G THE CHINESE REMAINDER THEOREM

The Chinese mathematician **Sun-Tsu** posed the following problem:

> When divided by 3, a number leaves a remainder of 1. When divided by 5 it leaves a remainder of 2, and when divided by 7 it leaves a remainder of 3. Find the number.

In congruence notation, we need to find x such that $x \equiv 1 \pmod 3$, $x \equiv 2 \pmod 5$, and $x \equiv 3 \pmod 7$.

The general method of solution of such simultaneous linear congruences in different moduli is termed the **Chinese Remainder Theorem**, named in honour of this problem and its Chinese heritage. To be fair, however, similar puzzles are also found in old manuscripts on the Indian subcontinent and in Greek manuscripts of the same era.

THE CHINESE REMAINDER THEOREM

If $m_1, m_2, m_3, ..., m_r$ are pairwise relatively prime positive integers, then the system of congruences

$x \equiv a_1 \pmod{m_1}$, $x \equiv a_2 \pmod{m_2}$, $x \equiv a_3 \pmod{m_3}$, ..., $x \equiv a_r \pmod{m_r}$

has a unique solution modulo $M = m_1 m_2 m_3 .... m_r$.

This solution is $x \equiv a_1 M_1 x_1 + a_2 M_2 x_2 + ... + a_r M_r x_r \pmod M$

where $M_k = \dfrac{M}{m_k}$ and x_i is the solution of $M_i x_i \equiv 1 \pmod{m_i}$.

Proof:

Existence: Let $M_k = \dfrac{M}{m_k} = m_1 m_2 m_3 .... m_{k-1} m_{k+1} .... m_r$.

Since $\gcd(M_k, m_k) = 1$, by our theory of linear congruences it is possible to solve all r linear congruences, $M_i x_i \equiv 1 \pmod{m_i}$, $i = 1, ..., r$.

The unique solution of $M_k x_k \equiv 1 \pmod{m_k}$ is denoted x_k.

Observe that $M_i \equiv 0 \pmod{m_k}$ for $i \neq k$ since $m_k \mid M_i$ in these cases.

Hence $a_1 M_1 x_1 + a_2 M_2 x_2 + ... + a_r M_r x_r \equiv a_k M_k x_k \pmod{m_k}$

$\equiv a_k(1) \pmod{m_k}$

$\equiv a_k \pmod{m_k}$

$\therefore$ $X \equiv a_1 M_1 x_1 + a_2 M_2 x_2 + ... + a_r M_r x_r$ is a solution of $x \equiv a_k \pmod{m_k}$ for $k = 1, 2, 3, ..., r$

$\therefore$ a solution exists.

Uniqueness: Suppose X' is any other integer which satisfies the system

$\therefore$ $X = a_1 M_1 x_1 + a_2 M_2 x_2 + ... + a_r M_r x_r \equiv a_k \equiv X' \pmod{m_k}$ for all $k = 1, 2, 3, 4, ..., r$

$\therefore$ $m_k \mid (X - X')$

Since the moduli are relatively prime,

$m_1 \mid (X - X')$, $m_2 \mid (X - X')$, ..., $m_r \mid (X - X')$

$\therefore$ $m_1 m_2 m_3 .... m_k \mid (X - X')$

$\therefore$ $M \mid (X - X')$

$\therefore$ $X \equiv X' \pmod M$

Example 38

Solve Sun-Tsu's problem:
$x \equiv 1 \pmod 3$, $x \equiv 2 \pmod 5$, $x \equiv 3 \pmod 7$

3, 5, and 7 are pairwise relatively prime ✓

$M = 3 \times 5 \times 7 = 105$

$\therefore \quad M_1 = \frac{105}{3} = 35, \quad M_2 = 21, \quad \text{and} \quad M_3 = 15$

To find x_1 we solve $35x_1 \equiv 1 \pmod 3 \quad \Rightarrow \quad x_1 = 2$
To find x_2 we solve $21x_2 \equiv 1 \pmod 5 \quad \Rightarrow \quad x_2 = 1$
To find x_3 we solve $15x_3 \equiv 1 \pmod 7 \quad \Rightarrow \quad x_3 = 1$

Hence, $x \equiv (1)(35)(2) + (2)(21)(1) + (3)(15)(1) \pmod{105}$
$\therefore \quad x \equiv 157 \pmod{105}$
$\therefore \quad x \equiv 52 \pmod{105}$

Check: $52 \equiv 1 \pmod 3$ ✓ $52 \equiv 2 \pmod 5$ ✓ $52 \equiv 3 \pmod 7$ ✓

So, there are infinitely many solutions, the smallest of which is $x = 52$. The other solutions are $x = 157$, $x = 209$, $x = 261$, and so on.

Example 39

Solve Sun-Tsu's problem *without* using the Chinese Remainder Theorem.

The first congruence is $x \equiv 1 \pmod 3 \qquad \therefore \quad x = 1 + 3t, \ t \in \mathbb{Z}$

Substituting into the 2nd congruence $x \equiv 2 \pmod 5$, we get

$$1 + 3t \equiv 2 \pmod 5$$
$$\therefore \quad 3t \equiv 1 \pmod 5$$
$$\therefore \quad t \equiv 2 \pmod 5$$
$$\therefore \quad t \equiv 2 + 5u, \ u \in \mathbb{Z}$$

Substituting into the 3rd congruence $x \equiv 3 \pmod 7$, we get

$$1 + 3(2 + 5u) \equiv 3 \pmod 7$$
$$\therefore \quad 7 + 15u \equiv 3 \pmod 7$$
$$\therefore \quad 15u \equiv -4 \pmod 7$$
$$\therefore \quad 15u \equiv 3 \pmod 7$$
$$\therefore \quad u \equiv 3 \pmod 7$$
$$\therefore \quad u \equiv 3 + 7v$$

$\therefore \quad x = 1 + 3t = 1 + 3(2 + 5u) = 7 + 15u = 7 + 15(3 + 7v) = 52 + 105v$

$\therefore \quad x \equiv 52 \pmod{105}$

Some congruence equations can be solved by converting to two or more simpler equations. The following example illustrates this procedure.

Example 35

Solve $13x \equiv 5 \pmod{276}$.

We notice that $276 = 3 \times 4 \times 23$ where 3, 4, and 23 are relatively prime.

$\therefore$ an equivalent problem is to find the simultaneous solution of

$13x \equiv 5 \pmod 3$, $13x \equiv 5 \pmod 4$ and $13x \equiv 5 \pmod{23}$

$\therefore\ x \equiv 2 \pmod 3$, $x \equiv 1 \pmod 4$ and $x \equiv 11 \pmod{23}$.

Using the Chinese Remainder Theorem, $M = 3 \times 4 \times 23 = 276$

$\therefore\ M_1 = 92$, $M_2 = 69$, and $M_3 = 12$

To find x_1 we solve $92x_1 \equiv 1 \pmod 3 \quad \Rightarrow \quad x_1 = 2$

To find x_2 we solve $69x_2 \equiv 1 \pmod 4 \quad \Rightarrow \quad x_2 = 1$

To find x_3 we solve $12x_3 \equiv 1 \pmod{23} \quad \Rightarrow \quad x_3 = 2$

Hence, $x = (2)(92)(2) + (1)(69)(1) + (11)(12)(2) \equiv 701 \pmod{276}$

$\equiv 149 \pmod{276}$

EXERCISE 1G

1 Solve these systems using the Chinese Remainder Theorem:

a $x \equiv 4 \pmod{11}$, $x \equiv 3 \pmod 7$

b $x \equiv 1 \pmod 5$, $x \equiv 2 \pmod 6$, $x \equiv 3 \pmod 7$

2 When divided by 3, a positive number leaves a remainder of 2. When divided by 5 it leaves a remainder of 3, and when divided by 7 it leaves a remainder of 2. Use the Chinese Remainder Theorem to find the number.

3 Solve these systems using the Chinese Remainder Theorem:

a $x \equiv 1 \pmod 2$, $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$

b $x \equiv 0 \pmod 2$, $x \equiv 0 \pmod 3$, $x \equiv 1 \pmod 5$, $x \equiv 6 \pmod 7$

4 Solve these systems *without* using the Chinese Remainder Theorem:

a $x \equiv 4 \pmod{11}$, $x \equiv 3 \pmod 7$

b $x \equiv 1 \pmod 5$, $x \equiv 2 \pmod 6$, $x \equiv 3 \pmod 7$

c $x \equiv 0 \pmod 2$, $x \equiv 0 \pmod 3$, $x \equiv 1 \pmod 5$, $x \equiv 6 \pmod 7$

5 Solve $17x \equiv 3 \pmod{210}$ by converting into simpler congruence equations and using the Chinese Remainder Theorem.

6 Which integers leave a remainder of 2 when divided by 3, and leave a remainder of 2 when divided by 4?

7 Find an integer that leaves a remainder of 2 when divided by either 5 or 7, but is divisible by 3.

8 Find an integer that leaves a remainder of 1 when divided by 3, and a remainder of 3 when divided by 5, but is divisible by 4.

9 Colin has a bag of sweets. If the sweets were removed from the bag 2, 3, 4, 5, or 6 at a time, the respective remainders would be 1, 2, 3, 4, and 5. However, if they were taken out 7 at a time, no sweets would be left in the bag. Find the smallest number of sweets that may be in the bag.

10 Seventeen robbers stole a bag of gold coins. They divided the coins into equal groups of 17, but 3 were left over. A fight began over the remaining coins and one of the robbers was killed. The coins were then redistributed, but this time 10 were left over. Another fight broke out and another of the robbers was killed in the conflict. Luckily, another equal redistribution of the coins was exact. What is the least number of coins that may have been stolen by the robbers?

11 a Solve the linear Diophantine equation $4x + 7y = 5$ by showing that the congruences $4x \equiv 5 \pmod 7$ and $7y \equiv 5 \pmod 4$ are equivalent to $x = 3 + 7t$ and $y = 3 + 4s$ and finding the relationship between t and s.

b Use a similar method to solve: i $11x + 8y = 31$ ii $7x + 5y = 13$

12 Find the smallest integer $a > 2$ such that $2 \mid a$, $3 \mid (a+1)$, $4 \mid (a+2)$, $5 \mid (a+3)$, and $6 \mid (a+4)$.

13 Solve the system: $2x \equiv 1 \pmod 5$, $3x \equiv 9 \pmod 6$, $4x \equiv 1 \pmod 7$, $5x \equiv 9 \pmod{11}$.