3.7 Exercises

1. For each of the following linear diophantine equations, either find all solutions, or show that there are no integral solutions.
   a) $2x + 5y = 11$
   b) $17x + 13y = 100$
   c) $21x + 14y = 147$
   d) $60x + 18y = 97$
   e) $1402x + 1969y = 1$

2. For each of the following linear diophantine equations, either find all solutions, or show that there are no integral solutions.
   a) $3x + 4y = 7$
   b) $12x + 18y = 50$
   c) $30x + 47y = -11$
   d) $25x + 95y = 970$
   e) $102x + 1001y = 1$

3. A Japanese businessman returning home from a trip to North America exchanges his U.S. and Canadian dollars for yen. If he receives 15,286 yen, and received 122 yen for each U.S. and 112 yen for each Canadian dollar, how many of each type of currency did he exchange?

4. A student returning from Europe changes his euros and Swiss francs into U.S. money. If she receives \$46.26, and received \$1.11 for each euro and 83¢ for each Swiss franc, how much of each type of currency did she exchange?

5. A professor returning home from conferences in Paris and London changes his euros and pounds into U.S. money. If he receives \$117.98, and received \$1.11 for each euro and \$1.69 for each pound, how much of each type of currency did he exchange?

6. The Indian astronomer and mathematician Mahavira, who lived in the ninth century, posed this puzzle: A band of 23 weary travelers entered a lush forest where they found 63 piles each containing the same number of plantains and a remaining pile containing seven plantains. They divided the plantains equally. How many plantains were in each of the 63 piles? Solve this puzzle.

7. A grocer orders apples and oranges at a total cost of \$8.39. If apples cost him 25¢ each and oranges cost him 18¢ each, how many of each type of fruit did he order?

8. A shopper spends a total of \$5.49 for oranges, which cost 18¢ each, and grapefruit, which cost 33¢ each. What is the minimum number of pieces of fruit the shopper could have bought?

9. A postal clerk has only 14- and 21-cent stamps to sell. What combinations of these may be used to mail a package requiring postage of exactly each of the following amounts?

   a) \$3.50 b) \$4.00 c) \$7.77

10. At a clambake, the total cost of a lobster dinner is \$11 and of a chicken dinner is \$8. What can you conclude if the total bill is each of the following amounts?

    a) \$777 b) \$96 c) \$69

* **11.** Find all integer solutions of each of the following linear diophantine equations.
  a) $2x + 3y + 4z = 5$
  b) $7x + 21y + 35z = 8$
  c) $101x + 102y + 103z = 1$

* **12.** Find all integer solutions of each of the following linear diophantine equations.
  a) $2x_1 + 5x_2 + 4x_3 + 3x_4 = 5$
  b) $12x_1 + 21x_2 + 9x_3 + 15x_4 = 9$
  c) $15x_1 + 6x_2 + 10x_3 + 21x_4 + 35x_5 = 1$

13. Which combinations of pennies, dimes, and quarters have a total value of 99¢?

14. How many ways can change be made for one dollar, using each of the following coins?
  a) dimes and quarters
  b) nickels, dimes, and quarters
  c) pennies, nickels, dimes, and quarters

In Exercises 15–17, we consider simultaneous linear diophantine equations. To solve these, first eliminate all but two variables and then solve the resulting equation in two variables.

15. Find all integer solutions of the following systems of linear diophantine equations.

a) $x + y + z = 100$
$x + 8y + 50z = 156$

b) $x + y + z = 100$
$x + 6y + 21z = 121$

c) $x + y + z + w = 100$
$x + 2y + 3z + 4w = 300$
$x + 4y + 9z + 16w = 1000$

16. A piggy bank contains 24 coins, all of which are nickels, dimes, or quarters. If the total value of the coins is two dollars, what combinations of coins are possible?

17. Nadir Airways offers three types of tickets on their Boston–New York flights. First-class tickets are \$140, second-class tickets are \$110, and standby tickets are \$78. If 69 passengers pay a total of \$6548 for their tickets on a particular flight, how many of each type of ticket were sold?

18. Is it possible to have 50 coins, all of which are pennies, dimes, or quarters, with a total worth \$3?

Let a and b be relatively prime positive integers, and let n be a positive integer. A solution (x, y) of the linear diophantine equation $ax + by = n$ is *nonnegative* when both x and y are nonnegative.

