Although we cannot divide both sides of a congruence by any integer to produce a valid congruence, we can if this integer is relatively prime to the modulus. Theorem 7 establishes this important fact. We use Lemma 2 in the proof.

**Theorem 7** Let $m$ be a positive integer and let $a$, $b$, and $c$ be integers. If $ac \equiv bc \pmod{m}$ and $\gcd(c, m) = 1$, then $a \equiv b \pmod{m}$.

**Proof:** Because $ac \equiv bc \pmod{m}$, $m \mid ac - bc = c(a - b)$, By Lemma 2, because $\gcd(c, m) = 1$, it follows that $m \mid a - b$. We conclude that $a \equiv b \pmod{m}$.

**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 101.

6. How many zeros are there at the end of 100!?

7. Express in pseudocode the trial division algorithm for determining whether an integer is prime.

8. Express in pseudocode the algorithm described in the text for finding the prime factorization of an integer.

9. Show that if $a^m + 1$ is composite if $a$ and $m$ are integers greater than 1 and $m$ is odd. [Hint: Show that $x + 1$ is a factor of the polynomial $x^m + 1$ if $m$ is odd.]

10. Show that if $2^m + 1$ is an odd prime, then $m = 2^n$ for some nonnegative integer $n$. [Hint: First show that the polynomial identity $x^m + 1 = (x + 1)(x^{m-1} - x^{m-2} + \cdots - x + 1)$ holds, where $m = kt$ and $t$ is odd.]

11. 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.

12. Prove that for every positive integer $n$, there are $n$ consecutive composite integers. [Hint: Consider the $n$ consecutive integers starting with $(n + 1)! + 2$.]

13. Prove or disprove that there are three consecutive odd positive integers that are primes, that is, odd primes of the form $p, p + 2, p + 4$.

14. Which positive integers less than 12 are relatively prime to 12?

15. Which positive integers less than 30 are relatively prime to 30?

16. 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

17. 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

18. 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 integers.
   b) Show that $2^{p-1}(2^p - 1)$ is a perfect number when $2^p - 1$ is prime.

19. Show that if $2^p - 1$ is prime, then $n$ is prime. [Hint: Use the identity $2^{ab} - 1 = (2^a - 1) \cdot (2^{b-1}) + 2^{b-2} + \cdots + 2^1$ + 1).

20. Determine whether each of these integers is prime, verifying some of Mersenne's claims.

   a) 27 - 1
   b) 29 - 1
   c) 211 - 1
   d) 213 - 1

The value of the Euler $\phi$-function at the positive integer $n$ is defined to be the number of positive integers less than $n$ that are relatively prime to $n$. [Note: $\phi$ is the Greek letter phi.]

21. Find these values of the Euler $\phi$-function.

   a) $\phi(4)$
   b) $\phi(10)$
   c) $\phi(13)$

22. Show that $n$ is prime if and only if $\phi(n) = n - 1$.

23. What is the value of $\phi(p^k)$ when $p$ is prime and $k$ is a positive integer?

24. What are the greatest common divisors of these pairs of integers?

   a) $2 \cdot 3 \cdot 5 \cdot 5^2, 2^3 \cdot 5^3 \cdot 2^3 \cdot 5^2$
   b) $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13, 2^{11} \cdot 3^9 \cdot 11 \cdot 17^{14}$
4.3 Primes and Greatest Common Divisors

25. What are the greatest common divisors of each of these pairs of integers?
   a) \(3^7 \cdot 5^3 \cdot 7^3, 2^{11} \cdot 3^5 \cdot 5^9\)
   b) \(11 \cdot 13 \cdot 17, 2^9 \cdot 3^7 \cdot 5^2 \cdot 7^3\)
   c) \(23^{31}, 23^{17}\)
   d) \(41 \cdot 43 \cdot 53, 41 \cdot 43 \cdot 53\)
   e) \(3^{13} \cdot 5^{17}, 2^{12} \cdot 7^{21}\)
   f) \(1111, 0\)

26. What is the least common multiple of each pair in Exercise 24?

27. Find \(\text{gcd}(1000, 625)\) and \(\text{lcm}(1000, 625)\) and verify that \(\text{gcd}(1000, 625) \cdot \text{lcm}(1000, 625) = 1000 \cdot 625\).

28. Find \(\text{gcd}(92928, 123552)\) and \(\text{lcm}(92928, 123552)\), and verify that \(\text{gcd}(92928, 123552) \cdot \text{lcm}(92928, 123552) = 92928 \cdot 123552\). [Hint: First find the prime factorizations of 92928 and 123552.]

