CHAPTER 4

THE THEORY OF CONGRUENCES

Gauss once said "Mathematics is the queen of the sciences and number-theory the queen of mathematics." If this be true we may add that the Disquisitiones *is the Magna Charta of number-theory.*
M. CANTOR

4.1 CARL FRIEDRICH GAUSS

Another approach to divisibility questions is through the arithmetic of remainders, or the *theory of congruences* as it is now commonly known. The concept, and the notation that makes it such a powerful tool, was first introduced by the German mathematician Carl Friedrich Gauss (1777–1855) in his *Disquisitiones Arithmeticae*; this monumental work, which appeared in 1801 when Gauss was 24 years old, laid the foundations of modern number theory. Legend has it that a large part of the *Disquisitiones Arithmeticae* had been submitted as a memoir to the French Academy the previous year and had been rejected in a manner that, even if the work had been as worthless as the referees believed, would have been inexcusable. (In an attempt to lay this defamatory tale to rest, the officers of the academy made an exhaustive search of their permanent records in 1935 and concluded that the *Disquisitiones* was never submitted, much less rejected.) "It is really astonishing," said Kronecker, "to think that a single man of such young years was able to bring to light such a wealth of results, and above all to present such a profound and well-organized treatment of an entirely new discipline."

Carl Friedrich Gauss
(1777–1855)

(*Dover Publications, Inc.*)

Gauss was one of those remarkable infant prodigies whose natural aptitude for mathematics soon became apparent. As a child of age three, according to a well-authenticated story, he corrected an error in his father's payroll calculations. His arithmetical powers so overwhelmed his schoolmasters that, by the time Gauss was 7 years old, they admitted that there was nothing more they could teach the boy. It is said that in his first arithmetic class Gauss astonished his teacher by instantly solving what was intended to be a "busy work" problem: Find the sum of all the numbers from 1 to 100. The young Gauss later confessed to having recognized the pattern

$$1 + 100 = 101, 2 + 99 = 101, 3 + 98 = 101, \ldots, 50 + 51 = 101$$

Because there are 50 pairs of numbers, each of which adds up to 101, the sum of all the numbers must be $50 \cdot 101 = 5050$. This technique provides another way of deriving the formula

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$$

for the sum of the first n positive integers. One need only display the consecutive integers 1 through n in two rows as follows:

$$\begin{array}{ccccccc} 1 & 2 & 3 & \cdots & n-1 & n \\ n & n-1 & n-2 & \cdots & 2 & 1 \end{array}$$

Addition of the vertical columns produces n terms, each of which is equal to $n + 1$; when these terms are added, we get the value $n(n + 1)$. Because the same sum is obtained on adding the two rows horizontally, what occurs is the formula $n(n + 1) = 2(1 + 2 + 3 + \cdots + n)$.

Gauss went on to a succession of triumphs, each new discovery following on the heels of a previous one. The problem of constructing regular polygons with only "Euclidean tools," that is to say, with ruler and compass alone, had long been laid aside in the belief that the ancients had exhausted all the possible constructions. In 1796, Gauss showed that the 17-sided regular polygon is so constructible, the first

advance in this area since Euclid's time. Gauss's doctoral thesis of 1799 provided a rigorous proof of the Fundamental Theorem of Algebra, which had been stated first by Girard in 1629 and then proved imperfectly by d'Alembert (1746), and later by Euler (1749). The theorem (it asserts that a polynomial equation of degree n has exactly n complex roots) was always a favorite of Gauss's, and he gave, in all, four distinct demonstrations of it. The publication of *Disquisitiones Arithmeticae* in 1801 at once placed Gauss in the front rank of mathematicians.

The most extraordinary achievement of Gauss was more in the realm of theoretical astronomy than of mathematics. On the opening night of the 19th century, January 1, 1801, the Italian astronomer Piazzi discovered the first of the so-called minor planets (planetoids or asteroids), later called Ceres. But after the course of this newly found body—visible only by telescope—passed the sun, neither Piazzi nor any other astronomer could locate it again. Piazzi's observations extended over a period of 41 days, during which the orbit swept out an angle of only nine degrees. From the scanty data available, Gauss was able to calculate the orbit of Ceres with amazing accuracy, and the elusive planet was rediscovered at the end of the year in almost exactly the position he had forecasted. This success brought Gauss worldwide fame, and led to his appointment as director of Göttingen Observatory.

By the middle of the 19th century, mathematics had grown into an enormous and unwieldy structure, divided into a large number of fields in which only the specialist knew his way. Gauss was the last complete mathematician, and it is no exaggeration to say that he was in some degree connected with nearly every aspect of the subject. His contemporaries regarded him as Princeps Mathematicorum (Prince of Mathematicians), on a par with Archimedes and Isaac Newton. This is revealed in a small incident: On being asked who was the greatest mathematician in Germany, Laplace answered, "Why, Pfaff." When the questioner indicated that he would have thought Gauss was, Laplace replied, "Pfaff is by far the greatest in Germany, but Gauss is the greatest in all Europe."

Although Gauss adorned every branch of mathematics, he always held number theory in high esteem and affection. He insisted that, "Mathematics is the Queen of the Sciences, and the theory of numbers is the Queen of Mathematics."

4.2 BASIC PROPERTIES OF CONGRUENCE

In the first chapter of *Disquisitiones Arithmeticae*, Gauss introduces the concept of congruence and the notation that makes it such a powerful technique (he explains that he was induced to adopt the symbol $\equiv$ because of the close analogy with algebraic equality). According to Gauss, "If a number n measures the difference between two numbers a and b, then a and b are said to be congruent with respect to n; if not, incongruent." Putting this into the form of a definition, we have Definition 4.1.

Definition 4.1. Let n be a fixed positive integer. Two integers a and b are said to be *congruent modulo* n, symbolized by

$$a \equiv b \pmod{n}$$

if n divides the difference $a - b$; that is, provided that $a - b = kn$ for some integer k.

To fix the idea, consider $n = 7$. It is routine to check that

$$3 \equiv 24 \pmod 7 \qquad -31 \equiv 11 \pmod 7 \qquad -15 \equiv -64 \pmod 7$$

because $3 - 24 = (-3)7$, $-31 - 11 = (-6)7$, and $-15 - (-64) = 7 \cdot 7$. When $n \nmid (a - b)$, we say that a is *incongruent to b modulo n*, and in this case we write $a \not\equiv b \pmod n$. For a simple example: $25 \not\equiv 12 \pmod 7$, because 7 fails to divide $25 - 12 = 13$.

It is to be noted that any two integers are congruent modulo 1, whereas two integers are congruent modulo 2 when they are both even or both odd. Inasmuch as congruence modulo 1 is not particularly interesting, the usual practice is to assume that $n > 1$.

Given an integer a, let q and r be its quotient and remainder upon division by n, so that

$$a = qn + r \qquad 0 \leq r < n$$

Then, by definition of congruence, $a \equiv r \pmod n$. Because there are n choices for r, we see that every integer is congruent modulo n to exactly one of the values $0, 1, 2, \ldots, n - 1$; in particular, $a \equiv 0 \pmod n$ if and only if $n \mid a$. The set of n integers $0, 1, 2, \ldots, n - 1$ is called the set of *least nonnegative residues modulo n*.

In general, a collection of n integers $a_1, a_2, \ldots, a_n$ is said to form a *complete set of residues* (or a *complete system of residues*) *modulo n* if every integer is congruent modulo n to one and only one of the a_k. To put it another way, $a_1, a_2, \ldots, a_n$ are congruent modulo n to $0, 1, 2, \ldots, n - 1$, taken in some order. For instance,

$$-12, -4, 11, 13, 22, 82, 91$$

constitute a complete set of residues modulo 7; here, we have

$$-12 \equiv 2 \quad -4 \equiv 3 \quad 11 \equiv 4 \quad 13 \equiv 6 \quad 22 \equiv 1 \quad 82 \equiv 5 \quad 91 \equiv 0$$

all modulo 7. An observation of some importance is that any n integers form a complete set of residues modulo n if and only if no two of the integers are congruent modulo n. We shall need this fact later.

Our first theorem provides a useful characterization of congruence modulo n in terms of remainders upon division by n.

Theorem 4.1. For arbitrary integers a and b, $a \equiv b \pmod n$ if and only if a and b leave the same nonnegative remainder when divided by n.

