4 Congruences

Introduction

The language of congruences was invented by the great German mathematician Gauss. It allows us to work with divisibility relationships in much the same way as we work with equalities. We will develop the basic properties of congruences in this chapter, describe how to do arithmetic with congruences, and study congruences involving unknowns, such as linear congruences. An example leading to a linear congruence is the problem of finding all integers x such that when $7x$ is divided by 11, the remainder is 3. We will also study systems of linear congruences that arise from such problems as the ancient Chinese puzzle that asks for a number that leaves a remainder of 2, 3, and 2, when divided by 3, 5, and 7, respectively. We will learn how to solve systems of linear congruences in one unknown, such as the system that results from this puzzle, using a famous method known as the Chinese remainder theorem. We will also learn how to solve polynomial congruences. Finally, we will introduce a factoring method, known as the Pollard rho method, which we use congruences to specify.

4.1 Introduction to Congruences

The special language of congruences that we introduce in this chapter, which is extremely useful in number theory, was developed at the beginning of the nineteenth century by *Karl Friedrich Gauss*, one of the most famous mathematicians in history.

The language of congruences makes it possible to work with divisibility relationships much as we work with equalities. Prior to the introduction of congruences, the notation used for divisibility relationships was awkward and difficult to work with. The introduction of a convenient notation helped accelerate the development of number theory.

Definition. Let m be a positive integer. If a and b are integers, we say that a is *congruent to b modulo m* if $m \mid (a - b)$.

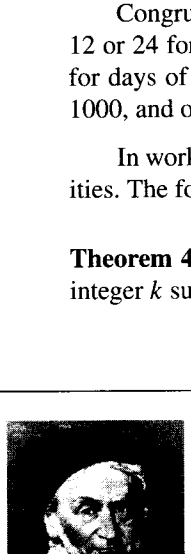
If a is congruent to b modulo m, we write $a \equiv b \pmod{m}$. If $m \nmid (a - b)$, we write $a \not\equiv b \pmod{m}$, and say that a and b are *incongruent modulo m.* The integer m is called the *modulus* of the congruence. The plural of modulus is *moduli.*

Example 4.1. We have $22 \equiv 4 \pmod{9}$, since $9 \mid (22 - 4) = 18$. Likewise $3 \equiv -6 \pmod{9}$ and $200 \equiv 2 \pmod{9}$. On the other hand, $13 \not\equiv 5 \pmod{9}$ since $9 \nmid (13 - 5) = 8$. ◀

Congruences often arise in everyday life. For instance, clocks work either modulo 12 or 24 for hours, and modulo 60 for minutes and seconds, calendars work modulo 7 for days of the week and modulo 12 for months. Utility meters often operate modulo 1000, and odometers usually work modulo 100,000.

In working with congruences, we will sometimes need to translate them into equalities. The following theorem helps us to do this.

Theorem 4.1. If a and b are integers, then $a \equiv b \pmod{m}$ if and only if there is an integer k such that $a = b + km$.



KARL FRIEDRICH GAUSS (1777–1855) was the son of a bricklayer. It was quickly apparent that he was a prodigy. In fact, at the age of three, he corrected an error in his father's payroll. In his first arithmetic class, the teacher gave an assignment designed to keep the class busy, namely to find the sum of the first 100 positive integers. Gauss, who was eight at the time, realized that this sum is $50 \cdot 101 = 5050$, because the terms can be grouped as $1 + 100 = 101$, $2 + 99 = 101$, . . . , $49 + 52 = 101$, and $50 + 51 = 101$. In 1796, Gauss made an important discovery in an area of geometry that had not progressed since ancient times. In particular, he showed that a regular heptadecagon (17-sided polygon) could be drawn using just a ruler and a compass. In 1799, he presented the first rigorous proof of the Fundamental Theorem of Algebra, which states that a polynomial of degree n with real coefficients has exactly n roots. Gauss made fundamental contributions to astronomy, including calculating the orbit of the asteroid Ceres. On the basis of this calculation, Gauss was appointed director of the Göttingen Observatory. He laid the foundations of modern number theory with his book *Disquisitiones Arithmeticae* in 1801. Gauss was called "Princeps Mathematicorum" (the Prince of Mathematicians) by his contemporaries. Although Gauss is noted for his many discoveries in geometry, algebra, analysis, astronomy, and mathematical physics, he had a special interest in number theory. This can be seen from his statement: "Mathematics is the queen of sciences, and the theory of numbers is the queen of mathematics." Gauss made most of his important discoveries early in his life, and spent his later years refining them. Gauss made several fundamental discoveries that he did not reveal. Mathematicians making the same discoveries were often surprised to find that Gauss had described the results years earlier in his unpublished notes.