29. If the product of two integers is \(2^7 \cdot 3^8 \cdot 5^2 \cdot 7^{11}\) and their greatest common divisor is \(2^3 \cdot 5^4\), what is their least common multiple?

30. Show that if \(a\) and \(b\) are positive integers, then \(\text{gcd}(a, b) \cdot \text{lcm}(a, b) = \text{gcd}(a, b) \cdot \text{lcm}(a, b)\). [Hint: Use the prime factorizations of \(a\) and \(b\) and the formulae for \(\text{gcd}(a, b)\) and \(\text{lcm}(a, b)\) in terms of these factorizations.]

31. Use the Euclidean algorithm to find
   a) \(\text{gcd}(1, 5)\)
   b) \(\text{gcd}(100, 101)\)
   c) \(\text{gcd}(123, 277)\)
   d) \(\text{gcd}(1529, 14039)\)
   e) \(\text{gcd}(1529, 14038)\)
   f) \(\text{gcd}(1111, 11111)\)

32. Use the Euclidean algorithm to find
   a) \(\text{gcd}(12, 18)\)
   b) \(\text{gcd}(111, 201)\)
   c) \(\text{gcd}(1001, 1331)\)
   d) \(\text{gcd}(12345, 54321)\)
   e) \(\text{gcd}(1000, 5040)\)
   f) \(\text{gcd}(9888, 6060)\)

33. How many divisions are required to find \(\text{gcd}(21, 34)\) using the Euclidean algorithm?

34. How many divisions are required to find \(\text{gcd}(34, 55)\) using the Euclidean algorithm?

35. Show that if \(a\) and \(b\) are both positive integers, then
   \((2^a - 1) \mod (2^b - 1) = 2^r \mod b - 1\).

36. Use Exercise 36 to show that if \(a\) and \(b\) are positive integers, then \(\text{gcd}(2^{a} - 1, 2^{b} - 1) = 2^{\text{gcd}(a, b) - 1}\).
   [Hint: Show that the remainders obtained when the Euclidean algorithm is used to compute \(\text{gcd}(2^{a} - 1, 2^{b} - 1)\) are of the form \(2^r - 1\), where \(r\) is a remainder arising when the Euclidean algorithm is used to find \(\text{gcd}(a, b)\).]

37. Use Exercise 37 to show that the integers \(2^{35} - 1, 2^{34} - 1, 2^{33} - 1, 2^{31} - 1, 2^{29} - 1, \) and \(2^{25} - 1\) are pairwise relatively prime.

38. Using the method followed in Example 17, express the greatest common divisor of each of these pairs of integers as a linear combination of these integers.

39. Prove that the product of any three consecutive integers is divisible by 6.

**Answer:**

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) \(10001, 13422\)

**The extended Euclidean algorithm** can be used to express \(\text{gcd}(a, b)\) as a linear combination with integer coefficients of the integers \(a\) and \(b\). We set \(s_0 = 1, s_1 = 0, t_0 = 0, t_1 = 1\) 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 \(\text{gcd}(a, b)\), as shown in the text. It can be shown (see [Ro10]) that \(\text{gcd}(a, b) = s_n a + t_n b\). The main advantage of the extended Euclidean algorithm is that it uses one pass through the steps of the Euclidean algorithm to find Bezout coefficients of \(a\) and \(b\), unlike the method in the text which uses two passes.

41. Use the extended Euclidean algorithm to express \(\text{gcd}(26, 91)\) as a linear combination of 26 and 91.

42. Use the extended Euclidean algorithm to express \(\text{gcd}(252, 356)\) as a linear combination of 252 and 356.

43. Use the extended Euclidean algorithm to express \(\text{gcd}(144, 89)\) as a linear combination of 144 and 89.

44. Use the extended Euclidean algorithm to express \(\text{gcd}(1001, 10001)\) as a linear combination of 1001 and 10001.