Proof. First take $a \equiv b \pmod n$, so that $a = b + kn$ for some integer k. Upon division by n, b leaves a certain remainder r; that is, $b = qn + r$, where $0 \leq r < n$. Therefore,

$$a = b + kn = (qn + r) + kn = (q + k)n + r$$

which indicates that a has the same remainder as b.

On the other hand, suppose we can write $a = q_1 n + r$ and $b = q_2 n + r$, with the same remainder r $(0 \leq r < n)$. Then

$$a - b = (q_1 n + r) - (q_2 n + r) = (q_1 - q_2)n$$

whence $n \mid a - b$. In the language of congruences, we have $a \equiv b \pmod n$.

Example 4.1. Because the integers -56 and -11 can be expressed in the form

$$-56 = (-7)9 + 7 \qquad -11 = (-2)9 + 7$$

with the same remainder 7, Theorem 4.1 tells us that $-56 \equiv -11 \pmod 9$. Going in the other direction, the congruence $-31 \equiv 11 \pmod 7$ implies that -31 and 11 have the same remainder when divided by 7; this is clear from the relations

$$-31 = (-5)7 + 4 \qquad 11 = 1 \cdot 7 + 4$$

Congruence may be viewed as a generalized form of equality, in the sense that its behavior with respect to addition and multiplication is reminiscent of ordinary equality. Some of the elementary properties of equality that carry over to congruences appear in the next theorem.

Theorem 4.2. Let $n > 1$ be fixed and a, b, c, d be arbitrary integers. Then the following properties hold:

(a) $a \equiv a \pmod n$.
(b) If $a \equiv b \pmod n$, then $b \equiv a \pmod n$.
(c) If $a \equiv b \pmod n$ and $b \equiv c \pmod n$, then $a \equiv c \pmod n$.
(d) If $a \equiv b \pmod n$ and $c \equiv d \pmod n$, then $a + c \equiv b + d \pmod n$ and $ac \equiv bd \pmod n$.
(e) If $a \equiv b \pmod n$, then $a + c \equiv b + c \pmod n$ and $ac \equiv bc \pmod n$.
(f) If $a \equiv b \pmod n$, then $a^k \equiv b^k \pmod n$ for any positive integer k.

Proof. For any integer a, we have $a - a = 0 \cdot n$, so that $a \equiv a \pmod n$. Now if $a \equiv b \pmod n$, then $a - b = kn$ for some integer k. Hence, $b - a = -(kn) = (-k)n$ and because $-k$ is an integer, this yields property (b).

Property (c) is slightly less obvious: Suppose that $a \equiv b \pmod n$ and also $b \equiv c \pmod n$. Then there exist integers h and k satisfying $a - b = hn$ and $b - c = kn$. It follows that

$$a - c = (a - b) + (b - c) = hn + kn = (h + k)n$$

which is $a \equiv c \pmod n$ in congruence notation.

In the same vein, if $a \equiv b \pmod n$ and $c \equiv d \pmod n$, then we are assured that $a - b = k_1 n$ and $c - d = k_2 n$ for some choice of k_1 and k_2. Adding these equations, we obtain

$$\begin{aligned}(a + c) - (b + d) &= (a - b) + (c - d) \\ &= k_1 n + k_2 n = (k_1 + k_2)n\end{aligned}$$

or, as a congruence statement, $a + c \equiv b + d \pmod n$. As regards the second assertion of property (d), note that

$$ac = (b + k_1 n)(d + k_2 n) = bd + (bk_2 + dk_1 + k_1 k_2 n)n$$

Because $bk_2 + dk_1 + k_1 k_2 n$ is an integer, this says that $ac - bd$ is divisible by n, whence $ac \equiv bd \pmod n$.

The proof of property (e) is covered by (d) and the fact that $c \equiv c \pmod n$. Finally, we obtain property (f) by making an induction argument. The statement certainly holds for $k = 1$, and we will assume it is true for some fixed k. From (d), we know

that $a \equiv b \pmod{n}$ and $a^k \equiv b^k \pmod{n}$ together imply that $aa^k \equiv bb^k \pmod{n}$, or equivalently $a^{k+1} \equiv b^{k+1} \pmod{n}$. This is the form the statement should take for $k+1$, and so the induction step is complete.

Before going further, we should illustrate that congruences can be a great help in carrying out certain types of computations.

Example 4.2. Let us endeavor to show that 41 divides $2^{20} - 1$. We begin by noting that $2^5 \equiv -9 \pmod{41}$, whence $(2^5)^4 \equiv (-9)^4 \pmod{41}$ by Theorem 4.2(f); in other words, $2^{20} \equiv 81 \cdot 81 \pmod{41}$. But $81 \equiv -1 \pmod{41}$, and so $81 \cdot 81 \equiv 1 \pmod{41}$. Using parts (b) and (e) of Theorem 4.2, we finally arrive at

$$2^{20} - 1 \equiv 81 \cdot 81 - 1 \equiv 1 - 1 \equiv 0 \pmod{41}$$

Thus, $41 \mid 2^{20} - 1$, as desired.

Example 4.3. For another example in the same spirit, suppose that we are asked to find the remainder obtained upon dividing the sum

$$1! + 2! + 3! + 4! + \cdots + 99! + 100!$$

by 12. Without the aid of congruences this would be an awesome calculation. The observation that starts us off is that $4! \equiv 24 \equiv 0 \pmod{12}$; thus, for $k \geq 4$,

$$k! \equiv 4! \cdot 5 \cdot 6 \cdots k \equiv 0 \cdot 5 \cdot 6 \cdots k \equiv 0 \pmod{12}$$

In this way, we find that

$$\begin{aligned} 1! + 2! + 3! + 4! + \cdots + 100! & \\ \equiv 1! + 2! + 3! + 0 + \cdots + 0 \equiv 9 \pmod{12} & \end{aligned}$$

Accordingly, the sum in question leaves a remainder of 9 when divided by 12.

In Theorem 4.1 we saw that if $a \equiv b \pmod{n}$, then $ca \equiv cb \pmod{n}$ for any integer c. The converse, however, fails to hold. As an example, perhaps as simple as any, note that $2 \cdot 4 \equiv 2 \cdot 1 \pmod{6}$, whereas $4 \not\equiv 1 \pmod{6}$. In brief: One cannot unrestrictedly cancel a common factor in the arithmetic of congruences.

With suitable precautions, cancellation can be allowed; one step in this direction, and an important one, is provided by the following theorem.

Theorem 4.3. If $ca \equiv cb \pmod{n}$, then $a \equiv b \pmod{n/d}$, where $d = \gcd(c, n)$.

Proof. By hypothesis, we can write

$$c(a - b) = ca - cb = kn$$

for some integer k. Knowing that $\gcd(c, n) = d$, there exist relatively prime integers r and s satisfying $c = dr$, $n = ds$. When these values are substituted in the displayed equation and the common factor d canceled, the net result is

$$r(a - b) = ks$$

Hence, $s \mid r(a - b)$ and $\gcd(r, s) = 1$. Euclid's lemma yields $s \mid a - b$, which may be recast as $a \equiv b \pmod{s}$; in other words, $a \equiv b \pmod{n/d}$.

Theorem 4.3 gets its maximum force when the requirement that $\gcd(c, n) = 1$ is added, for then the cancellation may be accomplished without a change in modulus.

Corollary 1. If $ca \equiv cb \pmod{n}$ and $\gcd(c, n) = 1$, then $a \equiv b \pmod{n}$.

We take a moment to record a special case of Corollary 1 that we shall have frequent occasion to use, namely, Corollary 2.

Corollary 2. If $ca \equiv cb \pmod{p}$ and $p \nmid c$, where p is a prime number, then $a \equiv b \pmod{p}$.

Proof. The conditions $p \nmid c$ and p a prime imply that $\gcd(c, p) = 1$.

Example 4.4. Consider the congruence $33 \equiv 15 \pmod{9}$ or, if one prefers, $3 \cdot 11 \equiv 3 \cdot 5 \pmod{9}$. Because $\gcd(3, 9) = 3$, Theorem 4.3 leads to the conclusion that $11 \equiv 5 \pmod{3}$. A further illustration is given by the congruence $-35 \equiv 45 \pmod{8}$, which is the same as $5 \cdot (-7) \equiv 5 \cdot 9 \pmod{8}$. The integers 5 and 8 being relatively prime, we may cancel the factor 5 to obtain a correct congruence $-7 \equiv 9 \pmod{8}$.

