we begin by expressing $3 = \gcd(9, 30)$ as a linear combination of 9 and 30. It is found, either by inspection or by 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

$$x = -21 + \tfrac{30}{3}t = -21 + 10t.$$

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

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

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

$$a_1 x \equiv b_1 \pmod{m_1}, a_2 x \equiv b_2 \pmod{m_2}, \ldots, a_r x \equiv b_r \pmod{m_r}$$

of simultaneous linear congruences. 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 cancelled 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 $i \neq j$; also, $\gcd(a'_i, n_i) = 1$. 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 first century A.D. Sun-Tsu asked: Find a number which 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 $n_1 n_2 \cdots n_r$.

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

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

in other 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, it is to be observed that $N_i \equiv 0 \pmod{n_k}$ for $i \neq k$, since $n_k \mid N_i$ in this case. The result is that

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

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 which 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 2-5 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 4-8

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

$$N_1 = n/3 = 35, \quad N_2 = n/5 = 21, \quad N_3 = n/7 = 15.$$

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

$$\bar{x} = 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 = 233.$$

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

Example 4-9

For a second illustration, let us solve the linear congruence

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

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

$$\begin{array}{lcl} 17x \equiv 9 \pmod 3 & \text{or} & x \equiv 0 \pmod 3 \\ 17x \equiv 9 \pmod 4 & & x \equiv 1 \pmod 4 \\ 17x \equiv 9 \pmod{23} & & 17x \equiv 9 \pmod{23} \end{array}$$

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 $3j \equiv 6 \pmod{23}$; that is, $j \equiv 2 \pmod{23}$. This yields $j = 2 + 23t$, 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 $17x \equiv 9 \pmod{276}$.

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 $x = 15 + 51t$, while $51y \equiv 9 \pmod{4}$ 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

$$17x \equiv 3 \pmod{2}, \quad 17x \equiv 3 \pmod{3}, \quad 17x \equiv 3 \pmod{5}, \quad 17x \equiv 3 \pmod{7}.$$

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

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

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 system

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

does not possess a solution.

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, 1436–1473.)