45. Describe the extended Euclidean algorithm using pseudocode.

46. Find the smallest positive integer with exactly \(n\) different positive factors when \(n\) is
   a) \(3\)
   b) \(4\)
   c) \(5\)
   d) \(6\)
   e) \(10\)

47. 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) \(0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, \ldots\)
   b) \(1, 2, 3, 2, 5, 2, 7, 2, 3, 2, 11, 2, 13, 2, \ldots\)
   c) \(1, 2, 3, 2, 4, 2, 4, 3, 4, 2, 6, 2, 4, \ldots\)
   d) \(1, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1, \ldots\)
   e) \(1, 2, 3, 5, 5, 7, 7, 7, 7, 11, 11, 13, 13, \ldots\)
   f) \(1, 2, 6, 30, 210, 2310, 30030, 510510, 96999690, 223092870, \ldots\)

48. 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) \(2, 2, 3, 5, 7, 11, 11, 11, 11, 13, 13, \ldots\)
   b) \(0, 1, 2, 2, 3, 3, 4, 4, 4, 5, 5, 6, \ldots\)
   c) \(1, 0, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, \ldots\)
   d) \(1, -1, -1, 0, -1, 1, -1, 0, 0, 0, 0, 0, \ldots\)
   e) \(1, 1, 1, 1, 0, 0, 1, 0, 1, 0, 1, 0, 0, \ldots\)
   f) \(4, 9, 25, 49, 121, 169, 289, 361, 529, 841, 961, 1369, \ldots\)

49. Prove that the product of any three consecutive integers is divisible by 6.
EXAMPLE 12  Determine whether 2 and 3 are primitive roots modulo 11.

**Solution:** When we compute the powers of 2 in $\mathbb{Z}_{11}$, we obtain $2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 = 5, 2^5 = 10, 2^6 = 9, 2^7 = 7, 2^8 = 3, 2^9 = 6, 2^{10} = 1$. Because every element of $\mathbb{Z}_{11}$ is a power of 2, 2 is a primitive root of 11.

When we compute the powers of 3 modulo 11, we obtain $3^1 = 3, 3^2 = 9, 3^3 = 5, 3^4 = 4, 3^5 = 1$. We note that this pattern repeats when we compute higher powers of 3. Because not all elements of $\mathbb{Z}_{11}$ are powers of 3, we conclude that 3 is not a primitive root of 11.

An important fact in number theory is that there is a primitive root modulo $p$ for every prime $p$. We refer the reader to [Ro10] for a proof of this fact. Suppose that $p$ is prime and $r$ is a primitive root modulo $p$. If $a$ is an integer between 1 and $p - 1$, that is, an element of $\mathbb{Z}_p$, we know that there is an unique exponent $e$ such that $r^e = a$ in $\mathbb{Z}_p$, that is, $r^e \equiv a \pmod{p}$.

**DEFINITION 4**  Suppose that $p$ is a prime, $r$ is a primitive root modulo $p$, and $a$ is an integer between 1 and $p - 1$ inclusive. If $r^e \equiv a \pmod{p}$ and $0 \leq e \leq p - 1$, we say that $e$ is the discrete logarithm of $a$ modulo $p$ to the base $r$ and we write $\log_r a = e$ (where the prime $p$ is understood).

EXAMPLE 13  Find the discrete logarithms of 3 and 5 modulo 11 to the base 2.

**Solution:** When we computed the powers of 2 modulo 11 in Example 12, we found that $2^8 = 3$ and $2^4 = 5$ in $\mathbb{Z}_{11}$. Hence, the discrete logarithms of 3 and 5 modulo 11 to the base 2 are 8 and 4, respectively. (These are the powers of 2 that equal 3 and 5, respectively, in $\mathbb{Z}_{11}$.) We write $\log_2 3 = 8$ and $\log_2 5 = 4$ (where the modulus 11 is understood and not explicitly noted in the notation).

The discrete logarithm problem is hard!

### Chap. 4.4

**Exercises**

1. Show that 15 is an inverse of 7 modulo 26.
2. Show that 937 is an inverse of 13 modulo 2436.
3. By inspection (as discussed prior to Example 1), find an inverse of 4 modulo 9.
4. By inspection (as discussed prior to Example 1), find an inverse of 2 modulo 17.
5. Find an inverse of $a$ modulo $m$ for each of these pairs of relatively prime integers using the method followed in Example 2.
   a) $a = 4, m = 9$
   b) $a = 19, m = 141$
   c) $a = 55, m = 89$
   d) $a = 89, m = 232$
6. Find an inverse of $a$ modulo $m$ for each of these pairs of relatively prime integers using the method followed in Example 2.
   a) $a = 2, m = 17$
   b) $a = 34, m = 89$
   c) $a = 144, m = 233$
   d) $a = 200, m = 1001$
7. 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 7 of Section 4.3 to show that $b \equiv c \pmod{m}$.
8. Show that an inverse of $a$ modulo $m$, where $a$ is an integer and $m > 2$ is a positive integer, does not exist if gcd($a$, $m$) $> 1$.
9. Solve the congruence $4x \equiv 5 \pmod{9}$ using the inverse of 4 modulo 9 found in part (a) of Exercise 5.
10. Solve the congruence $2x \equiv 7 \pmod{17}$ using the inverse of 2 modulo 7 found in part (a) of Exercise 6.
11. Solve each of these congruences using the modular inverses found in parts (b), (c), and (d) of Exercise 5.
   a) $19x \equiv 4 \pmod{141}$
   b) $55x \equiv 34 \pmod{89}$
   c) $89x \equiv 2 \pmod{232}$
12. Solve each of these congruences using the modular inverses found in parts (b), (c), and (d) of Exercise 6.
   a) $34x \equiv 77 \pmod{89}$
   b) $144x \equiv 4 \pmod{233}$
   c) $200x \equiv 13 \pmod{1001}$