Let us call attention to the fact that, in Theorem 4.3, it is unnecessary to stipulate that $c \not\equiv 0 \pmod{n}$. Indeed, if $c \equiv 0 \pmod{n}$, then $\gcd(c, n) = n$ and the conclusion of the theorem would state that $a \equiv b \pmod{1}$; but, as we remarked earlier, this holds trivially for all integers a and b.

There is another curious situation that can arise with congruences: The product of two integers, neither of which is congruent to zero, may turn out to be congruent to zero. For instance, $4 \cdot 3 \equiv 0 \pmod{12}$, but $4 \not\equiv 0 \pmod{12}$ and $3 \not\equiv 0 \pmod{12}$. It is a simple matter to show that if $ab \equiv 0 \pmod{n}$ and $\gcd(a, n) = 1$, then $b \equiv 0 \pmod{n}$: Corollary 1 permits us legitimately to cancel the factor a from both sides of the congruence $ab \equiv a \cdot 0 \pmod{n}$. A variation on this is that when $ab \equiv 0 \pmod{p}$, with p a prime, then either $a \equiv 0 \pmod{p}$ or $b \equiv 0 \pmod{p}$.

PROBLEMS 4.2

1. Prove each of the following assertions:
   (a) If $a \equiv b \pmod{n}$ and $m \mid n$, then $a \equiv b \pmod{m}$.
   (b) If $a \equiv b \pmod{n}$ and $c > 0$, then $ca \equiv cb \pmod{cn}$.
   (c) If $a \equiv b \pmod{n}$ and the integers a, b, n are all divisible by $d > 0$, then $a/d \equiv b/d \pmod{n/d}$.
2. Give an example to show that $a^2 \equiv b^2 \pmod{n}$ need not imply that $a \equiv b \pmod{n}$.
3. If $a \equiv b \pmod{n}$, prove that $\gcd(a, n) = \gcd(b, n)$.
4. (a) Find the remainders when 2^{50} and 41^{65} are divided by 7.
   (b) What is the remainder when the following sum is divided by 4?

$$1^5 + 2^5 + 3^5 + \cdots + 99^5 + 100^5$$

5. Prove that the integer $53^{103} + 103^{53}$ is divisible by 39, and that $111^{333} + 333^{111}$ is divisible by 7.

6. For $n \geq 1$, use congruence theory to establish each of the following divisibility statements:
(a) $7 \mid 5^{2n} + 3 \cdot 2^{5n-2}$.
(b) $13 \mid 3^{n+2} + 4^{2n+1}$.
(c) $27 \mid 2^{5n+1} + 5^{n+2}$.
(d) $43 \mid 6^{n+2} + 7^{2n+1}$.

7. For $n \geq 1$, show that

$$(-13)^{n+1} \equiv (-13)^n + (-13)^{n-1} \pmod{181}$$

[*Hint:* Notice that $(-13)^2 \equiv -13 + 1 \pmod{181}$; use induction on n.]

8. Prove the assertions below:
(a) If a is an odd integer, then $a^2 \equiv 1 \pmod 8$.
(b) For any integer a, $a^3 \equiv 0, 1$, or $6 \pmod 7$.
(c) For any integer a, $a^4 \equiv 0$ or $1 \pmod 5$.
(d) If the integer a is not divisible by 2 or 3, then $a^2 \equiv 1 \pmod{24}$.

9. If p is a prime satisfying $n < p < 2n$, show that

$$\binom{2n}{n} \equiv 0 \pmod p$$

10. If $a_1, a_2, \ldots, a_n$ is a complete set of residues modulo n and $\gcd(a, n) = 1$, prove that $aa_1, aa_2, \ldots, aa_n$ is also a complete set of residues modulo n.
[*Hint:* It suffices to show that the numbers in question are incongruent modulo n.]

11. Verify that $0, 1, 2, 2^2, 2^3, \ldots, 2^9$ form a complete set of residues modulo 11, but that $0, 1^2, 2^2, 3^2, \ldots, 10^2$ do not.

12. Prove the following statements:
(a) If $\gcd(a, n) = 1$, then the integers

$$c, c + a, c + 2a, c + 3a, \ldots, c + (n - 1)a$$

form a complete set of residues modulo n for any c.
(b) Any n consecutive integers form a complete set of residues modulo n.
[*Hint:* Use part (a).]
(c) The product of any set of n consecutive integers is divisible by n.

13. Verify that if $a \equiv b \pmod{n_1}$ and $a \equiv b \pmod{n_2}$, then $a \equiv b \pmod n$, where the integer $n = \operatorname{lcm}(n_1, n_2)$. Hence, whenever n_1 and n_2 are relatively prime, $a \equiv b \pmod{n_1 n_2}$.

14. Give an example to show that $a^k \equiv b^k \pmod n$ and $k \equiv j \pmod n$ need not imply that $a^j \equiv b^j \pmod n$.

15. Establish that if a is an odd integer, then for any $n \geq 1$

$$a^{2^n} \equiv 1 \pmod{2^{n+2}}$$

[*Hint:* Proceed by induction on n.]

16. Use the theory of congruences to verify that

$$89 \mid 2^{44} - 1 \qquad \text{and} \qquad 97 \mid 2^{48} - 1$$

17. Prove that whenever $ab \equiv cd \pmod n$ and $b \equiv d \pmod n$, with $\gcd(b, n) = 1$, then $a \equiv c \pmod n$.

18. If $a \equiv b \pmod{n_1}$ and $a \equiv c \pmod{n_2}$, prove that $b \equiv c \pmod n$, where the integer $n = \gcd(n_1, n_2)$.

4.3 BINARY AND DECIMAL REPRESENTATIONS OF INTEGERS

One of the more interesting applications of congruence theory involves finding special criteria under which a given integer is divisible by another integer. At their heart, these divisibility tests depend on the notational system used to assign "names" to integers and, more particularly, to the fact that 10 is taken as the base for our number system. Let us, therefore, start by showing that, given an integer $b > 1$, any positive integer N can be written uniquely in terms of powers of b as

$$N = a_m b^m + a_{m-1} b^{m-1} + \cdots + a_2 b^2 + a_1 b + a_0$$

where the coefficients a_k can take on the b different values $0, 1, 2, \ldots, b-1$. For the Division Algorithm yields integers q_1 and a_0 satisfying

$$N = q_1 b + a_0 \qquad 0 \leq a_0 < b$$

If $q_1 \geq b$, we can divide once more, obtaining

$$q_1 = q_2 b + a_1 \qquad 0 \leq a_1 < b$$

Now substitute for q_1 in the earlier equation to get

$$N = (q_2 b + a_1)b + a_0 = q_2 b^2 + a_1 b + a_0$$

As long as $q_2 \geq b$, we can continue in the same fashion. Going one more step: $q_2 = q_3 b + a_2$, where $0 \leq a_2 < b$; hence

$$N = q_3 b^3 + a_2 b^2 + a_1 b + a_0$$

Because $N > q_1 > q_2 > \cdots \geq 0$ is a strictly decreasing sequence of integers, this process must eventually terminate, say, at the $(m-1)$th stage, where

$$q_{m-1} = q_m b + a_{m-1} \qquad 0 \leq a_{m-1} < b$$

and $0 \leq q_m < b$. Setting $a_m = q_m$, we reach the representation

$$N = a_m b^m + a_{m-1} b^{m-1} + \cdots + a_1 b + a_0$$

which was our aim.

To show uniqueness, let us suppose that N has two distinct representations, say,

$$N = a_m b^m + \cdots + a_1 b + a_0 = c_m b^m + \cdots + c_1 b + c_0$$

with $0 \leq a_i < b$ for each i and $0 \leq c_j < b$ for each j (we can use the same m by simply adding terms with coefficients $a_i = 0$ or $c_j = 0$, if necessary). Subtracting the second representation from the first gives the equation

$$0 = d_m b^m + \cdots + d_1 b + d_0$$

where $d_i = a_i - c_i$ for $i = 0, 1, \ldots, m$. Because the two representations for N are assumed to be different, we must have $d_i \neq 0$ for some value of i. Take k to be the smallest subscript for which $d_k \neq 0$. Then

$$0 = d_m b^m + \cdots + d_{k+1} b^{k+1} + d_k b^k$$

and so, after dividing by b^k,

$$d_k = -b(d_m b^{m-k-1} + \cdots + d_{k+1})$$

This tells us that $b \mid d_k$. Now the inequalities $0 \leq a_k < b$ and $0 \leq c_k < b$ lead us to $-b < a_k - c_k < b$, or $|d_k| < b$. The only way of reconciling the conditions $b \mid d_k$ and $|d_k| < b$ is to have $d_k = 0$, which is impossible. From this contradiction, we conclude that the representation of N is unique.

