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

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

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 $1 \le i < j \le r$. 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.