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. This is even true when the algorithms used are intractable.

Exercises Chap 3.3

1. Give a big-$O$ estimate for the number of operations (where an operation is an addition or a multiplication) used in this segment of an algorithm.

   \[
   t := 0 \\
   \text{for } i := 1 \text{ to } 3 \\
   \text{for } j := 1 \text{ to } 4 \\
   t := t + ij
   \]

2. Give a big-$O$ estimate for the number additions used in this segment of an algorithm.

   \[
   t := 0 \\
   \text{for } i := 1 \text{ to } n \\
   \text{for } j := i + 1 \text{ to } n \\
   t := t + i + j
   \]

3. Give a big-$O$ estimate for the number of operations, where an operation is a comparison or a multiplication, used in this segment of an algorithm (ignoring comparisons used to test the conditions in the for loops, where \(a_1, a_2, \ldots, a_n\) are positive real numbers).

   \[
   m := 0 \\
   \text{for } i := 1 \text{ to } n \\
   \text{for } j := i + 1 \text{ to } n \\
   m := \max(a_i/a_j, m)
   \]

4. Give a big-$O$ estimate for the number of operations, where an operation is an addition or a multiplication, used in this segment of an algorithm (ignoring comparisons used to test the conditions in the while loop).

   \[
   i := 1 \\
   t := 0 \\
   \text{while } i \leq n \\
   t := t + i \\
   i := 2i
   \]

5. 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?

6. a) Use pseudocode to describe the algorithm that puts the first four terms of a list of real numbers of arbitrary length in increasing order using the insertion sort.

   b) Show that this algorithm has time complexity \(O(n)\) in terms of the number of comparisons used.

7. 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?

8. Given a real number \(x\) and a positive integer \(k\), determine the number of multiplications used to find \(x^k\) starting with \(x\) and successively squaring (to find \(x^2, x^4, \text{ and so on}\)). Is this a more efficient way to find \(x^k\) than by multiplying \(x\) by itself the appropriate number of times?

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

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

   \[
   \text{procedure bit count}(S: \text{bit string}) \\
   \text{count} := 0 \\
   \text{while } S \neq 0 \\
   \text{count} := \text{count} + 1 \\
   S := S \land (S - 1) \\
   \text{return } \text{count} \{ \text{count is the number of 1s in } S \}
   \]

   Here \(S - 1\) is the bit string obtained by changing the rightmost 1 bit of \(S\) to 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 \(S\) using the algorithm in part (a)?

11. a) Suppose we have \(n\) subsets \(S_1, S_2, \ldots, S_n\) of the set \(\{1, 2, \ldots, n\}\). Express a brute-force algorithm that determines whether there is a disjoint pair of these subsets. [Hint: The algorithm should loop through the subsets; for each subset \(S_i\), it should then loop through all other subsets; and for each of these other subsets \(S_j\), it should loop through all elements \(k\) in \(S_j\) to determine whether \(k\) also belongs to \(S_j\).]

   b) Give a big-$O$ estimate for the number of times the algorithm needs to determine whether an integer is in one of the subsets.

12. Consider the following algorithm, which takes as input a sequence of \(n\) integers \(a_1, a_2, \ldots, a_n\) and produces as output a matrix \(M = [m_{ij}]\) where \(m_{ij}\) is the minimum term in the sequence of integers \(a_1, a_{i+1}, \ldots, a_j\) for \(j \geq i\) and \(m_{ij} = 0\) otherwise.

   initialize \(M\) so that \(m_{ij} = a_i\) if \(j \geq i\) and \(m_{ij} = 0\) otherwise

   \[
   \text{for } i := 1 \text{ to } n \\
   \text{for } j := i + 1 \text{ to } n \\
   \text{for } k := i + 1 \text{ to } j \\
   m_{ij} := \min(m_{ij}, a_k) \\
   \text{return } M = [m_{ij}] \{ m_{ij} \text{ is the minimum term of } a_i, a_{i+1}, \ldots, a_j \} \]


**Remark:** Because \( \mathbb{Z}_m \) with the operations of addition and multiplication modulo \( m \) satisfies the properties listed, \( \mathbb{Z}_m \) with modular addition is said to be a **commutative group** and \( \mathbb{Z}_m \) with both of these operations is said to be a **commutative ring**. Note that the set of integers with ordinary addition and multiplication also forms a commutative ring. Groups and rings are studied in courses that cover abstract algebra.