* **19.** Show that whenever $n \geq (a-1)(b-1)$, there is a nonnegative solution of $ax + by = n$.

* **20.** Show that if $n = ab - a - b$, then there are no nonnegative solutions of $ax + by = n$.

* **21.** Show that there are exactly $(a-1)(b-1)/2$ nonnegative integers $n < ab - a - b$ such that the equation has a nonnegative solution.

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

Hence, $1 = 5 - 2 \cdot 2 = 5 - (7 - 5 \cdot 1) \cdot 2 = 5 \cdot 3 - 2 \cdot 7 = (12 - 7 \cdot 1) \cdot 3 - 2 \cdot 7 = 12 \cdot 3 - 5 \cdot 7$. Therefore, a particular solution to the linear diophantine equation is $x_0 = -20$ and $y_0 = 12$. Hence, all solutions of the linear congruences are given by $x \equiv -20 \equiv 4 \pmod{12}$. ◀

Later we will want to know which integers are their own inverses modulo p, where p is prime. The following theorem tells us which integers have this property.

Theorem 4.11. Let p be prime. The positive integer a is its own inverse modulo p if and only if $a \equiv 1 \pmod{p}$ or $a \equiv -1 \pmod{p}$.

Proof. If $a \equiv 1 \pmod{p}$ or $a \equiv -1 \pmod{p}$, then $a^2 \equiv 1 \pmod{p}$, so that a is its own inverse modulo p.

Conversely, if a is its own inverse modulo p, then $a^2 = a \cdot a \equiv 1 \pmod{p}$. Hence, $p \mid (a^2 - 1)$. Since $a^2 - 1 = (a - 1)(a + 1)$, either $p \mid (a - 1)$ or $p \mid (a + 1)$. Therefore, either $a \equiv 1 \pmod{p}$ or $a \equiv -1 \pmod{p}$. ■

4.2 Exercises

1. Find all solutions of each of the following linear congruences.

   a) $2x \equiv 5 \pmod{7}$
   b) $3x \equiv 6 \pmod{9}$
   c) $19x \equiv 30 \pmod{40}$
   d) $9x \equiv 5 \pmod{25}$
   e) $103x \equiv 444 \pmod{999}$
   f) $980x \equiv 1500 \pmod{1600}$

2. Find all solutions of each of the following linear congruences.

   a) $3x \equiv 2 \pmod{7}$
   b) $6x \equiv 3 \pmod{9}$
   c) $17x \equiv 14 \pmod{21}$
   d) $15x \equiv 9 \pmod{25}$
   e) $128x \equiv 833 \pmod{1001}$
   f) $987x \equiv 610 \pmod{1597}$

3. Find all solutions to the congruence $6{,}789{,}783x \equiv 2{,}474{,}010 \pmod{28{,}927{,}591}$.

4. Suppose that p is prime and that a and b are positive integers with $(p, a) = 1$. The following method can be used to solve the linear congruence $ax \equiv b \pmod{p}$.
   a) Show that if the integer x is a solution of $ax \equiv b \pmod{p}$, then x is also a solution of the linear congruence
   $$a_1 x \equiv -b[m/a] \pmod{p},$$
   where a_1 is the least positive residue of p modulo a. Note that this congruence is of the same type as the original congruence, with a positive integer smaller than a as the coefficient of x.
   b) When the procedure of part (a) is iterated, one obtains a sequence of linear congruences with coefficients of x equal to $a_0 = a > a_1 > a_2 > \cdots$. Show that there is a positive integer n with $a_n = 1$, so that at the nth stage, one obtains a linear congruence $x \equiv B \pmod{p}$.
   c) Use the method described in part (b) to solve the linear congruence $6x \equiv 7 \pmod{23}$.

5. An astronomer knows that a satellite orbits the Earth in a period that is an exact multiple of 1 hour that is less than 1 day. If the astronomer notes that the satellite completes 11 orbits in an interval that starts when a 24-hour clock reads 0 hours and ends when the clock reads 17 hours, how long is the orbital period of the satellite?

6. For which integers c, $0 \leq c < 30$, does the congruence $12x \equiv c \pmod{30}$ have solutions? When there are solutions, how many incongruent solutions are there?

7. For which integers c, $0 \leq c < 1001$, does the congruence $154x \equiv c \pmod{1001}$ have solutions? When there are solutions, how many incongruent solutions are there?

