq \) in the key used for RSA encryption.

The RSA method is now widely used. However, the most commonly used cryptosystems are private key cryptosystems. The use of public key cryptography, via the RSA system, is growing. However, there are applications that use both private key and public key systems. For example, a public key cryptosystem, such as RSA, can be used to distribute private keys to pairs of individuals when they wish to communicate. These people then use a private key system for encryption and decryption of messages.

### Exercises

1. Express the greatest common divisor of each of these pairs of integers as a linear combination of these integers.
   - a) 10, 11
   - b) 21, 44
   - c) 36, 48
   - d) 34, 55
   - e) 117, 213
   - f) 0, 223
   - g) 123, 2347
   - h) 3454, 4666
   - i) 9999, 11111

2. Express the greatest common divisor of each of these pairs of integers as a linear combination of these integers.
   - a) 9, 11
   - b) 33, 44
   - c) 35, 78
   - d) 21, 55
   - e) 101, 203
   - f) 124, 323
   - g) 2002, 2339
   - h) 3457, 4669
   - i) 10001, 13422

3. Show that 15 is an inverse of 7 modulo 26.
4. Show that 937 is an inverse of 13 modulo 2436.
6. Find an inverse of 2 modulo 17.
7. Find an inverse of 19 modulo 141.
8. Find an inverse of 144 modulo 233.

9. Show that if \( a \) and \( m \) are relatively prime positive integers, then the inverse of \( a \) modulo \( m \) is unique modulo \( m \). [Hint: Assume that there are two solutions \( b \) and \( c \) of the congruence \( ax \equiv 1 \pmod{m} \). Use Theorem 2 to show that \( b \equiv c \pmod{m} \).]
10. Show that an inverse of \( a \) modulo \( m \) does not exist if \( \gcd(a, m) > 1 \).
11. Solve the congruence \( 4x \equiv 5 \pmod{9} \).
12. Solve the congruence \( 2x \equiv 7 \pmod{17} \).

13. Show that if \( m \) is a positive integer greater than 1 and \( ac \equiv bc \pmod{m} \), then \( a \equiv b \pmod{m / \gcd(c, m)} \).

14. a) Show that the positive integers less than 11, except 1 and 10, can be split into pairs of integers such that each pair consists of integers that are inverses of each other modulo 11.
   b) Use part (a) to show that \( 10! \equiv -1 \pmod{11} \).
15. Show that if \( p \) is prime, the only solutions of \( x^2 \equiv 1 \pmod{p} \) are integers \( x \) such that \( x \equiv 1 \pmod{p} \) and \( x \equiv -1 \pmod{p} \).

16. a) Generalize the result in part (a) of Exercise 14; that is, show that if \( p \) is a prime, the positive integers less than \( p \), except 1 and \( p - 1 \), can be split into \( (p - 3)/2 \) pairs of integers such that each pair consists of integers that are inverses of each other. [Hint: Use the result of Exercise 15.]
   b) From part (a) conclude that \( (p - 1)! \equiv -1 \pmod{p} \) whenever \( p \) is prime. This result is known as Wilson's Theorem.
   c) What can we conclude if \( n \) is a positive integer such that \( (n - 1)! \not\equiv -1 \pmod{n} \)?

17. This exercise outlines a proof of Fermat's Little Theorem.
   a) Suppose that \( a \) is not divisible by the prime \( p \). Show that no two of the integers \( 1 \cdot a, 2 \cdot a, \ldots, (p - 1) \cdot a \) are congruent modulo \( p \).
   b) Conclude from part (a) that the product of \( 1, 2, \ldots, p - 1 \) is congruent modulo \( p \) to the product of \( a, 2a, \ldots, (p - 1)a \). Use this to show that
      \[
      (p - 1)! \equiv a^{p-1}(p - 1)! \pmod{p}.
      \]
c) Use Theorem 2 to show from part (b) that \( a^{p-1} \equiv 1 \mod p \) if \( p \nmid a \). [Hint: Use Lemma 2 to show that \( p \) does not divide \( (p - 1)! \) and then use Theorem 2. Alternatively, use Wilson's Theorem.]

d) Use part (c) to show that \( a^p \equiv a \mod p \) for all integers \( a \).

18. Find all solutions to the system of congruences.
\[
\begin{align*}
x & \equiv 2 \mod 3 \\
x & \equiv 1 \mod 4 \\
x & \equiv 3 \mod 5
\end{align*}
\]

19. Find all solutions to the system of congruences.
\[
\begin{align*}
x & \equiv 1 \mod 2 \\
x & \equiv 2 \mod 3 \\
x & \equiv 3 \mod 5 \\
x & \equiv 4 \mod 11
\end{align*}
\]

*20. Find all solutions, if any, to the system of congruences.
\[
\begin{align*}
x & \equiv 5 \mod 6 \\
x & \equiv 3 \mod 10 \\
x & \equiv 8 \mod 15
\end{align*}
\]

*21. Find all solutions, if any, to the system of congruences.
\[
\begin{align*}
x & \equiv 7 \mod 9 \\
x & \equiv 4 \mod 12 \\
x & \equiv 16 \mod 21
\end{align*}
\]

22. Use the Chinese Remainder Theorem to show that an integer \( a \), with \( 0 \leq a < m = m_1 m_2 \cdots m_n \), where the integers \( m_1, m_2, \ldots, m_n \) are pairwise relatively prime, can be represented uniquely by the \( n \)-tuple \((a \mod m_1, a \mod m_2, \ldots, a \mod m_n)\).

*23. Let \( m_1, m_2, \ldots, m_n \) be pairwise relatively prime integers greater than or equal to 2. Show that if \( a \equiv b \mod (m_i) \) for \( i = 1, 2, \ldots, n \), then \( a \equiv b \mod m \), where \( m = m_1 m_2 \cdots m_n \). (This result will be used in Exercise 24 to prove the Chinese remainder theorem. Consequently, do not use the Chinese remainder theorem to prove it.)

*24. Complete the proof of the Chinese Remainder Theorem by showing that the simultaneous solution of a system of linear congruences modulo pairwise relatively prime integers is unique modulo the product of these moduli. [Hint: Assume that \( x \) and \( y \) are two simultaneous solutions. Show that \( m_i | x - y \) for all \( i \). Using Exercise 23, conclude that \( m = m_1 m_2 \cdots m_n | x - y \).]

25. Which integers leave a remainder of 1 when divided by 2 and also leave a remainder of 1 when divided by 3?

26. Which integers are divisible by 5 but leave a remainder of 1 when divided by 3?

27. a) Show that \( 2^{340} \equiv 1 \mod 11 \) by Fermat's Little Theorem and noting that \( 2^{340} = (2^{10})^{34} \).

b) Show that \( 2^{340} \equiv 1 \mod 31 \) using the fact that \( 2^{340} = (2^5)^{68} = 32^{68} \).

c) Conclude from parts (a) and (b) that \( 2^{340} \equiv 1 \mod 341 \).

28. a) Use Fermat's Little Theorem to compute \( 3^{302} \mod 5 \), \( 3^{302} \mod 7 \), and \( 3^{302} \mod 11 \).

b) Use your results from part (a) and the Chinese Remainder Theorem to find \( 3^{302} \mod 385 \). (Note that \( 385 = 5 \cdot 7 \cdot 11 \).)

29. a) Use Fermat's Little Theorem to compute \( 5^{2003} \mod 7 \), \( 5^{2003} \mod 11 \), and \( 5^{2003} \mod 13 \).

b) Use your results from part (a) and the Chinese Remainder Theorem to find \( 5^{2003} \mod 1001 \). (Note that \( 1001 = 7 \cdot 11 \cdot 13 \).)

Let \( n \) be a positive integer and let \( n - 1 = 2^t s \), where \( s \) is a nonnegative integer and \( t \) is an odd positive integer. We say that \( n \) passes Miller's test for the base \( b \) if either \( b^{n-1} \equiv 1 \mod n \) or \( b^{2^j n-1} \equiv -1 \mod n \) for some \( j \) with \( 0 \leq j \leq s - 1 \). It can be shown (see [Ro05]) that a composite integer \( n \) passes Miller's test for fewer than \( n/4 \) bases \( b \) with \( 1 < b < n \).

*30. Show that if \( n \) is prime and \( b \) is a positive integer with \( n \nmid b \), then \( n \) passes Miller's test to the base \( b \).

31. Show that 2047 passes Miller's test to the base 2, but that it is composite. A composite positive integer \( n \) that passes Miller's test to the base \( b \) is called a strong pseudoprime to the base \( b \). It follows that 2047 is a strong pseudoprime to the base 2.

32. Show that 1729 is a Carmichael number.

33. Show that 2821 is a Carmichael number.

34. Show that if \( n = p_1 p_2 \cdots p_k \), where \( p_1, p_2, \ldots, p_k \) are distinct primes that satisfy \( p_j - 1 | n - 1 \) for \( j = 1, 2, \ldots, k \), then \( n \) is a Carmichael number.

35. a) Use Exercise 34 to show that every integer of the form \( (6m + 1)(12m + 1)(18m + 1) \), where \( m \) is a positive integer and \( 6m + 1, 12m + 1, \) and \( 18m + 1 \) are all primes, is a Carmichael number.

b) Use part (a) to show that 172,947,529 is a Carmichael number.

36. Find the nonnegative integer \( a \) less than 28 represented by each of these pairs, where each pair represents \((a \mod m, a \mod n)\).
\[
\begin{align*}
a & \equiv 0 \mod 4 \\
b & \equiv 1 \mod 7 \\
c & \equiv 1 \mod 11 \\
d & \equiv 2 \mod 3 \\
e & \equiv 2 \mod 5 \\
f & \equiv 0 \mod 3 \\
g & \equiv 2 \mod 3 \\
h & \equiv 3 \mod 5 \\
i & \equiv 3 \mod 6
\end{align*}
\]

37. Express each nonnegative integer \( a \) less than 15 using the pair \((a \mod 3, a \mod 5)\).

38. Explain how to use the pairs found in Exercise 37 to add 4 and 7.

39. Solve the system of congruences that arises in Example 8.

*40. Show that whenever \( a \) and \( b \) are both positive integers, then \( (2^a - 1) \mod (2^b - 1) = 2^{\gcd(a,b)} - 1 \).

**41. Use Exercise 40 to show that if \( a \) and \( b \) are positive integers, then \( \gcd(2^a - 1, 2^b - 1) = 2^\gcd(a,b) - 1 \). [Hint: Show that the remainders obtained when the Euclidean algorithm is used to compute \( \gcd(2^a - 1, 2^b - 1) \) are of the form \( 2^r - 1 \), where \( r \) is a remainder arising when the Euclidean algorithm is used to find \( \gcd(a, b) \).]

42. Use Exercise 41 to show that the integers \( 2^{35} - 1, 2^{34} - 1, 2^{33} - 1, 2^{31} - 1, 2^{29} - 1, \) and \( 2^{23} - 1 \) are pairwise relatively prime.

43. Show that if \( p \) is an odd prime, then every divisor of the...
Mersenne number $2^p - 1$ is of the form $2kp + 1$, where $k$ is a nonnegative integer. \[\text{[Hint: Use Fermat's Little Theorem and Exercise 41.]}\]

44. Use Exercise 43 to determine whether $M_{13} = 2^{13} - 1 = 8191$ and $M_{23} = 2^{23} - 1 = 8,388,607$ are prime.

*45. Show that we can easily factor $n$ when we know that $n$ is the product of two primes, $p$ and $q$, and we know the value of $(p - 1)(q - 1)$.

46. Encrypt the message ATTACK using the RSA system with $n = 43 \cdot 59$ and $e = 13$, translating each letter into integers and grouping together pairs of integers, as done in Example 11.

47. What is the original message encrypted using the RSA system with $n = 43 \cdot 59$ and $e = 13$ if the encrypted message is 0667 1947 0671? \[\text{(Note: Some computational aid is needed to do this in a realistic amount of time.)}\]

The extended Euclidean algorithm can be used to express \(\gcd(a, b)\) as a linear combination with integer coefficients of the integers $a$ and $b$. We set $s_0 = 1, s_1 = 0, t_0 = 0$, and $t_1 = 1$ and let $s_j = s_{j-2} - q_{j-1} s_{j-1}$ and $t_j = t_{j-2} - q_{j-1} t_{j-1}$ for $j = 2, 3, \ldots, n$, where the $q_j$ are the quotients in the divisions used when the Euclidean algorithm finds \(\gcd(a, b)\) (see page 228). It can be shown (see [Ro05]) that $\gcd(a, b) = s_n a + t_n b$.

48. Use the extended Euclidean algorithm to express $\gcd(252, 356)$ as a linear combination of 252 and 356.

49. Use the extended Euclidean algorithm to express $\gcd(144, 89)$ as a linear combination of 144 and 89.

50. Use the extended Euclidean algorithm to express $\gcd(1001, 100001)$ as a linear combination of 1001 and 100001.

51. Describe the extended Euclidean algorithm using pseudocode.

If $m$ is a positive integer, the integer $a$ is a quadratic residue of $m$ if $\gcd(a, m) = 1$ and the congruence $x^2 \equiv a \pmod{m}$ has a solution. In other words, a quadratic residue of $m$ is an integer relatively prime to $m$ that is a perfect square modulo $m$. For example, 2 is a quadratic residue of 7 because $\gcd(2, 7) = 1$ and $2^2 \equiv 4 \pmod{7}$ and 3 is a quadratic nonresidue of 7 because $\gcd(3, 7) = 1$ and $3^2 \equiv 9 \pmod{7}$ has no solution.

52. Which integers are quadratic residues of 11?

53. Show that if $p$ is an odd prime and $a$ is an integer not divisible by $p$, then the congruence $x^2 \equiv a \pmod{p}$ has either no solutions or exactly two incongruent solutions modulo $p$.

54. Show that if $p$ is an odd prime, then there are exactly $(p - 1)/2$ quadratic residues of $p$ among the integers $1, 2, \ldots, p - 1$.

If $p$ is an odd prime and $a$ is an integer not divisible by $p$, the Legendre symbol $\left(\frac{a}{p}\right)$ is defined to be 1 if $a$ is a quadratic residue of $p$ and $-1$ otherwise.

55. Show that if $p$ is an odd prime and $a$ and $b$ are integers with $a \equiv b \pmod{p}$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

56. Prove that if $p$ is an odd prime and $a$ is a positive integer not divisible by $p$, then $\left(\frac{a}{p}\right) = a^{(p-1)/2} \pmod{p}$.

57. Use Exercise 56 to show that if $p$ is an odd prime and $a$ and $b$ are integers not divisible by $p$, then $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$.

58. Show that if $p$ is an odd prime, then $-1$ is a quadratic residue of $p$ if $p \equiv 1 \pmod{4}$, and $-1$ is not a quadratic residue of $p$ if $p \equiv 3 \pmod{4}$. \[\text{[Hint: Use Exercise 56.]}\]

59. Find all solutions of the congruence $x^2 \equiv 29 \pmod{35}$. \[\text{[Hint: Find the solutions of this congruence modulo 5 and modulo 7, and then use the Chinese Remainder Theorem.]}\]

60. Find all solutions of the congruence $x^2 \equiv 16 \pmod{105}$. \[\text{[Hint: Find the solutions of this congruence modulo 3, modulo 5, and modulo 7, and then use the Chinese Remainder Theorem.]}\]

*61. Explain why it would not be suitable to use $p$, where $p$ is a large prime, as the modulus for encryption in the RSA cryptosystem. That is, explain how someone could, without excessive computation, find a private key from the corresponding public key if the modulus were a large prime, rather than the product of two large primes.

### 3.8 Matrices

**Introduction**

Matrices are used throughout discrete mathematics to express relationships between elements in sets. In subsequent chapters we will use matrices in a wide variety of models. For instance, matrices will be used in models of communications networks and transportation systems. Many algorithms will be developed that use these matrix models. This section reviews matrix arithmetic that will be used in these algorithms.
Supplementary Exercises

1. a) Describe an algorithm for locating the last occurrence of the largest number in a list of integers.
   b) Estimate the number of comparisons used.

2. a) Describe an algorithm for finding the first and second largest elements in a list of integers.
   b) Estimate the number of comparisons used.

3. a) Give an algorithm to determine whether a bit string contains a pair of consecutive zeros.
   b) How many comparisons does the algorithm use?

4. a) Suppose that a list contains integers that are in order of largest to smallest and an integer can appear repeatedly in this list. Devise an algorithm that locates all occurrences of an integer x in the list.
   b) Estimate the number of comparisons used.

5. a) Adapt Algorithm 1 in Section 3.1 to find the maximum and the minimum of a sequence of n elements by employing a temporary maximum and a temporary minimum that is updated as each successive element is examined.
   b) Describe the algorithm from part (a) in pseudocode.
   c) How many comparisons of elements in the sequence are carried out by this algorithm? (Do not count comparisons used to determine whether the end of the sequence has been reached.) How does this compare to the number of comparisons used by the algorithm in Exercise 5?

*7. Show that the worst-case complexity in terms of comparisons of an algorithm that finds the maximum and minimum of n elements is at least \( \lceil 3n/2 \rceil - 2 \).

8. Devise an efficient algorithm for finding the second largest element in a sequence of n elements and determine the worst-case complexity of your algorithm.

The shaker sort (or bidirectional bubble sort) successively compares adjacent pairs of elements, exchanging them if they are out of order, and alternately passing through the list from the beginning to the end and then from the end to the beginning until no exchanges are needed.