The essential feature in all of this is that the integer N is completely determined by the ordered array $a_m, a_{m-1}, \ldots, a_1, a_0$ of coefficients, with the plus signs and the powers of b being superfluous. Thus, the number

$$N = a_m b^m + a_{m-1} b^{m-1} + \cdots + a_2 b^2 + a_1 b + a_0$$

may be replaced by the simpler symbol

$$N = (a_m a_{m-1} \cdots a_2 a_1 a_0)_b$$

(the right-hand side is not to be interpreted as a product, but only as an abbreviation for N). We call this the *base b place-value notation for N*.

Small values of b give rise to lengthy representation of numbers, but have the advantage of requiring fewer choices for coefficients. The simplest case occurs when the base $b = 2$, and the resulting system of enumeration is called the *binary number system* (from the Latin *binarius*, two). The fact that when a number is written in the binary system only the integers 0 and 1 can appear as coefficients means that every positive integer is expressible in exactly one way as a sum of distinct powers of 2. For example, the integer 105 can be written as

$$\begin{aligned} 105 &= 1 \cdot 2^6 + 1 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0 \cdot 2 + 1 \\ &= 2^6 + 2^5 + 2^3 + 1 \end{aligned}$$

or, in abbreviated form,

$$105 = (1101001)_2$$

In the other direction, $(1001111)_2$ translates into

$$1 \cdot 2^6 + 0 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2 + 1 = 79$$

The binary system is most convenient for use in modern electronic computing machines, because binary numbers are represented by strings of zeros and ones; 0 and 1 can be expressed in the machine by a switch (or a similar electronic device) being either on or off.

We shall frequently wish to calculate the value of $a^k \pmod{n}$ when k is large. Is there a more efficient way of obtaining the least positive residue than multiplying a by itself k times before reducing modulo n? One such procedure, called the *binary exponential algorithm*, relies on successive squarings, with a reduction modulo n after each squaring. More specifically, the exponent k is written in binary form, as $k = (a_m a_{m-1} \ldots a_2 a_1 a_0)_2$, and the values $a^{2^j} \pmod{n}$ are calculated for the powers of 2, which correspond to the 1's in the binary representation. These partial results are then multiplied together to give the final answer.

An illustration should make this process clear.

Example 4.5. To calculate $5^{110} \pmod{131}$, first note that the exponent 110 can be expressed in binary form as

$$110 = 64 + 32 + 8 + 4 + 2 = (1101110)_2$$

Thus, we obtain the powers $5^{2^j} \pmod{131}$ for $0 \leq j \leq 6$ by repeatedly squaring while at each stage reducing each result modulo 131:

$$\begin{aligned} 5^2 &\equiv 25 \pmod{131} & 5^{16} &\equiv 27 \pmod{131} \\ 5^4 &\equiv 101 \pmod{131} & 5^{32} &\equiv 74 \pmod{131} \\ 5^8 &\equiv 114 \pmod{131} & 5^{64} &\equiv 105 \pmod{131} \end{aligned}$$

When the appropriate partial results—those corresponding to the 1's in the binary expansion of 110—are multiplied, we see that

$$\begin{aligned} 5^{110} &= 5^{64+32+8+4+2} \\ &= 5^{64} \cdot 5^{32} \cdot 5^8 \cdot 5^4 \cdot 5^2 \\ &\equiv 105 \cdot 74 \cdot 114 \cdot 101 \cdot 25 \equiv 60 \pmod{131} \end{aligned}$$

As a minor variation of the procedure, one might calculate, modulo 131, the powers $5, 5^2, 5^3, 5^6, 5^{12}, 5^{24}, 5^{48}, 5^{96}$ to arrive at

$$5^{110} = 5^{96} \cdot 5^{12} \cdot 5^2 \equiv 41 \cdot 117 \cdot 25 \equiv 60 \pmod{131}$$

which would require two fewer multiplications.

We ordinarily record numbers in the *decimal system* of notation, where $b = 10$, omitting the 10-subscript that specifies the base. For instance, the symbol 1492 stands for the more awkward expression

$$1 \cdot 10^3 + 4 \cdot 10^2 + 9 \cdot 10 + 2$$

The integers 1, 4, 9, and 2 are called the *digits* of the given number, 1 being the thousands digit, 4 the hundreds digit, 9 the tens digit, and 2 the units digit. In technical language we refer to the representation of the positive integers as sums of powers of 10, with coefficients at most 9, as their *decimal representation* (from the Latin *decem*, ten).

We are about ready to derive criteria for determining whether an integer is divisible by 9 or 11, without performing the actual division. For this, we need a result having to do with congruences involving polynomials with integral coefficients.

Theorem 4.4. Let $P(x) = \sum_{k=0}^{m} c_k x^k$ be a polynomial function of x with integral coefficients c_k. If $a \equiv b \pmod{n}$, then $P(a) \equiv P(b) \pmod{n}$.

Proof. Because $a \equiv b \pmod{n}$, part (f) of Theorem 4.2 can be applied to give $a^k \equiv b^k \pmod{n}$ for $k = 0, 1, \ldots, m$. Therefore,

$$c_k a^k \equiv c_k b^k \pmod{n}$$

for all such k. Adding these $m + 1$ congruences, we conclude that

$$\sum_{k=0}^{m} c_k a^k \equiv \sum_{k=0}^{m} c_k b^k \pmod{n}$$

or, in different notation, $P(a) \equiv P(b) \pmod{n}$.

If $P(x)$ is a polynomial with integral coefficients, we say that a is a solution of the congruence $P(x) \equiv 0 \pmod{n}$ if $P(a) \equiv 0 \pmod{n}$.

Corollary. If a is a solution of $P(x) \equiv 0 \pmod{n}$ and $a \equiv b \pmod{n}$, then b also is a solution.

Proof. From the last theorem, it is known that $P(a) \equiv P(b) \pmod{n}$. Hence, if a is a solution of $P(x) \equiv 0 \pmod{n}$, then $P(b) \equiv P(a) \equiv 0 \pmod{n}$, making b a solution.

One divisibility test that we have in mind is this. A positive integer is divisible by 9 if and only if the sum of the digits in its decimal representation is divisible by 9.

Theorem 4.5. Let $N = a_m 10^m + a_{m-1}10^{m-1} + \cdots + a_1 10 + a_0$ be the decimal expansion of the positive integer N, $0 \leq a_k < 10$, and let $S = a_0 + a_1 + \cdots + a_m$. Then $9 \mid N$ if and only if $9 \mid S$.

Proof. Consider $P(x) = \sum_{k=0}^{m} a_k x^k$, a polynomial with integral coefficients. The key observation is that $10 \equiv 1 \pmod{9}$, whence by Theorem 4.4, $P(10) \equiv P(1) \pmod{9}$. But $P(10) = N$ and $P(1) = a_0 + a_1 + \cdots + a_m = S$, so that $N \equiv S \pmod{9}$. It follows that $N \equiv 0 \pmod{9}$ if and only if $S \equiv 0 \pmod{9}$, which is what we wanted to prove.

Theorem 4.4 also serves as the basis for a well-known test for divisibility by 11: an integer is divisible by 11 if and only if the alternating sum of its digits is divisible by 11. We state this more precisely by Theorem 4.6.

Theorem 4.6. Let $N = a_m 10^m + a_{m-1}10^{m-1} + \cdots + a_1 10 + a_0$ be the decimal expansion of the positive integer N, $0 \leq a_k < 10$, and let $T = a_0 - a_1 + a_2 - \cdots + (-1)^m a_m$. Then $11 \mid N$ if and only if $11 \mid T$.

Proof. As in the proof of Theorem 4.5, put $P(x) = \sum_{k=0}^{m} a_k x^k$. Because $10 \equiv -1 \pmod{11}$, we get $P(10) \equiv P(-1) \pmod{11}$. But $P(10) = N$, whereas $P(-1) = a_0 - a_1 + a_2 - \cdots + (-1)^m a_m = T$, so that $N \equiv T \pmod{11}$. The implication is that either both N and T are divisible by 11 or neither is divisible by 11.

Example 4.6. To see an illustration of the last two results, consider the integer $N = 1{,}571{,}724$. Because the sum

$$1 + 5 + 7 + 1 + 7 + 2 + 4 = 27$$

is divisible by 9, Theorem 4.5 guarantees that 9 divides N. It also can be divided by 11; for, the alternating sum

$$4 - 2 + 7 - 1 + 7 - 5 + 1 = 11$$

is divisible by 11.