Proof. If $a \equiv b \pmod{m}$, then $m \mid (a - b)$. This means that there is an integer k with $km = a - b$, so that $a = b + km$.

Conversely, if there is an integer k with $a = b + km$, then $km = a - b$. Hence $m \mid (a - b)$, and consequently, $a \equiv b \pmod{m}$. ∎

Example 4.2. We have $19 \equiv -2 \pmod{7}$ and $19 = -2 + 3 \cdot 7$. ◀

The following proposition establishes some important properties of congruences.

Theorem 4.2. Let m be a positive integer. Congruences modulo m satisfy the following properties:

(i) *Reflexive property.* If a is an integer, then $a \equiv a \pmod{m}$.

(ii) *Symmetric property.* If a and b are integers such that $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$.

(iii) *Transitive property.* If a, b, and c are integers with $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

Proof.

(i) We see that $a \equiv a \pmod{m}$, since $m \mid (a - a) = 0$.

(ii) If $a \equiv b \pmod{m}$, then $m \mid (a - b)$. Hence, there is an integer k such that $km = a - b$. This shows that $(-k)m = b - a$, so that $m \mid (b - a)$. Consequently, $b \equiv a \pmod{m}$.

(iii) If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $m \mid (a - b)$ and $m \mid (b - c)$. Hence, there are integers k and l such that $km = a - b$ and $lm = b - c$. Therefore, $a - c = (a - b) + (b - c) = km + lm = (k + l)m$. It follows that $m \mid (a - c)$ and $a \equiv c \pmod{m}$. ∎

By Theorem 4.2, we see that the set of integers is divided into m different sets called *congruence classes modulo m,* each containing integers that are mutually congruent modulo m.

Example 4.3. The four congruence classes modulo 4 are given by

$$\begin{aligned}
&\ldots \equiv -8 \equiv -4 \equiv 0 \equiv 4 \equiv 8 \equiv \ldots \pmod{4}\\
&\ldots \equiv -7 \equiv -3 \equiv 1 \equiv 5 \equiv 9 \equiv \ldots \pmod{4}\\
&\ldots \equiv -6 \equiv -2 \equiv 2 \equiv 6 \equiv 10 \equiv \ldots \pmod{4}\\
&\ldots \equiv -5 \equiv -1 \equiv 3 \equiv 7 \equiv 11 \equiv \ldots \pmod{4}.
\end{aligned}$$ ◀

Suppose that m is a positive integer. Given an integer a, by the division algorithm we have $a = bm + r$ where $0 \leq r \leq m - 1$. We call r the *least nonnegative residue* of a modulo m. We say that r is the result of *reducing a modulo m.*

Another commonly used notation, especially in computer science applications, is a **mod** $m = r$, which denotes that r is the remainder obtained when a is divided by m.

For example, $17 \bmod 5 = 2$ and $-8 \bmod 7 = 6$. Although we do not use such notation in this book, it is commonly used in other contexts.

Now note that from the equation $a = bm + r$, it follows that $a \equiv r \pmod{m}$. Hence, every integer is congruent modulo m to one of the integers of the set $0, 1, \ldots, m-1$, namely the remainder when it is divided by m. Since no two of the integers $0, 1, \ldots, m-1$ are congruent modulo m, we have m integers such that every integer is congruent to exactly one of these m integers.

Definition. A *complete system of residues modulo m* is a set of integers such that every integer is congruent modulo m to exactly one integer of the set.

Example 4.4. The division algorithm shows that the set of integers $0, 1, 2, \ldots, m-1$ is a complete system of residues modulo m. This is called the set of *least nonnegative residues modulo m.* ◀

Example 4.5. Let m be an odd positive integer. Then the set of integers

$$-\frac{m-1}{2}, -\frac{m-3}{2}, \ldots, -1, 0, 1, \ldots, \frac{m-3}{2}, \frac{m-1}{2},$$

the set of *absolute least residues modulo m,* is a complete system of residues. ◀

We will often do arithmetic with congruences, which is called *modular arithmetic.* Congruences have many of the same properties that equalities do. First, we show that an addition, subtraction, or multiplication to both sides of a congruence preserves the congruence.