**Remark:** In Exercise 30, and in later sections, we will use the notations \( + \) and \( \cdot \) for \( +_m \) and \( \cdot_m \) without the subscript \( m \) on the symbol for the operator whenever we work with \( \mathbb{Z}_m \).

---

**Exercises Chap 4.1**

1. Does 17 divide each of these numbers?
   a) 68  
   b) 84  
   c) 357  
   d) 1001

2. Prove that if \( a \) is an integer other than 0, then
   a) 1 divides \( a \).  
   b) \( a \) divides 0.

3. Prove that part (ii) of Theorem 1 is true.

4. Prove 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, where \( a \neq 0 \), such that \( a \mid c \) and \( b \mid d \), then \( ab \mid cd \).

7. Show that if \( a, b, \) and \( c \) are integers, where \( a \neq 0 \) and \( c \neq 0 \), 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 and \( a \neq 0 \), then \( a \mid b \) or \( a \mid c \).

9. What are the quotient and remainder when
   a) 19 is divided by 7?  
   b) 111 is divided by 17?  
   c) 789 is divided by 23?  
   d) 1001 is divided by 13?  
   e) 0 is divided by 17?  
   f) 3 is divided by 5?  
   g) -1 is divided by 3?  
   h) 4 is divided by 17?

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. What time does a 12-hour clock read
    a) 80 hours after it reads 11:00?  
    b) 40 hours before it reads 12:00?  
    c) 100 hours after it reads 6:00?

12. What time does a 24-hour clock read
    a) 100 hours after it reads 2:00?  
    b) 45 hours before it reads 12:00?  
    c) 168 hours after it reads 19:00?

13. Suppose that \( a \) and \( b \) are integers, \( a \equiv 4 \pmod{13} \), and \( b \equiv 9 \pmod{13} \). Find the integer \( c \) with \( 0 \leq c \leq 12 \) such that
    a) \( c \equiv 9a \pmod{13} \).  
    b) \( c \equiv 11b \pmod{13} \).  
    c) \( c \equiv a + b \pmod{13} \).  
    d) \( c \equiv 2a + 3b \pmod{13} \).  
    e) \( c \equiv a^2 + b^2 \pmod{13} \).  
    f) \( c \equiv a^3 - b^3 \pmod{13} \).

14. Suppose that \( a \) and \( b \) are integers, \( a \equiv 11 \pmod{19} \), and \( b \equiv 3 \pmod{19} \). Find the integer \( c \) with \( 0 \leq c \leq 18 \) such that
    a) \( c \equiv 13a \pmod{19} \).  
    b) \( c \equiv 8b \pmod{19} \).  
    c) \( c \equiv a - b \pmod{19} \).  
    d) \( c \equiv 7a + 3b \pmod{19} \).  
    e) \( c \equiv 2a^2 + 3b^2 \pmod{19} \).  
    f) \( c \equiv a^3 + 4b^3 \pmod{19} \).

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

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

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

18. Show that if \( a \) is an integer and \( d \) is an 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.

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

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

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

22. Find \( a \div m \) and \( a \mod m \) when
    a) \( a = -111, m = 99\).
    b) \( a = -9999, m = 101\).
    c) \( a = 10299, m = 999\).
    d) \( a = 123456, m = 1001\).
Find \( a \mod m \) and \( a \div m \) when
\begin{align*}
a) & \quad a = 228, m = 119. \\
b) & \quad a = 9009, m = 223. \\
c) & \quad a = -10101, m = 333. \\
d) & \quad a = -765432, m = 38271.
\end{align*}

24. Find the integer \( a \) such that
\begin{align*}
a) & \quad a \equiv 43 \pmod{23} \text{ and } -22 \leq a \leq 0. \\
b) & \quad a \equiv 17 \pmod{29} \text{ and } -14 \leq a \leq 14. \\
c) & \quad a \equiv -11 \pmod{21} \text{ and } 90 \leq a \leq 110.
\end{align*}