Congruence theory is frequently used to append an extra check digit to identification numbers, in order to recognize transmission errors or forgeries. Personal

identification numbers of some kind appear on passports, credit cards, bank accounts, and a variety of other settings.

Some banks use an eight-digit identification number $a_1a_2 \ldots a_8$ together with a final check digit a_9. The check digit is usually obtained by multiplying the digits $a_i (1 \leq i \leq 8)$ by certain "weights" and calculating the sum of the weighted products modulo 10. For instance, the check digit might be chosen to satisfy

$$a_9 \equiv 7a_1 + 3a_2 + 9a_3 + 7a_4 + 3a_5 + 9a_6 + 7a_7 + 3a_8 \pmod{10}$$

The identification number 81504216 would then have check digit

$$a_9 \equiv 7 \cdot 8 + 3 \cdot 1 + 9 \cdot 5 + 7 \cdot 0 + 3 \cdot 4 + 9 \cdot 2 + 7 \cdot 1 + 3 \cdot 6 \equiv 9 \pmod{10}$$

so that 815042169 would be printed on the check.

This weighting scheme for assigning check digits detects any single-digit error in the identification number. For suppose that the digit a_i is replaced by a different a_i'. By the manner in which the check digit is calculated, the difference between the correct a_9 and the new a_9' is

$$a_9 - a_9' \equiv k(a_i - a_i') \pmod{10}$$

where k is 7, 3, or 9 depending on the position of a_i'. Because $k(a_i - a_i') \not\equiv 0 \pmod{10}$, it follows that $a_9 \neq a_9'$ and the error is apparent. Thus, if the valid number 81504216 were incorrectly entered as 81504316 into a computer programmed to calculate check digits, an 8 would come up rather than the expected 9.

The modulo 10 approach is not entirely effective, for it does not always detect the common error of transposing distinct adjacent entries a and b within the string of digits. To illustrate: the identification numbers 81504216 and 81504261 have the same check digit 9 when our example weights are used. (The problem occurs when $|a - b| = 5$.) More sophisticated methods are available, with larger moduli and different weights, that would prevent this possible error.

PROBLEMS 4.3

1. Use the binary exponentiation algorithm to compute both $19^{53} \pmod{503}$ and $141^{47} \pmod{1537}$.

2. Prove the following statements:
   (a) For any integer a, the units digit of a^2 is 0, 1, 4, 5, 6, or 9.
   (b) Any one of the integers 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 can occur as the units digit of a^3.
   (c) For any integer a, the units digit of a^4 is 0, 1, 5, or 6.
   (d) The units digit of a triangular number is 0, 1, 3, 5, 6, or 8.

3. Find the last two digits of the number 9^{9^9}.
   [*Hint:* $9^9 \equiv 9 \pmod{10}$; hence, $9^{9^9} = 9^{9+10k}$; notice that $9^9 \equiv 89 \pmod{100}$.]

4. Without performing the divisions, determine whether the integers 176521221 and 149235678 are divisible by 9 or 11.

5. (a) Obtain the following generalization of Theorem 4.6: If the integer N is represented in the base b by

$$N = a_m b^m + \cdots + a_2 b^2 + a_1 b + a_0 \qquad 0 \leq a_k \leq b - 1$$

then $b - 1 \mid N$ if and only if $b - 1 \mid (a_m + \cdots + a_2 + a_1 + a_0)$.

(b) Give criteria for the divisibility of N by 3 and 8 that depend on the digits of N when written in the base 9.
(c) Is the integer $(447836)_9$ divisible by 3 and 8?

6. Working modulo 9 or 11, find the missing digits in the calculations below:
(a) $51840 \cdot 273581 = 1418243x040$.
(b) $2x99561 = [3(523 + x)]^2$.
(c) $2784x = x \cdot 5569$.
(d) $512 \cdot 1x53125 = 1000000000$.

7. Establish the following divisibility criteria:
(a) An integer is divisible by 2 if and only if its units digit is 0, 2, 4, 6, or 8.
(b) An integer is divisible by 3 if and only if the sum of its digits is divisible by 3.
(c) An integer is divisible by 4 if and only if the number formed by its tens and units digits is divisible by 4.
[*Hint:* $10^k \equiv 0 \pmod 4$ for $k \geq 2$.]
(d) An integer is divisible by 5 if and only if its units digit is 0 or 5.

8. For any integer a, show that $a^2 - a + 7$ ends in one of the digits 3, 7, or 9.

9. Find the remainder when 4444^{4444} is divided by 9.
[*Hint:* Observe that $2^3 \equiv -1 \pmod 9$.]

10. Prove that no integer whose digits add up to 15 can be a square or a cube.
[*Hint:* For any a, $a^3 \equiv 0, 1$, or $8 \pmod 9$.]

11. Assuming that 495 divides $273x49y5$, obtain the digits x and y.

12. Determine the last three digits of the number 7^{999}.
[*Hint:* $7^{4n} \equiv (1 + 400)^n \equiv 1 + 400n \pmod{1000}$.]

13. If t_n denotes the nth triangular number, show that $t_{n+2k} \equiv t_n \pmod k$; hence, t_n and t_{n+20} must have the same last digit.

14. For any $n \geq 1$, prove that there exists a prime with at least n of its digits equal to 0.
[*Hint:* Consider the arithmetic progression $10^{n+1}k + 1$ for $k = 1, 2, \ldots$.]

15. Find the values of $n \geq 1$ for which $1! + 2! + 3! + \cdots + n!$ is a perfect square.
[*Hint:* Problem 2(a).]

16. Show that 2^n divides an integer N if and only if 2^n divides the number made up of the last n digits of N.
[*Hint:* $10^k = 2^k 5^k \equiv 0 \pmod{2^n}$ for $k \geq n$.]

17. Let $N = a_m 10^m + \cdots + a_2 10^2 + a_1 10 + a_0$, where $0 \leq a_k \leq 9$, be the decimal expansion of a positive integer N.
(a) Prove that 7, 11, and 13 all divide N if and only if 7, 11, and 13 divide the integer

$$M = (100a_2 + 10a_1 + a_0) - (100a_5 + 10a_4 + a_3) + (100a_8 + 10a_7 + a_6) - \cdots$$

[*Hint:* If n is even, then $10^{3n} \equiv 1$, $10^{3n+1} \equiv 10$, $10^{3n+2} \equiv 100 \pmod{1001}$; if n is odd, then $10^{3n} \equiv -1$, $10^{3n+1} \equiv -10$, $10^{3n+2} \equiv -100 \pmod{1001}$.]
(b) Prove that 6 divides N if and only if 6 divides the integer

$$M = a_0 + 4a_1 + 4a_2 + \cdots + 4a_m$$

18. Without performing the divisions, determine whether the integer 1010908899 is divisible by 7, 11, and 13.

19. (a) Given an integer N, let M be the integer formed by reversing the order of the digits of N (for example, if $N = 6923$, then $M = 3296$). Verify that $N - M$ is divisible by 9.

(b) A *palindrome* is a number that reads the same backward as forward (for instance, 373 and 521125 are palindromes). Prove that any palindrome with an even number of digits is divisible by 11.

20. Given a repunit R_n, show that
(a) $9 \mid R_n$ if and only if $9 \mid n$.
(b) $11 \mid R_n$ if and only if n is even.

21. Factor the repunit $R_6 = 111111$ into a product of primes.
[*Hint:* Problem 17(a).]

22. Explain why the following curious calculations hold:

$$\begin{aligned}
1 \cdot 9 + 2 &= 11 \\
12 \cdot 9 + 3 &= 111 \\
123 \cdot 9 + 4 &= 1111 \\
1234 \cdot 9 + 5 &= 11111 \\
12345 \cdot 9 + 6 &= 111111 \\
123456 \cdot 9 + 7 &= 1111111 \\
1234567 \cdot 9 + 8 &= 11111111 \\
12345678 \cdot 9 + 9 &= 111111111 \\
123456789 \cdot 9 + 10 &= 1111111111
\end{aligned}$$

[*Hint:* Show that

$$(10^{n-1} + 2 \cdot 10^{n-2} + 3 \cdot 10^{n-3} + \cdots + n)(10 - 1) + (n + 1) = \frac{10^{n+1} - 1}{9}.]$$

23. An old and somewhat illegible invoice shows that 72 canned hams were purchased for $\$x\,67.9y$. Find the missing digits.

