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 which 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. 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

$$3 \equiv 24 \pmod{7}, \quad -31 \equiv 11 \pmod{7}, \quad -15 \equiv -64 \pmod{7},$$

since $3 - 24 = (-3)7$, $-31 - 11 = (-6)7$, and $-15 - (-64) = 7 \cdot 7$. If $n \nmid (a - b)$, then we say that a is *incongruent to* b *modulo* n and in this case we write $a \not\equiv b \pmod{n}$. For example: $25 \not\equiv 12 \pmod{7}$, since 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, $a \equiv r \pmod{n}$. Since 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 positive 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

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

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 on.

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: $b = qn + r$, 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, this says that $a \equiv b \pmod{n}$.

Example 4-1

Since the integers -56 and -11 can be expressed in the form

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

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

$$-31 = (-5)7 + 4, \quad 11 = 1 \cdot 7 + 4.$$

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 which carry over to congruences appear in the next theorem.

THEOREM 4-2. *Let $n > 0$ be fixed and a, b, c, d be arbitrary integers. Then the following properties hold:*

(1) $a \equiv a \pmod{n}$.
(2) *If* $a \equiv b \pmod{n}$, *then* $b \equiv a \pmod{n}$.
(3) *If* $a \equiv b \pmod{n}$ *and* $b \equiv c \pmod{n}$, *then* $a \equiv c \pmod{n}$.
(4) *If* $a \equiv b \pmod{n}$ *and* $c \equiv d \pmod{n}$, *then* $a + c \equiv b + d \pmod{n}$ and $ac \equiv bd \pmod{n}$.
(5) *If* $a \equiv b \pmod{n}$, *then* $a + c \equiv b + c \pmod{n}$ *and* $ac \equiv bc \pmod{n}$.
(6) *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, since $-k$ is an integer, this yields (2).

Property (3) is slightly less obvious: Suppose that $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$. Then there exist integers h and k satisfying $a - b = hn$ and $b - c = kn$. It follows that

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

in consequence of which $a \equiv c \pmod{n}$.

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, one gets

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

or, as a congruence statement, $a + c \equiv b + d \pmod{n}$. As regards the second assertion of (4), note that

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

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

The proof of property (5) is covered by (4) and the fact that $c \equiv c \pmod{n}$. Finally, we obtain (6) by making an induction argument. The statement certainly holds for $k = 1$, and we will assume it is true for some fixed k. From (4), 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 $k + 1$, so the induction step is complete.

Before going further, we should illustrate the great help that congruences can be 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(6); 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 (2) and (5) 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 $k \geq 4$,

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