Theorem 4.3. If a, b, c, and m are integers, with $m > 0$, such that $a \equiv b \pmod{m}$, then

(i) $a + c \equiv b + c \pmod{m}$,

(ii) $a - c \equiv b - c \pmod{m}$,

(iii) $ac \equiv bc \pmod{m}$.

Proof. Because $a \equiv b \pmod{m}$, we know that $m \mid (a - b)$. From the identity $(a + c) - (b + c) = a - b$, we see that $m \mid ((a + c) - (b + c))$, so that (i) follows. Likewise, (ii) follows from the fact that $(a - c) - (b - c) = a - b$. To show that (iii) holds, note that $ac - bc = c(a - b)$. Because $m \mid (a - b)$, it follows that $m \mid c(a - b)$, and hence, $ac \equiv bc \pmod{m}$. ■

Example 4.6. Because $19 \equiv 3 \pmod{8}$, it follows from Theorem 4.3 that $26 = 19 + 7 \equiv 3 + 7 = 10 \pmod{8}$, $15 = 19 - 4 \equiv 3 - 4 \equiv -1 \pmod{8}$, and $38 = 19 \cdot 2 \equiv 3 \cdot 2 = 6 \pmod{8}$. ◀

What happens when both sides of a congruence are divided by an integer? Consider the following example.

Example 4.7. We have $14 = 7 \cdot 2 \equiv 4 \cdot 2 = 8 \pmod 6$. But we cannot cancel the common factor of 2, because $7 \not\equiv 4 \pmod 6$. ◀

This example shows that it is not necessarily true that we preserve a congruence when we divide both sides by an integer. However, the following theorem gives a valid congruence when both sides of a congruence are divided by the same integer.

Theorem 4.4. If a, b, c and m are integers such that $m > 0$, $d = (c, m)$, and $ac \equiv bc \pmod m$, then $a \equiv b \pmod{m/d}$.

Proof. If $ac \equiv bc \pmod m$, we know that $m \mid (ac - bc) = c(a - b)$. Hence, there is an integer k with $c(a - b) = km$. By dividing both sides by d, we have $(c/d)(a - b) = k(m/d)$. Because $(m/d, c/d) = 1$, by Lemma 3.4 it follows that $m/d \mid (a - b)$. Hence, $a \equiv b \pmod{m/d}$. ■

Example 4.8. Because $50 \equiv 20 \pmod{15}$ and $(10, 15) = 5$, we see that $50/10 \equiv 20/10 \pmod{15/5}$, or $5 \equiv 2 \pmod 3$. ◀

The following corollary, which is a special case of Theorem 4.4, is used often; it allows us to cancel number that are relatively prime to the modulus m in congruences modulo m.

Corollary 4.4.1. If a, b, c, and m are integers such that $m > 0$, $(c, m) = 1$, and $ac \equiv bc \pmod m$, then $a \equiv b \pmod m$.

Example 4.9. Since $42 \equiv 7 \pmod 5$ and $(5, 7) = 1$, we can conclude that $42/7 \equiv 7/7 \pmod 5$, or that $6 \equiv 1 \pmod 5$. ◀

The following theorem, which is more general than Theorem 4.3, is also useful. Its proof is similar to the proof of Theorem 4.3.

Theorem 4.5. If a, b, c, d, and m are integers such that $m > 0$, $a \equiv b \pmod m$, and $c \equiv d \pmod m$, then

(i) $a + c \equiv b + d \pmod m$,

(ii) $a - c \equiv b - d \pmod m$,

(iii) $ac \equiv bd \pmod m$.

Proof. Because $a \equiv b \pmod m$ and $c \equiv d \pmod m$, we know that $m \mid (a - b)$ and $m \mid (c - d)$. Hence, there are integers k and l with $km = a - b$ and $lm = c - d$.

To prove (i), note that $(a + c) - (b + d) = (a - b) + (c - d) = km + lm = (k + l)m$. Hence, $m \mid [(a + c) - (b + d)]$. Therefore, $a + c \equiv b + d \pmod m$.