13. Find the solutions of the congruence $15x^2 + 19x \equiv 5 \pmod{11}$. [Hint: Show the congruence is equivalent to the congruence $15x^2 + 19x + 6 \equiv 0 \pmod{11}$]. Factor the left-hand side of the congruence; show that a solution of the quadratic congruence is a solution of one of the two different linear congruences.

14. Find the solutions of the congruence $12x^2 + 25x \equiv 10 \pmod{11}$. [Hint: Show the congruence is equivalent to the congruence $12x^2 + 25x + 12 \equiv 0 \pmod{11}$]. Factor the left-hand side of the congruence; show that a solution of the quadratic congruence is a solution of one of two different linear congruences.

*15. Show that if $m$ is an integer greater than 1 and $ac \equiv bc \pmod{m}$, then $a \equiv b \pmod{m/\gcd(c, m)}$.

16. 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 $10! \equiv -1 \pmod{11}$.

17. Show that if $p$ is prime, the only solutions of $x^2 \equiv 1 \pmod{p}$ are integers $x$ such that $x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$.

*18. a) Generalize the result in part (a) of Exercise 16; 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 17.]
   b) From part (a) conclude that $(p - 1)! \equiv -1 \pmod{p}$ whenever $p$ is prime. This result is known as Wilson's theorem.

19. 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 $1 \cdot a, 2 \cdot a, \ldots, (p - 1)a$ 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
      $$ (p - 1)! \equiv a^{p-1} (p - 1)! \pmod{p}. $$

*20. Use the construction in the proof of the Chinese remainder theorem to find all solutions to the system of congruences $x \equiv 2 \pmod{3}$, $x \equiv 1 \pmod{4}$, and $x \equiv 3 \pmod{5}$.

21. Use the construction in the proof of the Chinese remainder theorem to find all solutions to the system of congruences $x \equiv 1 \pmod{2}$, $x \equiv 2 \pmod{3}$, $x \equiv 3 \pmod{5}$, and $x \equiv 4 \pmod{11}$.

22. Solve the system of congruences $x \equiv 3 \pmod{6}$ and $x \equiv 4 \pmod{7}$ using the method of back substitution.

23. Solve the system of congruences in Exercise 20 using the method of back substitution.

24. Solve the system of congruences in Exercise 21 using the method of back substitution.

25. Write out in pseudocode an algorithm for solving a simultaneous system of linear congruences based on the construction in the proof of the Chinese remainder theorem.

*26. Find all solutions, if any, to the system of congruences $x \equiv 5 \pmod{6}$, $x \equiv 3 \pmod{10}$, and $x \equiv 8 \pmod{15}$.

*27. Find all solutions, if any, to the system of congruences $x \equiv 7 \pmod{9}$, $x \equiv 4 \pmod{12}$, and $x \equiv 16 \pmod{21}$.

28. 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 positive integers $m_1, m_2, \ldots, m_n$ are pairwise relatively prime, can be represented uniquely by the $n$-tuple $(a \pmod{m_1}, a \pmod{m_2}, \ldots, a \pmod{m_n})$.

*29. Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime integers greater than or equal to 2. Show that if $a \equiv b \pmod{m_i}$ for $i = 1, 2, \ldots, n$, then $a \equiv b \pmod{m}$, where $m = m_1 m_2 \cdots m_n$. (This result will be used in Exercise 30 to prove the Chinese remainder theorem. Consequently, do not use the Chinese remainder theorem to prove it.)