9. Show the steps used by the shaker sort to sort the list 3, 5, 1, 4, 6, 2.

10. Express the shaker sort in pseudocode.

11. Show that the shaker sort has \( O(n^2) \) complexity measured in terms of the number of comparisons it uses.

12. Explain why the shaker sort is efficient for sorting lists that are already in close to the correct order.

13. Show that \( (n \log n + n^2) \) is \( O(n^2) \).

14. Show that \( 8x^3 + 12x + 100 \log x \) is \( O(x^3) \).

15. Give a big-O estimate for \( (x^2 + x(\log x)^3) \cdot (2^x + x^3) \).

16. Find a big-O estimate for \( \sum_{j=1}^{n} j(j+1) \).

*17. Show that \( n! \) is not \( O(2^n) \).
18. Show that \( n^a \) is not \( O(n! \).
19. Find four numbers congruent to 5 modulo 17.
20. Show that if \( a \) and \( d \) are positive integers, then there are integers \( q \) and \( r \) such that \( a = dq + r \) where \(-d/2 < r \leq d/2\).
21. Show that if \( ac \equiv bc \pmod{m} \), then \( a \equiv b \pmod{md/d} \), where \( d = \gcd(m,c) \).
22. How many zeros are at the end of the binary expansion of 100!?
23. Use the Euclidean algorithm to find the greatest common divisor of 10,223 and 33,341.
24. How many divisions are required to find \( \gcd(144, 233) \) using the Euclidean algorithm?
25. Find \( \gcd(2n + 1, 3n + 2) \), where \( n \) is a positive integer. [Hint: Use the Euclidean algorithm.]
26. a) Show that if \( a \) and \( b \) are positive integers with \( a \geq b \), then \( \gcd(a, b) = a \) if \( a = b \), \( \gcd(a, b) = 2 \gcd(a/2, b/2) \) if \( a \) and \( b \) are even, \( \gcd(a, b) = \gcd(a/2, b) \) if \( a \) is even and \( b \) is odd, and \( \gcd(a, b) = \gcd(a - b, b) \) if both \( a \) and \( b \) are odd.
   b) Explain how to use (a) to construct an algorithm for computing the greatest common divisor of two positive integers that uses only comparisons, subtractions, and shifts of binary expansions, without using any divisions.
   c) Find \( \gcd(1202, 4848) \) using this algorithm.
27. Show that an integer is divisible by 9 if and only if the sum of its decimal digits is divisible by 9.
28. Prove that if \( n \) is a positive integer such that the sum of the divisors of \( n \) is \( n + 1 \), then \( n \) is prime.
29. Adapt the proof that there are infinitely many primes (Theorem 3 in Section 3.5) to show that there are infinitely many primes of the form \( 6k + 5 \) where \( k \) is a positive integer.
30. a) Explain why \( n \equiv 7 \pmod{24} \) equals the number of weeks in \( n \) days.
   b) Explain why \( n \equiv 24 \pmod{24} \) equals the number of days in \( n \) hours.
31. Determine whether these sets of integers are mutually relatively prime.
   a) 8, 10, 12
   b) 12, 15, 25
   c) 15, 21, 28
   d) 21, 24, 28, 32
32. Find a set of four mutually relatively prime integers such that no two of them are relatively prime.
33. a) Suppose that messages are encrypted using the function \( f(p) = (ap + b) \pmod{26} \) such that \( \gcd(a, 26) = 1 \). Determine a function that can be used to decrypt messages.
   b) The encrypted version of a message is LJMKG MGMXQ EXMWM. If it was encrypted using the function \( f(p) = (7p + 10) \pmod{26} \), what was the original message?
34. Show that the system of congruences \( x \equiv 2 \pmod{6} \) and \( x \equiv 3 \pmod{9} \) has no solutions.
35. Find all solutions of the system of congruences \( x \equiv 4 \pmod{6} \) and \( x \equiv 13 \pmod{15} \).
36. a) Show that the system of congruences \( x \equiv a_1 \pmod{m_1} \) and \( x \equiv a_2 \pmod{m_2} \) has a solution if and only if \( \gcd(m_1, m_2) \mid a_1 - a_2 \).
   b) Show that the solution in part (a) is unique modulo \( \text{lcm}(m_1, m_2) \).
37. Show that if \( f(x) \) is a nonconstant polynomial with integer coefficients, then there is an integer \( y \) such that \( f(y) \) is composite. [Hint: Assume that \( f(x_0) = p \) is prime. Show that \( p \) divides \( f(x_0 + kp) \) for all integers \( k \). Obtain a contradiction of the fact that a polynomial of degree \( n \), where \( n > 1 \), takes on each value at most \( n \) times.]
38. Show that if \( a \) and \( b \) are positive irrational numbers such that \( 1/a + 1/b = 1 \), then every positive integer can be uniquely expressed as either \( \lceil ka \rceil \) or \( \lfloor kb \rfloor \) for some positive integer \( k \).
39. Show that Goldbach's conjecture, which states that every even integer greater than 2 is the sum of two primes, is equivalent to the statement that every integer greater than 5 is the sum of three primes.
40. Prove that there are no solutions in integers \( x \) and \( y \) to the equation \( x^2 - 5y^2 = 2 \). [Hint: Consider this equation modulo 5.]
41. Find \( A^n \) if \( A \) is:
   \[ \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \]
42. Show that if \( A = cI \), where \( c \) is a real number and \( I \) is the \( n \times n \) identity matrix, then \( AB = BA \) whenever \( B \) is an \( n \times n \) matrix.
43. Show that if \( A \) is a \( 2 \times 2 \) matrix such that \( AB = BA \) whenever \( B \) is a \( 2 \times 2 \) matrix, then \( A = cI \), where \( c \) is a real number and \( I \) is the \( 2 \times 2 \) identity matrix.
   An \( n \times n \) matrix is called upper triangular if \( a_{ij} = 0 \) whenever \( i > j \).
44. From the definition of the matrix product, devise an algorithm for computing the product of two upper triangular matrices that ignores those products in the computation that are automatically equal to zero.
45. Give a pseudocode description of the algorithm in Exercise 44 for multiplying two upper triangular matrices.
46. How many multiplications of entries are used by the algorithm found in Exercise 44 for multiplying two \( n \times n \) upper triangular matrices?
47. Show that if \( A \) and \( B \) are invertible matrices and \( AB \) exists, then \( (AB)^{-1} = B^{-1}A^{-1} \).
48. What is the best order to form the product \( \text{ABCD} \) if \( A, B, C, \) and \( D \) are matrices with dimensions 30 \times 10, 10 \times 40, 40 \times 50, \) and \( 50 \times 30 \), respectively? Assume that the number of multiplications of entries used to multiply a \( p \times q \) matrix and a \( q \times r \) matrix is \( pqr \).
49. Let \( A \) be an \( n \times n \) matrix and let \( 0 \) be the \( n \times n \) matrix all of whose entries are zero. Show that the following are true.
50. Show that if the denominations of coins are \( c^0, c^1, \ldots, c^k \), where \( k \) is a positive integer and \( c \) is a positive integer, \( c > 1 \), the greedy algorithm always produces change using the fewest coins possible.

Computer Projects

Write programs with these inputs and outputs.

1. Given a list of \( n \) integers, find the largest integer in the list.
2. Given a list of \( n \) integers, find the first and last occurrences of the largest integer in the list.
3. Given a list of \( n \) distinct integers, determine the position of an integer in the list using a linear search.
4. Given an ordered list of \( n \) distinct integers, determine the position of an integer in the list using a binary search.
5. Given a list of \( n \) integers, sort them using a bubble sort.
6. Given a list of \( n \) integers, sort them using an insertion sort.
7. Given an integer \( n \), use the greedy algorithm to find the change for \( n \) cents using quarters, dimes, nickels, and pennies.
8. Given an ordered list of \( n \) integers and an integer \( x \), find the number of comparisons used to determine the position of an integer in the list using a linear search and using a binary search.
9. Given a list of integers, determine the number of comparisons used by the bubble sort and by the insertion sort to sort this list.
10. Given a positive integer, determine whether it is prime.
11. Given a message, encrypt this message using the Caesar cipher; and given a message encrypted using the Caesar cipher, decrypt this message.
12. Given two positive integers, find their greatest common divisor using the Euclidean algorithm.
13. Given two positive integers, find their least common multiple.
14. Given a positive integer, find the prime factorization of this integer.
15. Given a positive integer and a positive integer \( b \) greater than 1, find the base \( b \) expansion of this integer.
16. Given the positive integers \( a \), \( b \), and \( m > 1 \), find \( a^b \mod m \).
17. Given a positive integer, find the Cantor expansion of this integer (see the preamble to Exercise 3.6).
18. Given a positive integer \( n \), a modulus \( m \), multiplier \( a \), increment \( c \), and seed \( x_0 \), with \( 0 \leq a < m \), \( 0 \leq c < m \), and \( 0 \leq x_0 < m \), generate the sequence of \( n \) pseudo-random numbers using the linear congruential generator \( x_{n+1} = (ax_n + c) \mod m \).
19. Given positive integers \( a \) and \( b \), find integers \( s \) and \( t \) such that \( sa + tb = \gcd(a, b) \).
20. Given \( n \) linear congruences modulo pairwise relatively prime moduli, find the simultaneous solution of these congruences modulo the product of these moduli.
21. Given an \( m \times k \) matrix \( A \) and a \( k \times n \) matrix \( B \), find \( AB \).
22. Given a square matrix \( A \) and a positive integer \( n \), find \( A^n \).
23. Given a square matrix, determine whether it is symmetric.
24. Given an \( n_1 \times n_2 \) matrix \( A \), an \( n_2 \times n_3 \) matrix \( B \), an \( n_3 \times n_4 \) matrix \( C \), and an \( n_4 \times n_5 \) matrix \( D \), all with integer entries, determine the most efficient order to multiply these matrices (in terms of the number of multiplications and additions of integers).
25. Given two \( m \times n \) Boolean matrices, find their meet and join.
26. Given an \( m \times k \) Boolean matrix \( A \) and a \( k \times n \) Boolean matrix \( B \), find the Boolean product of \( A \) and \( B \).
27. Given a square Boolean matrix \( A \) and a positive integer \( n \), find \( A^n \).

Computations and Explorations

Use a computational program or programs you have written to do these exercises.

1. We know that \( n^b \) is \( O(d^n) \) when \( b \) and \( d \) are positive numbers with \( d \geq 2 \). Give values of the constants \( C \) and \( k \) such that \( n^b \leq Cd^n \) whenever \( x > k \) for each of these sets of values: \( b = 10, d = 2; b = 20, d = 3; b = 1000, d = 7 \).
2. Compute the change for different values of \( n \) with coins of different denominations using the greedy algorithm and determine whether the smallest number of coins was used. Can you find conditions so that the
Note that it is sometimes difficult to locate the error in a faulty proof by mathematical induction, as Example 14 illustrates.

**EXAMPLE 14**

Find the error in this “proof” of the clearly false claim that every set of lines in the plane, no two of which are parallel, meet in a common point.

“Proof”: Let $P(n)$ be the statement that every set of $n$ lines in the plane, no two of which are parallel, meet in a common point. We will attempt to prove that $P(n)$ is true for all positive integers $n \geq 2$.

**BASIS STEP:** The statement $P(2)$ is true because any two lines in the plane that are not parallel meet in a common point (by the definition of parallel lines).

**INDUCTIVE STEP:** The inductive hypothesis is the statement that $P(k)$ is true for the positive integer $k$, that is, the assumption that every set of $k$ lines in the plane, no two of which are parallel, meet in a common point. To complete the inductive step, we must show that if $P(k)$ is true, then $P(k + 1)$ must also be true. That is, we must show that if every set of $k$ lines in the plane, no two of which are parallel, meet in a common point, then every set of $k + 1$ lines in the plane, no two of which are parallel, meet in a common point. So, consider a set of $k + 1$ distinct lines in the plane. By the inductive hypothesis, the first $k$ of these lines meet in a common point $P_1$. Moreover, by the inductive hypothesis, the last $k$ of these lines meet in a common point $P_2$. We will show that $P_1$ and $P_2$ must be the same point. If $P_1$ and $P_2$ were different points, all lines containing both of them must be the same line because two points determine a line. This contradicts our assumption that all these lines are distinct. Thus, $P_1$ and $P_2$ are the same point. We conclude that the point $P_1 = P_2$ lies on all $k + 1$ lines. We have shown that $P(k + 1)$ is true assuming that $P(k)$ is true. That is, we have shown that if we assume that every $k$, $k \geq 2$, distinct lines meet in a common point, then every $k + 1$ distinct lines meet in a common point. This completes the inductive step.

We have completed the basis step and the inductive step, and supposedly we have a correct proof by mathematical induction.

**Solution:** Examining this supposed proof by mathematical induction it appears that everything is in order. However, there is an error, as there must be. The error is rather subtle. Carefully looking at the inductive step shows that this step requires that $k \geq 3$. We cannot show that $P(2)$ implies $P(3)$. When $k = 2$, our goal is to show that every three distinct lines meet in a common point. The first two lines must meet in a common point $P_1$ and the last two lines must meet in a common point $P_2$. But in this case, $P_1$ and $P_2$ do not have to be the same, because only the second line is common to both sets of lines. Here is where the inductive step fails.

**Exercises**

1. There are infinitely many stations on a train route. Suppose that the train stops at the first station and suppose that if the train stops at a station, then it stops at the next station. Show that the train stops at all stations.

2. Suppose that you know that a golfer plays the first hole of a golf course with an infinite number of holes and that if this golfer plays one hole, then the golfer goes on to play the next hole. Prove that this golfer plays every hole on the course.

Use mathematical induction in Exercises 3–17 to prove summation formulae.

3. Let $P(n)$ be the statement that $1^2 + 2^2 + \ldots + n^2 = n(n + 1)(2n + 1)/6$ for the positive integer $n$.
   a) What is the statement $P(1)$?
   b) Show that $P(1)$ is true, completing the basis step of the proof.
   c) What is the inductive hypothesis?
   d) What do you need to prove in the inductive step?
   e) Complete the inductive step.
   f) Explain why these steps show that this formula is true whenever $n$ is a positive integer.

4. Let $P(n)$ be the statement that $1^3 + 2^3 + \ldots + n^3 = (n(n + 1)/2)^2$ for the positive integer $n$.
   a) What is the statement $P(1)$?
   b) Show that $P(1)$ is true, completing the basis step of the proof.
c) What is the inductive hypothesis?
d) What do you need to prove in the inductive step?
e) Complete the inductive step.
f) Explain why these steps show that this formula is true whenever $n$ is a nonnegative integer.

5. Prove that $1^2 + 3^2 + 5^2 + \cdots + (2n+1)^2 = (n+1)^3 - 1/3$ whenever $n$ is a nonnegative integer.

6. Prove that $1! + 2! + \cdots + n! = (n+1)! - 1$ whenever $n$ is a positive integer.

7. Prove that $3 + 3^2 + 5^2 + \cdots + 3 \cdot 5^n = 3(5^{n+1} - 1)/4$ whenever $n$ is a nonnegative integer.

8. Prove that $2 - 2 \cdot 7 + 2 \cdot 7^2 - \cdots + 2(-7)^n = (1 - (-7)^{n+1})/4$ whenever $n$ is a nonnegative integer.

9. a) Find a formula for the sum of the first $n$ even positive integers.
   b) Prove the formula that you conjectured in part (a).

10. a) Find a formula for
    \[
    \sum_{j=0}^{n} \left( \frac{1}{2^j} \right) = \frac{2^{n+1} + (-1)^n}{3 \cdot 2^n}
    \]
    by examining the values of this expression for small values of $n$.
   b) Prove the formula you conjectured in part (a).

11. a) Find a formula for
    \[
    \sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}
    \]
    by examining the values of this expression for small values of $n$.
   b) Prove the formula you conjectured in part (a).

12. Prove that
    \[
    \sum_{j=0}^{n} \left( \frac{1}{2^j} \right) = \frac{2^{n+1} + (-1)^n}{3 \cdot 2^n}
    \]
    whenever $n$ is a nonnegative integer.

13. Prove that $1^2 - 2^2 + 3^2 - \cdots + (-1)^{n-1} n^2 = (-1)^{n-1} n(n+1)/2$ whenever $n$ is a positive integer.

14. Prove that for every positive integer $n$, $\sum_{k=1}^{n} k^2 = (n-1)2^{n+1} + 2$.

15. Prove that for every positive integer $n$,
    \[
    1 \cdot 2 + 2 \cdot 3 + \cdots + n(n+1) = n(n+1)(n+2)/3.
    \]

16. Prove that for every positive integer $n$,
    \[
    1 \cdot 2 \cdot 3 + 2 \cdot 3 \cdot 4 + \cdots + n(n+1)(n+2)
    = n(n+1)(n+2)(n+3)/4.
    \]

17. Prove that $\sum_{j=1}^{n} j^2 = n(n+1)(2n+1)(3n^2 + 3n - 1)/30$ whenever $n$ is a positive integer.

Use mathematical induction to prove the inequalities in Exercises 18–30.

18. Let $P(n)$ be the statement that $n! < n^n$, where $n$ is an integer greater than 1.
   a) What is the statement $P(2)$?
   b) Show that $P(2)$ is true, completing the basis step of the proof.
   c) What is the inductive hypothesis?
   d) What do you need to prove in the inductive step?
   e) Complete the inductive step.
   f) Explain why these steps show that this inequality is true whenever $n$ is an integer greater than 1.

19. Let $P(n)$ be the statement that
    \[
    1 + \frac{1}{4} + \frac{1}{9} + \cdots + \frac{1}{n^2} < 2 - \frac{1}{n},
    \]
    where $n$ is an integer greater than 1.
   a) What is the statement $P(2)$?
   b) Show that $P(2)$ is true, completing the basis step of the proof.
   c) What is the inductive hypothesis?
   d) What do you need to prove in the inductive step?
   e) Complete the inductive step.
   f) Explain why these steps show that this inequality is true whenever $n$ is an integer greater than 1.

20. Prove that $3^n < n!$ if $n$ is an integer greater than 6.

21. Prove that $2^n > n^2$ if $n$ is an integer greater than 4.

22. For which nonnegative integers $n$ is $n^2 < n!$? Prove your answer.

23. For which nonnegative integers $n$ is $2n + 3 < 2^n$? Prove your answer.

24. Prove that $1/(2n) \leq [1 \cdot 3 \cdot 5 \cdots (2n-1)]/(2 \cdot 4 \cdots 2n)$ whenever $n$ is a positive integer.

*25. Prove that $1 + nh \leq (1 + h)^n$ for all nonnegative integers $n$. This is called **Bernoulli's inequality**.

*26. Suppose that $a$ and $b$ are real numbers with $0 < b < a$. Prove that if $n$ is a positive integer, then $a^n - b^n \leq na^{n-1}(a - b)$.

*27. Prove that for every positive integer $n$,
    \[
    1 + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \cdots + \frac{1}{\sqrt{n}} > 2(\sqrt{n+1} - 1).
    \]

28. Prove that $n^2 - 7n + 12$ is nonnegative whenever $n$ is an integer with $n \geq 3$.

In Exercises 29 and 30, $H_n$ denotes the $n$th harmonic number.

*29. Prove that $H_{2n} \leq 1 + n$ whenever $n$ is a nonnegative integer.

*30. Prove that
    \[
    H_1 + H_2 + \cdots + H_n = (n + 1)H_n - n.
    \]

Use mathematical induction in Exercises 31–37 to prove divisibility facts.

31. Prove that 2 divides $n^2 + n$ whenever $n$ is a positive integer.

32. Prove that 3 divides $n^3 + 2n$ whenever $n$ is a positive integer.

33. Prove that 5 divides $n^5 - n$ whenever $n$ is a nonnegative integer.

34. Prove that 6 divides $n^3 - n$ whenever $n$ is a nonnegative integer.
35. Prove that \( n^2 - 1 \) is divisible by 8 whenever \( n \) is an odd positive integer.

36. Prove that 21 divides \( 4^{n+1} + 52^{n-1} \) whenever \( n \) is a positive integer.

37. Prove that if \( n \) is a positive integer, then 133 divides \( 11^{n+1} + 12^{n-1} \).

Use mathematical induction in Exercises 38–46 to prove results about sets.

38. Prove that if \( A_1, A_2, \ldots, A_n \) and \( B_1, B_2, \ldots, B_n \) are sets such that \( A_j \subseteq B_j \) for \( j = 1, 2, \ldots, n \), then
\[
\bigcup_{j=1}^{n} A_j \subseteq \bigcup_{j=1}^{n} B_j.
\]

39. Prove that if \( A_1, A_2, \ldots, A_n \) and \( B_1, B_2, \ldots, B_n \) are sets such that \( A_j \subseteq B_j \) for \( j = 1, 2, \ldots, n \), then
\[
\bigcap_{j=1}^{n} A_j \subseteq \bigcap_{j=1}^{n} B_j.
\]

40. Prove that if \( A_1, A_2, \ldots, A_n \) and \( B \) are sets, then
\[
(A_1 \cap A_2 \cap \cdots \cap A_n) \cup B = (A_1 \cup B) \cap (A_2 \cup B) \cap \cdots \cap (A_n \cup B).
\]

41. Prove that if \( A_1, A_2, \ldots, A_n \) and \( B \) are sets, then
\[
(A_1 \cup A_2 \cup \cdots \cup A_n) \cap B = (A_1 \cap B) \cup (A_2 \cap B) \cup \cdots \cup (A_n \cap B).
\]

42. Prove that if \( A_1, A_2, \ldots, A_n \) and \( B \) are sets, then
\[
(A_1 - B) \cap (A_2 - B) \cap \cdots \cap (A_n - B) = (A_1 \cap A_2 \cap \cdots \cap A_n) - B.
\]

43. Prove that if \( A_1, A_2, \ldots, A_n \) are subsets of a universal set \( U \), then
\[
\bigcup_{k=1}^{n} A_k = \bigcap_{k=1}^{n} A_k.
\]

44. Prove that if \( A_1, A_2, \ldots, A_n \) and \( B \) are sets, then
\[
(A_1 - B) \cup (A_2 - B) \cup \cdots \cup (A_n - B) = (A_1 \cup A_2 \cup \cdots \cup A_n) - B.
\]

45. Prove that a set with \( n \) elements has \( n(n - 1)/2 \) subsets containing exactly two elements whenever \( n \) is an integer greater than or equal to 2.

46. Prove that a set with \( n \) elements has \( n(n - 1)(n - 2)/6 \) subsets containing exactly three elements whenever \( n \) is an integer greater than or equal to 3.

Exercises 47–49 present incorrect proofs using mathematical induction. You will need to identify an error in reasoning in each exercise.

47. What is wrong with this “proof” that all horses are the same color?

Let \( P(n) \) be the proposition that all the horses in a set of \( n \) horses are the same color.

\[ P(1) \text{ is true.} \]

\[ P(k) \text{ is true, so that all} \]

the horses in any set of \( k \) horses are the same color.

Consider any \( k + 1 \) horses; number these as horses 1, 2, 3, \ldots, \( k \), \( k + 1 \). Now the first \( k \) of these horses all must have the same color, and the last \( k \) of these must also have the same color. Because the set of the first \( k \) horses and the set of the last \( k \) horses overlap, all \( k + 1 \) must be the same color. This shows that \( P(k + 1) \) is true and finishes the proof by induction.