To prove (ii), note that $(a - c) - (b - d) = (a - b) - (c - d) = km - lm = (k - l)m$. Hence, $m|[(a - c) - (b - d)]$, so that $a - c \equiv b - d \pmod m$.

To prove (iii), note that $ac - bd = ac - bc + bc - bd = c(a - b) + b(c - d) = ckm + blm = m(ck + bl)$. Hence, $m \mid (ac - bd)$. Therefore, $ac \equiv bd \pmod m$. ■

Example 4.10. Because $13 \equiv 3 \pmod 5$ and $7 \equiv 2 \pmod 5$, using Theorem 3.5 we see that $20 = 13 + 7 \equiv 3 + 2 = 5 \pmod 5$, $6 = 13 - 7 \equiv 3 - 2 = 1 \pmod 5$, and $91 = 13 \cdot 7 \equiv 3 \cdot 2 = 6 \pmod 5$. ◀

The following lemma helps us to determine whether a set of m numbers forms a complete set of residues modulo m.

Lemma 4.1. A set of m incongruent integers modulo m forms a complete set of residues modulo m.

Proof. Suppose that a set of m incongruent integers modulo m does not form a complete set of residues modulo m. This implies that at least one integer a is not congruent to any of the integers in the set. Hence, there is no integer in the set congruent modulo m to the remainder of a when it is divided by m. Hence, there can be at most $m - 1$ different remainders of the integers when they are divided by m. It follows (by the pigeonhole principle, which says that if more than n objects are distributed into n boxes, at least two objects are in the same box) that at least two integers in the set have the same remainder modulo m. This is impossible, because these integers are incongruent modulo m. Hence, any m incongruent integers modulo m form a complete system of residues modulo m. ■

Theorem 4.6. If $r_1, r_2, \ldots, r_m$ is a complete system of residues modulo m, and if a is a positive integer with $(a, m) = 1$, then

$$ar_1 + b, ar_2 + b, \ldots, ar_m + b$$

is a complete system of residues modulo m for any integer b.

Proof. First, we show that no two of the integers

$$ar_1 + b, ar_2 + b, \ldots, ar_m + b$$

are congruent modulo m. To see this, note that if

$$ar_j + b \equiv ar_k + b \pmod m,$$

then, by (ii) of Theorem 4.3, we know that

$$ar_j \equiv ar_k \pmod m.$$

Because $(a, m) = 1$, Corollary 4.4.1 shows that

$$r_j \equiv r_k \pmod m.$$

Given that $r_j \not\equiv r_k \pmod m$ if $j \neq k$, we conclude that $j = k$.

By Lemma 4.1, because the set of integers in question consists of m incongruent integers modulo m, these integers form a complete system of residues modulo m. ■

The following theorem shows that a congruence is preserved when both sides are raised to the same positive integral power.

Theorem 4.7. If a, b, k, and m are integers such that $k > 0$, $m > 0$, and $a \equiv b \pmod{m}$, then $a^k \equiv b^k \pmod{m}$.

Proof. Because $a \equiv b \pmod{m}$, we have $m \mid (a - b)$, and because

$$a^k - b^k = (a - b)(a^{k-1} + a^{k-2}b + \cdots + ab^{k-2} + b^{k-1}),$$

we see that $(a - b) \mid (a^k - b^k)$. Therefore, by Theorem 1.4 it follows that $m \mid (a^k - b^k)$. Hence, $a^k \equiv b^k \pmod{m}$. ∎

Example 4.11. Since $7 \equiv 2 \pmod{5}$, Theorem 4.7 tells us that $343 = 7^3 \equiv 2^3 = 8 \pmod{5}$. ◀

The following result shows how to combine congruences of two numbers to different moduli.

Theorem 4.8. If $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}$, . . . , $a \equiv b \pmod{m_k}$, where a, b, $m_1, m_2, \ldots, m_k$ are integers with $m_1, m_2, \ldots, m_k$ positive, then

$$a \equiv b \pmod{[m_1, m_2, \ldots, m_k]},$$

where $[m_1, m_2, \ldots, m_k]$ is the least common multiple of $m_1, m_2, \ldots, m_k$.