*30. Complete the proof of the Chinese remainder theorem by showing that the simultaneous solution of a system of linear congruences modulo pairwise relatively prime moduli 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 29, conclude that $m = m_1 m_2 \cdots m_n | x - y$.]

31. Which integers leave a remainder of 1 when divided by 2 and also leave a remainder of 1 when divided by 3?

32. Which integers are divisible by 5 but leave a remainder of 1 when divided by 3?

33. Use Fermat's little theorem to find $7^{121} \pmod{13}$.

34. Use Fermat's little theorem to find $23^{1002} \pmod{41}$.

35. Use Fermat's little theorem to show that if $p$ is prime and $p \nmid a$, then $a^{p-2}$ is an inverse of a modulo $p$.

36. Use Exercise 35 to find an inverse of 5 modulo 41.

*37. a) Show that $2^{340} \equiv 1 \pmod{11}$ by Fermat's little theorem and noting that $2^{340} = (2^{10})^{34}$.
   b) Show that $2^{340} \equiv 1 \pmod{31}$ using the fact that $2^{340} = (2^{5})^{68} \equiv 32^{68}$.
   c) Conclude from parts (a) and (b) that $2^{340} \equiv 1 \pmod{341}$. 

37c.
These last two congruences hold because $\sum_{i=1}^{10} x_i \equiv 0 \mod 10$ and $11 \not| ja$, because $11 \not| j$ and $11 \not| a$. We conclude that $y_1 y_2 \ldots y_{10}$ is not a valid ISBN. So, we have detected the single error.

Now suppose that two unequal digits have been transposed. It follows that there are distinct integers $j$ and $k$ such that $y_j = x_k$ and $y_k = x_j$, and $y_i = x_i$ for $i \neq j$ and $i \neq k$. Hence,

$$\sum_{i=1}^{10} iy_i = \left( \sum_{i=1}^{10} ix_i \right) + (jx_k - jx_j) + (kx_j - kx_k) \equiv (j - k)(x_k - x_j) \not\equiv 0 \mod 11,$$

because $\sum_{i=1}^{10} x_i \equiv 0 \mod 10$ and $11 \not| (j - k)$ and $11 \not| (x_k - x_j)$. We see that $y_1 y_2 \ldots y_{10}$ is not a valid ISBN. Thus, we can detect the interchange of two unequal digits.

Exercises

1. Which memory locations are assigned by the hashing function $h(k) = k \mod 97$ to the records of insurance company customers with these Social Security numbers?
   a) 034567981  
   b) 183211232  
   c) 220195744  
   d) 987255335

2. 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) 43222187  
   c) 372201919  
   d) 501338753

3. 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.

Another way to resolve collisions in hashing is to use double hashing. We use an initial hashing function $h(k) = k \mod p$ where $p$ is prime. We also use a second hashing function $g(k) = (k + 1) \mod (p - 2)$. When a collision occurs, we use a probing sequence $h(k, i) = (h(k) + i \cdot g(k)) \mod p$.

4. Use the double hashing procedure we have described with $p = 4969$ to assign memory locations to files for employees with social security numbers $k_1 = 132489971$, $k_2 = 509496993$, $k_3 = 546332190$, $k_4 = 034367980$, $k_5 = 047900151$, $k_6 = 329938157$, $k_7 = 212228844$, $k_8 = 325510778$, $k_9 = 353354519$, $k_{10} = 053708912$.

5. What sequence of pseudorandom numbers is generated using the linear congruential generator $x_{n+1} = (3x_n + 2) \mod 13$ with seed $x_0 = 1$?

6. What sequence of pseudorandom numbers is generated using the linear congruential generator $x_{n+1} = (4x_n + 1) \mod 7$ with seed $x_0 = 2$?

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

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

The middle-square method for generating pseudorandom numbers begins with an $n$-digit integer. This number is squared, initial zeros are appended to ensure that the result has $2n$ digits, and its middle $n$ digits are used to form the next number in the sequence. This process is repeated to generate additional terms.

9. Find the first eight terms of the sequence of four-digit pseudorandom numbers generated by the middle square method starting with 2357.

10. Explain why both 3792 and 2916 would be bad choices for the initial term of a sequence of four-digit pseudorandom numbers generated by the middle square method.

The power generator is a method for generating pseudorandom numbers. To use the power generator, parameters $p$ and $d$ are specified, where $p$ is a prime, $d$ is a positive integer such that $p \not| d$, and a seed $x_0$ is specified. The pseudorandom numbers $x_1, x_2, \ldots$ are generated using the recursive definition $x_{n+1} = x_n^d \mod p$.