48. What is wrong with this “proof”?

"Theorem" For every positive integer \( n \), \( \sum_{i=1}^{n} i = (n + \frac{1}{2})^2/2 \).

\[ P(1) \text{ is true for} \]

\( n = 1 \).

\[ P(n) \text{ is true} \]

then \( \sum_{i=1}^{n+1} i = (\sum_{i=1}^{n} i) + (n + 1) \). By the inductive hypothesis,
\[\sum_{i=1}^{n+1} i = (n + \frac{1}{2})^2/2 + n + 1 = (n^2 + n + \frac{1}{4})/2 + n + 1 = (n^2 + 3n + \frac{9}{4})/2 = (n + \frac{3}{2})^2/2 = (n + 1) + \frac{1}{2})^2/2, \] completing the inductive step.

49. What is wrong with this “proof”?

"Theorem" For every positive integer \( n \), if \( x \) and \( y \) are positive integers with \( \text{max}(x, y) = n \), then \( x = y \).

\[ P(1) \text{ is true for} \]

\( n = 1 \).

\[ P(n) \text{ is true} \]

then \( \text{max}(x, y) = n \). Now let \( \text{max}(x, y) = k + 1 \), where \( x \) and \( y \) are positive integers. Then \( \text{max}(x - 1, y - 1) = k \), so by the inductive hypothesis, \( x - 1 = y - 1 \). It follows that \( x = y \), completing the inductive step.

50. Use mathematical induction to show that given a set of \( n + 1 \) positive integers, none exceeding \( 2n \), there is at least one integer in this set that divides another integer in the set.

51. A knight on a chessboard can move one space horizontally (in either direction) and two spaces vertically (in either direction) or two spaces horizontally (in either direction) and one space vertically (in either direction). Suppose that we have an infinite chessboard, made up of all squares \((m, n)\) where \( m \) and \( n \) are nonnegative integers. Use mathematical induction to show that a knight starting at \((0, 0)\) can visit every square using a finite sequence of moves. [Hint: Use induction on the variable \( s = m + n \).]

52. Suppose that
\[
A = \begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix},
\]

where \( a \) and \( b \) are real numbers. Show that
\[
A^n = \begin{bmatrix} a^n & 0 \\ 0 & b^n \end{bmatrix}
\]

for every positive integer \( n \).
53. *(Requires calculus)* Use mathematical induction to prove that the derivative of \( f(x) = x^n \) equals \( nx^{n-1} \) whenever \( n \) is a positive integer. (For the inductive step, use the product rule for derivatives.)

54. Suppose that \( A \) and \( B \) are square matrices with the property \( AB = BA \). Show that \( AB^n = B^nA \) for every positive integer \( n \).

55. Suppose that \( m \) is a positive integer. Use mathematical induction to prove that if \( a \) and \( b \) are integers with \( a \equiv b \pmod{m} \), then \( a^k \equiv b^k \pmod{m} \) whenever \( k \) is a nonnegative integer.

56. Use mathematical induction to show that \( \neg(p_1 \lor p_2 \lor \cdots \lor p_n) \) is equivalent to \( \neg p_1 \land \neg p_2 \land \cdots \land \neg p_n \) whenever \( p_1, p_2, \ldots, p_n \) are propositions.

**57.** Show that
\[
[(p_1 \to p_2) \land (p_2 \to p_3) \land \cdots \land (p_{n-1} \to p_n)] \to [(p_1 \land p_2 \land \cdots \land p_{n-1}) \to p_n]
\]
is a tautology whenever \( p_1, p_2, \ldots, p_n \) are propositions, where \( n \geq 2 \).

**58.** Show that \( n \) lines separate the plane into \( (n^2 + n + 2)/2 \) regions if no two of these lines are parallel and no three pass through a common point.

**59.** Let \( a_1, a_2, \ldots, a_n \) be positive real numbers. The **arithmetic mean** of these numbers is defined by
\[
A = (a_1 + a_2 + \cdots + a_n)/n,
\]
and the **geometric mean** of these numbers is defined by
\[
G = (a_1a_2 \cdots a_n)^{1/n}.
\]
Use mathematical induction to prove that \( A \geq G \).

60. Use mathematical induction to prove Lemma 2 of Section 3.6, which states that if \( p \) is a prime and \( p \mid a_1a_2 \cdots a_n \), where \( a_i \) is an integer for \( i = 1, 2, 3, \ldots, n \), then \( p \mid a_i \) for some integer \( i \).

61. Show that if \( n \) is a positive integer, then
\[
\sum_{[a_1, \ldots, a_k] \subseteq \{1, 2, \ldots, n\}} \frac{1}{a_1a_2 \cdots a_k} = n.
\]
(Here the sum is over all nonempty subsets of the set of the \( n \) smallest positive integers.)

**62.** Use the well-ordering property to show that the following form of mathematical induction is a valid method to prove that \( P(n) \) is true for all positive integers \( n \).

**Basis Step:** \( P(1) \) and \( P(2) \) are true.

**Inductive Step:** For each positive integer \( k \), if \( P(k) \) and \( P(k + 1) \) are both true, then \( P(k + 2) \) is true.

63. Show that if \( A_1, A_2, \ldots, A_n \) are sets where \( n \geq 2 \), and for all pairs of integers \( i \) and \( j \) with \( 1 \leq i < j \leq n \) either \( A_i \) is a subset of \( A_j \) or \( A_j \) is a subset of \( A_i \), then there is an integer \( i \), \( 1 \leq i \leq n \) such that \( A_i \) is a subset of \( A_j \) for all integers \( j \) with \( 1 \leq j \leq n \).

**64.** A guest at a party is a **celebrity** if this person is known by every other guest, but knows none of them. There is at most one celebrity at a party, for if there were two, they would know each other. A particular party may have no celebrity. Your assignment is to find the celebrity, if one exists, at a party, by asking only one type of question—asking a guest whether they know a second guest. Everyone must answer your questions truthfully. That is, if Alice and Bob are two people at the party, you can ask Alice whether she knows Bob; she must answer correctly. Use mathematical induction to show that if there are \( n \) people at the party, then you can find the celebrity, if there is one, with \( 3(n - 1) \) questions. [Hint: First ask a question to eliminate one person as a celebrity. Then use the inductive hypothesis to identify a potential celebrity. Finally, ask two more questions to determine whether that person is actually a celebrity.]

Suppose there are \( n \) people in a group, each aware of a scandal no one else in the group knows about. These people communicate by telephone; when two people in the group talk, they share information about all scandals each knows about. For example, on the first call, two people share information, so by the end of the call, each of these people knows about two scandals. The **gossip problem** asks for \( G(n) \), the minimum number of telephone calls that are needed for all \( n \) people to learn about all the scandals. Exercises 65–67 deal with the gossip problem.

65. Find \( G(1), G(2), G(3), \) and \( G(4) \).

66. Use mathematical induction to prove that \( G(n) \leq 2n - 4 \) for \( n \geq 4 \). [Hint: In the inductive step, have a new person call a particular person at the start and at the end.]

**67.** Prove that \( G(n) = 2n - 4 \) for \( n \geq 4 \).

68. Show that it is possible to arrange the numbers 1, 2, \ldots, \( n \) in a row so that the average of any two of these numbers never appears between them. [Hint: Show that it suffices to prove this fact when \( n \) is a power of 2. Then use mathematical induction to prove the result when \( n \) is a power of 2.]

69. Show that if \( I_1, I_2, \ldots, I_n \) is a collection of open intervals on the real number line, \( n \geq 2 \), and every pair of these intervals has a nonempty intersection, that is, \( I_i \cap I_j \neq \emptyset \) whenever \( 1 \leq i \leq n \) and \( 1 \leq j \leq n \), then the intersection of all these sets is nonempty, that is, \( I_1 \cap I_2 \cap \cdots \cap I_n \neq \emptyset \). (Recall that an **open interval** is the set of real numbers \( x \) with \( a < x < b \), where \( a \) and \( b \) are real numbers with \( a < b \).)

Sometimes we cannot use mathematical induction to prove a result we believe to be true, but we can use mathematical induction to prove a stronger result. Because the inductive hypothesis of the stronger result provides more to work with, this process is called **inductive loading**. We use inductive loading in Exercise 70.

70. Suppose that we want to prove that
\[
\frac{1}{2} \cdot \frac{3}{4} \cdots \frac{2n - 1}{2n} < \frac{1}{\sqrt{3n}}
\]
for all positive integers \( n \).
a) Show that if we try to prove this inequality using mathematical induction, the basis step works, but the inductive step fails.
b) Show that mathematical induction can be used to prove the stronger inequality
\[
\frac{1}{2} \cdot \frac{3}{4} \cdot \cdots \cdot \frac{2n-1}{2n} < \frac{1}{\sqrt{3n+1}}
\]
for all integers greater than 1, which, together with a verification for the case where \( n = 1 \), establishes the weaker inequality we originally tried to prove using mathematical induction.

71. Let \( n \) be an even positive integer. Show that when \( n \) people stand in a yard at mutually distinct distances and each person throws a pie at their nearest neighbor, it is possible that everyone is hit by a pie.

72. Construct a tiling using right triominoes of the \( 4 \times 4 \) checkerboard with the square in the upper left corner removed.

73. Construct a tiling using right triominoes of the \( 8 \times 8 \) checkerboard with the square in the upper left corner removed.

74. Prove or disprove that all checkerboards of these shapes can be completely covered using right triominoes whenever \( n \) is a positive integer.
   a) \( 3 \times 2^n \)  
   b) \( 6 \times 2^n \)  
   c) \( 2^3 \times 3^n \)  
   d) \( 6^n \times 6^n \)

*75. Show that a three-dimensional \( 2^n \times 2^n \times 2^n \) checkerboard with one \( 1 \times 1 \times 1 \) cube missing can be completely covered by \( 2 \times 2 \times 2 \) cubes with one \( 1 \times 1 \times 1 \) cube removed.

*76. Show that an \( n \times n \) checkerboard with one square removed can be completely covered using right triominoes if \( n \geq 5 \), \( n \) is odd, and \( 3 \nmid n \).

77. Show that a \( 5 \times 5 \) checkerboard with a corner square removed can be tiled using right triominoes.

*78. Find a \( 5 \times 5 \) checkerboard with a square removed that cannot be tiled using right triominoes. Prove that such a tiling does not exist for this board.

79. Use the principle of mathematical induction to show that \( P(n) \) is true for \( n = b, b + 1, b + 2, \ldots \), where \( b \) is an integer, if \( P(b) \) is true and the conditional statement \( P(k) \implies P(k + 1) \) is true for all positive integers \( k \) with \( k \geq b \).

4.2 Strong Induction and Well-Ordering

Introduction

In Section 4.1 we introduced mathematical induction and we showed how to use it to prove a variety of theorems. In this section we will introduce another form of mathematical induction, called strong induction, which can often be used when we cannot easily prove a result using mathematical induction. The basis step of a proof by strong induction is the same as a proof of the same result using mathematical induction. That is, in a strong induction proof that \( P(n) \) is true for all positive integers \( n \), the basis step shows that \( P(1) \) is true. However, the inductive steps in these two proof methods are different. In a proof by mathematical induction, the inductive step shows that if the inductive hypothesis \( P(k) \) is true, then \( P(k + 1) \) is also true. In a proof by strong induction, the inductive step shows that if \( P(j) \) is true for all positive integers not exceeding \( k \), then \( P(k + 1) \) is true. That is, for the inductive hypothesis we assume that \( P(j) \) is true for \( j = 1, 2, \ldots, k \).

The validity of both mathematical induction and strong induction follow from the well-ordering property in Appendix 1. In fact, mathematical induction, strong induction, and well-ordering are all equivalent principles. That is, the validity of each can be proved from either of the other two. This means that a proof using one of these two principles can be rewritten as a proof using either of the other two principles. Just as it is sometimes the case that it is much easier to see how to prove a result using strong induction rather than mathematical induction, it is sometimes easier to use well-ordering than one of the two forms of mathematical induction. In this section we will give some examples of how the well-ordering property can be used to prove theorems.

Strong Induction

Before we illustrate how to use strong induction, we state this principle again.
Exercises

1. Use strong induction to show that if you can run one mile or two miles, and if you can always run two more miles once you have run a specified number of miles, then you can run any number of miles.

2. Use strong induction to show that all dominoes fall in an infinite arrangement of dominoes if you know that the first three dominoes fall, and that when a domino falls, the domino three farther down in the arrangement also falls.

3. Let \( P(n) \) be the statement that a postage of \( n \) cents can be formed using just 3-cent and 5-cent stamps. The parts of this exercise outline a strong induction proof that \( P(n) \) is true for \( n \geq 8 \).
   a) Show that the statements \( P(8) \), \( P(9) \), and \( P(10) \) are true, completing the basis step of the proof.
   b) What is the inductive hypothesis of the proof?
   c) What do you need to prove in the inductive step?
   d) Complete the inductive step for \( k \geq 10 \).
   e) Explain why these steps show that this statement is true whenever \( n \geq 18 \).

4. Let \( P(n) \) be the statement that a postage of \( n \) cents can be formed using just 4-cent and 7-cent stamps. The parts of this exercise outline a strong induction proof that \( P(n) \) is true for \( n \geq 18 \).
   a) Show statements \( P(18) \), \( P(19) \), \( P(20) \), and \( P(21) \) are true, completing the basis step of the proof.
   b) What is the inductive hypothesis of the proof?
   c) What do you need to prove in the inductive step?
   d) Complete the inductive step for \( k \geq 21 \).
   e) Explain why these steps show that this statement is true whenever \( n \geq 18 \).

5. a) Determine which amounts of postage can be formed using just 4-cent and 11-cent stamps.
   b) Prove your answer to (a) using the principle of mathematical induction. Be sure to state explicitly your inductive hypothesis in the inductive step.
   c) Prove your answer to (a) using strong induction. How does the inductive hypothesis in this proof differ from that in the inductive hypothesis for a proof using mathematical induction?

6. a) Determine which amounts of postage can be formed using just 3-cent and 10-cent stamps.
b) Prove your answer to (a) using the principle of mathematical induction. Be sure to state explicitly your inductive hypothesis in the inductive step.

c) Prove your answer to (a) using strong induction. How does the inductive hypothesis in this proof differ from that in the inductive hypothesis for a proof using mathematical induction?

7. Which amounts of money can be formed using just two-dollar bills and five-dollar bills? Prove your answer using strong induction.

8. Suppose that a store offers gift certificates in denominations of 25 dollars and 40 dollars. Determine the possible total amounts you can form using these gift certificates. Prove your answer using strong induction.

9. Use strong induction to prove that \( \sqrt{2} \) is irrational. [Hint: Let \( P(n) \) be the statement that \( \sqrt{2} \neq n/b \) for any positive integer \( b \).]

10. Assume that a chocolate bar consists of \( n \) squares arranged in a rectangular pattern. The bar, a smaller rectangular piece of the bar, can be broken along a vertical or a horizontal line separating the squares. Assuming that only one piece can be broken at a time, determine how many breaks you must successively make to break the bar into \( n \) separate squares. Use strong induction to prove your answer.

11. Consider this variation of the game of Nim. The game begins with \( n \) matches. Two players take turns removing matches, one, two, or three at a time. The player removing the last match loses. Use strong induction to show that if each player plays the best strategy possible, the first player wins if \( n = 4j, 4j + 2, \) or \( 4j + 3 \) for some nonnegative integer \( j \) and the second player wins in the remaining case when \( n = 4j + 1 \) for some nonnegative integer \( j \).

12. Use strong induction to show that every positive integer \( n \) can be written as a sum of distinct powers of two, that is, as a sum of a subset of the integers \( 2^0 = 1, 2^1 = 2, 2^2 = 4, \) and so on. [Hint: For the inductive step, separately consider the case where \( k + 1 \) is even and where it is odd. When it is even, note that \( (k + 1)/2 \) is an integer.]

13. A jigsaw puzzle is put together by successively joining pieces that fit together into blocks. A move is made each time a piece is added to a block, or when two blocks are joined. Use strong induction to prove that no matter how the moves are carried out, exactly \( n - 1 \) moves are required to assemble a puzzle with \( n \) pieces.

14. Suppose you begin with a pile of \( n \) stones and split this pile into \( n \) piles of one stone each by successively splitting a pile of stones into two smaller piles. Each time you split a pile you multiply the number of stones in each of the two smaller piles you form, so that if these piles have \( r \) and \( s \) stones in them, respectively, you compute \( rs \). Show that no matter how you split the piles, the sum of the products computed at each step equals \( n(n - 1)/2 \).

15. Prove that the first player has a winning strategy for the game of Chomp, introduced in Example 12 in Section 1.7, if the initial board is square. [Hint: Use strong induction to show that this strategy works. For the first move, the first player chomps all cookies except those in the left and top edges. On subsequent moves, after the second player has chomped cookies on either the top or left edge, the first player chomps cookies in the same relative positions in the left or top edge, respectively.]

16. Prove that the first player has a winning strategy for the game of Chomp, introduced in Example 12 in Section 1.7, if the initial board is two squares wide, that is, a \( 2 \times n \) board. [Hint: Use strong induction. The first move of the first player should be to chomp the cookie in the bottom row at the far right.]

17. Use strong induction to show that if a simple polygon with at least four sides is triangulated, then at least two of the triangles in the triangulation have two sides that border the exterior of the polygon.

18. Use strong induction to show that when a convex polygon \( P \) with consecutive vertices \( v_1, v_2, \ldots, v_n \) is triangulated into \( n - 2 \) triangles, the \( n - 2 \) triangles can be numbered 1, 2, \ldots, \( n - 2 \) so that \( v_i \) is a vertex of triangle \( i \) for \( i = 1, 2, \ldots, n - 2 \).

19. Pick's theorem says that the area of a simple polygon \( P \) in the plane with vertices that are all lattice points (that is, points with integer coordinates) equals \( I(P) + B(P)/2 - 1 \), where \( I(P) \) and \( B(P) \) are the number of lattice points in the interior of \( P \) and on the boundary of \( P \), respectively. Use strong induction on the number of vertices of \( P \) to prove Pick's theorem. [Hint: For the basis step, first prove the theorem for rectangles, then for right triangles, and finally for all triangles by noting that the area of a triangle is the area of a larger rectangle containing it with the areas of at most three triangles subtracted. For the inductive step, take advantage of Lemma 1.]
Exercises 22 and 23 present examples that show inductive loading can be used to prove results in computational geometry.

*22. Let \( P(n) \) be the statement that when nonintersecting diagonals are drawn inside a convex polygon with \( n \) sides, at least two vertices of the polygon are not endpoints of any of these diagonals.

a) Show that when we attempt to prove \( P(n) \) for all integers \( n \) with \( n \geq 3 \) using strong induction, the inductive step does not go through.

b) Show that we can prove that \( P(n) \) is true for all integers \( n \) with \( n \geq 3 \) by proving by strong induction the stronger assertion \( Q(n) \), for \( n \geq 4 \), where \( Q(n) \) states that whenever nonintersecting diagonals are drawn inside a convex polygon with \( n \) sides, at least two non-adjacent vertices are not endpoints of any of these diagonals.

23. Let \( E(n) \) be the statement that in a triangulation of a simple polygon with \( n \) sides, at least one of the triangles in the triangulation has two sides bordering the exterior of the polygon.

a) Explain where a proof using strong induction that \( E(n) \) is true for all integers \( n \geq 4 \) runs into difficulties.

b) Show that we can prove that \( E(n) \) is true for all integers \( n \geq 4 \) by proving by strong induction the stronger statement \( T(n) \) for all integers \( n \geq 4 \), which states that in every triangulation of a simple polygon, at least two of the triangles in the triangulation have two sides bordering the exterior of the polygon.

*24. A stable assignment, defined in the preamble to Exercise 58 in Section 3.1, is called \textbf{optimal for suitors} if no stable assignment exists in which a suitor is paired with a suitee whom this suitor prefers to the person to whom this suitor is paired in this stable assignment. Use strong induction to show that the deferred acceptance algorithm produces a stable assignment that is optimal for suitors.

25. Suppose that \( P(n) \) is a propositional function. Determine for which positive integers \( n \) the statement \( P(n) \) must be true, and justify your answer, if

a) \( P(1) \) is true; for all positive integers \( n \), if \( P(n) \) is true, then \( P(n + 2) \) is true.

b) \( P(1) \) and \( P(2) \) are true; for all positive integers \( n \), if \( P(n) \) and \( P(n + 1) \) are true, then \( P(n + 2) \) is true.

c) \( P(1) \) is true; for all positive integers \( n \), if \( P(n) \) is true, then \( P(2n) \) is true.

d) \( P(1) \) is true; for all positive integers \( n \), if \( P(n) \) is true, then \( P(n + 1) \) is true.