25. Find the integer \( a \) such that
\begin{align*}
a) & \quad a \equiv -15 \pmod{27} \text{ and } -26 \leq a \leq 0. \\
b) & \quad a \equiv 24 \pmod{31} \text{ and } -15 \leq a \leq 15. \\
c) & \quad a \equiv 99 \pmod{41} \text{ and } 100 \leq a \leq 140.
\end{align*}

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

27. List all integers between -100 and 100 that are congruent to -1 modulo 25.

28. Decide whether each of these integers is congruent to 3 modulo 7.
\begin{align*}
a) & \quad 37 \\
b) & \quad 66 \\
c) & \quad -17 \\
d) & \quad -67
\end{align*}

29. Decide whether each of these integers is congruent to 5 modulo 17.
\begin{align*}
a) & \quad 80 \\
b) & \quad 103 \\
c) & \quad -29 \\
d) & \quad -122
\end{align*}

30. Find each of these values.
\begin{align*}
n) & \quad 177 \mod 31 + 270 \mod 31 \mod 31 \\
o) & \quad 177 \mod 31 \cdot 270 \mod 31 \mod 31
\end{align*}

31. Find each of these values.
\begin{align*}
a) & \quad (-133 \mod 23 + 261 \mod 23) \mod 23 \\
b) & \quad (457 \mod 23 \cdot 182 \mod 23) \mod 23
\end{align*}

32. Find each of these values.
\begin{align*}
a) & \quad (19^2 \mod 41) \mod 9 \\
b) & \quad (32^3 \mod 13)^2 \mod 11 \\
c) & \quad (7^3 \mod 23)^2 \mod 31 \\
d) & \quad (21^2 \mod 15)^3 \mod 22
\end{align*}

33. Find each of these values.
\begin{align*}
a) & \quad (99^2 \mod 32)^3 \mod 15 \\
b) & \quad (3^4 \mod 17)^2 \mod 11 \\
c) & \quad (19^3 \mod 23)^2 \mod 31 \\
d) & \quad (89^3 \mod 79)^4 \mod 26
\end{align*}

34. 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 \( a - c \equiv b - d \pmod m \).

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

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

37. Find counterexamples to each of these statements about congruences.
\begin{align*}
a) & \quad If ac \equiv bc \pmod m, \text{ where } a, b, c, \text{ and } m \text{ are integers with } m \geq 2, \text{ then } a \equiv b \pmod m. \\
b) & \quad If a \equiv b \pmod m \text{ and } c \equiv d \pmod m, \text{ where } a, b, c, \text{ and } d \text{ are integers with } c \text{ and } d \text{ positive and } m \geq 2, \text{ then } ac \equiv bd \pmod m.
\end{align*}

38. Show that if \( n \) is an integer then \( n^2 \equiv 0 \text{ or } 1 \pmod 4 \).

39. Use Exercise 38 to show that if \( m \) is a positive integer of the form \( 4k + 3 \) for some nonnegative integer \( k \), then \( m \) is not the sum of the squares of two integers.

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

41. 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 \( a^k \equiv b^k \pmod m \).

42. Show that \( Z_m \) with addition modulo \( m \), where \( m \geq 2 \) is an integer, satisfies the closure, associative, and commutative properties, 0 is an additive identity, and for every nonzero \( a \in Z_m \), \(-a\) is the inverse of \( a \) modulo \( m \).

43. Show that \( Z_m \) with multiplication modulo \( m \), where \( m \geq 2 \) is an integer, satisfies the closure, associative, and commutative properties, and \( 1 \) is a multiplicative identity.

44. Show that the distributive property of multiplication over addition holds for \( Z_m \), where \( m \geq 2 \) is an integer.

45. Write out the addition and multiplication tables for \( Z_5 \) (where by addition and multiplication we mean \(+_5 \) and \( \cdot_5 \)).

46. Write out the addition and multiplication tables for \( Z_6 \) (where by addition and multiplication we mean \(+_6 \) and \( \cdot_6 \)).

