The Chinese Remainder Theorem

Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime positive integers greater than 1 and $a_1, a_2, \ldots, a_n$ arbitrary integers. Then the system of linear congruences

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

has a unique solution $m = m_1 m_2 \ldots m_n$. (That is, there is a solution x with $0 \leq x \leq m$, and all other solutions are congruent $\pmod{m}$ to this solution.)

Proof: Let $M_x = \frac{m}{m_k}$ for $k = 1, 2, \ldots, n$. Thus, M_k is the product of all moduli except m_k. