One finds in this way that

$$1! + 2! + 3! + 4! + \cdots + 100!$$
$$\equiv 1! + 2! + 3! + 0 + \cdots + 0 \equiv 9 \pmod{12}.$$

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

In the last theorem, it was seen that if $a \equiv b \pmod{n}$, then $ca \equiv cb \pmod{n}$ for any integer c. The converse, however, fails to hold. For an example perhaps as simple as any, note that $2 \cdot 4 \equiv 2 \cdot 1 \pmod{6}$, while $4 \not\equiv 1 \pmod{6}$. 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 cancelled, the net result is

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

Hence, $s \mid r(a - b)$ and $\gcd(r, s) = 1$. Euclid's Lemma implies that $s \mid a - b$, 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 the moment to record a special case of Corollary 1 which we shall have frequent occasion to use, namely, 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, $3 \cdot 11 \equiv 3 \cdot 5 \pmod{9}$. Since $\gcd(3, 9) = 3$, Theorem 4-3 leads to the conclusion that $11 \equiv 5 \pmod{3}$. A further illustration is furnished 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 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, were $c \equiv 0 \pmod{n}$, 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 $b \equiv 0 \pmod{n}$; for, Corollary 1 above 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 if $ab \equiv 0 \pmod{p}$, 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 sum

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

is divided by 4?

5. 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.]

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

7. 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.

8. 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, $a \equiv b \pmod{n_1 n_2}$.

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

10. Prove the statements below:

(a) If a is an odd integer, then $a^2 \equiv 1 \pmod{8}$.

(b) For any integer a, $a^3 \equiv 0, 1, \text{ or } 8 \pmod{9}$.

(c) For any integer a, $a^3 \equiv a \pmod{6}$.

(d) If an integer a is not divisible by 2 or 3, then $a^2 \equiv 1 \pmod{24}$.

(e) If an integer a is both a square and a cube, then $a \equiv 0, 1, 9, \text{ or } 28 \pmod{36}$.

11. Establish that if a is an odd integer, then

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

for any $n \geq 1$. [*Hint:* Proceed by induction on n.]

12. Use the theory of congruences to verify that

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

13. Prove that if $ab \equiv cd \pmod{n}$ and $b \equiv d \pmod{n}$, with $\gcd(b, n) = 1$, then $a \equiv c \pmod{n}$.

14. 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 SPECIAL DIVISIBILITY TESTS

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, ..., $b - 1$. 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

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

Since $N > q_1 > q_2 > \cdots \geq 0$ 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

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