26. Suppose that \( P(n) \) is a propositional function. Determine for which nonnegative integers \( n \) the statement \( P(n) \) must be true if

a) \( P(0) \) is true; for all nonnegative integers \( n \), if \( P(n) \) is true, then \( P(n + 2) \) is true.

b) \( P(0) \) is true; for all nonnegative integers \( n \), if \( P(n) \) is true, then \( P(n + 3) \) is true.

c) \( P(0) \) and \( P(1) \) are true; for all nonnegative integers \( n \), if \( P(n) \) and \( P(n + 1) \) are true, then \( P(n + 2) \) is true.

d) \( P(0) \) is true; for all nonnegative integers \( n \), if \( P(n) \) is true, then \( P(n + 2) \) and \( P(n + 3) \) are true.

27. Show that if the statement \( P(n) \) is true for infinitely many positive integers \( n \) and \( P(n + 1) \rightarrow P(n) \) is true for all positive integers \( n \), then \( P(n) \) is true for all positive integers \( n \).

28. Let \( b \) be a fixed integer and \( j \) a fixed positive integer. Show that if \( P(b, P(b + 1), \ldots, P(b + j) \) are true and \( [P(b) \land P(b + 1) \land \cdots \land P(k)] \rightarrow P(k + 1) \) is true for every positive integer \( k \geq b + j \), then \( P(n) \) is true for all integers \( n \) with \( n \geq b \).

29. What is wrong with this “proof” by strong induction?

"Theorem" For every nonnegative integer \( n \), \( 5n = 0 \).

\[ \text{Basis Step: } 5 \cdot 0 = 0. \]

\[ \text{Inductive Step: Suppose that } 5j = 0 \text{ for all nonnegative integers } j \text{ with } 0 \leq j \leq k. \text{ Write } k + 1 = i + j, \text{ where } i \text{ and } j \text{ are natural numbers less than } k + 1. \text{ By the inductive hypothesis, } 5(k + 1) = 5(i + j) = 5i + 5j = 0 + 0 = 0. \]

*30. Find the flaw with the following “proof” that \( a^n = 1 \) for all nonnegative integers \( n \), whenever \( a \) is a nonzero real number.

\[ \text{Basis Step: } a^0 = 1 \text{ is true by the definition of } a^0. \]

\[ \text{Inductive Step: Assume that } a^l = 1 \text{ for all nonnegative integers } j \text{ with } j \leq k. \text{ Then note that } \]

\[ a^{k+1} = a^k \cdot a^1 = 1 \cdot 1 = 1. \]

31. Show that strong induction is a valid method of proof by showing that it follows from the well-ordering property.

32. Find the flaw with the following “proof” that every postage of three cents or more can be formed using just three-cent and four-cent stamps.

\[ \text{Basis Step: We can form postage of three cents with a single three-cent stamp and we can form postage of four cents using a single four-cent stamp.} \]

\[ \text{Inductive Step: Assume that we can form postage of } j \text{ cents for all nonnegative integers } j \text{ with } j \leq k \text{ using just } \]
three-cent and four-cent stamps. We can then form postage of \( k + 1 \) cents by replacing one three-cent stamp with a four-cent stamp or by replacing two four-cent stamps by three three-cent stamps.

33. Show that we can prove that \( P(n, k) \) is true for all pairs of positive integers \( n \) and \( k \) if we show
   a) \( P(1, 1) \) is true and \( P(n, k) \rightarrow [P(n + 1, k) \land P(n, k + 1)] \) is true for all positive integers \( n \) and \( k \).
   b) \( P(1, k) \) is true for all positive integers \( k \), and \( P(n, k) \rightarrow P(n + 1, k) \) is true for all positive integers \( n \) and \( k \).
   c) \( P(n, 1) \) is true for all positive integers \( n \), and \( P(n, k) \rightarrow P(n, k + 1) \) is true for all positive integers \( n \) and \( k \).

34. Prove that \( \sum_{j=1}^{n} j(j+1)(j+2) \cdots (j+k-1) = n(n+1)(n+2) \cdots (n+k)/(k+1) \) for all positive integers \( k \) and \( n \). [Hint: Use a technique from Exercise 33.]

35. Show that if \( a_1, a_2, \ldots, a_n \) are \( n \) distinct real numbers, exactly \( n - 1 \) multiplications are used to compute the product of these \( n \) numbers no matter how parentheses are inserted into their product. [Hint: Use strong induction and consider the last multiplication.]

36. The well-ordering property can be used to show that there is a unique greatest common divisor of two positive integers. Let \( a \) and \( b \) be positive integers, and let \( S \) be the set of positive integers of the form \( as + bt \), where \( s \) and \( t \) are integers.
   a) Show that \( S \) is nonempty.
   b) Use the well-ordering property to show that \( S \) has a smallest element \( c \).
   c) Show that if \( d \) is a common divisor of \( a \) and \( b \), then \( d \) is a divisor of \( c \).
   d) Show that \( c \mid a \) and \( c \mid b \). [Hint: First, assume that \( c \not\mid a \). Then \( a = qc + r \), where \( 0 < r < c \). Show that \( r \in S \), contradicting the choice of \( c \).]
   e) Conclude from (c) and (d) that the greatest common divisor of \( a \) and \( b \) exists. Finish the proof by showing that this greatest common divisor is unique.

37. Let \( a \) be an integer and \( d \) be a positive integer. Show that the integers \( q \) and \( r \) with \( a = dq + r \) and \( 0 \leq r < d \), which were shown to exist in Example 5, are unique.

38. Use mathematical induction to show that a rectangular checkerboard with an even number of cells and two squares missing, one white and one black, can be covered by dominoes.

39. Can you use the well-ordering property to prove the statement: “Every positive integer can be described using no more than fifteen English words”? Assume the words come from a particular dictionary of English. [Hint: Suppose that there are positive integers that cannot be described using no more than fifteen English words. By well ordering, the smallest positive integer that cannot be described using no more than fifteen English words would then exist.]

40. Use the well-ordering principle to show that if \( x \) and \( y \) are real numbers with \( x < y \), then there is a rational number \( r \) with \( x < r < y \). [Hint: Use the Archimedean property, given in Appendix 1, to find a positive integer \( A \) with \( A > 1/(y - x) \). Then show that there is a rational number \( r \) with denominator \( A \) between \( x \) and \( y \) by looking at the numbers \( \lfloor x \rfloor + j/A \), where \( j \) is a positive integer.]

41. Show that the well-ordering property can be proved when the principle of mathematical induction is taken as an axiom.

42. Show that the principle of mathematical induction and strong induction are equivalent; that is, each can be shown to be valid from the other.

43. Show that we can prove the well-ordering property when we take either the principle of mathematical induction or strong induction as an axiom instead of taking the well-ordering property as an axiom.

4.3 Recursive Definitions and Structural Induction

Introduction

Sometimes it is difficult to define an object explicitly. However, it may be easy to define this object in terms of itself. This process is called recursion. For instance, the picture shown in Figure 1 is produced recursively. First, an original picture is given. Then a process of successively superimposing centered smaller pictures on top of the previous pictures is carried out.

We can use recursion to define sequences, functions, and sets. In previous discussions, we specified the terms of a sequence using an explicit formula. For instance, the sequence of powers of 2 is given by \( a_n = 2^n \) for \( n = 0, 1, 2, \ldots \) However, this sequence can also be defined by giving the first term of the sequence, namely, \( a_0 = 1 \), and a rule for finding a term of the
Exercises

1. Find \( f(1), f(2), f(3), \) and \( f(4) \) if \( f(n) \) is defined recursively by \( f(0) = 1 \) and for \( n = 0, 1, 2, \ldots \)
   a) \( f(n + 1) = f(n) + 2 \).
   b) \( f(n + 1) = 3f(n) \).
   c) \( f(n + 1) = 2f(n) \).
   d) \( f(n + 1) = f(n)^2 + f(n) + 1 \).

2. Find \( f(1), f(2), f(3), \) and \( f(5) \) if \( f(n) \) is defined recursively by \( f(0) = 3 \) for \( n = 0, 1, 2, \ldots \)
   a) \( f(n + 1) = -2f(n) \).
   b) \( f(n + 1) = 3f(n) + 7 \).
   c) \( f(n + 1) = f(n)^2 - 2f(n) - 2 \).
   d) \( f(n + 1) = 3f(n) + 7 \).

3. Find \( f(2), f(3), f(4), \) and \( f(5) \) if \( f \) is defined recursively by \( f(0) = -1, f(1) = 2 \) and for \( n = 1, 2, \ldots \)
   a) \( f(n + 1) = f(n) + 3f(n - 1) \).
   b) \( f(n + 1) = f(n)^2 - f(n - 1) \).
   c) \( f(n + 1) = 3f(n)^2 - 4f(n - 1)^2 \).
   d) \( f(n + 1) = f(n - 1)/f(n) \).

4. Find \( f(2), f(3), f(4), \) and \( f(5) \) if \( f \) is defined recursively by \( f(0) = f(1) = 1 \) and for \( n = 1, 2, \ldots \)
   a) \( f(n + 1) = f(n) - f(n - 1) \).
   b) \( f(n + 1) = f(n)f(n - 1) \).
   c) \( f(n + 1) = f(n)^2 + f(n - 1)^3 \).
   d) \( f(n + 1) = f(n)f(n - 1) \).

5. Determine whether each of these proposed definitions is a valid recursive definition of a function \( f \) from the set of nonnegative integers to the set of integers. If \( f \) is well defined, find a formula for \( f(n) \) when \( n \) is a nonnegative integer and prove that your formula is valid.
   a) \( f(0) = 0, f(n) = 2f(n - 2) \) for \( n \geq 1 \)
   b) \( f(0) = 1, f(n) = f(n - 1) - 1 \) for \( n \geq 1 \)
   c) \( f(0) = 2, f(1) = 3, f(n) = f(n - 2) + f(n - 1) \) for \( n \geq 2 \)
   d) \( f(0) = 2, f(1) = 3, f(n) = 2f(n - 2) + f(n - 1) \) for \( n \geq 2 \)
   e) \( f(0) = 1, f(n) = 3f(n - 1) \) if \( n \) is odd and \( n \geq 1 \) and \( f(n) = 9f(n - 2) \) if \( n \) is even and \( n \geq 2 \)

6. Determine whether each of these proposed definitions is a valid recursive definition of a function \( f \) from the set of nonnegative integers to the set of integers. If \( f \) is well defined, find a formula for \( f(n) \) when \( n \) is a nonnegative integer and prove that your formula is valid.
   a) \( f(0) = 1, f(n) = -f(n - 1) \) for \( n \geq 1 \)
   b) \( f(0) = 1, f(1) = 0, f(2) = 2, f(n) = 2f(n - 3) \) for \( n \geq 3 \)
   c) \( f(0) = 0, f(1) = 1, f(n) = 2f(n + 1) \) for \( n \geq 2 \)
   d) \( f(0) = 0, f(1) = 1, f(n) = 2f(n - 1) \) for \( n \geq 1 \)
   e) \( f(0) = 2, f(n) = f(n - 1) \) if \( n \) is odd and \( n \geq 1 \) and \( f(n) = 2f(n - 2) \) if \( n \geq 2 \)

7. Give a recursive definition of the sequence \( \{a_n\} \), \( n = 1, 2, 3, \ldots \)
   a) \( a_n = 6n \)
   b) \( a_n = 2n + 1 \)
   c) \( a_n = 10^n \)
   d) \( a_n = 5 \)

8. Give a recursive definition of the sequence \( \{a_n\} \), \( n = 1, 2, 3, \ldots \)
   a) \( a_n = 4n - 2 \)
   b) \( a_n = 1 + (-1)^n \)
   c) \( a_n = n(n + 1) \)
   d) \( a_n = n^2 \)

9. Let \( F \) be the function such that \( F(n) \) is the sum of the first \( n \) positive integers. Give a recursive definition of \( F(n) \).

10. Give a recursive definition of \( S_m(n) \), the sum of the integer \( m \) and the nonnegative integer \( n \).

In Exercises 12–19 \( f_n \) is the \( n \)th Fibonacci number.

12. Prove that \( f_1^2 + f_2^2 + \cdots + f_n^2 = f_n f_{n+1} \) when \( n \) is a positive integer.

13. Prove that \( f_1 + f_3 + \cdots + f_{2n-1} = f_{2n} \) when \( n \) is a positive integer.

14. Show that \( f_{n+1} f_{n-1} - f_n^2 = (-1)^n \) when \( n \) is a positive integer.

15. Show that \( f_0 f_1 + f_1 f_2 + \cdots + f_{2n-2} f_{2n-1} = f_{2n}^2 \) when \( n \) is a positive integer.

16. Show that \( f_0 - f_1 + f_2 - \cdots - f_{2n-1} + f_{2n} = f_{2n-1} - 1 \) when \( n \) is a positive integer.

17. Determine the number of divisions used by the Euclidean algorithm to find the greatest common divisor of the Fibonacci numbers \( f_n \) and \( f_{n+1} \), where \( n \) is a nonnegative integer. Verify your answer using mathematical induction.

18. Let
   \[
   A = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}
   \]
   Show that
   \[
   A^n = \begin{bmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{bmatrix}
   \]
   when \( n \) is a positive integer.
19. By taking determinants of both sides of the equation in Exercise 18, prove the identity given in Exercise 14. (Recall that the determinant of the matrix \( \begin{vmatrix} a & b \\ c & d \end{vmatrix} \) is \( ad - bc \).)

20. Give a recursive definition of the functions \( \max \) and \( \min \) so that \( \max(a_1, a_2, \ldots, a_n) \) and \( \min(a_1, a_2, \ldots, a_n) \) are the maximum and minimum of the \( n \) numbers \( a_1, a_2, \ldots, a_n \), respectively.

21. Let \( a_1, a_2, \ldots, a_n \), and \( b_1, b_2, \ldots, b_n \) be real numbers. Use the recursive definitions that you gave in Exercise 20 to prove these.
   a) \( \max(-a_1, -a_2, \ldots, -a_n) = -\min(a_1, a_2, \ldots, a_n) \)
   b) \( \max(a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n) \leq \max(a_1, a_2, \ldots, a_n) + \max(b_1, b_2, \ldots, b_n) \)
   c) \( \min(a_1 + b_1, a_2 + b_2, \ldots, a_n + b_n) \geq \min(a_1, a_2, \ldots, a_n) + \min(b_1, b_2, \ldots, b_n) \)

22. Show that the set \( S \) defined by \( 1 \in S \) and \( s + t \in S \) whenever \( s \in S \) and \( t \in S \) is the set of positive integers.

23. Give a recursive definition of the set of positive integers that are multiples of 5.

24. Give a recursive definition of
   a) the set of odd positive integers.
   b) the set of positive integer powers of 3.
   c) the set of polynomials with integer coefficients.

25. Give a recursive definition of
   a) the set of even integers.
   b) the set of positive integers congruent to 2 modulo 3.
   c) the set of positive integers not divisible by 5.

26. Let \( S \) be the subset of the set of ordered pairs of integers defined recursively by
    Basis step: \((0, 0) \in S\).
    Recursive step: If \((a, b) \in S\), then \((a + 2, b + 3) \in S\) and \((a + 3, b + 2) \in S\).
    a) List the elements of \( S \) produced by the first five applications of the recursive definition.
    b) Use strong induction on the number of applications of the recursive step of the definition to show that \( 5 \mid a + b \) when \((a, b) \in S\).
    c) Use structural induction to show that \( 5 \mid a + b \) when \((a, b) \in S\).

27. Let \( S \) be the subset of the set of ordered pairs of integers defined recursively by
    Basis step: \((0, 0) \in S\).
    Recursive step: If \((a, b) \in S\), then \((a + b + 1) \in S\), \((a + 1, b + 1) \in S\), and \((a + 2, b + 1) \in S\).
    a) List the elements of \( S \) produced by the first four applications of the recursive definition.
    b) Use strong induction on the number of applications of the recursive step of the definition to show that \( a \leq 2b \) whenever \((a, b) \in S\).
    c) Use structural induction to show that \( a \leq 2b \) whenever \((a, b) \in S\).

28. Give a recursive definition of each of these sets of ordered pairs of positive integers. [Hint: Plot the points in the set in the plane and look for lines containing points in the set.]
   a) \( S = \{(a, b) \mid a \in \mathbb{Z}^+, b \in \mathbb{Z}^+, \text{ and } a + b \text{ is odd}\} \)
   b) \( S = \{(a, b) \mid a \in \mathbb{Z}^+, b \in \mathbb{Z}^+, \text{ and } a \mid b\} \)
   c) \( S = \{(a, b) \mid a \in \mathbb{Z}^+, b \in \mathbb{Z}^+, \text{ and } 3 \mid a + b\} \)

29. Give a recursive definition of each of these sets of ordered pairs of positive integers. Use structural induction to prove that the recursive definition you found is correct. [Hint: To find a recursive definition, plot the points in the set in the plane and look for patterns.]
   a) \( S = \{(a, b) \mid a \in \mathbb{Z}^+, b \in \mathbb{Z}^+, \text{ and } a + b \text{ is even}\} \)
   b) \( S = \{(a, b) \mid a \in \mathbb{Z}^+, b \in \mathbb{Z}^+, \text{ and } a \text{ or } b \text{ is odd}\} \)
   c) \( S = \{(a, b) \mid a \in \mathbb{Z}^+, b \in \mathbb{Z}^+, a + b \text{ is odd, and } 3 \mid b\} \)

30. Prove that in a bit string, the string 01 occurs at most one more time than the string 10.

31. Define well-formed formulae of sets, variables representing sets, and operators from \{-, \cup, \cap, \cdot, \}_\text{.}

32. a) Give a recursive definition of the function \( \text{ones}(s) \), which counts the number of ones in a bit string \( s \).
   b) Use structural induction to prove that \( \text{ones}(st) = \text{ones}(s) + \text{ones}(t) \).

33. a) Give a recursive definition of the function \( \text{m}(s) \), which counts the number of ones in a nonempty string of decimal digits.
   b) Use structural induction to prove that \( \text{m}(st) = \min(\text{m}(s), \text{m}(t)) \).

   The reversal of a string is the string consisting of the symbols of the string in reverse order. The reversal of the string \( w \) is denoted by \( w^R \).

34. Find the reversal of the following bit strings.
   a) 0101
   b) 11011
   c) 1000100111

35. Give a recursive definition of the reversal of a string. [Hint: First define the reversal of the empty string. Then write a string \( w \) of length \( n + 1 \) as \( xy \), where \( x \) is a string of length \( n \), and express the reversal of \( w \) in terms of \( x^R \) and \( y \).]

36. Use structural induction to prove that \( (w_1w_2)^R = w_2^Rw_1^R \).

37. Give a recursive definition of \( w^i \), where \( w \) is a string and \( i \) is a nonnegative integer. (Here \( w^i \) represents the concatenation of \( i \) copies of the string \( w \).)

38. Give a recursive definition of the set of bit strings that are palindromes.

39. When does a string belong to the set \( A \) of bit strings defined recursively by
   \[
   \lambda \in A \\
   0x1 \in A \text{ if } x \in A,
   \]
   where \( \lambda \) is the empty string?

40. Recursively define the set of bit strings that have more zeros than ones.

41. Use Exercise 37 and mathematical induction to show that \( l(w^i) = i \cdot l(w) \), where \( w \) is a string and \( i \) is a nonnegative integer.
42. Show that \((w^i)^r = (w^r)^i\) whenever \(w\) is a string and \(i\) is a nonnegative integer; that is, show that the \(i\)th power of the reversal of a string is the reversal of the \(i\)th power of the string.

43. Use structural induction to show that \(n(T) \geq 2h(T) + 1\), where \(T\) is a full binary tree, \(n(T)\) equals the number of vertices of \(T\), and \(h(T)\) is the height of \(T\).

The set of leaves and the set of internal vertices of a full binary tree can be defined recursively.

Basis step: The root \(r\) is a leaf of the full binary tree with exactly one vertex \(r\). This tree has no internal vertices.