8. Find an inverse modulo 13 of each of the following integers.

   a) 2 c) 5
   b) 3 d) 11

9. Find an inverse modulo 17 of each of the following integers.

   a) 4 c) 7
   b) 5 d) 16

10. a) Determine which integers a, where $1 \leq a \leq 14$, have an inverse modulo 14.
    b) Find the inverse of each of the integers from part (a) that have an inverse modulo 14.

11. a) Determine which integers a, where $1 \leq a \leq 30$, have an inverse modulo 30.
    b) Find the inverse of each of the integers from part (a) that have an inverse modulo 30.

12. Show that if $\bar{a}$ is an inverse of a modulo m and $\bar{b}$ is an inverse of b modulo m, then $\bar{a}\,\bar{b}$ is an inverse of ab modulo m.

13. Show that the linear congruence in two variables $ax + by \equiv c \pmod{m}$, where a, b, c, and m are integers, $m > 0$, with $d = (a, b, m)$, has exactly dm incongruent solutions if $d \mid c$, and no solutions otherwise.

14. Find all solutions of each of the following linear congruences in two variables.

    a) $2x + 3y \equiv 1 \pmod{7}$ c) $6x + 3y \equiv 0 \pmod{9}$
    b) $2x + 4y \equiv 6 \pmod{8}$ d) $10x + 5y \equiv 9 \pmod{15}$

15. Let p be an odd prime and k a positive integer. Show that the congruence $x^2 \equiv 1 \pmod{p^k}$ has exactly two incongruent solutions, namely $x \equiv \pm 1 \pmod{p^k}$.

16. Show that the congruence $x^2 \equiv 1 \pmod{2^k}$ has exactly four incongruent solutions, namely $x \equiv \pm 1$ or $\pm(1 + 2^{k-1}) \pmod{2^k}$, when $k > 2$. Show that when $k = 1$ there is one solution and that when $k = 2$ there are two incongruent solutions.

17. Show that if a and m are relatively prime positive integers such that $a < m$, then an inverse of a modulo m can be found using $O(\log^3 m)$ bit operations.

18. Show that if p is an odd prime and a is a positive integer not divisible by p, then the congruence $x^2 \equiv a \pmod{p}$ has either no solution or exactly two incongruent solutions.

Using Lemma 4.2, and the steps of the Euclidean algorithm with $a = r_0$ and $b = r_1$, when we perform the Euclidean algorithm on the pair $2^a - 1 = R_0$ and $2^b - 1 = R_1$, we obtain

$$\begin{aligned} R_0 &= R_1Q_1 + R_2 & R_2 &= 2^{r_2} - 1 \\ R_1 &= R_2Q_2 + R_3 & R_3 &= 2^{r_3} - 1 \\ &\vdots \\ R_{n-3} &= R_{n-2}Q_{n-2} + R_{n-1} & R_{n-1} &= 2^{r_{n-1}} - 1 \\ R_{n-2} &= R_{n-1}Q_{n-1}. \end{aligned}$$

Here, the last nonzero remainder, $R_{n-1} = 2^{r_{n-1}} - 1 = 2^{(a,b)} - 1$, is the greatest common divisor of R_0 and R_1. ∎

Using Lemma 4.3, we have the following theorem.

Theorem 4.13. The positive integers $2^a - 1$ and $2^b - 1$ are relatively prime if and only if a and b are relatively prime.

We can now use Theorem 4.13 to produce a set of pairwise relatively prime integers, each of which is less than 2^{35}, with product greater than a specified integer. Suppose that we wish to do arithmetic with integers as large as 2^{184}. We pick $m_1 = 2^{35} - 1$, $m_2 = 2^{34} - 1$, $m_3 = 2^{33} - 1$, $m_4 = 2^{31} - 1$, $m_5 = 2^{29} - 1$, and $m_6 = 2^{23} - 1$. Since the exponents of 2 in the expressions for the m_j are pairwise relatively prime, by Theorem 4.13, the m_j are pairwise relatively prime. Also, we have $M = m_1m_2m_3m_4m_5m_6 > 2^{184}$. We can now use modular arithmetic and the Chinese remainder theorem to perform arithmetic with integers as large as 2^{184}.