11. Find the sequence of pseudorandom numbers generated by the power generator with $p = 7$, $d = 3$, and seed $x_0 = 2$.

12. Find the sequence of pseudorandom numbers generated by the power generator with $p = 11$, $d = 2$, and seed $x_0 = 3$.

13. Suppose you received these bit strings over a communications link, where the last bit is a parity check bit. In which string are you sure there is an error?
   a) 0000011111  
   b) 1010101010  
   c) 11111100000  
   d) 10111101111

14. Prove that a parity check bit can detect an error in a string if and only if the string contains an odd number of errors.
1. Encrypt the message DO NOT PASS GO by translating the letters into numbers, applying the given encryption function, 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) $f(p) = (3p + 7) \mod 26$

2. Encrypt the message STOP POLLUTION by translating the letters into numbers, applying the given encryption function, and then translating the numbers back into letters.
   a) $f(p) = (p + 4) \mod 26$
   b) $f(p) = (p + 21) \mod 26$
   c) $f(p) = (17p + 22) \mod 26$

3. Encrypt the message WATCH YOUR STEP by translating the letters into numbers, applying the given encryption function, and then translating the numbers back into letters.
   a) $f(p) = (p + 14) \mod 26$
   b) $f(p) = (14p + 21) \mod 26$
   c) $f(p) = (-7p + 1) \mod 26$

4. Decrypt these messages that were encrypted using the Caesar cipher.
   a) EOXMHDQV
   b) WHVWWRGDB
   c) HDWGLPWXP

5. Decrypt these messages encrypted using the shift cipher $f(p) = (p + 10) \mod 26$.
   a) CEBXNOBXGBY
   b) LOWIPOSXN
   c) DSWOPBYPX

6. Suppose that when a long string of text is encrypted using a shift cipher $f(p) = (p + k) \mod 26$, the most common letter in the ciphertext is X. What is the most likely value for k assuming that the distribution of letters in the text is typical of English text?

7. Suppose that when a string of English text is encrypted using a shift cipher $f(p) = (p + k) \mod 26$, the resulting ciphertext is DY CVOOZ ZOBMRKXMO DY NBOKW. What was the original plaintext string?

8. Suppose that the ciphertext DVE CFMV KF NFEUVI, REU KYRK ZJ KYV JVVU FW JTZVETV was produced by encrypting a plaintext message using a shift cipher. What is the original plaintext?

9. Suppose that the ciphertext ERC WYJGMIRXPC EHZERCHI XIGLRSPSKC MW MRHMWXM RKYMWLEPPF JVSQ QEMK MG was produced by encrypting a plaintext message using a shift cipher. What is the original plaintext?

10. Determine whether there is a key for which the encryption function for the shift cipher is the same as the decryption function.

11. What is the decryption function for an affine cipher if the encryption function is $c = (15p + 13) \mod 26$?

12. Find all pairs of integers keys $(a, b)$ for affine ciphers for which the encryption function $c = (ap + b) \mod 26$ is the same as the corresponding decryption function.

13. Suppose that the most common letter and the second most common letter in a long ciphertext produced by encrypting a plaintext using an affine cipher $f(p) = (ap + b) \mod 26$ are Z and J, respectively. What are the most likely values of $a$ and $b$?

14. Encrypt the message GRIZZLY BEARS using blocks of five letters and the transposition cipher based on the permutation of $(1, 2, 3, 4, 5)$ with $\sigma(1) = 3, \sigma(2) = 5, \sigma(3) = 1, \sigma(4) = 2, \sigma(5) = 4$. For this exercise, use the letter X as many times as necessary to fill out the final block of fewer than five letters.

15. Decrypt the message EABW EFRO ATM R ASIN which is the ciphertext produced by encrypting a plaintext message using the transposition cipher with blocks of four letters and the permutation $\sigma$ of $(1, 2, 3, 4)$ defined by $\sigma(1) = 3, \sigma(2) = 1, \sigma(3) = 4, \sigma(4) = 2$.

16. Suppose that you know that a ciphertext was produced by encrypting a plaintext message with a transposition cipher. How might you go about breaking it?

17. Suppose you have intercepted a ciphertext message and when you determine the frequencies of letters in this message, you find the frequencies are similar to the frequency of letters in English text. Which type of cipher do you suspect was used?