Recursive step: The set of leaves of the tree \(T = T_1 \cdot T_2\) is the union of the set of leaves of \(T_1\) and the set of leaves of \(T_2\). The internal vertices of \(T\) are the root \(r\) of \(T\) and the union of the set of internal vertices of \(T_1\) and the set of internal vertices of \(T_2\).

44. Use structural induction to show that \(l(T)\), the number of leaves of a full binary tree \(T\), is 1 more than \(i(T)\), the number of internal vertices of \(T\).

45. Use generalized induction as was done in Example 15 to show that if \(a_{m,n}\) is defined recursively by \(a_{0,0} = 0\) and

\[
a_{m,n} = \begin{cases} 
    a_{m-1,n} + 1 & \text{if } n \leq m > 0 \\
    a_{m,n-1} + 1 & \text{if } n > 0,
\end{cases}
\]

then \(a_{m,n} = m + n\) for all \((m, n) \in \mathbb{N} \times \mathbb{N}\).

46. Use generalized induction as was done in Example 15 to show that if \(a_{m,n}\) is defined recursively by \(a_{1,1} = 5\) and

\[
a_{m,n} = \begin{cases} 
    a_{m-1,n} + 2 & \text{if } n = 1 \text{ and } m > 1 \\
    a_{m,n-1} + 2 & \text{if } n > 1,
\end{cases}
\]

then \(a_{m,n} = 2(m + n) + 1\) for all \((m, n) \in \mathbb{Z}^+ \times \mathbb{Z}^+\).

47. A partition of a positive integer \(n\) is a way to write \(n\) as a sum of positive integers where the order of terms in the sum does not matter. For instance, \(7 = 3 + 2 + 1 + 1\) is a partition of 7. Let \(P_m\) equal the number of different partitions of \(m\), and let \(P_{m,n}\) be the number of different ways to express \(m\) as the sum of positive integers not exceeding \(n\).

a) Show that \(P_{m,m} = P_m\).

b) Show that the following recursive definition for \(P_{m,n}\) is correct:

\[
P_{m,n} = \begin{cases} 
    1 & \text{if } m = 1 \\
    1 & \text{if } n = 1 \\
    P_{m,m} & \text{if } m < n \\
    1 + P_{m,m-1} & \text{if } m = n > 1 \\
    P_{m,n-1} + P_{m-n,n} & \text{if } m > n > 1.
\end{cases}
\]

c) Find the number of partitions of 5 and of 6 using this recursive definition.

Consider an inductive definition of a version of Ackermann's function. This function was named after Wilhelm Ackermann, a German mathematician who was a student of the great mathematician David Hilbert. Ackermann's function plays an important role in the theory of recursive functions and in the study of the complexity of certain algorithms involving set unions. (There are several different variants of this function. All are called Ackermann's function and have similar properties even though their values do not always agree.)

\[
A(m, n) = \begin{cases} 
    2n & \text{if } m = 0 \\
    0 & \text{if } m \geq 1 \text{ and } n = 0 \\
    2 & \text{if } m \geq 1 \text{ and } n = 1 \\
    A(m-1, A(m, n-1)) & \text{if } m \geq 1 \text{ and } n \geq 2.
\end{cases}
\]

Exercises 48–55 involve this version of Ackermann's function.

48. Find these values of Ackermann's function.

a) \(A(1, 0)\) 

b) \(A(0, 1)\)

c) \(A(1, 1)\) 

d) \(A(2, 2)\)

49. Show that \(A(m, 2) = 4\) whenever \(m \geq 1\).

50. Show that \(A(1, n) = 2^n\) whenever \(n \geq 1\).

51. Find these values of Ackermann's function.

a) \(A(2, 3)\) 

b) \(A(3, 3)\)

*52. Find \(A(3, 4)\).

**53. Prove that \(A(m, n + 1) > A(m, n)\) whenever \(m\) and \(n\) are nonnegative integers.

54. Prove that \(A(m + 1, n) \geq A(m, n)\) whenever \(m\) and \(n\) are nonnegative integers.

55. Prove that \(A(i, j) \geq j\) whenever \(i\) and \(j\) are nonnegative integers.

56. Use mathematical induction to prove that a function \(F\) defined by specifying \(F(0)\) and a rule for obtaining \(F(n + 1)\) from \(F(n)\) is well defined.

57. Use strong induction to prove that a function \(F\) defined by specifying \(F(0)\) and a rule for obtaining \(F(n + 1)\) from the values \(F(k)\) for \(k = 0, 1, 2, \ldots, n\) is well defined.

58. Show that each of these proposed recursive definitions of a function on the set of positive integers does not produce a well-defined function.

a) \(F(n) = 1 + F((n/2))\) for \(n \geq 1\) and \(F(1) = 1\).

b) \(F(n) = 1 + F(n - 3)\) for \(n \geq 2\), \(F(1) = 2\), and \(F(2) = 3\).

c) \(F(n) = 1 + F(n/2)\) for \(n \geq 2\), \(F(1) = 1\), and \(F(2) = 2\).

d) \(F(n) = 1 + F(n/2)\) if \(n\) is even and \(n \geq 2\), \(F(n) = 1 - F(n - 1)\) if \(n\) is odd, and \(F(1) = 1\).

e) \(F(n) = 1 + F(n/2)\) if \(n\) is even and \(n \geq 2\), \(F(n) = F(3n - 1)\) if \(n\) is odd and \(n \geq 3\), and \(F(1) = 1\).

59. Show that each of these proposed recursive definitions of a function on the set of positive integers does not produce a well-defined function.

a) \(F(n) = 1 + F((n + 1)/2))\) for \(n \geq 1\) and \(F(1) = 1\).

b) \(F(n) = 1 + F(n - 2)\) for \(n \geq 2\) and \(F(1) = 0\).

c) \(F(n) = 1 + F(n/3)\) for \(n \geq 3\), \(F(1) = 1\), \(F(2) = 2\), and \(F(3) = 3\).

d) \(F(n) = 1 + F(n/2)\) if \(n\) is even and \(n \geq 2\), \(F(n) = 1 + F(n - 2)\) if \(n\) is odd, and \(F(1) = 1\).

e) \(F(n) = 1 + F(F(n - 1))\) if \(n \geq 2\) and \(F(1) = 2\).
Exercises 60–62 deal with iterations of the logarithm function. Let \( \log n \) denote the logarithm of \( n \) to the base 2, as usual. The function \( \log^k n \) is defined recursively by

\[
\log^k n = \begin{cases} 
  n & \text{if } k = 0 \\
  \log(\log^{k-1}(n)) & \text{if } \log^{k-1}(n) \text{ is defined and positive} \\
  \text{undefined} & \text{otherwise.}
\end{cases}
\]

The **iterated logarithm** is the function \( \log^* n \) whose value at \( n \) is the smallest nonnegative integer \( k \) such that \( \log^k n \leq 1 \).

60. Find each of these values:
   a) \( \log^2 16 \)
   b) \( \log^3 256 \)
   c) \( \log^3 65536 \)
   d) \( \log^4 2^{2048} \)

61. Find the value of \( \log^* n \) for each of these values of \( n \):
   a) 2   b) 4   c) 8   d) 16   e) 256   f) 65536   g) 2^{1048}

62. Find the largest integer \( n \) such that \( \log^* n = 5 \). Determine the number of decimal digits in this number.

4.4 Recursive Algorithms

**Introduction**

Sometimes we can reduce the solution to a problem with a particular set of input to the solution of the same problem with smaller input values. For instance, the problem of finding the greatest common divisor of two positive integers \( a \) and \( b \), where \( b > a \), can be reduced to finding the greatest common divisor of a pair of smaller integers, namely, \( b \mod a \) and \( a \), because \( \gcd(b \mod a, a) = \gcd(a, b) \). When such a reduction can be done, the solution to the original problem can be found with a sequence of reductions, until the problem has been reduced to some initial case for which the solution is known. For instance, for finding the greatest common divisor, the reduction continues until the smaller of the two numbers is zero, because \( \gcd(a, 0) = a \) when \( a > 0 \).

We will see that algorithms that successively reduce a problem to the same problem with smaller input are used to solve a wide variety of problems.

**DEFINITION 1** An algorithm is called **recursive** if it solves a problem by reducing it to an instance of the same problem with smaller input.

**Links** We will describe a variety of different recursive algorithms in this section.

**EXAMPLE 1** Give a recursive algorithm for computing \( n! \), where \( n \) is a nonnegative integer.

**Solution:** We can build a recursive algorithm that finds \( n! \), where \( n \) is a nonnegative integer, based on the recursive definition of \( n! \), which specifies that \( n! = n \cdot (n - 1)! \) when \( n \) is a positive integer, and that \( 0! = 1 \). To find \( n! \) for a particular integer, we use the recursive step \( n \) times, each time replacing a value of the factorial function with the value of the factorial function at
The number of comparisons needed to merge sort a list with \( n \) elements is \( O(n \log n) \).

**Exercises**

1. Trace Algorithm 1 when it is given \( n = 5 \) as input. That is, show all steps used by Algorithm 1 to find \( 5! \), as is done in Example 1 to find \( 4! \).
2. Trace Algorithm 1 when it is given \( n = 6 \) as input. That is, show all steps used by Algorithm 1 to find \( 6! \), as is done in Example 1 to find \( 4! \).
3. Trace Algorithm 3 when it is given \( m = 5, n = 11 \), and \( b = 3 \) as input. That is, show all the steps Algorithm 3 uses to find \( 3^{11} \mod 5 \).
4. Trace Algorithm 3 when it is given \( m = 7, n = 10 \), and \( b = 2 \) as input. That is, show all the steps Algorithm 3 uses to find \( 2^{10} \mod 7 \).
5. Trace Algorithm 4 when it finds \( \gcd(8, 13) \). That is, show all the steps used by Algorithm 4 to find \( \gcd(8, 13) \).
6. Trace Algorithm 4 when it finds \( \gcd(12, 17) \). That is, show all the steps used by Algorithm 4 to find \( \gcd(12, 17) \).
7. Give a recursive algorithm for computing \( nx \) whenever \( n \) is a positive integer and \( x \) is an integer, using just addition.
8. Give a recursive algorithm for finding the sum of the first \( n \) positive integers.
9. Give a recursive algorithm for finding the sum of the first \( n \) odd positive integers.
10. Give a recursive algorithm for finding the maximum of a finite set of integers, making use of the fact that the maximum of \( n \) integers is the larger of the last integer in the list and the maximum of the first \( n - 1 \) integers in the list.
11. Give a recursive algorithm for finding the minimum of a finite set of integers, making use of the fact that the minimum of \( n \) integers is the smaller of the last integer in the list and the minimum of the first \( n - 1 \) integers in the list.
12. Devise a recursive algorithm for finding \( x^n \mod m \) whenever \( n, x, \) and \( m \) are positive integers based on the fact that \( x^n \mod m = (x^{n-1} \mod m \cdot x \mod m) \mod m \).
13. Give a recursive algorithm for finding \( n! \mod m \) whenever \( n \) and \( m \) are positive integers.
14. Give a recursive algorithm for finding a mode of a list of integers. (A mode is an element in the list that occurs at least as often as every other element.)
15. Devise a recursive algorithm for computing the greatest common divisor of two nonnegative integers \( a \) and \( b \) with \( a < b \) using the fact that \( \gcd(a, b) = \gcd(a, b - a) \).
16. Prove that the recursive algorithm for finding the sum of the first \( n \) positive integers you found in Exercise 8 is correct.
17. Devise a recursive algorithm for multiplying two nonnegative integers \( x \) and \( y \) based on the fact that \( xy = 2(x \cdot \lfloor y/2 \rfloor) + x \) when \( y \) is odd, together with the initial condition \( xy = 0 \) when \( y = 0 \).
18. Prove that Algorithm 1 for computing \( n! \) when \( n \) is a nonnegative integer is correct.
19. Prove that Algorithm 4 for computing \( \gcd(a, b) \) when \( a \) and \( b \) are positive integers with \( a < b \) is correct.
20. Prove that the algorithm you devised in Exercise 11 is correct.
21. Prove that the recursive algorithm that you found in Exercise 7 is correct.
22. Prove that the recursive algorithm that you found in Exercise 10 is correct.
23. Devise a recursive algorithm for computing \( n^2 \) where \( n \) is a nonnegative integer using the fact that \( (n + 1)^2 = n^2 + 2n + 1 \). Then prove that this algorithm is correct.
24. Devise a recursive algorithm to find \( a^{2^n} \), where \( a \) is a real number and \( n \) is a positive integer. [Hint: Use the equality \( a^{2^n} = (a^{2^{n-1}})^2 \).]
25. How does the number of multiplications used by the algorithm in Exercise 24 compare to the number of multiplications used by Algorithm 2 to evaluate \( a^{2^n} \)?
26. Use the algorithm in Exercise 24 to devise an algorithm for evaluating \( a^n \) when \( n \) is a nonnegative integer. [Hint: Use the binary expansion of \( n \).]
27. How does the number of multiplications used by the algorithm in Exercise 26 compare to the number of multiplications used by Algorithm 2 to evaluate \( a^n \)?
28. How many additions are used by the recursive and iterative algorithms given in Algorithms 7 and 8, respectively, to find the Fibonacci number \( f_n \)?
29. Devise a recursive algorithm to find the \( n \)th term of the sequence defined by \( a_0 = 1, a_1 = 2, \) and \( a_n = a_{n-1} \cdot a_{n-2} \), for \( n = 2, 3, 4, \ldots \).
30. Devise an iterative algorithm to find the \( n \)th term of the sequence defined in Exercise 29.
31. Is the recursive or the iterative algorithm for finding the sequence in Exercise 29 more efficient?

32. Devise a recursive algorithm to find the \( n \)th term of the sequence defined by \( a_0 = 1, a_1 = 2, a_2 = 3, \) and \( a_n = a_{n-1} + a_{n-2} + a_{n-3}, \) for \( n = 3, 4, 5, \ldots \)

33. Devise an iterative algorithm to find the \( n \)th term of the sequence defined in Exercise 32.

34. Is the recursive or the iterative algorithm for finding the sequence in Exercise 32 more efficient?

35. Give iterative and recursive algorithms for finding the \( n \)th term of the sequence defined by \( a_0 = 1, a_1 = 3, a_2 = 5, \) and \( a_n = a_{n-1} \cdot a_{n-2} \cdot a_{n-3}. \) Which is more efficient?

36. Give a recursive algorithm to find the number of partitions of a positive integer based on the recursive definition given in Exercise 48 in Section 4.3.

37. Give a recursive algorithm for finding the reversal of a bit string. (See the definition of the reversal of a bit string in the preamble of Exercise 34 in Section 4.3.)

38. Give a recursive algorithm for finding the string \( w^i \), the concatenation of \( i \) copies of \( w \), when \( w \) is a bit string.

39. Prove that the recursive algorithm for finding the reversal of a bit string that you gave in Exercise 37 is correct.

40. Prove that the recursive algorithm for finding the concatenation of \( i \) copies of a bit string that you gave in Exercise 38 is correct.

41. Give a recursive algorithm for tiling a \( 2^n \times 2^n \) checkerboard with one square missing using right triominoes.

42. Give a recursive algorithm for triangulating a simple polygon with \( n \) sides, using Lemma 1 in Section 4.2.

43. Give a recursive algorithm for computing values of the Ackermann function. [Hint: See the preamble to Exercise 38 in Section 4.3.]

44. Use a merge sort to sort 4, 3, 2, 5, 1, 8, 7, 6. Show all the steps used by the algorithm.

45. Use a merge sort to sort \( b, d, a, f, g, h, z, p, o, k. \) Show all the steps used by the algorithm.

46. How many comparisons are required to merge these pairs of lists using Algorithm 10?
   a) 1, 3, 5, 7, 9; 2, 4, 6, 8, 10
   b) 1, 2, 3, 4, 5; 6, 7, 8, 9, 10
   c) 1, 5, 6, 7, 8; 2, 3, 4, 9, 10

47. Show that for all positive integers \( m \) and \( n \) there are lists with \( m \) elements and \( n \) elements, respectively, such that Algorithm 10 uses \( m + n - 1 \) comparisons to merge them into one sorted list.

48. What is the least number of comparisons needed to merge any two lists in increasing order into one list in increasing order when the number of elements in the two lists are
   a) 1, 4?  
   b) 2, 4?  
   c) 3, 4?  
   d) 4, 4?

49. Prove that the merge sort algorithm is correct.

The quick sort is an efficient algorithm. To sort \( a_1, a_2, \ldots, a_n, \) this algorithm begins by taking the first element \( a_1 \) and forming two sublists, the first containing those elements that are less than \( a_1, \) in the order they arise, and the second containing those elements greater than \( a_1, \) in the order they arise. Then \( a_1 \) is put at the end of the first sublist. This procedure is repeated recursively for each sublist, until all sublists contain one item. The ordered list of \( n \) items is obtained by combining the sublists of one item in the order they occur.

50. Sort 3, 5, 7, 8, 1, 9, 2, 4, 6 using the quick sort.

51. Let \( a_1, a_2, \ldots, a_n \) be a list of \( n \) distinct real numbers. How many comparisons are needed to form two sublists from this list, the first containing elements less than \( a_1 \) and the second containing elements greater than \( a_1? \)

52. Describe the quick sort algorithm using pseudocode.

53. What is the largest number of comparisons needed to order a list of four elements using the quick sort algorithm?

54. What is the least number of comparisons needed to order a list of four elements using the quick sort algorithm?

55. Determine the worst-case complexity of the quick sort algorithm in terms of the number of comparisons used.

### 4.5 Program Correctness

**Introduction**

Suppose that we have designed an algorithm to solve a problem and have written a program to implement it. How can we be sure that the program always produces the correct answer? After all the bugs have been removed so that the syntax is correct, we can test the program with sample input. It is not correct if an incorrect result is produced for any sample input. But even if the program gives the correct answer for all sample input, it may not always produce the correct answer (unless all possible input has been tested). We need a proof to show that the program always gives the correct output.

Program verification, the proof of correctness of programs, uses the rules of inference and proof techniques described in this chapter, including mathematical induction. Because an incorrect program can lead to disastrous results, a large amount of methodology has been constructed for verifying programs. Efforts have been devoted to automating program verification so that it
Recursive definition of a set: a definition of a set that specifies an initial set of elements in the set and a rule for obtaining other elements from those in the set.

Structural induction: a technique for proving results about recursively defined sets.

Recursive algorithm: an algorithm that proceeds by reducing a problem to the same problem with smaller input.

Merge sort: a sorting algorithm that sorts a list by splitting it in two, sorting each of the two resulting lists, and merging the results into a sorted list.

Review Questions

1. a) Can you use the principle of mathematical induction to find a formula for the sum of the first n terms of a sequence? b) Can you use the principle of mathematical induction to determine whether a given formula for the sum of the first n terms of a sequence is correct? c) Find a formula for the sum of the first n even positive integers, and prove it using mathematical induction.

2. a) For which positive integers n is 11n + 17 ≤ 2^n? b) Prove the conjecture you made in part (a) using mathematical induction.

3. a) Which amounts of postage can be formed using only 5-cent and 9-cent stamps? b) Prove the conjecture you made using mathematical induction. c) Prove the conjecture you made using strong induction. d) Find a proof of your conjecture different from the ones you gave in (b) and (c).

4. Give two different examples of proofs that use strong induction.

5. a) State the well-ordering property for the set of positive integers. b) Use this property to show that every positive integer can be written as the product of primes.

6. a) Explain why a function is well-defined if it is defined recursively by specifying f(1) and a rule for finding f(n) from f(n - 1). b) Provide a recursive definition of the function f(n) = (n + 1)!. c) Give a recursive definition of the Fibonacci numbers. b) Show that f_n > α^{n-2} whenever n ≥ 3, where f_n is the nth term of the Fibonacci sequence and α = (1 + √5)/2.

7. a) Explain why a sequence a_n is well defined if it is defined recursively by specifying a_1 and a_2 and a rule for finding a_n from a_1, a_2, ..., a_{n-1} for n = 3, 4, 5, ........ b) Find the value of a_n if a_1 = 1, a_2 = 2, and a_n = a_{n-1} + a_{n-2} + ... + a_1, for n = 3, 4, 5, ........

8. a) Give a recursive definition of the length of a string. b) Use the recursive definition from part (a) and structural induction to prove that l(xy) = l(x) + l(y).

9. Give two examples of how well-formed formulae are defined recursively for different sets of elements and operators.

10. a) Give a recursive definition of the greatest common divisor of two positive integers. b) Use the merge sort algorithm to put the list 4, 10, 1, 5, 3, 8, 7, 2, 6, 9 in increasing order. c) Give a big-O estimate for the number of comparisons used by the merge sort.