Proof. Because $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}$, . . . , $a \equiv b \pmod{m_k}$, we know that $m_1 \mid (a - b), m_2 \mid (a - b), \ldots, m_k \mid (a - b)$. By Exercise 39 of Section 3.4 we see that

$$[m_1, m_2, \ldots, m_k] \mid (a - b).$$

Consequently,

$$a \equiv b \pmod{[m_1, m_2, \ldots, m_k]}.$$ ∎

The following result is an immediate and useful consequence of this theorem.

Corollary 4.8.1. If $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}$, . . . , $a \equiv b \pmod{m_k}$ where a and b are integers and $m_1, m_2, \ldots, m_k$ are pairwise relatively prime positive integers, then

$$a \equiv b \pmod{m_1 m_2 \cdots m_k}.$$

Proof. Since $m_1, m_2, \ldots, m_k$ are pairwise relatively prime, Exercise 68 of Section 3.4 tells us that

$$[m_1, m_2, \ldots, m_k] = m_1 m_2 \cdots m_k.$$

Hence, by Theorem 4.8, we know that

$$a \equiv b \pmod{m_1 m_2 \cdots m_k}.$$ ∎

Modular Exponentiation

In our subsequent studies, we will be working with congruences involving large powers of integers. For example, we will want to find the least positive residue of 2^{644}

modulo 645. If we attempt to find this least positive residue by first computing 2^{644}, we would have an integer with 194 decimal digits, a most undesirable thought. Instead, to find 2^{644} modulo 645 we first express the exponent 644 in binary notation:

$$(644)_{10} = (1010000100)_2.$$

Next, we compute the least positive residues of $2, 2^2, 2^4, 2^8, \ldots, 2^{512}$ by successively squaring and reducing modulo 645. This gives us the congruences

$$\begin{aligned}
2 &\equiv 2 \pmod{645},\\
2^2 &\equiv 4 \pmod{645},\\
2^4 &\equiv 16 \pmod{645},\\
2^8 &\equiv 256 \pmod{645},\\
2^{16} &\equiv 391 \pmod{645},\\
2^{32} &\equiv 16 \pmod{645},\\
2^{64} &\equiv 256 \pmod{645},\\
2^{128} &\equiv 391 \pmod{645},\\
2^{256} &\equiv 16 \pmod{645},\\
2^{512} &\equiv 256 \pmod{645}.
\end{aligned}$$

We can now compute 2^{644} modulo 645 by multiplying the least positive residues of the appropriate powers of 2. This gives

$$2^{644} = 2^{512+128+4} = 2^{512}2^{128}2^4 \equiv 256 \cdot 391 \cdot 16 = 1{,}601{,}536 \equiv 1 \pmod{645}.$$

We have just illustrated a general procedure for *modular exponentiation,* that is, for computing b^N modulo m where b, m, and N are positive integers. We first express the exponent N in binary notation, as $N = (a_k a_{k-1} \ldots a_1 a_0)_2$. We then find the least positive residues of $b, b^2, b^4, \ldots, b^{2^k}$ modulo m, by successively squaring and reducing modulo m. Finally, we multiply the least positive residues modulo m of b^{2^j} for those j with $a_j = 1$, reducing modulo m after each multiplication.

In our subsequent discussions, we will need an estimate for the number of bit operations needed for modular exponentiation. This is provided by the following proposition.

Theorem 4.9. Let b, m, and N be positive integers such that $b < m$. Then the least positive residue of b^N modulo m can be computed using $O((\log_2 m)^2 \log_2 N)$ bit operations.

Proof. To find the least positive residue of b^N modulo m, we can use the algorithm just described. First, we find the least positive residues of $b, b^2, b^4, \ldots, b^{2^k}$ modulo m, where $2^k \leq N < 2^{k+1}$, by successively squaring and reducing modulo m. This requires a total of $O((\log_2 m)^2 \log_2 N)$ bit operations, because we perform $[\log_2 N]$ squarings modulo m, each requiring $O((\log_2 m)^2)$ bit operations. Next, we multiply together the least positive residues of the integers b^{2^j} corresponding to the binary digits of N that are equal to one, and we reduce modulo m after each multiplication. This also requires

$O((\log_2 m)^2 \log_2 N)$ bit operations, because there are at most $\log_2 N$ multiplications, 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 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.

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 $7651^{20!}$.

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.