Although it is somewhat awkward to do computer operations with large integers using modular arithmetic and the Chinese remainder theorem, there are some definite advantages to this approach. First, on many high-speed computers, operations can be performed simultaneously. So, reducing an operation involving two large integers to a set of operations involving smaller integers, namely the least positive residues of the large integers with respect to the various moduli, leads to simultaneous computations which may be performed more rapidly than one operation with large integers, especially when parallel processing is used. Second, even without taking into account the advantages of simultaneous computations, multiplication of large integers may be done faster using these ideas than with many other multiprecision methods. The interested reader should consult Knuth [Kn97].

4.3 Exercises

1. Which integers leave a remainder of 1 when divided by both 2 and 3?
2. Find an integer that leaves a remainder of 1 when divided by either 2 or 5, but that is divisible by 3.
3. Find an integer that leaves a remainder of 2 when divided by either 3 or 5, but that is divisible by 4.

4. Find all the solutions of each of the following systems of linear congruences.

a) $x \equiv 4 \pmod{11}$
$x \equiv 3 \pmod{17}$

b) $x \equiv 1 \pmod{2}$
$x \equiv 2 \pmod{3}$
$x \equiv 3 \pmod{5}$

c) $x \equiv 0 \pmod{2}$
$x \equiv 0 \pmod{3}$
$x \equiv 1 \pmod{5}$
$x \equiv 6 \pmod{7}$

d) $x \equiv 2 \pmod{11}$
$x \equiv 3 \pmod{12}$
$x \equiv 4 \pmod{13}$
$x \equiv 5 \pmod{17}$
$x \equiv 6 \pmod{19}$

5. Find all the solutions to the system of linear congruences $x \equiv 1 \pmod{2}$, $x \equiv 2 \pmod{3}$, $x \equiv 3 \pmod{5}$, $x \equiv 4 \pmod{7}$, and $x \equiv 5 \pmod{11}$.

6. Find all the solutions to the system of linear congruences $x \equiv 1 \pmod{999}$, $x \equiv 2 \pmod{1001}$, $x \equiv 3 \pmod{1003}$, $x \equiv 4 \pmod{1004}$, and $x \equiv 5 \pmod{1007}$.

7. A troop of 17 monkeys store their bananas in 11 piles of equal size, each containing more than 1 banana, with a twelfth pile of 6 left over. When they divide the bananas into 17 equal groups, none remain. What is the smallest number of bananas they can have?

8. As an odometer check, a special counter measures the miles a car travels modulo 7. Explain how this counter can be used to determine whether the car has been driven 49,335; 149,335; or 249,335 miles when the odometer reads 49,335 and works modulo 100,000.

9. Chinese generals counted troops remaining after a battle by lining them up in rows of different lengths, counting the number left over each time, and calculating the total from these remainders. If a general had 1200 troops at the start of a battle and if there were 3 left over when they lined up 5 at a time, 3 left over when they lined up 6 at a time, 1 left over when they lined up 7 at a time, and none left over when they lined up 11 at a time, how many troops remained after the battle?

10. Find an integer that leaves a remainder of 9 when it is divided by either 10 or 11, but that is divisible by 13.

11. Find a multiple of 11 that leaves a remainder of 1 when divided by each of the integers 2, 3, 5, and 7.

12. Solve the following ancient Indian problem: If eggs are removed from a basket 2, 3, 4, 5, and 6 at a time, there remain, respectively, 1, 2, 3, 4, and 5 eggs. But if the eggs are removed 7 at a time, no eggs remain. What is the least number of eggs that could have been in the basket?

13. Show that there are arbitrarily long strings of consecutive integers each divisible by a perfect square greater than 1. (*Hint:* Use the Chinese remainder theorem to show that there is a simultaneous solution to the system of congruences $x \equiv 0 \pmod{4}$, $x \equiv -1 \pmod{9}$, $x \equiv -2 \pmod{25}$, $\ldots$, $x \equiv -k + 1 \pmod{p_k^2}$, where p_k is the kth prime.)

*** 14.** Show that if a, b, and c are integers such that $(a, b) = 1$, then there is an integer n such that $(an + b, c) = 1$.

In Exercises 15–18, we will consider systems of congruences where the moduli of the congruences are not necessarily relatively prime.

15. Show that the system of congruences

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$

has a solution if and only if $(m_1, m_2) \mid (a_1 - a_2)$. Show that when there is a solution, it is unique modulo $[m_1, m_2]$. (*Hint:* Write the first congruence as $x = a_1 + km_1$, where k is an integer, and then insert this expression for x into the second congruence.)