The **Vigenère cipher** is a block cipher, with a key that is a string of letters with numerical equivalents $k_1 k_2 \ldots k_m$, where $k_i \in \mathbb{Z}_{26}$ for $i = 1, 2, \ldots, m$. Suppose that the numerical equivalents of the letters of a plaintext block are $p_1 p_2 \ldots p_m$. The corresponding numerical ciphertext block is $(p_1 + k_1) \mod 26 (p_2 + k_2) \mod 26 \ldots (p_m + k_m) \mod 26$. Finally, we translate back to letters. For example, suppose that the key string is RED, with numerical equivalents $17 4 3$. Then, the plaintext ORANGE, with numerical equivalents $14 17 00 13 06 04$, is encrypted by first splitting it into two blocks $14 17 00$ and $13 06 04$. Then, in each block we shift the first letter by 17, the second by 4, and the third by 3. We obtain 5 21 03 and 04 10 07. The ciphertext is FVDEKH.

18. Use the Vigenère cipher with key BLUE to encrypt the message SNOWFALL.

19. The ciphertext OIKYWHBXX was produced by encrypting a plaintext message using the Vigenère cipher with key HOT. What is the plaintext message?
4.6 Cryptography

28. Suppose that \( (n, e) \) is an RSA encryption key, with \( n = pq \) where \( p \) and \( q \) are large primes and \( \gcd(e, (p-1)(q-1)) = 1 \). Furthermore, suppose that \( d \) is an inverse of \( e \) modulo \( (p-1)(q-1) \). Suppose that \( C^d \equiv M^e \pmod{pq} \). In the text we showed that RSA encryption, that is, the congruence \( C^d \equiv M \pmod{pq} \) holds when \( \gcd(M, pq) = 1 \). Show that this decryption congruence also holds when \( \gcd(M, pq) > 1 \). [Hint: Use congruences modulo \( p \) and modulo \( q \) and apply the Chinese remainder theorem.]

29. Describe the steps that Alice and Bob follow when they use the Diffie-Hellman key exchange protocol to generate a shared key. Assume that they use the prime \( p = 23 \) and take \( a = 5 \), which is a primitive root of 23, and that Alice selects \( k_A = 8 \) and Bob selects \( k_B = 5 \). (You may want to use some computational aid.)

30. Describe the steps that Alice and Bob follow when they use the Diffie-Hellman key exchange protocol to generate a shared key. Assume that they use the prime \( p = 101 \) and take \( a = 2 \), which is a primitive root of 101, and that Alice selects \( k_A = 7 \) and Bob selects \( k_B = 9 \). (You may want to use some computational aid.)

In Exercises 31–32 suppose that Alice and Bob have these public keys and corresponding private keys: \( (n_{Alice}, e_{Alice}) = (2867, 7) \), \( d_{Alice} = 1183 \), \( (n_{Bob}, e_{Bob}) = (3127, 21) \), \( d_{Bob} = 1149 \). First express your answers without carrying out the calculations. Then, using a computational aid, if available, perform the calculation to get the numerical answers.

31. Alice wants to send to all her friends, including Bob, the message "SELL EVERYTHING" so that he knows that she sent it. What should she send to her friends, assuming she signs the message using the RSA cryptosystem.

32. Alice wants to send to Bob the message "BUY NOW" so that he knows that she sent it and so that only Bob can read it. What should she send to Bob, assuming she signs the message and then encrypts it using Bob's public key?

33. We describe a basic key exchange protocol using private key cryptography upon which more sophisticated protocols for key exchange are based. Encryption within the protocol is done using a private key cryptosystem (such as AES) that is considered secure. The protocol involves three parties, Alice and Bob, who wish to exchange a key, and a trusted third party Cathy. Assume that Alice has a secret key \( k_{Alice} \) that only she and Cathy know, and Bob has a secret key \( k_{Bob} \) which only he and Cathy know. The protocol has three steps:

(i) Alice sends the trusted third party Cathy the message "request a shared key with Bob" encrypted using Alice's key \( k_{Alice} \).

(ii) Cathy sends back to Alice a key \( k_{Alice,Bob} \), which she generates, encrypted using the key \( k_{Alice} \), followed by this same key \( k_{Alice,Bob} \) encrypted using Bob's key, \( k_{Bob} \).

(iii) Alice sends to Bob the key \( k_{Alice,Bob} \) encrypted using \( k_{Bob} \), known only to Bob and to Cathy.

