each requiring $O((\log_2 m)^2)$ bit operations. Therefore, a total of $O((\log_2 m)^2 \log_2 N)$ bit operations is needed. ■

4.1 Exercises

1. Show that each of the following congruences holds.

a) $13 \equiv 1 \pmod 2$
b) $22 \equiv 7 \pmod 5$
c) $91 \equiv 0 \pmod{13}$
d) $69 \equiv 62 \pmod 7$
e) $-2 \equiv 1 \pmod 3$
f) $-3 \equiv 30 \pmod{11}$
g) $111 \equiv -9 \pmod{40}$
h) $666 \equiv 0 \pmod{37}$

2. Determine whether each of the following pairs of integers is congruent modulo 7.

a) 1,15
b) 0,42
c) 2,99
d) -1,8
e) -9,5
f) -1,699

3. For which positive integers m is each of the following statements true?

a) $27 \equiv 5 \pmod m$
b) $1000 \equiv 1 \pmod m$
c) $1331 \equiv 0 \pmod m$

4. Show that if a is an even integer, then $a^2 \equiv 0 \pmod 4$, and if a is an odd integer, then $a^2 \equiv 1 \pmod 4$.

☞ **5.** Show that if a is an odd integer, then $a^2 \equiv 1 \pmod 8$.

6. Find the least nonnegative residue modulo 13 of each of the following integers.

a) 22
b) 100
c) 1001
d) -1
e) -100
f) -1000

7. Find the least positive residue of $1! + 2! + 3! + \cdots + 100!$ modulo each of the following integers.

a) 2
b) 7
c) 12
d) 25

8. Show that if a, b, m, and n are integers such that $m > 0$, $n > 0$, $n \mid m$, and $a \equiv b \pmod m$, then $a \equiv b \pmod n$.

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

10. Show that if a, b, and c are integers with $c > 0$ such that $a \equiv b \pmod c$, then $(a, c) = (b, c)$.

11. Show that if $a_j \equiv b_j \pmod m$ for $j = 1, 2, \ldots, n$, where m is a positive integer and a_j, b_j, $j = 1, 2, \ldots, n$, are integers, then

a) $\sum_{j=1}^{n} a_j \equiv \sum_{j=1}^{n} b_j \pmod{m}$.

b) $\prod_{j=1}^{n} a_j \equiv \prod_{j=1}^{n} b_j \pmod{m}$.

In Exercises 12–14, construct tables for arithmetic modulo 6 using the least nonnegative residues modulo 6 to represent the congruence classes.

12. Construct a table for addition modulo 6.

13. Construct a table for subtraction modulo 6.

14. Construct a table for multiplication modulo 6.

15. What time does a clock read

a) 29 hours after it reads 11 o'clock?

b) 100 hours after it reads 2 o'clock?

c) 50 hours before it reads 6 o'clock?

16. Which decimal digits occur as the final digit of a fourth power of an integer?

17. What can you conclude if $a^2 \equiv b^2 \pmod{p}$, where a and b are integers and p is prime?

18. Show that if $a^k \equiv b^k \pmod{m}$ and $a^{k+1} \equiv b^{k+1} \pmod{m}$, where a, b, k, and m are integers with $k > 0$ and $m > 0$ such that $(a, m) = 1$, then $a \equiv b \pmod{m}$. If the condition $(a, m) = 1$ is dropped, is the conclusion that $a \equiv b \pmod{m}$ still valid?

19. Show that if n is an odd positive integer, then

$$1 + 2 + 3 + \cdots + (n-1) \equiv 0 \pmod{n}.$$

Is this statement true if n is even?

20. Show that if n is an odd positive integer or if n is a positive integer divisible by 4, then

$$1^3 + 2^3 + 3^3 + \cdots + (n-1)^3 \equiv 0 \pmod{n}.$$

Is this statement true if n is even but not divisible by 4?

21. For which positive integers n is it true that

$$1^2 + 2^2 + 3^2 + \cdots + (n-1)^2 \equiv 0 \pmod{n}?$$

22. Show by mathematical induction that if n is a positive integer, then $4^n \equiv 1 + 3n \pmod{9}$.

23. Show by mathematical induction that if n is a positive integer, then $5^n \equiv 1 + 4n \pmod{16}$.

24. Give a complete system of residues modulo 13 consisting entirely of odd integers.

25. Show that if $n \equiv 3 \pmod{4}$, then n cannot be the sum of the squares of two integers.

26. Show that if p is prime, then the only solutions of the congruence $x^2 \equiv x \pmod{p}$ are those integers x such that $x \equiv 0$ or $1 \pmod{p}$.