16. Using Exercise 15, solve each of the following simultaneous systems of congruences.

a) $x \equiv 4 \pmod{6}$
$x \equiv 13 \pmod{15}$

b) $x \equiv 7 \pmod{10}$
$x \equiv 4 \pmod{15}$

17. Using Exercise 15, solve each of the following simultaneous systems of congruences.

a) $x \equiv 10 \pmod{60}$
$x \equiv 80 \pmod{350}$

b) $x \equiv 2 \pmod{910}$
$x \equiv 93 \pmod{1001}$

18. Does the system of congruences $x \equiv 1 \pmod{8}$, $x \equiv 3 \pmod{9}$, and $x \equiv 2 \pmod{12}$ have any simultaneous solutions?

What happens when the moduli in a simultaneous system of more than two congruences in one unknown are not pairwise relatively prime (such as in Exercise 18)? The following exercise provides compatability conditions for there to be a unique solution of such a system, modulo the least common multiple of the moduli.

19. Show that the system of congruences

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\vdots$$
$$x \equiv a_r \pmod{m_r}$$

has a solution if and only if $(m_i, m_j) \mid (a_i - a_j)$ for all pairs of integers (i, j), where $1 \leq i < j \leq r$. Show that if a solution exists, then it is unique modulo $[m_1, m_2, \ldots, m_r]$. (*Hint:* Use Exercise 15 and mathematical induction.)

20. Using Exercise 19, solve each of the following systems of congruences.

a) $x \equiv 5 \pmod{6}$
$x \equiv 3 \pmod{10}$
$x \equiv 8 \pmod{15}$

b) $x \equiv 2 \pmod{14}$
$x \equiv 16 \pmod{21}$
$x \equiv 10 \pmod{30}$

c) $x \equiv 2 \pmod{9}$
$x \equiv 8 \pmod{15}$
$x \equiv 10 \pmod{25}$

d) $x \equiv 2 \pmod{6}$
$x \equiv 4 \pmod{8}$
$x \equiv 2 \pmod{14}$
$x \equiv 14 \pmod{15}$

e) $x \equiv 7 \pmod{9}$
$x \equiv 2 \pmod{10}$
$x \equiv 3 \pmod{12}$
$x \equiv 6 \pmod{15}$

21. What is the smallest number of lobsters in a tank if 1 lobster is left over when they are removed 2, 3, 5, or 7 at a time, but no lobsters are left over when they are removed 11 at a time?

22. An ancient Chinese problem asks for the least number of gold coins a band of 17 pirates could have stolen. The problem states that when the pirates divided the coins into equal piles, 3 coins were left over. When they fought over who should get the extra coins, one of the pirates was slain. When the remaining pirates divided the coins into equal piles, 10 coins were left over. When the pirates fought again over who should get the extra coins, another pirate was slain. When they divided the coins in equal piles again, no coins were left over. What is the answer to this problem?

23. Solve the following problem originally posed by Ch'in Chiu-Shao (using different weight units). Three farmers equally divide a quantity of rice with a weight that is an integral number of pounds. The farmers each sell their rice, selling as much as possible, at three different markets where the markets use weights of 83 pounds, 110 pounds, and 135 pounds, and only buy rice in multiples of these weights. What is the least amount of rice the farmers could have divided if the farmers return home with 32 pounds, 70 pounds, and 30 pounds, respectively?

24. Using the Chinese remainder theorem, explain how to add and how to multiply 784 and 813 on a computer of word size 100.

A positive integer $x \neq 1$ with n base b digits is called an *automorph to the base b* if the last n base b digits of x^2 are the same as those of x.

* **25.** Find the base 10 automorphs with four digits (with initial zeros allowed).

* **26.** How many base b automorphs are there with n or fewer base b digits, if b has prime-power factorization $b = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$?

According to the theory of *biorhythms*, there are three cycles in your life that start the day you are born. These are the *physical, emotional,* and *intellectual cycles,* of lengths 23, 28, and 33 days, respectively. Each cycle follows a sine curve with period equal to the length of that cycle, starting with value 0, climbing to value 1 one-quarter of the way through the cycle, dropping back to value 0 one-half of the way through the cycle, dropping further to value -1 three-quarters of the way through the cycle, and climbing back to value 0 at the end of the cycle.