12. Describe a recursive algorithm for computing the greatest common divisor of two positive integers.

13. a) Describe the merge sort algorithm. b) Use the merge sort algorithm to put the list 4, 10, 1, 5, 3, 8, 7, 2, 6, 9 in increasing order. c) Give a big-O estimate for the number of comparisons used by the merge sort.

14. a) Does testing a computer program to see whether it produces the correct output for certain input values verify that the program always produces the correct output? b) Does showing that a computer program is partially correct with respect to an initial assertion and a final assertion verify that the program always produces the correct output? If not, what else is needed?

15. What techniques can you use to show that a long computer program is partially correct with respect to an initial assertion and a final assertion?

16. What is a loop invariant? How is a loop invariant used?

Supplementary Exercises

1. Use mathematical induction to show that \(\frac{2}{3} + \frac{2}{5} + \frac{2}{7} + \cdots + \frac{2}{3^n} = 1 - \frac{1}{3^n}\) whenever n is a positive integer.

2. Use mathematical induction to show that \(1^3 + 3^3 + 5^3 + \cdots + (2n + 1)^3 = (n + 1)^2(2n^2 + 4n + 1)\) whenever n is a positive integer.
3. Use mathematical induction to show that \( 1 \cdot 2^0 + 2 \cdot 2^1 + 3 \cdot 2^2 + \cdots + n \cdot 2^{n-1} = (n-1) \cdot 2^n + 1 \) whenever \( n \) is a positive integer.

4. Use mathematical induction to show that
   \[
   \frac{1}{1 \cdot 3} + \frac{1}{3 \cdot 5} + \cdots + \frac{1}{(2n-1)(2n+1)} = \frac{n}{2n+1}
   \]
   whenever \( n \) is a positive integer.

5. Show that
   \[
   \frac{1}{1 \cdot 4} + \frac{1}{4 \cdot 7} + \cdots + \frac{1}{(3n-2)(3n+1)} = \frac{n}{3n+1}
   \]
   whenever \( n \) is a positive integer.

6. Use mathematical induction to show that \( 2^n > n^2 + n \) whenever \( n \) is an integer greater than 4.

7. Use mathematical induction to show that \( 2^n > n^3 \) whenever \( n \) is an integer greater than 9.

8. Find an integer \( N \) such that \( 2^n > n^4 \) whenever \( n \) is greater than \( N \). Prove that your result is correct using mathematical induction.

9. Use mathematical induction to prove that \( a - b \) is a factor of \( a^n - b^n \) whenever \( n \) is a positive integer.

10. Use mathematical induction to prove that 9 divides \( n^3 + (n+1)^3 + (n+2)^3 \) whenever \( n \) is a nonnegative integer.

11. Use mathematical induction to prove this formula for the sum of the terms of an arithmetic progression:
   \[
a + (a+d) + \cdots + (a+nd) = (n+1)(2a+nd)/2
   \]

12. Suppose that \( a_j \equiv b_j \pmod{m} \) for \( j = 1, 2, \ldots, n \). Use mathematical induction to prove that
   a) \( \sum_{j=1}^{n} a_j \equiv \sum_{j=1}^{n} b_j \pmod{m} \).
   b) \( \prod_{j=1}^{n} a_j \equiv \prod_{j=1}^{n} b_j \pmod{m} \).

13. Show that if \( n \) is a positive integer, then
   \[
   \sum_{k=1}^{n} \frac{k+4}{k(k+1)(k+2)} = \frac{n(3n+7)}{2(n+1)(n+2)}.
   \]

14. For which positive integers \( n \) is \( n + 6 < (n^2 - 8n)/16? \) Prove your answer using mathematical induction.

15. \( \text{(Requires calculus)} \) Suppose that \( f(x) = e^x \) and \( g(x) = xe^x \). Use mathematical induction together with the product rule and the fact that \( f'(x) = e^x \) to prove that \( g^{(n)}(x) = (x+n)e^x \) whenever \( n \) is a positive integer.

16. \( \text{(Requires calculus)} \) Suppose that \( f(x) = e^x \) and \( g(x) = c^x \), where \( c \) is a constant. Use mathematical induction together with the chain rule and the fact that \( f'(x) = e^x \) to prove that \( g^{(n)} = c^n e^x \) whenever \( n \) is a positive integer.

17. Determine which Fibonacci numbers are even, and use a form of mathematical induction to prove your conjecture.

18. Determine which Fibonacci numbers are divisible by 3. Use a form of mathematical induction to prove your conjecture.

19. Prove that \( f_k f_n + f_{k+1} f_{n+1} = f_{n+k+1} \) for all nonnegative integers \( n \), where \( k \) is a nonnegative integer and \( f_i \) denotes the \( i \)th Fibonacci number.

The sequence of \( \text{Lucas numbers} \) is defined by \( l_0 = 2, l_1 = 1, \) and \( l_n = l_{n-1} + l_{n-2} \) for \( n = 2, 3, 4, \ldots \).

20. Show that \( f_n + f_{n+2} = l_{n+1} \) whenever \( n \) is a positive integer, where \( f_i \) and \( l_i \) are the \( i \)th Fibonacci number and \( i \)th Lucas number, respectively.

21. Show that \( l_n^2 + l_{n+1}^2 + \cdots + l_{n+2}^2 = l_n l_{n+1} + 2 \) whenever \( n \) is a nonnegative integer and \( l_i \) is the \( i \)th Lucas number.

22. Use mathematical induction to show that the product of any \( n \) consecutive positive integers is divisible by \( n! \). \( \text{[Hint: Use the identity } m(m+1)\cdots(m+n-1)/n! = (m-1)m(m+1)\cdots(m+n-2)/n! + m(m+1)\cdots(m+n-2)/(n-1)! \} \]

23. Use mathematical induction to show that \( \cos x + i \sin x)^n = \cos nx + i \sin nx \) whenever \( n \) is a positive integer. \( \text{[Hint: Use the identities } \cos(a+b) = \cos a \cos b - \sin a \sin b \text{ and } \sin(a+b) = \sin a \cos b + \cos a \sin b \}\]

24. Use mathematical induction to show that \( \sum_{j=1}^{n} \cos jx = \cos((n+1)x/2) \sin(nx/2)/\sin(x/2) \) whenever \( n \) is a positive integer and \( \sin(x/2) \neq 0 \).

25. Use mathematical induction to prove that \( \sum_{j=1}^{n} j^2/2! = n^2 2^{n+1} - n 2^{n+2} + 3 \cdot 2^{n+1} - 6 \) for every positive integer \( n \).

26. \( \text{(Requires calculus)} \) Suppose that the sequence \( x_1, x_2, \ldots, x_n, \ldots \) is recursively defined by \( x_1 = 0 \) and \( x_{n+1} = \sqrt{x_n + 6} \).
   a) Use mathematical induction to show that \( x_1 < x_2 < \cdots < x_n < \cdots \), that is, the sequence \( \{x_n\} \) is monotonically increasing.
   b) Use mathematical induction to prove that \( x_n < 3 \) for \( n = 1, 2, \ldots \).
   c) Show that \( \lim_{n \to \infty} x_n = 3 \).

27. Show if \( n \) is a positive integer with \( n \geq 2 \), then
   \[
   \sum_{j=2}^{n} \frac{1}{j^2 - 1} = \frac{(n-1)(3n+2)}{4n(n+1)}.
   \]

28. Use mathematical induction to prove Theorem 1 in Section 3.6, that is, show if \( b \) is a positive integer, \( b > 1 \), and \( n \) is a positive integer, then \( n \) can be expressed uniquely in the form \( n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0 \).

29. A lattice point in the plane is a point \((x, y)\) where both \( x \) and \( y \) are integers. Use mathematical induction to show that at least \( n+1 \) straight lines are needed to ensure that every lattice point \((x, y)\) with \( x \geq 0, y \geq 0, \) and \( x + y \leq n \) lies on one of these lines.

30. \( \text{(Requires calculus)} \) Use mathematical induction and the product rule to show that if \( n \) is a positive integer and
Supplementary Exercises

331

4-69

\[ f_1(x), f_2(x), \ldots, f_n(x), \] are all differentiable functions, then

\[ \frac{(f_1(x)f_2(x) \cdots f_n(x))'}{f_1(x)f_2(x) \cdots f_n(x)} = \frac{f_1'(x)}{f_1(x)} + \frac{f_2'(x)}{f_2(x)} + \cdots + \frac{f_n'(x)}{f_n(x)}. \]

31. **(Requires material in Section 3.7)** Suppose that \( B = MAM^{-1} \), where \( A \) and \( B \) are \( n \times n \) matrices and \( M \) is invertible. Show that \( B^k = MA^kM^{-1} \) for all positive integers \( k \).

32. Use mathematical induction to show that if you draw lines in the plane you only need two colors to color the regions formed so that no two regions that have an edge in common have a common color.

33. Show that \( n! \) can be represented as the sum of \( n \) of its distinct positive divisors whenever \( n \geq 3 \). [Hint: Use inductive loading. First try to prove this result using mathematical induction. By examining where your proof fails, find a stronger statement that you can easily prove using mathematical induction.]

*34. Use mathematical induction to prove that if \( x_1, x_2, \ldots, x_n \) are positive real numbers with \( n \geq 2 \), then

\[ \left( \frac{1}{x_1} \right) \left( \frac{1}{x_2} \right) \cdots \left( \frac{1}{x_n} \right) \geq \left( \frac{1}{x_1 + \frac{1}{x_2}} \right) \left( \frac{1}{x_2 + \frac{1}{x_3}} \right) \cdots \left( \frac{1}{x_n + \frac{1}{x_1}} \right). \]

35. Use mathematical induction to prove that if \( n \) people stand in a line, where \( n \) is a positive integer, and if the first person in the line is a woman and the last person in line is a man, then somewhere in the line there is a woman directly in front of a man.

*36. Suppose that for every pair of cities in a country there is a direct one-way road connecting them in one direction or the other. Use mathematical induction to show that there is a city that can be reached from every other city either directly or via exactly one other city.

37. Use mathematical induction to show that when \( n \) circles divide the plane into regions, these regions can be colored with two different colors such that no regions with a common boundary are colored the same.

*38. Suppose that among a group of cars on a circular track there is enough fuel for one car to complete a lap. Use mathematical induction to show that there is a car in the group that can complete a lap by obtaining gas from other cars as it travels around the track.

39. Show that if \( n \) is a positive integer, then

\[ \sum_{j=1}^{n} (2j - 1) \left( \sum_{k=j}^{n} 1/k \right) = n(n+1)/2. \]

40. A unit or Egyptian fraction is a fraction of the form \( 1/n \), where \( n \) is a positive integer. In this exercise, we will use strong induction to show that a greedy algorithm can be used to express every rational number \( p/q \) with \( 0 < p/q < 1 \) as the sum of distinct unit fractions. At each step of the algorithm, we find the smallest positive integer \( n \) such that \( 1/n \) can be added to the sum without exceeding \( p/q \). For example, to express 5/7 we first start the sum with 1/2. Because 5/7 - 1/2 = 3/14 we add 1/5 to the sum because 5/7 is the smallest positive integer \( k \) such that \( 1/k < 3/14 \). Because 3/14 - 1/5 = 1/70, the algorithm terminates, showing that 5/7 = 1/2 + 1/5 + 1/70. Let \( T(p) \) be the statement that this algorithm terminates for all rational numbers \( p/q \) with \( 0 < p/q < 1 \). We will prove that the algorithm always terminates by showing that \( T(p) \) holds for all positive integers \( p \).

a) Show that the basis step \( T(1) \) holds.

b) Suppose that \( T(k) \) holds for positive integers \( k \) with \( k < p \). That is, assume that the algorithm terminates for all rational numbers \( k/r \), where \( 1 \leq k < p \). Show that if we start with \( p/q \) and the fraction \( 1/n \) is selected in the first step of the algorithm, then \( p/q = p'/q' + 1/n \), where \( p' = np - q \) and \( q' = nq \). After considering the case where \( p/q = 1/n \), use the inductive hypothesis to show that the greedy algorithm terminates when it begins with \( p'/q' \) and complete the inductive step.

The **McCarthy 91 function** (defined by John McCarthy, one of the founders of artificial intelligence) is defined using the rule

\[ M(n) = \begin{cases} n - 10 & \text{if } n > 100 \\ M(M(n+1)) & \text{if } n \leq 100 \end{cases} \]

for all positive integers \( n \).

41. By successively using the defining rule for \( M(n) \), find

a) \( M(102) \). b) \( M(101) \). c) \( M(99) \).

d) \( M(97) \). e) \( M(87) \). f) \( M(76) \).

**42.** Show that the function \( M(n) \) is a well-defined function from the set of positive integers to the set of positive integers. [Hint: Prove that \( M(n) = 91 \) for all positive integers \( n \) with \( n \leq 101 \).]

43. Is this proof that

\[ \frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \cdots + \frac{1}{(n-1)n} = 3 - \frac{1}{n}, \]

whenever \( n \) is a positive integer, correct? Justify your answer.

**Basis step:** The result is true when \( n = 1 \) because

\[ \frac{1}{1 \cdot 2} = \frac{1}{2} - \frac{1}{1}. \]

**Inductive step:** Assume that the result is true for \( n \). Then

\[ \frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \cdots + \frac{1}{(n-1)n} + \frac{1}{n(n+1)} \]

\[ = 3 - \frac{1}{n} + \left( \frac{1}{n-1} - \frac{1}{n+1} \right) \]

\[ = 3 - \frac{1}{n} + \frac{1}{n+1}. \]

Hence, the result is true for \( n+1 \) if it is true for \( n \). This completes the proof.
44. Suppose that $A_1$, $A_2$, ..., $A_n$ are a collection of sets. Suppose that $R_3 = A_1 \oplus A_2$ and $R_k = R_{k-1} \oplus A_k$ for $k = 3, 4, \ldots, n$ Use mathematical induction to prove that $x \in R_n$ if and only if $x$ belongs to an odd number of the sets $A_1, A_2, \ldots, A_n$. (Recall that $S \oplus T$ is the symmetric difference of the sets $S$ and $T$ defined in Section 2.2.)

*45. Show that $n$ circles divide the plane into $n^2 - n + 2$ regions if every two circles intersect in exactly two points and no three circles contain a common point.

*46. Show that $n$ planes divide three-dimensional space into \((n^3 + 5n + 6)/6\) regions if any three of these planes have a point in common and no four contain a common point.

*47. Use the well-ordering property to show that $\sqrt{2}$ is irrational. [Hint: Assume that $\sqrt{2}$ is rational. Show that the set of positive integers of the form $b\sqrt{2}$ has a least element $a$. Then show that $a\sqrt{2} - a$ is a smaller positive integer of this form.]

48. A set is **well ordered** if every nonempty subset of this set has a least element. Determine whether each of the following sets is well ordered.

a) the set of integers  

b) the set of integers greater than $-100$  

c) the set of positive rationals with denominator less than 100

d) the set of positive rationals

49. a) Show that if $a_1, a_2, \ldots, a_n$ are positive integers, then \(\gcd(a_1, a_2, \ldots, a_{n-1}, a_n) = \gcd(a_1, a_2, \ldots, a_{n-2}, \gcd(a_{n-1}, a_n))\).

b) Use part (a), together with the Euclidean algorithm, to develop a recursive algorithm for computing the greatest common divisor of a set of $n$ positive integers.

*50. Describe a recursive algorithm for writing the greatest common divisor of $n$ positive integers as a linear combination of these integers.

51. Find an explicit formula for $f(n)$ if $f(1) = 1$ and $f(n) = f(n-1) + 2n - 1$ for $n \geq 2$. Prove your result using mathematical induction.

**52.** Give a recursive definition of the set of bit strings that contain twice as many 0s as 1s.

53. Let $S$ be the set of bit strings defined recursively by $\lambda \in S$ and $0x \in S$, $x1 \in S$ if $x \in S$, where $\lambda$ is the empty string.

a) Find all strings in $S$ of length not exceeding five.

b) Give an explicit description of the elements of $S$.

54. Let $S$ be the set of strings defined recursively by $abc \in S$, $bac \in S$, and $acb \in S$, where $a$, $b$, and $c$ are fixed letters; and for all $x \in S$, $abcx \in S$, $axbc \in S$, and $xabc \in S$, where $x$ is a variable representing a string of letters.

a) Find all elements of $S$ of length eight or less.

b) Show that every element of $S$ has a length divisible by three.

The set $B$ of all **balanced strings of parentheses** is defined recursively by $\lambda \in B$, where $\lambda$ is the empty string; $(x) \in B$, $xy \in B$ if $x, y \in B$.

55. Show that $((x))$ is a balanced string of parentheses and $(((x)))$ is not a balanced string of parentheses.

56. Find all balanced strings of parentheses with exactly six symbols.

57. Find all balanced strings of parentheses with four or fewer symbols.

58. Use induction to show that if $x$ is a balanced string of parentheses, then the number of left parentheses equals the number of right parentheses in $x$.

Define the function $N$ on the set of strings of parentheses by

\[ N(\lambda) = 0, \quad N((x)) = 1, \quad N((x)) = -1, \]

\[ N(uv) = N(u) + N(v), \]

where $\lambda$ is the empty string, and $u$ and $v$ are strings. It can be shown that $N$ is well defined.

---

JOHN McCARTHY (BORN 1927)  
John McCarthy was born in Boston. He grew up in Boston and in Los Angeles. He studied mathematics as both an undergraduate and a graduate student, receiving his B.S. in 1948 from the California Institute of Technology and his Ph.D. in 1951 from Princeton. After graduating from Princeton, McCarthy held positions at Princeton, Stanford, Dartmouth, and M.I.T. He held a position at Stanford from 1962 until 1994, and is now an emeritus professor there. At Stanford, he was the director of the Artificial Intelligence Laboratory, held a named chair in the School of Engineering, and was a senior fellow in the Hoover Institution.

McCarthy was a pioneer in the study of artificial intelligence, a term he coined in 1955. He worked on problems related to the reasoning and information needs required for intelligent computer behavior. McCarthy was among the first computer scientists to design time-sharing computer systems. He developed LiSP, a programming language for computing using symbolic expressions. He played an important role in using logic to verify the correctness of computer programs. McCarthy has also worked on the social implications of computer technology. He is currently working on the problem of how people and computers make conjectures through assumptions that complications are absent from situations. McCarthy is an advocate of the sustainability of human progress and is an optimist about the future of humanity. He has also begun writing science fiction stories. Some of his recent writing explores the possibility that the world is a computer program written by some higher force.

Among the awards McCarthy has won are the Turing Award from the Association for Computing Machinery, the Research Excellence Award of the International Conference on Artificial Intelligence, the Kyoto Prize, and the National Medal of Science.
is a particular solution. Hence, all solutions of the original recurrence relation \( a_n = a_{n-1} + n \) are
given by \( a_n = a^{(h)}_n + a^{(p)}_n = c + n(n + 1)/2 \). Because \( a_1 = 1 \), we have \( 1 = a_1 = c + 1 \cdot 2/2 = 
\)
c + 1, so \( c = 0 \). It follows that \( a_n = n(n + 1)/2 \). (This is the same formula given in Table 2 in
Section 2.4 and derived previously.)