27. Show that if p is prime and k is a positive integer, then the only solutions of $x^2 \equiv x \pmod{p^k}$ are those integers x such that $x \equiv 0$ or $1 \pmod{p^k}$.

28. Find the least positive residues modulo 47 of each of the following integers.

a) 2^{32} b) 2^{47} c) 2^{200}

29. Let $m_1, m_2, \ldots, m_k$ be pairwise relatively prime positive integers. Let $M = m_1 m_2 \cdots m_k$ and $M_j = M/m_j$ for $j = 1, 2, \ldots, k$. Show that

$$M_1 a_1 + M_2 a_2 + \cdots + M_k a_k$$

runs through a complete system of residues modulo M when $a_1, a_2, \ldots, a_k$ run through complete systems of residues modulo $m_1, m_2, \ldots, m_k$, respectively.

30. Explain how to find the sum $u + v$ from the least positive residue of $u + v$ modulo m, where u and v are positive integers less than m. (*Hint:* Assume that $u \leq v$, and consider separately the cases where the least positive residue of $u + v$ is less than u, and where it is greater than v.)

31. On a computer with word size w, multiplication modulo n where $n < w/2$ can be performed as outlined. Let $T = [\sqrt{n} + 1/2]$, and $t = T^2 - n$. For each computation, show that all the required computer arithmetic can be done without exceeding the word size. (This method was described by Head [He80]).

a) Show that $|t| \leq T$.

b) Show that if x and y are nonnegative integers less than n, then

$$x = aT + b, \quad y = cT + d,$$

where a, b, c, and d are integers such that $0 \leq a \leq T$, $0 \leq b < T$, $0 \leq c \leq T$, and $0 \leq d < T$.

c) Let $z \equiv ad + bc \pmod{n}$, such that $0 \leq z < n$. Show that

$$xy \equiv act + zT + bd \pmod{n}.$$

d) Let $ac = eT + f$, where e and f are integers with $0 \leq e \leq T$ and $0 \leq f < T$. Show that

$$xy \equiv (z + et)T + ft + bd \pmod{n}.$$

e) Let $v \equiv z + et \pmod{n}$, such that $0 \leq v < n$. Show that we can write

$$v = gT + h,$$

where g and h are integers with $0 \leq g \leq T$, $0 \leq h < T$, and such that

$$xy \equiv hT + (f + g)t + bd \pmod{n}.$$

f) Show that the right-hand side of the congruence of part (e) can be computed without exceeding the word size, by first finding j such that

$$j \equiv (f + g)t \pmod{n}$$

and $0 \leq j < n$, and then finding k such that

$$k \equiv j + bd \pmod{n}$$

and $0 \leq k < n$, so that

$$xy \equiv hT + k \pmod{n}.$$

This gives the desired result.

32. Develop an algorithm for modular exponentiation from the base 3 expansion of the exponent.

33. Find the least positive residue of each of the following.
   a) 3^{10} modulo 11
   b) 2^{12} modulo 13
   c) 5^{16} modulo 17
   d) 3^{22} modulo 23
   e) Can you propose a theorem from the above congruences?

34. Find the least positive residues of each of the following.
   a) 6! modulo 7
   b) 10! modulo 11
   c) 12! modulo 13
   d) 16! modulo 17
   e) Can you propose a theorem from the above congruences?

* **35.** Show that for every positive integer m there are infinitely many Fibonacci numbers f_n such that m divides f_n. (*Hint:* Show that the sequence of least positive residues modulo m of the Fibonacci numbers is a repeating sequence.)

36. Prove Theorem 4.7 using mathematical induction.

37. Show that the least nonnegative residue modulo m of the product of two positive integers less than m can be computed using $O(\log^2 m)$ bit operations.

* **38.** Five men and a monkey are shipwrecked on an island. The men have collected a pile of coconuts which they plan to divide equally among themselves the next morning. Not trusting the other men, one of the group wakes up during the night and divides the coconuts into five equal parts with one left over, which he gives to the monkey. He then hides his portion of the pile. During the night, each of the other four men does exactly the same thing by dividing the pile he finds into five equal parts leaving one coconut for the monkey and hiding his portion. In the morning, the men gather and split the remaining pile of coconuts into five parts and one is left over for the monkey. What is the minimum number of coconuts the men could have collected for their original pile?

