21. Explain why the following curious calculations hold:

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

[Hint: Show that

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

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

23. If 792 divides the integer 13xy 45z, find the digits x, y, and z.

[Hint: By Problem 15, 8|45z.]

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

[Hint: By Problem 16(a), $10^p \equiv 1 \pmod{13}$.]

4.4 LINEAR CONGRUENCES

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

\[
x = x_0 + \frac{n}{d} t \quad y = y_0 + \frac{a}{d} t
\]

for some choice of \( t \).

Among the various integers satisfying the first of these formulas, consider those 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 \( t = qd + r \), where \( 0 \leq r \leq d - 1 \). Hence

\[
x_0 + \frac{n}{d} t = x_0 + \frac{n}{d} (qd + r)
\]

\[
= x_0 + nq + \frac{n}{d} r
\]

\[
\equiv x_0 + \frac{n}{d} r \pmod{n}
\]

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 \( n \).
We now pause to look at two concrete examples.

**Example 4.6.** 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:

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

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, 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, \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

$$x = 9 + 10t$$

we obtain 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 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 \( x = -21 + 10r \), where \( r = 0, 1, 2 \), are incongruent modulo 30 (but all are congruent modulo 10); thus, we end up with the incongruent solutions
\[
   x \equiv -21 \pmod{30} \quad x \equiv -11 \pmod{30} \quad x \equiv -1 \pmod{30}
\]
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 \( k \)th 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 \textit{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
\[
x \equiv a_1 \pmod{n_1}
\]
\[
x \equiv a_2 \pmod{n_2}
\]
\[
\vdots
\]
\[
x \equiv a_r \pmod{n_r}
\]
has a simultaneous solution, which is unique modulo the integer \( n_1n_2\cdots n_r \).

**Proof.** We start by forming the product \( n = n_1n_2\cdots n_r \). 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 \( \gcd(N_k, n_i) = 1 \). According to the theory of a single linear congruence, it is therefore possible to solve the congruence \( N_kx \equiv 1 \pmod{n_k} \); call the unique solution \( x_k \). Our aim is to prove that the integer

\[
\tilde{x} = a_1N_1x_1 + a_2N_2x_2 + \cdots + a_rN_rx_r
\]

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

\[
\tilde{x} = a_1N_1x_1 + \cdots + a_rN_rx_r \equiv a_kN_kx_k \pmod{n_k}
\]

But the integer \( x_k \) was chosen to satisfy the congruence \( N_kx \equiv 1 \pmod{n_k} \), which forces

\[
\tilde{x} \equiv a_k \cdot 1 \equiv a_k \pmod{n_k}
\]

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

\[
\tilde{x} \equiv a_k \equiv x' \pmod{n_k} \quad k = 1, 2, \ldots, r
\]

and so \( n_k \mid \tilde{x} - x' \) for each value of \( k \). Because \( \gcd(n_1, n_j) = 1 \), Corollary 2 to Theorem 2.4 supplies us with the crucial point that \( n_1n_2 \cdots n_r \mid \tilde{x} - x' \); hence \( \tilde{x} \equiv x' \pmod{n} \). With this, the Chinese Remainder Theorem is proven.

**Example 4.8.** The problem posed by Sun-Tsu corresponds to the system of three congruences

\[
\begin{align*}
x &\equiv 2 \pmod{3} \\
x &\equiv 3 \pmod{5} \\
x &\equiv 2 \pmod{7}
\end{align*}
\]

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

\[
N_1 = \frac{n}{3} = 35 \quad N_2 = \frac{n}{5} = 21 \quad N_3 = \frac{n}{7} = 15
\]

Now the linear congruences

\[
35x \equiv 1 \pmod{3} \quad 21x \equiv 1 \pmod{5} \quad 15x \equiv 1 \pmod{7}
\]

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 4.9.** 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{align*}
17x &\equiv 9 \pmod{3} \quad \text{or} \quad x \equiv 0 \pmod{3} \\
17x &\equiv 9 \pmod{4} \quad x \equiv 1 \pmod{4} \\
17x &\equiv 9 \pmod{23} \quad 17x \equiv 9 \pmod{23}
\end{align*}

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.