Exercises

1. Determine which of these are linear homogeneous recurrence relations with constant coefficients. Also, find the
degree of those that are.
   a) \( a_n = 3a_{n-1} + 4a_{n-2} + 5a_{n-3} \)
   b) \( a_n = 2a_{n-1} + a_{n-2} \)
   c) \( a_n = a_{n-1} + a_{n-4} \)
   d) \( a_n = a_{n-1} + 2 \)
   e) \( a_n = a^{(h)}_n + a^{(p)}_n \)
   f) \( a_n = a_{n-2} \)
   g) \( a_n = a_{n-1} + n \)

2. Determine which of these are linear homogeneous recurrence relations with constant coefficients. Also, find the
degree of those that are.
   a) \( a_n = 3a_{n-2} \)
   b) \( a_n = 3 \)
   c) \( a_n = a^{2}_{n-1} \)
   d) \( a_n = a_{n-1} + 2a_{n-3} \)
   e) \( a_n = a_{n-1}/n \)
   f) \( a_n = a_{n-1} + a_{n-2} + n + 3 \)
   g) \( a_n = 4a_{n-2} + 5a_{n-4} + 9a_{n-7} \)

3. Solve these recurrence relations together with the initial conditions given.
   a) \( a_n = 2a_{n-1} \) for \( n \geq 1 \), \( a_0 = 3 \)
   b) \( a_n = a_{n-1} \) for \( n \geq 1 \), \( a_0 = 2 \)
   c) \( a_n = 5a_{n-1} - 6a_{n-2} \) for \( n \geq 2 \), \( a_0 = 1 \), \( a_1 = 0 \)
   d) \( a_n = 4a_{n-1} - 4a_{n-2} \) for \( n \geq 2 \), \( a_0 = 6 \), \( a_1 = 8 \)
   e) \( a_n = -3a_{n-1} - 4a_{n-2} \) for \( n \geq 2 \), \( a_0 = 0 \), \( a_1 = 1 \)
   f) \( a_n = 4a_{n-2} \) for \( n \geq 2 \), \( a_0 = 0 \), \( a_1 = 4 \)
   g) \( a_n = a_{n-2}/4 \) for \( n \geq 2 \), \( a_0 = 1 \), \( a_1 = 0 \)

4. Solve these recurrence relations together with the initial conditions given.
   a) \( a_n = a_{n-1} + 6a_{n-2} \) for \( n \geq 2 \), \( a_0 = 3 \), \( a_1 = 6 \)
   b) \( a_n = 7a_{n-1} - 10a_{n-2} \) for \( n \geq 2 \), \( a_0 = 2 \), \( a_1 = 1 \)
   c) \( a_n = 5a_{n-1} - 8a_{n-2} \) for \( n \geq 2 \), \( a_0 = 4 \), \( a_1 = 10 \)
   d) \( a_n = 2a_{n-1} - a_{n-2} \) for \( n \geq 2 \), \( a_0 = 4 \), \( a_1 = 1 \)
   e) \( a_n = a_{n-2} \) for \( n \geq 2 \), \( a_0 = 5 \), \( a_1 = -1 \)
   f) \( a_n = -6a_{n-1} - 9a_{n-2} \) for \( n \geq 2 \), \( a_0 = 3 \), \( a_1 = -3 \)
   g) \( a_{n+2} = -4a_{n+1} + 5a_n \) for \( n \geq 0 \), \( a_0 = 2 \), \( a_1 = 8 \)

5. How many different messages can be transmitted in \( n \) microseconds using the two signals described in Exercise 35 in Section 7.1?

6. How many different messages can be transmitted in \( n \) microseconds using three different signals if one signal requires 1 microsecond for transmission, the other two signals require 2 microseconds each for transmission, and a signal in a message is followed immediately by the next signal?

7. In how many ways can a \( 2 \times n \) rectangular checkerboard be tiled using \( 1 \times 2 \) and \( 2 \times 2 \) pieces?

8. A model for the number of lobsters caught per year is based on the assumption that the number of lobsters
   caught in a year is the average of the number caught in the two previous years.
   a) Find a recurrence relation for \( \{L_n\} \), where \( L_n \) is the
   number of lobsters caught in year \( n \), under the assumption
   for this model.
   b) Find \( L_n \) if 100,000 lobsters were caught in year 1 and
   300,000 were caught in year 2.

9. A deposit of $100,000 is made to an investment fund at the beginning of a year. On the last day of each year two
dividends are awarded. The first dividend is 20% of the amount in the account during that year. The second divid­
end is 45% of the amount in the account in the previous year.
   a) Find a recurrence relation for \( \{P_n\} \), where \( P_n \) is the
   amount in the account at the end of \( n \) years if no money is
   ever withdrawn.
   b) How much is in the account after \( n \) years if no money has
   been withdrawn?


11. The Lucas numbers satisfy the recurrence relation

\[
L_n = L_{n-1} + L_{n-2},
\]

and the initial conditions \( L_0 = 2 \) and \( L_1 = 1 \).
   a) Show that \( L_n = f_{n-1} + f_{n+1} \) for \( n = 2, 3, \ldots \), where
   \( f_n \) is the nth Fibonacci number.
   b) Find an explicit formula for the Lucas numbers.

12. Find the solution to \( a_n = 2a_{n-1} + a_{n-2} - 2a_{n-3} \) for \( n = 3, 4, 5, \ldots \), with \( a_0 = 3 \), \( a_1 = 6 \), and \( a_2 = 0 \).

13. Find the solution to \( a_n = 7a_{n-2} + 6a_{n-3} \) with \( a_0 = 9 \),
   \( a_1 = 10 \), and \( a_2 = 32 \).

14. Find the solution to \( a_n = 5a_{n-2} - 4a_{n-4} \) with \( a_0 = 3 \),
   \( a_1 = 2 \), \( a_2 = 6 \), and \( a_3 = 8 \).

15. Find the solution to \( a_n = 2a_{n-1} + 5a_{n-2} - 6a_{n-3} \) with
   \( a_0 = 7 \), \( a_1 = -4 \), and \( a_2 = 8 \).

*16. Prove Theorem 3.

17. Prove this identity relating the Fibonacci numbers and the binomial coefficients:

\[
f_{n+1} = C(n, 0) + C(n - 1, 1) + \cdots + C(n - k, k),
\]

where \( n \) is a positive integer and \( k = \lfloor n/2 \rfloor \). [Hint: Let
\( a_n = C(n, 0) + C(n - 1, 1) + \cdots + C(n - k, k) \). Show
that the sequence \( \{a_n\} \) satisfies the same recurrence re­
lation and initial conditions satisfied by the sequence of
Fibonacci numbers.]
18. Solve the recurrence relation \( a_n = 6a_{n-1} - 12a_{n-2} + 8a_{n-3} \) with \( a_0 = -5, a_1 = 4, \) and \( a_2 = 88. \)

19. Solve the recurrence relation \( a_n = 3a_{n-1} - 3a_{n-2} - a_{n-3} \) with \( a_0 = 5, a_1 = -9, \) and \( a_2 = 15. \)

20. Find the general form of the solutions of the recurrence relation \( a_n = 8a_{n-2} - 16a_{n-4}. \)

21. What is the general form of the solutions of a linear homogeneous recurrence relation if its characteristic equation has roots 1, 1, 1, 1, \(-2, -2, -2, 3, 3, -4)?

22. What is the general form of the solutions of a linear homogeneous recurrence relation if its characteristic equation has the roots \(-1, -1, 2, 2, 5, 5, ?\)

23. Consider the nonhomogeneous linear recurrence relation \( a_n = 3a_{n-1} + 2^n. \)

a) Show that \( a_n = -2^{n+1} \) is a solution of this recurrence relation.

b) Use Theorem 5 to find all solutions of this recurrence relation.

c) Find the solution with \( a_0 = 1. \)

24. Consider the nonhomogeneous linear recurrence relation \( a_n = 2a_{n-1} + 2^n. \)

a) Show that \( a_n = n2^n \) is a solution of this recurrence relation.

b) Use Theorem 5 to find all solutions of this recurrence relation.

c) Find the solution with \( a_0 = 2. \)

25. a) Determine values of the constants \( A \) and \( B \) such that \( a_n = An + B \) is a solution of recurrence relation \( a_n = 2a_{n-1} + n + 5. \)

b) Use Theorem 5 to find all solutions of this recurrence relation.

c) Find the solution of this recurrence relation with \( a_0 = 4. \)

26. What is the general form of the particular solution guaranteed to exist by Theorem 6 of the linear nonhomogeneous recurrence relation \( a_n = 6a_{n-1} - 12a_{n-2} + 8a_{n-3} + F(n) \) if

a) \( F(n) = n^2 \)
b) \( F(n) = 2^n \)
c) \( F(n) = n2^n \)
d) \( F(n) = (-2)^n \)
e) \( F(n) = n^22^n \)
f) \( F(n) = n^3(-2)^n \)
g) \( F(n) = 3^n \)

27. What is the general form of the particular solution guaranteed to exist by Theorem 6 of the linear nonhomogeneous recurrence relation \( a_n = 8a_{n-2} - 16a_{n-4} + F(n) \) if

a) \( F(n) = n^3 \)
b) \( F(n) = (2)^n \)
c) \( F(n) = n2^n \)
d) \( F(n) = n^4 \)
e) \( F(n) = (n^2 - 2)(-2)^n \)
f) \( F(n) = n^52^n \)
g) \( F(n) = 2^n \)

28. a) Find all solutions of the recurrence relation \( a_n = 2a_{n-1} + 2n^3. \)

b) Find the solution of the recurrence relation in part (a) with initial condition \( a_1 = 4. \)

29. a) Find all solutions of the recurrence relation \( a_n = 2a_{n-1} + 3^n. \)

b) Find the solution of the recurrence relation in part (a) with initial condition \( a_1 = 5. \)

30. a) Find all solutions of the recurrence relation \( a_n = -5a_{n-1} - 6a_{n-2} + 42 \cdot 4^n. \)

b) Find the solution of this recurrence relation with \( a_1 = 56 \) and \( a_2 = 278. \)

31. Find all solutions of the recurrence relation \( a_n = 5a_{n-1} - 6a_{n-2} + 2^n + 3n. \) [Hint: Look for a particular solution of the form \( qn2^n + p_1 n + p_2 \), where \( q, p_1, \) and \( p_2 \) are constants.]

32. Find the solution of the recurrence relation \( a_n = 2a_{n-1} + 3 \cdot 2^n. \)

33. Find all solutions of the recurrence relation \( a_n = 4a_{n-1} - 4a_{n-2} + (n + 1)^2n. \)

34. Find all solutions of the recurrence relation \( a_n = 7a_{n-1} - 16a_{n-2} + 12a_{n-3} + n4^n \) with \( a_0 = -2, a_1 = 0, \) and \( a_2 = 5. \)

35. Find the solution of the recurrence relation \( a_n = 4a_{n-1} - 3a_{n-2} + 2^n + n + 3 \) with \( a_0 = 1 \) and \( a_1 = 4. \)

36. Let \( a_n \) be the sum of the first \( n \) perfect squares, that is, \( a_n = \sum_{k=1}^{n} k^2. \) Show that the sequence \( \{a_n\} \) satisfies the linear nonhomogeneous recurrence relation \( a_n = a_{n-1} + n^2 \) and the initial condition \( a_1 = 1. \) Use Theorem 6 to determine a formula for \( a_n \) by solving this recurrence relation.

37. Let \( a_n \) be the sum of the first \( n \) triangular numbers, that is, \( a_n = \sum_{k=1}^{n} \frac{k(k+1)}{2}. \) Show that \( \{a_n\} \) satisfies the linear nonhomogeneous recurrence relation \( a_n = a_{n-1} + n(n+1)/2 \) and the initial condition \( a_1 = 1. \) Use Theorem 6 to determine a formula for \( a_n \) by solving this recurrence relation.

38. a) Find the characteristic roots of the linear homogeneous recurrence relation \( a_n = 2a_{n-1} - 2a_{n-2}. \) (Note: These are complex numbers.)

b) Find the solution of the recurrence relation in part (a) with \( a_0 = 1 \) and \( a_1 = 2. \)

39. a) Find the characteristic roots of the linear homogeneous recurrence relation \( a_n = a_{n-4}. \) (Note: These include complex numbers.)

b) Find the solution of the recurrence relation in part (a) with \( a_0 = 1, a_1 = 0, a_2 = -1, \) and \( a_3 = 1. \)

40. Solve the simultaneous recurrence relations

\( a_n = 3a_{n-1} + 2b_{n-1} \)
\( b_n = a_{n-1} + 2b_{n-1} \)

with \( a_0 = 1 \) and \( b_0 = 2. \)

41. a) Use the formula found in Example 4 for \( f_n, \) the \( n \)th Fibonacci number, to show that \( f_n \) is the integer closest to

\[ \frac{1}{\sqrt{5}} \left( \frac{1 + \sqrt{5}}{2} \right)^n. \]
b) Determine for which \( n \) \( f_n \) is greater than
\[
\frac{1}{\sqrt{5}} \left( \frac{1 + \sqrt{5}}{2} \right)^n
\]
and for which \( n \) \( f_n \) is less than
\[
\frac{1}{\sqrt{5}} \left( \frac{1 + \sqrt{5}}{2} \right)^n.
\]

42. Show that if \( a_n = a_{n-1} + a_{n-2}, a_0 = s \) and \( a_1 = t \), where \( s \) and \( t \) are constants, then \( a_n = sf_{n-1} + tf_n \) for all positive integers \( n \).

43. Express the solution of the linear nonhomogeneous recurrence relation \( a_n = a_{n-1} + a_{n-2} + 1 \) for \( n \geq 2 \) where \( a_0 = 0 \) and \( a_1 = 1 \) in terms of the Fibonacci numbers. [Hint: Let \( b_n = a_n + 1 \) and apply Exercise 42 to the sequence \( b_n \).]

*44. (Linear algebra required) Let \( A_n \) be the \( n \times n \) matrix with 2s on its main diagonal, 1s in all positions next to a diagonal element, and 0s everywhere else. Find a recurrence relation for \( d_n \), the determinant of \( A_n \). Solve this recurrence relation to find a formula for \( d_n \).

45. Suppose that each pair of a genetically engineered species of rabbits left on an island produces two new pairs of rabbits at the age of 1 month and six new pairs of rabbits at the age of 2 months and every month afterward. None of the rabbits ever die or leave the island.

a) Find a recurrence relation for the number of pairs of rabbits on the island \( n \) months after one newborn pair is left on the island.

b) By solving the recurrence relation in (a) determine the number of pairs of rabbits on the island \( n \) months after one pair is left on the island.

46. Suppose that there are two goats on an island initially. The number of goats on the island doubles every year by natural reproduction, and some goats are either added or removed each year.

a) Construct a recurrence relation for the number of goats on the island at the start of the \( n \)th year, assuming that during each year an extra 100 goats are put on the island.

b) Solve the recurrence relation from part (a) to find the number of goats on the island at the start of the \( n \)th year.

c) Construct a recurrence relation for the number of goats on the island at the start of the \( n \)th year, assuming that \( n \) goats are removed during the \( n \)th year for each \( n \geq 3 \).

d) Solve the recurrence relation in part (c) for the number of goats on the island at the start of the \( n \)th year.

47. A new employee at an exciting new software company starts with a salary of $50,000 and is promised that at the end of each year her salary will be double her salary of the previous year, with an extra increment of $10,000 for each year she has been with the company.

a) Construct a recurrence relation for her salary for her \( n \)th year of employment.

b) Solve this recurrence relation to find her salary for her \( n \)th year of employment.

Some linear recurrence relations that do not have constant coefficients can be systematically solved. This is the case for recurrence relations of the form \( f(n)a_n = g(n)a_{n-1} + h(n) \). Exercises 48–50 illustrate this.

*48. a) Show that the recurrence relation
\[
f(n)a_n = g(n)a_{n-1} + h(n),
\]
for \( n \geq 1 \), and with \( a_0 = C \), can be reduced to a recurrence relation of the form
\[
b_n = b_{n-1} + Q(n)h(n),
\]
where \( b_n = g(n + 1)Q(n + 1)a_n \), with
\[
Q(n) = (f(1)f(2)\cdots f(n - 1))/(g(1)g(2)\cdots g(n)).
\]

b) Use part (a) to solve the original recurrence relation to obtain
\[
a_n = \frac{C + \sum_{i=1}^{n} Q(i)h(i)}{g(n + 1)Q(n + 1)}.
\]

*49. Use Exercise 48 to solve the recurrence relation \( (n + 1) \)
\[
a_n = (n + 3)a_{n-1} + n, \text{ for } n \geq 1, \text{ with } a_0 = 1.
\]

50. It can be shown that the average number of comparisons made by the quick sort algorithm (described in preamble to Exercise 50 in Section 4.4), when sorting \( n \) elements in random order, satisfies the recurrence relation
\[
C_n = n + 1 + 2\sum_{k=0}^{n-1} C_k
\]
for \( n = 1, 2, \ldots \), with initial condition \( C_0 = 0 \).

a) Show that \( \{C_n\} \) also satisfies the recurrence relation
\[
nC_n = (n + 1)C_{n-1} + 2n \text{ for } n = 1, 2, \ldots .
\]

b) Use Exercise 48 to solve the recurrence relation in part (a) to find an explicit formula for \( C_n \).

**51. Prove Theorem 4.

**52. Prove Theorem 6.

53. Solve the recurrence relation \( T(n) = nT^2(n/2) \) with initial condition \( T(1) = 6 \). [Hint: Let \( n = 2^k \) and then make the substitution \( a_k = \log T(2^k) \) to obtain a linear nonhomogeneous recurrence relation.]
where \( f(2) = 1 \), exceeds the number of comparisons needed to solve the closest-pair problem for \( n \) points. By the Master Theorem (Theorem 2), it follows that \( f(n) = O(n \log n) \). The two sorts of points by their \( x \) coordinates and by their \( y \) coordinates each can be done using \( O(n \log n) \) comparisons, by using the merge sort, and the sorted subsets of these coordinates at each of the \( O(\log n) \) steps of the algorithm can be done using \( O(n) \) comparisons each. Thus, we find that the closest-pair problem can be solved using \( O(n \log n) \) comparisons.

**Exercises**

1. How many comparisons are needed for a binary search in a set of 64 elements?
2. How many comparisons are needed to locate the maximum and minimum elements in a sequence with 128 elements using the algorithm in Example 2?
3. Multiply \((1110)_{2}\) and \((1010)_{2}\) using the fast multiplication algorithm.
4. Express the fast multiplication algorithm in pseudocode.
5. Determine a value for the constant \( C \) in Example 4 and use it to estimate the number of bit operations needed to multiply two 64-bit integers using the fast multiplication algorithm.
6. How many operations are needed to multiply two \( 32 \times 32 \) matrices using the algorithm referred to in Example 4?
7. Suppose that \( f(n) = f(n/3) + 1 \) when \( n \) is divisible by 3, and \( f(1) = 1 \). Find
   a) \( f(3) \).  
   b) \( f(27) \).  
   c) \( f(729) \).
8. Suppose that \( f(n) = 2f(n/2) + 3 \) when \( n \) is even, and \( f(1) = 5 \). Find
   a) \( f(2) \).  
   b) \( f(8) \).  
   c) \( f(64) \).  
   d) \( f(1024) \).
9. Suppose that \( f(n) = f(n/5) + 3n^2 \) when \( n \) is divisible by 5, and \( f(1) = 4 \). Find
   a) \( f(5) \).  
   b) \( f(125) \).  
   c) \( f(3125) \).
10. Find \( f(n) \) when \( n = 2^k \), where \( f \) satisfies the recurrence relation \( f(n) = f(n/2) + 1 \) with \( f(1) = 1 \).
11. Estimate the size of \( f \) in Exercise 10 if \( f \) is an increasing function.
12. Find \( f(n) \) when \( n = 3^k \), where \( f \) satisfies the recurrence relation \( f(n) = 2f(n/3) + 4 \) with \( f(1) = 1 \).
13. Estimate the size of \( f \) in Exercise 12 if \( f \) is an increasing function.
14. Suppose that there are \( n = 2^k \) teams in an elimination tournament, where there are \( n/2 \) games in the first round, with the \( n/2 = 2^{k-1} \) winners playing in the second round, and so on. Develop a recurrence relation for the number of rounds in the tournament.
15. How many rounds are in the elimination tournament described in Exercise 14 when there are 32 teams?
16. Solve the recurrence relation for the number of rounds in the tournament described in Exercise 14.
17. Suppose that the votes of \( n \) people for different candidates (where there can be more than two candidates) for a particular office are the elements of a sequence. A person wins the election if this person receives a majority of the votes.
   a) Devise a divide-and-conquer algorithm that determines whether a candidate received a majority and, if so, determine who this candidate is. [Hint: Assume that \( n \) is even and split the sequence of votes into two sequences, each with \( n/2 \) elements. Note that a candidate could not have received a majority of votes without receiving a majority of votes in at least one of the two halves.]
   b) Use the Master Theorem to estimate the number of comparisons needed by the algorithm you devised in part (a).
18. Suppose that each person in a group of \( n \) people votes for exactly two people from a slate of candidates to fill two positions on a committee. The top two finishers both win positions as long as each receives more than \( n/2 \) votes.
   a) Devise a divide-and-conquer algorithm that determines whether the two candidates who received the most votes each received at least \( n/2 \) votes and, if so, determine who these two candidates are.
   b) Use the Master Theorem to estimate the number of comparisons needed by the algorithm you devised in part (a).
19. a) Set up a divide-and-conquer recurrence relation for the number of multiplications required to compute \( x^n \), where \( x \) is a real number and \( n \) is a positive integer, using the recursive algorithm from Exercise 26 in Section 4.4.
   b) Use the recurrence relation you found in part (a) to construct a big-\( O \) estimate for the number of multiplications used to compute \( x^n \) using the recursive algorithm.
20. a) Set up a divide-and-conquer recurrence relation for the number of modular multiplications required to compute \( a^n \mod m \), where \( a, m, \) and \( n \) are positive integers, using the recursive algorithms from Example 3 in Section 4.4.
   b) Use the recurrence relation you found in part (a) to construct a big-\( O \) estimate for the number of modular multiplications used to compute \( a^n \mod m \) using the recursive algorithm.
21. Suppose that the function \( f \) satisfies the recurrence relation \( f(n) = 2f(\sqrt{n}) + 1 \) whenever \( n \) is a perfect square greater than 1 and \( f(2) = 1 \).
   a) Find \( f(16) \).
   b) Find a big-O estimate for \( f(n) \). [Hint: Make the substitution \( m = \log n \).]

