4.1

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

4. Prove that part (*iii*) of Theorem 1 is true.

18. Suppose that a and b are integers, $a \equiv 11 \pmod{19}$, and $b \equiv 3 \pmod{19}$. Find the integer c with $0 \le c \le 18$ 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)** $c \equiv a^3 + 4b^3 \pmod{19}$.

40. Show that if $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$, where a, b, c, d, and m are integers with $m \ge 2$, then $a - c \equiv b - d \pmod{m}$.

42. Show that if a, b, c, and m are integers such that $m \ge 2$, $c > 0$, and $a \equiv b \pmod{m}$, then $ac \equiv bc \pmod{mc}$.

52. Write out the addition and multiplication tables for $\mathbf{Z}_6$ (where by addition and multiplication we mean $+_6$ and $\cdot_6$).

4.2

10. Convert each of the integers in Exercise 6 from a binary expansion to a hexadecimal expansion.
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.
25. Use Algorithm 5 to find 7^{644} **mod** 645.
53. 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 011110010001. How many bits are required to represent a number with *n*
decimal digits using this type of encoding?
59. Describe an algorithm for finding the difference of two binary expansions.
63. Estimate the complexity of Algorithm 1 for finding the base *b* expansion of an integer *n* in terms of the number of divisions used.

4.3

3. Find the prime factorization of each of these integers.

a) 88 **b)** 126 **c)** 729 **d)** 1001 **e)** 1111 **f)** 909,090

9. Show that $a^m + 1$ 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.]

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

The value of the **Euler $\boldsymbol{\phi}$-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. For instance, $\phi(6) = 2$ because of the positive integers less or equal to 6, only 1 and 5 are relatively prime to 6. [*Note:* ϕ is the Greek letter phi.]

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

44. Use the extended Euclidean algorithm to express gcd(1001, 100001) as a linear combination of 1001 and 100001.

52. Prove or disprove that $p_1 p_2 \cdots p_n + 1$ is prime for every positive integer n, where $p_1, p_2, \ldots, p_n$ are the n smallest prime numbers.

4.4

2. Show that 937 is an inverse of 13 modulo 2436.

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) $a = 200$, $m = 1001$

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) $200x \equiv 13 \pmod{1001}$

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 $x \equiv 4 \pmod{11}$.

Let n be a positive integer and let $n - 1 = 2^s t$, 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 $b^t \equiv 1 \pmod{n}$ or $b^{2^j t} \equiv -1 \pmod{n}$ for some j with $0 \le j \le s - 1$. It can be shown (see [Ro10]) that a composite integer n passes Miller's test for fewer than $n/4$ bases b with $1 < b < n$. A composite positive integer n that passes Miller's test to the base b is called a **strong pseudoprime to the base *b***.

45. Show that 2047 is a strong pseudoprime to the base 2 by showing that it passes Miller's test to the base 2, but is composite.

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.

61. Show that if p is an odd prime and a and b are integers with $a \equiv b \pmod{p}$, then

$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right).$$

66. Find all solutions of the congruence $x^2 \equiv 16 \pmod{105}$. [*Hint:* Find the solutions of this congruence modulo 3, modulo 5, and modulo 7, and then use the Chinese remainder theorem.]

4.5

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

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.

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 $p \nmid d$, 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 $x_0 = 2$.

20. One digit in each of these identification numbers of a postal money order is smudged. Can you recover the smudged digit, indicated by a Q, in each of these numbers?

a) Q1223139784

b) 6702120Q988

c) 27Q41007734

d) 213279032Q1

Periodicals are identified using an **International Standard Serial Number (ISSN)**. An ISSN consists of two blocks of four digits. The last digit in the second block is a check digit. This check digit is determined by the congruence $d_8 \equiv 3d_1 + 4d_2 + 5d_3 + 6d_4 + 7d_5 + 8d_6 + 9d_7 \pmod{11}$. When $d_8 \equiv 10 \pmod{11}$, we use the letter X to represent d_8 in the code.

35. Does the check digit of an ISSN detect every error where two consecutive digits are accidentally interchanged? Justify your answer with either a proof or a counterexample.

Chapter 4—Test 1

1. Decide whether $175 \equiv 22 \pmod{17}$.

2. Find the prime factorization of 45617.

3. Use the Euclidean algorithm to find

(a) $\gcd(203, 101)$.

(b) $\gcd(34, 21)$.

4. The binary expansion of an integer is $(110101)_2$. What is the base 10 expansion of this integer?

5. Prove or disprove that a positive integer congruent to 1 modulo 4 cannot have a prime factor congruent to 3 modulo 4.

Chapter 4—Test 2

1. Find the prime factorization of 111111.

2. Find each of the following values.
(a) $18 \textbf{ mod } 7$
(b) $-88 \textbf{ mod } 13$
(c) $289 \textbf{ mod } 17$

3. Let m be a positive integer, and let a, b, and c be integers. Show that if $a \equiv b \pmod{m}$, then $a-c \equiv b-c \pmod{m}$.

4. Use the Euclidean algorithm to find
(a) $\gcd(201, 302)$.
(b) $\gcd(144, 233)$.

5. What is the hexadecimal expansion of the $(\mathrm{ABC})_{16} + (\mathrm{2F5})_{16}$?

6. Prove or disprove that there are six consecutive composite integers.