24. If 792 divides the integer $13xy\,45z$, find the digits x, y, and z.
[*Hint:* By Problem 17, $8 \mid 45z$.]

25. For any prime $p > 3$, prove that 13 divides $10^{2p} - 10^p + 1$.

26. Consider the eight-digit bank identification number $a_1a_2 \ldots a_8$, which is followed by a ninth check digit a_9 chosen to satisfy the congruence

$$a_9 \equiv 7a_1 + 3a_2 + 9a_3 + 7a_4 + 3a_5 + 9a_6 + 7a_7 + 3a_8 \pmod{10}$$

(a) Obtain the check digits that should be appended to the two numbers 55382006 and 81372439.
(b) The bank identification number $237a_418538$ has an illegible fourth digit. Determine the value of the obscured digit.

27. The International Standard Book Number (ISBN) used in many libraries consists of nine digits $a_1a_2 \ldots a_9$ followed by a tenth check digit a_{10}, which satisfies

$$a_{10} \equiv \sum_{k=1}^{9} ka_k \pmod{11}$$

Determine whether each of the ISBNs below is correct:
(a) 0-07-232569-0 (United States).
(b) 91-7643-497-5 (Sweden).
(c) 1-56947-303-10 (England).

28. When printing the ISBN $a_1a_2 \ldots a_9$, two unequal digits were transposed. Show that the check digits detected this error.

4.4 LINEAR CONGRUENCES AND THE CHINESE REMAINDER THEOREM

This is a convenient place in our development of number theory at which to investigate the theory of linear congruences: an equation of the form $ax \equiv b \pmod{n}$ is called a *linear congruence*, and by a solution of such an equation we mean an integer x_0 for which $ax_0 \equiv b \pmod{n}$. By definition, $ax_0 \equiv b \pmod{n}$ if and only if $n \mid ax_0 - b$ or, what amounts to the same thing, if and only if $ax_0 - b = ny_0$ for some integer y_0. Thus, the problem of finding all integers that will satisfy the linear congruence $ax \equiv b \pmod{n}$ is identical with that of obtaining all solutions of the linear Diophantine equation $ax - ny = b$. This allows us to bring the results of Chapter 2 into play.

It is convenient to treat two solutions of $ax \equiv b \pmod{n}$ that are congruent modulo n as being "equal" even though they are not equal in the usual sense. For instance, $x = 3$ and $x = -9$ both satisfy the congruence $3x \equiv 9 \pmod{12}$; because $3 \equiv -9 \pmod{12}$, they are not counted as different solutions. In short: When we refer to the number of solutions of $ax \equiv b \pmod{n}$, we mean the number of incongruent integers satisfying this congruence.

With these remarks in mind, the principal result is easy to state.

Theorem 4.7. The linear congruence $ax \equiv b \pmod{n}$ has a solution if and only if $d \mid b$, where $d = \gcd(a, n)$. If $d \mid b$, then it has d mutually incongruent solutions modulo n.

Proof. We already have observed that the given congruence is equivalent to the linear Diophantine equation $ax - ny = b$. From Theorem 2.9, it is known that the latter equation can be solved if and only if $d \mid b$; moreover, if it is solvable and x_0, y_0 is one specific solution, then any other solution has the form

$$x = x_0 + \frac{n}{d}t \qquad y = y_0 + \frac{a}{d}t$$

for some choice of t.

Among the various integers satisfying the first of these formulas, consider those that occur when t takes on the successive values $t = 0, 1, 2, \ldots, d - 1$:

$$x_0, x_0 + \frac{n}{d}, x_0 + \frac{2n}{d}, \ldots, x_0 + \frac{(d-1)n}{d}$$

We claim that these integers are incongruent modulo n, and all other such integers x are congruent to some one of them. If it happened that

$$x_0 + \frac{n}{d}t_1 \equiv x_0 + \frac{n}{d}t_2 \pmod{n}$$

where $0 \leq t_1 < t_2 \leq d - 1$, then we would have

$$\frac{n}{d}t_1 \equiv \frac{n}{d}t_2 \pmod{n}$$

Now $\gcd(n/d, n) = n/d$, and therefore by Theorem 4.3 the factor n/d could be canceled to arrive at the congruence

$$t_1 \equiv t_2 \pmod{d}$$

which is to say that $d \mid t_2 - t_1$. But this is impossible in view of the inequality $0 < t_2 - t_1 < d$.

It remains to argue that any other solution $x_0 + (n/d)t$ is congruent modulo n to one of the d integers listed above. The Division Algorithm permits us to write t as $t = qd + r$, where $0 \leq r \leq d - 1$. Hence

$$\begin{aligned} x_0 + \frac{n}{d}t &= x_0 + \frac{n}{d}(qd + r) \\ &= x_0 + nq + \frac{n}{d}r \\ &\equiv x_0 + \frac{n}{d}r \pmod{n} \end{aligned}$$

with $x_0 + (n/d)r$ being one of our d selected solutions. This ends the proof.

The argument that we gave in Theorem 4.7 brings out a point worth stating explicitly: If x_0 is any solution of $ax \equiv b \pmod{n}$, then the $d = \gcd(a, n)$ incongruent solutions are given by

$$x_0, x_0 + \frac{n}{d}, x_0 + 2\left(\frac{n}{d}\right), \ldots, x_0 + (d-1)\left(\frac{n}{d}\right)$$

For the reader's convenience, let us also record the form Theorem 4.7 takes in the special case in which a and n are assumed to be relatively prime.

Corollary. If $\gcd(a, n) = 1$, then the linear congruence $ax \equiv b \pmod{n}$ has a unique solution modulo n.

Given relatively prime integers a and n, the congruence $ax \equiv 1 \pmod{n}$ has a unique solution. This solution is sometimes called the (multiplicative) inverse of a modulo n.

We now pause to look at two concrete examples.

Example 4.7. First consider the linear congruence $18x \equiv 30 \pmod{42}$. Because $\gcd(18, 42) = 6$ and 6 surely divides 30, Theorem 4.7 guarantees the existence of exactly six solutions, which are incongruent modulo 42. By inspection, one solution is found to be $x = 4$. Our analysis tells us that the six solutions are as follows:

$$x \equiv 4 + (42/6)t \equiv 4 + 7t \pmod{42} \qquad t = 0, 1, \ldots, 5$$

or, plainly enumerated,

$$x \equiv 4, 11, 18, 25, 32, 39 \pmod{42}$$

Example 4.8. Let us solve the linear congruence $9x \equiv 21 \pmod{30}$. At the outset, because $\gcd(9, 30) = 3$ and $3 \mid 21$, we know that there must be three incongruent solutions.

One way to find these solutions is to divide the given congruence through by 3, thereby replacing it by the equivalent congruence $3x \equiv 7 \pmod{10}$. The relative primeness of 3 and 10 implies that the latter congruence admits a unique solution modulo 10. Although it is not the most efficient method, we could test the integers

0, 1, 2, . . . ,9 in turn until the solution is obtained. A better way is this: Multiply both sides of the congruence $3x \equiv 7 \pmod{10}$ by 7 to get

$$21x \equiv 49 \pmod{10}$$

which reduces to $x \equiv 9 \pmod{10}$. (This simplification is no accident, for the multiples $0 \cdot 3,\ 1 \cdot 3,\ 2 \cdot 3, \ldots, 9 \cdot 3$ form a complete set of residues modulo 10; hence, one of them is necessarily congruent to 1 modulo 10.) But the original congruence was given modulo 30, so that its incongruent solutions are sought among the integers 0, 1, 2, . . . , 29. Taking $t = 0, 1, 2$, in the formula

$$x = 9 + 10t$$

we obtain 9, 19, 29, whence

$$x \equiv 9 \pmod{30} \qquad x \equiv 19 \pmod{30} \qquad x \equiv 29 \pmod{30}$$

are the required three solutions of $9x \equiv 21 \pmod{30}$.