Answer the following questions about biorhythms, measuring time in quarter days (so that the units will be integers).

27. For which days of your life will you be at a triple peak, where all of your three cycles are at maximum values?

28. For which days of your life will you be at a triple nadir, where all three of your cycles have minimum values?

29. When in your life will all three cycles be at a neutral position (value 0)?

A set of congruences to distinct moduli greater than 1 that has the property that every integer satisfies at least one of the congruences is called a *covering set of congruences.*

30. Show that the set of congruences $x \equiv 0 \pmod 2$, $x \equiv 0 \pmod 3$, $x \equiv 1 \pmod 4$, $x \equiv 1 \pmod 6$, and $x \equiv 11 \pmod{12}$ is a covering set of congruences.

31. Show that the set of congruences $x \equiv 0 \pmod 2$, $x \equiv 0 \pmod 3$, $x \equiv 0 \pmod 5$, $x \equiv 0 \pmod 7$, $x \equiv 1 \pmod 6$, $x \equiv 1 \pmod{10}$, $x \equiv 1 \pmod{14}$, $x \equiv 2 \pmod{15}$, $x \equiv 2 \pmod{21}$, $x \equiv 23 \pmod{30}$, $x \equiv 4 \pmod{35}$, $x \equiv 5 \pmod{42}$, $x \equiv 59 \pmod{70}$, and $x \equiv 104 \pmod{105}$ is a covering set of congruences.

* 32. Let m be a positive integer with prime-power factorization $m = 2^{a_0} p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$. Show that the congruence $x^2 \equiv 1 \pmod m$ has exactly 2^{r+e} solutions, where $e = 0$ if $a_0 = 0$ or 1, $e = 1$ if $a_0 = 2$, and $e = 2$ if $a_0 > 2$. (*Hint:* Use Exercises 15 and 16 of Section 4.2.)

33. The three children in a family have feet that are 5 inches, 7 inches, and 9 inches long. When they measure the length of the dining room of their house using their feet, they each find that there are 3 inches left over. How long is the dining room?

34. Find all solutions of the congruence $x^2 + 6x - 31 \equiv 0 \pmod{72}$. (*Hint:* First note that $72 = 2^3 3^2$. Find, by trial and error, the solutions of this congruence modulo 8 and modulo 9. Then apply the Chinese remainder theorem.)

35. Find all solutions of the congruence $x^2 + 18x - 823 \equiv 0 \pmod{1800}$. (*Hint:* First note that $1800 = 2^3 3^2 5^2$. Find, by trial and error, the solutions of this congruence modulo 8, modulo 9, and modulo 25. Then apply the Chinese remainder theorem.)

* 36. Give a positive integer R, a prime p that is the only prime between $p - R$ and $p + R$, including the end points, is called *R-reclusive*. Show that for every positive integer R, there are infinitely many R-reclusive primes. (*Hint:* Use the Chinese remainder theorem to find an integer x such that $x - j$ is divisible by p_j and $x + j$ is divisible by p_{R+j}, where p_k is the kth prime. Then invoke Dirichlet's theorem on primes in arithmetic progressions.)

4.3 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. Solve the simultaneous system of congruences $x \equiv 1 \pmod{12{,}341{,}234{,}567}$, $x \equiv 2 \pmod{750{,}000{,}057}$, and $x \equiv 3 \pmod{1{,}099{,}511{,}627{,}776}$.
2. Solve the simultaneous system of congruences $x \equiv 5269 \pmod{40{,}320}$, $x \equiv 1248 \pmod{11{,}111}$, $x \equiv 16{,}645 \pmod{30{,}003}$, and $x \equiv 2911 \pmod{12{,}321}$.
3. Using Exercise 13 of this section, find a string of 100 consecutive positive integers each divisible by a perfect square. Can you find such a set of smaller integers?
4. Find a covering set of congruences (as described in the preamble to Exercise 30) where the smallest modulus of one of the congruences in the covering set is 3; where the smallest modulus of one of the congruences in the covering set is 6; and where the smallest modulus of one of the congruences in the covering set is 8.

Programming Projects

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

1. Solve systems of linear congruences of the type found in the Chinese remainder theorem.
2. Solve systems of linear congruences of the type given in Exercises 15–20.