3.4 The Chinese Remainder Theorem

In many situations, it is useful to break a congruence mod n into a system of congruences mod factors of n. Consider the following example. Suppose we know that a number x satisfies $x \equiv 25 \pmod{42}$. This means that we can write $x = 25 + 42k$ for some integer k. Rewriting 42 as $7 \cdot 6$, we obtain $x = 25 + 7(6k)$, which implies that $x \equiv 25 \equiv 4 \pmod 7$. Similarly, since $x = 25 + 6(7k)$, we have $x \equiv 25 \equiv 1 \pmod 6$. Therefore,

$$x \equiv 25 \pmod{42} \Rightarrow \begin{cases} x \equiv 4 \pmod 7 \\ x \equiv 1 \pmod 6. \end{cases}$$

The Chinese remainder theorem shows that this process can be reversed; namely, a system of congruences can be replaced by a single congruence under certain conditions.

Chinese Remainder Theorem. *Suppose* $\gcd(m, n) = 1$. *Given a and b, there exists exactly one solution x* $\pmod{mn}$ *to the simultaneous congruences*

$$x \equiv a \pmod m, \qquad x \equiv b \pmod n.$$

Proof. There exist integers s, t such that $ms+nt = 1$. Then $ms \equiv 1 \pmod n$ and $nt \equiv 1 \pmod m$. Let $x = bms + ant$. Then $x \equiv ant \equiv a \pmod m$, and $x \equiv bms \equiv b \pmod n$, as desired. Suppose x_1 is another solution. Then $x \equiv x_1 \pmod m$ and $x \equiv x_1 \pmod n$, so $x - x_1$ is a multiple of both m and n.

Lemma. *Let m, n be integers with* $\gcd(m, n) = 1$. *If an integer c is a multiple of both m and n, then c is a multiple of mn.*

Proof. Let $c = mk = n\ell$. Write $ms + nt = 1$ with integers s, t. Multiply by c to obtain $c = cms + cnt = mn\ell s + mnkt = mn(\ell s + kt)$. □

To finish the proof of the theorem, let $c = x - x_1$ in the lemma to find that $x - x_1$ is a multiple of mn. Therefore, $x \equiv x_1 \pmod{mn}$. This means that any two solutions x to the system of congruences are congruent mod mn, as claimed. □

Example. Solve $x \equiv 3 \pmod 7$, $\quad x \equiv 5 \pmod{15}$.
Solution: $x \equiv 80 \pmod{105}$ (note: $105 = 7 \cdot 15$). Since $80 \equiv 3 \pmod 7$ and $80 \equiv 5 \pmod{15}$, 80 is a solution. The theorem guarantees that such a solution exists, and says that it is uniquely determined mod the product mn, which is 105 in the present example. ∎