A different approach to the problem is to use the method that is suggested in the proof of Theorem 4.7. Because the congruence $9x \equiv 21 \pmod{30}$ is equivalent to the linear Diophantine equation

$$9x - 30y = 21$$

we begin by expressing $3 = \gcd(9, 30)$ as a linear combination of 9 and 30. It is found, either by inspection or by using the Euclidean Algorithm, that $3 = 9(-3) + 30 \cdot 1$, so that

$$21 = 7 \cdot 3 = 9(-21) - 30(-7)$$

Thus, $x = -21$, $y = -7$ satisfy the Diophantine equation and, in consequence, all solutions of the congruence in question are to be found from the formula

$$x = -21 + (30/3)t = -21 + 10t$$

The integers $x = -21 + 10t$, where $t = 0, 1, 2$, are incongruent modulo 30 (but all are congruent modulo 10); thus, we end up with the incongruent solutions

$$x \equiv -21 \pmod{30} \qquad x \equiv -11 \pmod{30} \qquad x \equiv -1 \pmod{30}$$

or, if one prefers positive numbers, $x \equiv 9, 19, 29 \pmod{30}$.

Having considered a single linear congruence, it is natural to turn to the problem of solving a system of simultaneous linear congruences:

$$a_1x \equiv b_1 \pmod{m_1},\ a_2x \equiv b_2 \pmod{m_2},\ \ldots,\ a_rx \equiv b_r \pmod{m_r}$$

We shall assume that the moduli m_k are relatively prime in pairs. Evidently, the system will admit no solution unless each individual congruence is solvable; that is, unless $d_k \mid b_k$ for each k, where $d_k = \gcd(a_k, m_k)$. When these conditions are satisfied, the factor d_k can be canceled in the kth congruence to produce a new system having the same set of solutions as the original one:

$$a_1'x \equiv b_1' \pmod{n_1},\ a_2'x \equiv b_2' \pmod{n_2},\ \ldots,\ a_r'x \equiv b_r' \pmod{n_r}$$

where $n_k = m_k/d_k$ and $\gcd(n_i, n_j) = 1$ for $i \neq j$; in addition, $\gcd(a_i', n_i) = 1$. The solutions of the individual congruences assume the form

$$x \equiv c_1 \pmod{n_1}, x \equiv c_2 \pmod{n_2}, \ldots, x \equiv c_r \pmod{n_r}$$

Thus, the problem is reduced to one of finding a simultaneous solution of a system of congruences of this simpler type.

The kind of problem that can be solved by simultaneous congruences has a long history, appearing in the Chinese literature as early as the 1st century A.D. Sun-Tsu asked: Find a number that leaves the remainders 2, 3, 2 when divided by 3, 5, 7, respectively. (Such mathematical puzzles are by no means confined to a single cultural sphere; indeed, the same problem occurs in the *Introductio Arithmeticae* of the Greek mathematician Nicomachus, circa 100 A.D.) In honor of their early contributions, the rule for obtaining a solution usually goes by the name of the Chinese Remainder Theorem.

Theorem 4.8 Chinese Remainder Theorem. Let $n_1, n_2, \ldots, n_r$ be positive integers such that $\gcd(n_i, n_j) = 1$ for $i \neq j$. Then the system of linear congruences

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_r \pmod{n_r} \end{aligned}$$

has a simultaneous solution, which is unique modulo the integer $n_1 n_2 \cdots n_r$.

Proof. We start by forming the product $n = n_1 n_2 \cdots n_r$. For each $k = 1, 2, \ldots, r$, let

$$N_k = \frac{n}{n_k} = n_1 \cdots n_{k-1} n_{k+1} \cdots n_r$$

In words, N_k is the product of all the integers n_i with the factor n_k omitted. By hypothesis, the n_i are relatively prime in pairs, so that $\gcd(N_k, n_k) = 1$. According to the theory of a single linear congruence, it is therefore possible to solve the congruence $N_k x \equiv 1 \pmod{n_k}$; call the unique solution x_k. Our aim is to prove that the integer

$$\bar{x} = a_1 N_1 x_1 + a_2 N_2 x_2 + \cdots + a_r N_r x_r$$

is a simultaneous solution of the given system.

First, observe that $N_i \equiv 0 \pmod{n_k}$ for $i \neq k$, because $n_k \mid N_i$ in this case. The result is

$$\bar{x} = a_1 N_1 x_1 + \cdots + a_r N_r x_r \equiv a_k N_k x_k \pmod{n_k}$$

But the integer x_k was chosen to satisfy the congruence $N_k x \equiv 1 \pmod{n_k}$, which forces

$$\bar{x} \equiv a_k \cdot 1 \equiv a_k \pmod{n_k}$$

This shows that a solution to the given system of congruences exists.

As for the uniqueness assertion, suppose that x' is any other integer that satisfies these congruences. Then

$$\bar{x} \equiv a_k \equiv x' \pmod{n_k} \qquad k = 1, 2, \ldots, r$$

and so $n_k \mid \bar{x} - x'$ for each value of k. Because $\gcd(n_i, n_j) = 1$, Corollary 2 to Theorem 2.4 supplies us with the crucial point that $n_1 n_2 \cdots n_r \mid \bar{x} - x'$; hence $\bar{x} \equiv x' \pmod{n}$. With this, the Chinese Remainder Theorem is proven.

Example 4.9. The problem posed by Sun-Tsu corresponds to the system of three congruences

$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 2 \pmod 7$$

In the notation of Theorem 4.8, we have $n = 3 \cdot 5 \cdot 7 = 105$ and

$$N_1 = \frac{n}{3} = 35 \qquad N_2 = \frac{n}{5} = 21 \qquad N_3 = \frac{n}{7} = 15$$

Now the linear congruences

$$35x \equiv 1 \pmod 3 \qquad 21x \equiv 1 \pmod 5 \qquad 15x \equiv 1 \pmod 7$$

are satisfied by $x_1 = 2, x_2 = 1, x_3 = 1$, respectively. Thus, a solution of the system is given by

$$x = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233$$

Modulo 105, we get the unique solution $x = 233 \equiv 23 \pmod{105}$.

Example 4.10. For a second illustration, let us solve the linear congruence

$$17x \equiv 9 \pmod{276}$$

Because $276 = 3 \cdot 4 \cdot 23$, this is equivalent to finding a solution for the system of congruences

$$\begin{aligned} 17x &\equiv 9 \pmod 3 \quad \text{or} \quad x \equiv 0 \pmod 3 \\ 17x &\equiv 9 \pmod 4 \qquad\quad x \equiv 1 \pmod 4 \\ 17x &\equiv 9 \pmod{23} \qquad 17x \equiv 9 \pmod{23} \end{aligned}$$

Note that if $x \equiv 0 \pmod 3$, then $x = 3k$ for any integer k. We substitute into the second congruence of the system and obtain

$$3k \equiv 1 \pmod 4$$

Multiplication of both sides of this congruence by 3 gives us

$$k \equiv 9k \equiv 3 \pmod 4$$

so that $k = 3 + 4j$, where j is an integer. Then

$$x = 3(3 + 4j) = 9 + 12j$$

For x to satisfy the last congruence, we must have

$$17(9 + 12j) \equiv 9 \pmod{23}$$

or $204j \equiv -144 \pmod{23}$, which reduces to $3j \equiv 6 \pmod{23}$; in consequence, $j \equiv 2 \pmod{23}$. This yields $j = 2 + 23t$, with t an integer, whence

$$x = 9 + 12(2 + 23t) = 33 + 276t$$

All in all, $x \equiv 33 \pmod{276}$ provides a solution to the system of congruences and, in turn, a solution to $17x \equiv 9 \pmod{276}$.

We should say a few words about linear congruences in two variables; that is, congruences of the form

$$ax + by \equiv c \pmod{n}$$

In analogy with Theorem 4.7, such a congruence has a solution if and only if $\gcd(a, b, n)$ divides c. The condition for solvability holds if either $\gcd(a, n) = 1$ or $\gcd(b, n) = 1$. Say $\gcd(a, n) = 1$. When the congruence is expressed as

$$ax \equiv c - by \pmod{n}$$

the corollary to Theorem 4.7 guarantees a unique solution x for each of the n incongruent values of y. Take as a simple illustration $7x + 4y \equiv 5 \pmod{12}$, that would be treated as $7x \equiv 5 - 4y \pmod{12}$. Substitution of $y \equiv 5 \pmod{12}$ gives $7x \equiv -15 \pmod{12}$; but this is equivalent to $-5x \equiv -15 \pmod{12}$ so that $x \equiv 3 \pmod{12}$. It follows that $x \equiv 3 \pmod{12}$, $y \equiv 5 \pmod{12}$ is one of the 12 incongruent solutions of $7x + 4y \equiv 5 \pmod{12}$. Another solution having the same value of x is $x \equiv 3 \pmod{12}, y \equiv 8 \pmod{12}$.

The focus of our concern here is how to solve a system of two linear congruences in two variables with the same modulus. The proof of the coming theorem adopts the familiar procedure of eliminating one of the unknowns.