* **39.** Answer the question in Exercise 38, where instead of five men and one monkey, there are n men and k monkeys, and at each stage the monkeys receive one coconut each.

We say that the polynomials $f(x)$ and $g(x)$ are *congruent modulo n as polynomials* if for each power of x the coefficients of that power in $f(x)$ and $g(x)$ are congruent modulo n. For example, $11x^3 + x^2 + 2$ and $x^3 - 4x^2 + 5x + 22$ are congruent as polynomials modulo 5. The notation $f(x) \equiv g(x) \pmod{n}$ is often used to denote that $f(x)$ and $g(x)$ are congruent as polynomials modulo n. In Exercises 40–44 assume that n is a positive integer with $n > 1$ and that all polynomials have integer coefficients.

40. a) Show that if $f(x)$ and $g(x)$ are congruent as polynomials modulo n, then for every integer a, $f(a) \equiv g(a) \pmod{n}$.
   b) Show that it is not necessarily true that $f(x)$ and $g(x)$ are congruent as polynomials modulo n if $f(a) \equiv g(a) \pmod{n}$ for every integer a.

41. Show that if $f_1(x)$ and $g_1(x)$ are congruent as polynomials modulo n and $f_2(x)$ and $g_2(x)$ are congruent as polynomials modulo n, then
   a) $(f_1 + f_2)(x)$ and $(g_1 + g_2)(x)$ are congruent as polynomials modulo n.
   b) $(f_1 f_2)(x)$ and $(g_1 g_2)(x)$ are congruent as polynomials modulo n.

42. Show that if $f(x)$ is a polynomial with integer coefficients and $f(a) \equiv 0 \pmod{n}$, then there is a polynomial $g(x)$ with integer coefficients such that $f(x)$ and $(x - a)g(x)$ are congruent as polynomials modulo n.

43. Suppose that p is prime, $f(x)$ is a polynomial with integer coefficients, $a_1, a_2, \ldots, a_k$ are incongruent integers modulo p, and $f(a_j) \equiv 0 \pmod{p}$ for $j = 1, 2, \ldots, k$. Show that there exists a polynomial $g(x)$ with integer coefficients such that $f(x)$ and $(x - a_1)(x - a_2) \cdots (x - a_k)g(x)$ are congruent as polynomials modulo p.

44. Use Exercise 43 to show that if p is a prime, $f(x)$ is a polynomial with integer coefficients, and x^n is the largest power of x with a coefficient divisible by p, then the congruence $f(x) \equiv 0 \pmod{p}$ has at most p incongruent solutions modulo p.

4.1 Computational and Programming Exercises

Computations and Explorations

Using a computation program such as Maple or *Mathematica*, or programs you have written, carry out the following computations and explorations.

1. Compute the least positive residue modulo 10,403 of 7651^{891}.
2. Compute the least positive residue modulo 10,403 of 7651^{201}.

Programming Projects

Write programs using Maple, *Mathematica*, or a language of your choice to do the following.

1. Find the least nonnegative residue of an integer with respect to a fixed modulus.
2. Perform modular addition and subtraction when the modulus is less than half of the word size of the computer.
3. Perform modular multiplication when the modulus is less than half of the word size of the computer, using Exercise 31.
4. Perform modular exponentiation using the algorithm described in the text.

4.2 Linear Congruences

A congruence of the form

$$ax \equiv b \pmod{m},$$

where x is an unknown integer, is called a *linear congruence in one variable*. In this section, we will see that the study of such congruences is similar to the study of linear diophantine equations in two variables.

We first note that if $x = x_0$ is a solution of the congruence $ax \equiv b \pmod{m}$, and if $x_1 \equiv x_0 \pmod{m}$, then $ax_1 \equiv ax_0 \equiv b \pmod{m}$, so that x_1 is also a solution. Hence, if one member of a congruence class modulo m is a solution, then all members of this class are solutions. Therefore, we may ask how many of the m congruence classes modulo m give solutions; this is exactly the same as asking how many incongruent solutions there are modulo m. The following theorem tells us when a linear congruence in one