Explain why this protocol allows Alice and Bob to share the secret key \( k_{Alice,Bob} \), known only to them and to Cathy.
Template for Proofs by Mathematical Induction

1. Express the statement that is to be proved in the form “for all \( n \geq b \), \( P(n) \)” for a fixed integer \( b \).
2. Write out the words “Basis Step.” Then show that \( P(b) \) is true, taking care that the correct value of \( b \) is used. This completes the first part of the proof.
3. Write out the words “Inductive Step.”
4. State, and clearly identify, the inductive hypothesis, in the form “assume that \( P(k) \) is true for an arbitrary fixed integer \( k \geq b \).”
5. State what needs to be proved under the assumption that the inductive hypothesis is true. That is, write out what \( P(k + 1) \) says.
6. Prove the statement \( P(k + 1) \) making use the assumption \( P(k) \). Be sure that your proof is valid for all integers \( k \) with \( k \geq b \), taking care that the proof works for small values of \( k \), including \( k = b \).
7. Clearly identify the conclusion of the inductive step, such as by saying “this completes the inductive step.”
8. After completing the basis step and the inductive step, state the conclusion, namely that by mathematical induction, \( P(n) \) is true for all integers \( n \) with \( n \geq b \).

It is worthwhile to revisit each of the mathematical induction proofs in Examples 1–14 to see how these steps are completed. It will be helpful to follow these guidelines in the solutions of the exercises that ask for proofs by mathematical induction. The guidelines that we presented can be adapted for each of the variants of mathematical induction that we introduce in the exercises and later in this chapter.

Chap 5.1 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. Be sure to identify where you use the inductive hypothesis.

3. Let \( P(n) \) be the statement that \( 1^2 + 2^2 + \cdots + n^2 = n(n + 1)(2n + 1)/6 \) 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, identifying where you use the inductive hypothesis.
   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 \( 1^3 + 2^3 + \cdots + n^3 = (n(n + 1)/2)^2 \) 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, identifying where you use the inductive hypothesis.
   f) Explain why these steps show that this formula is true whenever \( n \) is a positive integer.

5. Prove that \( 1^2 + 3^2 + 5^2 + \cdots + (2n + 1)^2 = (n + 1)(2n + 3)/3 \) whenever \( n \) is a nonnegative integer.

6. Prove that \( 1 \cdot 1! + 2 \cdot 2! + \cdots + n \cdot n! = (n + 1)! - 1 \) whenever \( n \) is a positive integer.

7. Prove that \( 3 + 3 \cdot 5 + 3 \cdot 5^2 + \cdots + 3 \cdot 5^n = 3(5^{n+1} - 1)/4 \) 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
\[
\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \cdots + \frac{1}{n(n+1)}
\]
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
\[
\frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \cdots + \frac{1}{2^n}
\]
by examining the values of this expression for small values of \( n \).
b) Prove the formula you conjectured in part (a).

12. Prove that
\[
\sum_{j=0}^{n} \left( -\frac{1}{2} \right)^j = \frac{2^{n+1} + (-1)^n}{3 \cdot 2^n}
\]
whenever \( n \) is a nonnegative integer.

13. Prove that \( i^2 - 2^2 + 3^2 - \cdots + (-1)^{n-1}n^2 = (-1)^{n-1}n(n+1)/2 \) whenever \( n \) is a positive integer.

14. Prove that for every positive integer \( n \), \( \sum_{k=1}^{n} k2^k = (n+1)(2^{n+1} + 2) \).

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 \( n \),
\[
1 \cdot 2 + 2 \cdot 3 + 2 \cdot 4 + \cdots + n(n+1)(n+2)
= n(n+1)(n+2)(n+3)/4.
\]

17. Prove that \( \sum_{j=1}^{n} j^4 = n(n+1)(2n+1)(3n^2 + 3n - 1)/30 \) 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 \( 3^0 < n! \) if \( n \) is an integer greater than 1.

21. Prove that \( 2^n > n^2 \) if \( n \) is an integer greater than 4.

22. For which nonnegative integers \( n \) is \( n^2 \leq n! \)? Prove your answer.

23. For which nonnegative integers \( n \) is \( 2n + 3 \leq 2^n \)? 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 if \( h > -1 \), then \( 1 + nh \leq (1 + h)^n \) 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 \( H_{2^n} \leq 1 + n \) 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 \( 4n+1 + 52n-1 \) whenever \( n \) is a positive integer.

*37. Prove that if \( n \) is a positive integer, then \( 133 \) divides \( 11n+1 + 12^{2n-1} \).

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
\[
\bigcup_{j=1}^{n} A_j \subseteq \bigcup_{j=1}^{n} B_j.
\]