47. Determine whether each of the functions \( f(a) = a \div d \) and \( g(a) = a \mod d \), where \( d \) is a fixed positive integer, from the set of integers to the set of integers, is one-to-one, and determine whether each of these functions is onto.
4.2 Integer Representations and Algorithms 255

Exercises Chap 4.2

1. Convert the decimal expansion of each of these integers to a binary expansion.
   a) 231  
   b) 4532  
   c) 97644

2. Convert the decimal expansion of each of these integers to a binary expansion.
   a) 321  
   b) 1023  
   c) 100632

3. Convert the binary expansion of each of these integers to a decimal expansion.
   a) (1111)₂  
   b) (100000001)₂  
   c) (101010101)₂  
   d) (11010010010000)₂

4. Convert the binary expansion of each of these integers to a decimal expansion.
   a) (10101010101)₂  
   b) (110111011101)₂  
   c) (11101000011111)₂

5. Convert the octal expansion of each of these integers to a binary expansion.
   a) (572)₈  
   b) (1604)₈  
   c) (423)₈  
   d) (2417)₈

6. Convert the binary expansion of each of these integers to an octal expansion.
   a) (111101111)₂  
   b) (10101010101)₂  
   c) (10011101110111)₂  
   d) (1010010100101)₂

7. Convert the hexadecimal expansion of each of these integers to a binary expansion.
   a) (80E)₁₆  
   b) (135AB)₁₆  
   c) (ABBA)₁₆  
   d) (DEFACED)₁₆

8. Convert (BADFACED)₁₆ from its hexadecimal expansion to its binary expansion.

9. Convert (ABCD)₁₆ from its hexadecimal expansion to its binary expansion.

10. Convert each of the integers in Exercise 6 from a binary expansion to a hexadecimal expansion.

11. Convert (10110111011111)₂ from its binary expansion to its hexadecimal expansion.

12. Convert (1010000110001111)₂ from its binary expansion to its hexadecimal expansion.

13. 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 zeros if necessary, and translating each block of four binary digits into a single hexadecimal digit.

14. 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.

15. Show that the octal expansion of a positive integer can be obtained from its binary expansion by grouping together blocks of three binary digits, adding initial zeros if necessary, and translating each block of three binary digits into a single octal digit.

16. Show that the binary expansion of a positive integer can be obtained from its octal expansion by translating each octal digit into a block of three binary digits.

17. Convert (7345321)₈ to its binary expansion and (1010110111)₂ to its octal expansion.

18. Give a procedure for converting from the hexadecimal expansion of an integer to its octal expansion using binary notation as an intermediate step.

19. Give a procedure for converting from the octal expansion of an integer to its hexadecimal expansion using binary notation as an intermediate step.

20. Explain how to convert from binary to base 64 expansions and from base 64 expansions to binary expansions and from octal to base 64 expansions and from base 64 expansions to octal expansions.

21. Find the sum and the product of each of these pairs of numbers. Express your answers as a binary expansion.
   a) (10001111)₂, (1111111)₂  
   b) (11011111)₂, (10111011)₂  
   c) (1010101010)₂, (11111000000)₂  
   d) (100000001)₂, (1111111111)₂

22. Find the sum and product of each of these pairs of numbers. Express your answers as a base 3 expansion.
   a) (112)₃, (210)₃  
   b) (2112)₃, (12021)₃  
   c) (20001)₃, (1111)₃  
   d) (120021)₃, (2002)₃

23. Find the sum and product of each of these pairs of numbers. Express your answers as an octal expansion.
   a) (763)₈, (147)₈  
   b) (6001)₈, (272)₈  
   c) (1111)₈, (777)₈  
   d) (54321)₈, (3456)₈

24. Find the sum and product of each of these pairs of numbers. Express your answers as a hexadecimal expansion.
   a) (1AE)₁₆, (BBC)₁₆  
   b) (20CBA)₁₆, (A01)₁₆  
   c) (ABCDE)₁₆, (11111)₁₆  
   d) (E0000E)₁₆, (BAAA)₁₆

25. Use Algorithm 5 to find $7^{644} \mod 645$.

26. Use Algorithm 5 to find $11^{644} \mod 645$.

27. Use Algorithm 5 to find $3^{2003} \mod 99$.

28. Use Algorithm 5 to find $123^{1001} \mod 101$.

29. Show that every positive integer can be represented uniquely as the sum of distinct powers of 2. [Hint: Consider binary expansions of integers.]