Theorem 4.9. The system of linear congruences

$$ax + by \equiv r \pmod{n}$$
$$cx + dy \equiv s \pmod{n}$$

has a unique solution modulo n whenever $\gcd(ad - bc, n) = 1$.

Proof. Let us multiply the first congruence of the system by d, the second congruence by b, and subtract the lower result from the upper. These calculations yield

$$(ad - bc)x \equiv dr - bs \pmod{n} \tag{1}$$

The assumption $\gcd(ad - bc, n) = 1$ ensures that the congruence

$$(ad - bc)z \equiv 1 \pmod{n}$$

posseses a unique solution; denote the solution by t. When congruence (1) is multiplied by t, we obtain

$$x \equiv t(dr - bs) \pmod{n}$$

A value for y is found by a similar elimination process. That is, multiply the first congruence of the system by c, the second one by a, and subtract to end up with

$$(ad - bc)y \equiv as - cr \pmod{n} \tag{2}$$

Multiplication of this congruence by t leads to

$$y \equiv t(as - cr) \pmod{n}$$

A solution of the system is now established.

We close this section with an example illustrating Theorem 4.9.

Example 4.11. Consider the system

$$7x + 3y \equiv 10 \pmod{16}$$
$$2x + 5y \equiv 9 \pmod{16}$$

Because $\gcd(7 \cdot 5 - 2 \cdot 3, 16) = \gcd(29, 16) = 1$, a solution exists. It is obtained by the method developed in the proof of Theorem 4.9. Multiplying the first congruence by 5, the second one by 3, and subtracting, we arrive at

$$29x \equiv 5 \cdot 10 - 3 \cdot 9 \equiv 23 \pmod{16}$$

or, what is the same thing, $13x \equiv 7 \pmod{16}$. Multiplication of this congruence by 5 (noting that $5 \cdot 13 \equiv 1 \pmod{16}$) produces $x \equiv 35 \equiv 3 \pmod{16}$. When the variable x is eliminated from the system of congruences in a like manner, it is found that

$$29y \equiv 7 \cdot 9 - 2 \cdot 10 \equiv 43 \pmod{16}$$

But then $13y \equiv 11 \pmod{16}$, which upon multiplication by 5, results in $y \equiv 55 \equiv 7 \pmod{16}$. The unique solution of our system turns out to be

$$x \equiv 3 \pmod{16} \qquad y \equiv 7 \pmod{16}$$

PROBLEMS 4.4

1. Solve the following linear congruences:
(a) $25x \equiv 15 \pmod{29}$.
(b) $5x \equiv 2 \pmod{26}$.
(c) $6x \equiv 15 \pmod{21}$.
(d) $36x \equiv 8 \pmod{102}$.
(e) $34x \equiv 60 \pmod{98}$.
(f) $140x \equiv 133 \pmod{301}$.
[*Hint:* $\gcd(140, 301) = 7$.]

2. Using congruences, solve the Diophantine equations below:
(a) $4x + 51y = 9$.
[*Hint:* $4x \equiv 9 \pmod{51}$ gives $x = 15 + 51t$, whereas $51y \equiv 9 \pmod{4}$ gives $y = 3 + 4s$. Find the relation between s and t.]
(b) $12x + 25y = 331$.
(c) $5x - 53y = 17$.

3. Find all solutions of the linear congruence $3x - 7y \equiv 11 \pmod{13}$.

4. Solve each of the following sets of simultaneous congruences:
(a) $x \equiv 1 \pmod{3}$, $x \equiv 2 \pmod{5}$, $x \equiv 3 \pmod{7}$.
(b) $x \equiv 5 \pmod{11}$, $x \equiv 14 \pmod{29}$, $x \equiv 15 \pmod{31}$.
(c) $x \equiv 5 \pmod{6}$, $x \equiv 4 \pmod{11}$, $x \equiv 3 \pmod{17}$.
(d) $2x \equiv 1 \pmod{5}$, $3x \equiv 9 \pmod{6}$, $4x \equiv 1 \pmod{7}$, $5x \equiv 9 \pmod{11}$.

5. Solve the linear congruence $17x \equiv 3 \pmod{2 \cdot 3 \cdot 5 \cdot 7}$ by solving the system

$$17x \equiv 3 \pmod{2} \qquad 17x \equiv 3 \pmod{3}$$
$$17x \equiv 3 \pmod{5} \qquad 17x \equiv 3 \pmod{7}$$

6. Find the smallest integer $a > 2$ such that

$$2 \mid a,\ 3 \mid a + 1,\ 4 \mid a + 2, 5 \mid a + 3, 6 \mid a + 4$$

7. (a) Obtain three consecutive integers, each having a square factor.
[*Hint:* Find an integer a such that $2^2 \mid a, 3^2 \mid a+1, 5^2 \mid a+2$.]
(b) Obtain three consecutive integers, the first of which is divisible by a square, the second by a cube, and the third by a fourth power.

8. (Brahmagupta, 7th century A.D.) When eggs in a basket are removed 2, 3, 4, 5, 6 at a time there remain, respectively, 1, 2, 3, 4, 5 eggs. When they are taken out 7 at a time, none are left over. Find the smallest number of eggs that could have been contained in the basket.

9. The basket-of-eggs problem is often phrased in the following form: One egg remains when the eggs are removed from the basket 2, 3, 4, 5, or 6 at a time; but, no eggs remain if they are removed 7 at a time. Find the smallest number of eggs that could have been in the basket.

10. (Ancient Chinese Problem.) A band of 17 pirates stole a sack of gold coins. When they tried to divide the fortune into equal portions, 3 coins remained. In the ensuing brawl over who should get the extra coins, one pirate was killed. The wealth was redistributed, but this time an equal division left 10 coins. Again an argument developed in which another pirate was killed. But now the total fortune was evenly distributed among the survivors. What was the least number of coins that could have been stolen?

11. Prove that the congruences

$$x \equiv a \pmod{n} \qquad \text{and} \qquad x \equiv b \pmod{m}$$

admit a simultaneous solution if and only if $\gcd(n, m) \mid a - b$; if a solution exists, confirm that it is unique modulo $\operatorname{lcm}(n, m)$.

12. Use Problem 11 to show that the following system does not possess a solution:

$$x \equiv 5 \pmod{6} \qquad \text{and} \qquad x \equiv 7 \pmod{15}$$

13. If $x \equiv a \pmod{n}$, prove that either $x \equiv a \pmod{2n}$ or $x \equiv a + n \pmod{2n}$.

14. A certain integer between 1 and 1200 leaves the remainders 1, 2, 6 when divided by 9, 11, 13, respectively. What is the integer?

15. (a) Find an integer having the remainders 1, 2, 5, 5 when divided by 2, 3, 6, 12, respectively. (Yih-hing, died 717).
(b) Find an integer having the remainders 2, 3, 4, 5 when divided by 3, 4, 5, 6, respectively. (Bhaskara, born 1114).
(c) Find an integer having the remainders 3, 11, 15 when divided by 10, 13, 17, respectively. (Regiomontanus, 1436–1476).

16. Let t_n denote the nth triangular number. For which values of n does t_n divide

$$t_1^2 + t_2^2 + \cdots + t_n^2$$

[*Hint:* Because $t_1^2 + t_2^2 + \cdots + t_n^2 = t_n(3n^3 + 12n^2 + 13n + 2)/30$, it suffices to determine those n satisfying $3n^3 + 12n^2 + 13n + 2 \equiv 0 \pmod{2 \cdot 3 \cdot 5}$.]

17. Find the solutions of the system of congruences:

$$3x + 4y \equiv 5 \pmod{13}$$
$$2x + 5y \equiv 7 \pmod{13}$$

18. Obtain the two incongruent solutions modulo 210 of the system

$$2x \equiv 3 \pmod{5}$$
$$4x \equiv 2 \pmod{6}$$
$$3x \equiv 2 \pmod{7}$$

19. Obtain the eight incongruent solutions of the linear congruence $3x + 4y \equiv 5 \pmod 8$.

20. Find the solutions of each of the following systems of congruences:

(a) $5x + 3y \equiv 1 \pmod 7$

$3x + 2y \equiv 4 \pmod 7$.

(b) $7x + 3y \equiv 6 \pmod{11}$

$4x + 2y \equiv 9 \pmod{11}$.

(c) $11x + 5y \equiv 7 \pmod{20}$

$6x + 3y \equiv 8 \pmod{20}$.