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

(c) Show that the integers

$$1111,\ 111111,\ 11111111, \ldots,\ 111\cdots 11, \ldots$$

where an even number of digits are involved, are all composite.

11. 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

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

12. An old and somewhat illegible invoice shows that 72 canned hams were purchased for \$$x67.9y$. Find the missing digits.

4.4 LINEAR CONGRUENCES

This is a convenient place in our development 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 satisfying 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 $ax \equiv b \pmod{n}$ which 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 $3x \equiv 9 \pmod{12}$; since $3 \equiv -9 \pmod{12}$, 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 have already 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

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

for some choice of t.

Among the various integers satisfying the first of these formulas, consider those which 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, while 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 one would have

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

Now $\gcd(n/d, n) = n/d$ and so, by Theorem 4-3, the factor n/d could be cancelled 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

$$x_0,\ x_0 + n/d,\ x_0 + 2(n/d), \ldots, x_0 + (d-1)(n/d).$$

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.

We now pause to look at two concrete examples.

Example 4-6

Consider the linear congruence $18x \equiv 30 \pmod{42}$. Since $\gcd(18, 42) = 6$ 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 4-7

Let us solve the linear congruence $9x \equiv 21 \pmod{30}$. At the outset, since 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 $0, 1, 2, \ldots, 9$ 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 $0, 1, 2, \ldots, 29$. Taking $t = 0, 1, 2$, in the formula

$$x = 9 + 10t,$$

one gets 9, 19, 29, whence

$$x \equiv 9 \pmod{30}, \quad x \equiv 19 \pmod{30}, \quad x \equiv 29 \pmod{30}$$

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

A different approach to the problem would be to use the method that is suggested in the proof of Theorem 4-7. Since the congruence $9x \equiv 21 \pmod{30}$ is equivalent to the linear Diophantine equation

$$9x - 30y = 21,$$