22. Suppose that the function \( f \) satisfies the recurrence relation \( f(n) = 2f(\sqrt{n}) + \log n \) whenever \( n \) is a perfect square greater than 1 and \( f(2) = 1 \).
   a) Find \( f(16) \).
   b) Find a big-O estimate for \( f(n) \). [Hint: Make the substitution \( m = \log n \).]

**23.** This exercise deals with the problem of finding the largest sum of consecutive terms of a sequence of \( n \) real numbers. When all terms are positive, the sum of all terms provides the answer, but the situation is more complicated when some terms are negative. For example, the maximum sum of consecutive terms of the sequence \(-2, 3, -1, 6, -7, 4\) is \(3 + (-1) + 6 = 8\). (This exercise is based on [Be86].)
   a) Use pseudocode to describe an algorithm that solves this problem by finding the sums of consecutive terms starting with the first term, the sums of consecutive terms starting with the second term, and so on, keeping track of the maximum sum found so far as the algorithm proceeds.
   b) Determine the computational complexity of the algorithm in part (a) in terms of the number of sums computed and the number of comparisons made.
   c) Devise a divide-and-conquer algorithm to solve this problem. [Hint: Assume that there are an even number of terms in the sequence and split the sequence into two halves. Explain how to handle the case when the maximum sum of consecutive terms includes terms in both halves.]
   d) Use the algorithm from part (c) to find the maximum sum of consecutive terms of each of the sequences: \(-2, 4, -1, 3, 5, -6, 1, 2, 4, 1, -3, 7, -1, -5, 3, -2\); and \(-1, 6, 3, -4, -5, 8, -1, 7\).
   e) Find a recurrence relation for the number of sums and comparisons used by the divide-and-conquer algorithm from part (c).
   f) Use the Master Theorem to estimate the computational complexity of the divide-and-conquer algorithm. How does it compare in terms of computational complexity with the algorithm from part (a)?

24. Apply the algorithm described in Example 12 for finding the closest pair of points, using the Euclidean distance between points, to find the closest pair of the points \((1, 3), (1, 7), (2, 4), (2, 9), (3, 1), (3, 5), (4, 3), \) and \((4, 7)\).

25. Apply the algorithm described in Example 12 for finding the closest pair of points, using the Euclidean distance between points, to find the closest pair of the points \( (1, 2), (1, 6), (2, 4), (2, 8), (3, 1), (3, 6), (3, 10), (4, 3), (5, 1), (5, 5), (5, 9), (6, 7), (7, 1), (7, 4), (7, 9), \) and \((8, 6)\).

26. Use pseudocode to describe the recursive algorithm for solving the closest-pair problem as described in Example 12.

27. Construct a variation of the algorithm described in Example 12 along with justifications of the steps used by the algorithm to find the smallest distance between two points if the distance between two points is defined to be \(d((x_i, y_i), (x_j, y_j)) = \max(|x_i - x_j|, |y_i - y_j|)\).

28. Suppose someone picks a number \( x \) from a set of \( n \) numbers. A second person tries to guess the number by successively selecting subsets of the \( n \) numbers and asking the first person whether \( x \) is in each set. The first person answers either "yes" or "no." When the first person answers each query truthfully, we can find \( x \) using \( \log n \) queries by successively splitting the sets used in each query in half. Ulam's problem, proposed by Stanislaw Ulam in 1976, asks for the number of queries required to find \( x \), supposing that the first person is allowed to lie exactly once.
   a) Show that by asking each question twice, given a number \( x \) and a set with \( n \) elements, and asking one more question when we find the lie, Ulam's problem can be solved using \( 2 \log n + 1 \) queries.
   b) Show that by dividing the initial set of \( n \) elements into four parts, each with \( n/4 \) elements, \( 1/4 \) of the elements can be eliminated using two queries. [Hint: Use two queries, where each of the queries asks whether the element is in the union of two of the subsets with \( n/4 \) elements and where one of the subsets contains the \( n/4 \) elements used in both queries.]
   c) Show from part (b) that if \( f(n) \) equals the number of queries used to solve Ulam's problem using the method from part (b) and \( n \) is divisible by 4, then \( f(n) = f(3n/4) + 2 \).
   d) Solve the recurrence relation in part (c) for \( f(n) \).
   e) Is the naive way to solve Ulam's problem by asking each question twice or the divide-and-conquer method based on part (b) more efficient? The most efficient way to solve Ulam's problem has been determined by A. Pelc [Pe87].

In Exercises 29–33, assume that \( f \) is an increasing function satisfying the recurrence relation \( f(n) = af(n/b) + cn^d \), where \( a \geq 1 \), \( b \) is an integer greater than 1, and \( c \) and \( d \) are positive real numbers. These exercises supply a proof of Theorem 2.

29. Show that if \( a = b^d \) and \( n \) is a power of \( b \), then \( f(n) = f((1)n^d) + cn^d \log_b n \).
30. Use Exercise 29 to show that if \( a = b^d \), then \( f(n) \) is \( O(n^d \log n) \).
31. Show that if \( a \neq b^d \) and \( n \) is a power of \( b \), then \( f(n) = C_1n^d + C_2n^{\log_b a} \), where \( C_1 = b^d c/(b^d - a) \) and \( C_2 = f(1) + b^d c/(a - b^d) \).
32. Use Exercise 31 to show that if \( a < b^d \), then \( f(n) \) is \( O(n^d) \).
33. Use Exercise 31 to show that if \( a > b^d \), then \( f(n) \) is \( O(n^{\log_b a}) \).
34. Find \( f(n) \) when \( n = 4^k \), where \( f \) satisfies the recurrence relation \( f(n) = 5f(n/4) + 6n \), with \( f(1) = 1 \).

35. Estimate the size of \( f \) in Exercise 34 if \( f \) is an increasing function.

36. Find \( f(n) \) when \( n = 2^k \), where \( f \) satisfies the recurrence relation \( f(n) = 8f(n/2) + n^2 \) with \( f(1) = 1 \).

37. Estimate the size of \( f \) in Exercise 36 if \( f \) is an increasing function.

### 7.4 Generating Functions

#### Introduction

Generating functions are used to represent sequences efficiently by coding the terms of a sequence as coefficients of powers of a variable \( x \) in a formal power series. Generating functions can be used to solve many types of counting problems, such as the number of ways to select or distribute objects of different kinds, subject to a variety of constraints, and the number of ways to make change for a dollar using coins of different denominations. Generating functions can be used to solve recurrence relations by translating a recurrence relation for the terms of a sequence into an equation involving a generating function. This equation can then be solved to find a closed form for the generating function. From this closed form, the coefficients of the power series for the generating function can be found, solving the original recurrence relation. Generating functions can also be used to prove combinatorial identities by taking advantage of relatively simple relationships between functions that can be translated into identities involving the terms of sequences. Generating functions are a helpful tool for studying many properties of sequences besides those described in this section, such as their use for establishing asymptotic formulae for the terms of a sequence.

We begin with the definition of the generating function for a sequence.

**DEFINITION 1** The generating function for the sequence \( a_0, a_1, \ldots, a_k, \ldots \) of real numbers is the infinite series

\[
G(x) = a_0 + a_1 x + \cdots + a_k x^k + \cdots = \sum_{k=0}^{\infty} a_k x^k.
\]

**Remark:** The generating function for \( \{a_k\} \) given in Definition 1 is sometimes called the **ordinary generating function** of \( \{a_k\} \) to distinguish it from other types of generating functions for this sequence.

**EXAMPLE 1** The generating functions for the sequences \( \{a_k\} \) with \( a_k = 3 \), \( a_k = k + 1 \), and \( a_k = 2^k \) are \( \sum_{k=0}^{\infty} 3x^k \), \( \sum_{k=0}^{\infty} (k + 1)x^k \), and \( \sum_{k=0}^{\infty} 2^k x^k \), respectively.

We can define generating functions for finite sequences of real numbers by extending a finite sequence \( a_0, a_1, \ldots, a_n \) into an infinite sequence by setting \( a_{n+1} = 0 \), \( a_{n+2} = 0 \), and so on. The generating function \( G(x) \) of this infinite sequence \( \{a_n\} \) is a polynomial of degree \( n \) because no terms of the form \( a_j x^j \) with \( j > n \) occur, that is,

\[
G(x) = a_0 + a_1 x + \cdots + a_n x^n.
\]
Supplementary Exercises

1. A group of 10 people begin a chain letter, with each person sending the letter to four other people. Each of these people sends the letter to four additional people.
   a) Find a recurrence relation for the number of letters sent at the nth stage of this chain letter, if no person ever receives more than one letter.
   b) What are the initial conditions for the recurrence relation in part (a)?
   c) Solve this recurrence relation.

2. A nuclear reactor has created 18 grams of a particular radioactive isotope. Every hour 1% of a radioactive isotope decays.
   a) Set up a recurrence relation for the amount of this isotope left after n hours.
   b) What are the initial conditions for the recurrence relation in part (a)?
   c) Solve this recurrence relation.

3. Every hour the U.S. government prints 10,000 more $1 bills, 4000 more $5 bills, 3000 more $10 bills, 2500 more $20 bills, 1000 more $50 bills, and the same number of $100 bills as it did the previous hour. In the initial hour 1000 of each bill were produced.
   a) Set up a recurrence relation for the amount of money produced in the nth hour.
   b) What are the initial conditions for the recurrence relation in part (a)?
   c) Solve the recurrence relation for the amount of money produced in the nth hour.
   d) Set up a recurrence relation for the total amount of money produced in the first n hours.
   e) Solve the recurrence relation for the total amount of money produced in the first n hours.

4. Suppose that every hour there are two new bacteria in a colony for each bacterium that was present the previous hour, and that all bacteria 2 hours old die. The colony starts with 100 new bacteria.
   a) How many ways are there to assign seven jobs to three employees so that each employee is assigned at least one job?
   b) How many ways are there to assign three employees so that each employee is assigned at least one job?
   c) How many letters are sent at the nth stage of this chain letter, if no person ever receives more than one letter.

5. Messages are sent over a communications channel using two different signals. One signal requires 2 microseconds for transmittal, and the other signal requires 3 microseconds for transmittal. Each signal of a message is followed immediately by the next signal.
   a) Find a recurrence relation for the number of different signals that can be sent in n microseconds.
   b) What are the initial conditions for the recurrence relation in part (a)?
   c) How many different messages can be sent in 12 microseconds?

6. A small post office has only 4-cent stamps, 6-cent stamps, and 10-cent stamps. Find a recurrence relation for the number of ways to form postage of n cents with these stamps if the order that the stamps are used matters. What are the initial conditions for this recurrence relation?
   a) Set up a recurrence relation for the number of bacteria present after n hours.
   b) What is the solution of this recurrence relation?
   c) When will the colony contain more than 1 million bacteria?

7. How many ways are there to form these postages using the rules described in Exercise 6?
   a) 12 cents
   b) 14 cents
   c) 18 cents
   d) 22 cents

8. Find the solutions of the simultaneous system of congruences

\[ a_n = a_{n-1} - b_{n-1} \]
\[ b_n = a_{n-1} + b_{n-1} \]

with \( a_0 = 1 \) and \( b_0 = 2 \).

9. Solve the recurrence relation \( a_n = a_{n-1}^2 / a_{n-2} \) if \( a_0 = 1 \) and \( a_1 = 2 \). [Hint: Take logarithms of both sides to obtain a recurrence relation for the sequence \( \log a_n, n = 0, 1, 2, \ldots \)]
10. Solve the recurrence relation \( a_n = a_{n-1}^2 + 2a_{n-2} \) if \( a_0 = 2 \) and \( a_1 = 2 \). (See the hint for Exercise 9.)

11. Find the solution of the recurrence relation \( a_n = 3a_{n-1} - 3a_{n-2} + a_{n-3} + 1 \) if \( a_0 = 2, a_1 = 4, \) and \( a_2 = 8 \).

12. Find the solution of the recurrence relation \( a_n = 3a_{n-1} - 3a_{n-2} + a_{n-3} \) if \( a_0 = 2, a_1 = 2, \) and \( a_2 = 4 \).

13. Suppose that in Example 4 of Section 7.1 a pair of rabbits leaves the island after reproducing twice. Find a recurrence relation for the number of rabbits on the island in the middle of the \( n \)th month.

14. Find the solution to the recurrence relation \( f(n) = 3f(n/5) + 2n^4 \), when \( n \) is divisible by 5, for \( n = 5^k \), where \( k \) is a positive integer and \( f(1) = 1 \).

15. Estimate the size of \( f \) in Exercise 14 if \( f \) is an increasing function.

16. Find a recurrence relation that describes the number of comparisons used by the following algorithm: Find the largest and second largest elements of a sequence of \( n \) numbers recursively by splitting the sequence into two subsequences with an equal number of terms, or where there is one more term in one subsequence than in the other, at each stage. Stop when subsequences with two terms are reached.

17. Estimate the number of comparisons used by the algorithm described in Exercise 16.

Let \( \{a_n\} \) be a sequence of real numbers. The **forward differences** of this sequence are defined recursively as follows: The **first forward difference** \( \Delta a_n = a_{n+1} - a_n \); the **\( k+1 \)st forward difference** \( \Delta^{k+1} a_n = \Delta \Delta^k a_n \) is obtained from \( \Delta^k a_n \).

18. Find \( \Delta a_n \), where
   \[ a_n = 3. \quad b_n = 4n + 7. \quad c_n = n^2 + n + 1. \]

19. Let \( a_n = 3n^3 + n + 2 \). Find \( \Delta^k a_n \), where \( k \) equals
   \[ a) \ 2. \quad b) \ 3. \quad c) \ 4. \]

20. Suppose that \( a_n = P(n) \), where \( P \) is a polynomial of degree \( d \). Prove that \( \Delta^{d+1} a_n = 0 \) for all nonnegative integers \( n \).

21. Let \( \{a_n\} \) and \( \{b_n\} \) be sequences of real numbers. Show that
   \[ \Delta(a_n b_n) = a_{n+1}(\Delta b_n) + b_n(\Delta a_n). \]

22. Show that if \( F(x) \) and \( G(x) \) are the generating functions for the sequences \( \{a_k\} \) and \( \{b_k\} \), respectively, and \( c \) and \( d \) are real numbers, then \( (cF + dG)(x) \) is the generating function for \( \{ca_k + db_k\} \).

23. (Requires calculus) This exercise shows how generating functions can be used to solve the recurrence relation \( (n+1)a_{n+1} = a_n + (1/n!) \) for \( n \geq 0 \) with initial condition \( a_0 = 1 \).

   a) Let \( G(x) \) be the generating function for \( \{a_n\} \). Show that \( G'(x) = G(x) + e^x \) and \( G(0) = 1 \).
   b) Show from part (a) that \( (e^{-x}G(x))' = 1 \), and conclude that \( G(x) = xe^x + e^x \).
   c) Use part (b) to find a closed form for \( a_n \).

24. Suppose that 14 students receive an A on the first exam in a discrete mathematics class, and 18 receive an A on the second exam. If 22 students received an A on either the first exam or the second exam, how many students received an A on both exams?

25. There are 323 farms in Monmouth County that have at least one of horses, cows, and sheep. If 224 have horses, 85 have cows, 57 have sheep, and 18 farms have all three types of animals, how many farms have exactly two of these three types of animals?

26. Queries to a database of student records at a college produced the following data: There are 2175 students at the college, 1675 of these are not freshmen, 1074 students have taken a course in calculus, 444 students have taken a course in discrete mathematics, 607 students are not freshmen and have taken calculus, 350 students have taken calculus and discrete mathematics, 201 students are not freshmen and have taken discrete mathematics, and 143 students are not freshmen and have taken both calculus and discrete mathematics. Can all the responses to the queries be correct?

27. Students in the school of mathematics at a university major in one or more of the following four areas: applied mathematics (AM), pure mathematics (PM), operations research (OR), and computer science (CS). How many students are in this school if (including joint majors) there are 23 students majoring in AM; 17 students majoring in PM; 44 in OR; 63 in CS; 5 in AM and PM; 8 in AM and CS; 4 in AM and OR; 6 in PM and CS; 5 in PM and OR; 14 in OR and CS; 2 in PM, OR, and CS; 2 in AM, OR, and CS; 1 in PM, AM, and OR; 1 in PM, AM, and CS; and 1 in all four fields.

28. How many terms are needed when the inclusion–exclusion principle is used to express the number of elements in the union of seven sets if no more than five of these sets have a common element?

29. How many solutions in positive integers are there to the equation \( x_1 + x_2 + x_3 = 20 \) with \( 2 < x_1 < 6, 6 < x_2 < 10, \) and \( 0 < x_3 < 5 \)?

30. How many positive integers less than 1,000,000 are
   \[ a) \ divisible by 2, 3, 5? \]
   \[ b) \ not divisible by 7, 11, or 13? \]
   \[ c) \ divisible by 3 but not by 7? \]

31. How many positive integers less than 200 are
   \[ a) \ second or higher powers of integers? \]
   \[ b) \ either second or higher powers of integers or primes? \]
   \[ c) \ not divisible by the square of an integer greater than 1? \]
   \[ d) \ not divisible by the cube of an integer greater than 1? \]
   \[ e) \ not divisible by three or more primes? \]

32. How many ways are there to assign six different jobs to three different employees if the hardest job is assigned
Use a computational program or programs you have written to do these exercises.

1. Find the exact value of $f_{100}$, $f_{500}$, and $f_{1000}$, where $f_n$ is the $n$th Fibonacci number.
2. Find the smallest Fibonacci number greater than 1,000,000, greater than 1,000,000,000, and greater than 1,000,000,000,000.
3. Find as many prime Fibonacci numbers as you can. It is unknown whether there are infinitely many of these.
4. Write out all the moves required to solve the Tower of Hanoi puzzle with 10 disks.
5. Write out all the moves required to use the Frame–Stewart algorithm to move 20 disks from one peg to another peg using four pegs according to the rules of the Reve's puzzle.
6. Verify the Frame conjecture for solving the Reve's puzzle for $n$ disks for as many integers $n$ as possible by showing that the puzzle cannot be solved using fewer moves than are made by the Frame–Stewart algorithm with the optimal choice of $k$.
7. Compute the number of operations required to multiply two integers with $n$ bits for various integers $n$ including 16, 64, 256, and 1024 using the fast multiplication described in Section 7.3 and the standard algorithm for multiplying integers (Algorithm 3 in Section 3.6).
8. Compute the number of operations required to multiply two $n \times n$ matrices for various integers $n$ including 4, 16, 64, and 128 using the fast matrix multiplication described in Section 7.3 and the standard algorithm for multiplying matrices (Algorithm 1 in Section 3.8).
9. Use the sieve of Eratosthenes to find all the primes not exceeding 1000.
10. Find the number of primes not exceeding 10,000 using the method described in Section 7.6 to find the number of primes not exceeding 100.
11. List all the derangements of \{1, 2, 3, 4, 5, 6, 7, 8\}.
12. Compute the probability that a permutation of $n$ objects is a derangement for all positive integers not exceeding 20 and determine how quickly these probabilities approach the number $e$. 
33. What is the probability that exactly one person is given back the correct hat by a hatcheck person who gives $n$ people their hats back at random?
34. How many bit strings of length six do not contain four consecutive 1s?
35. What is the probability that a bit string of length six contains at least four 1s?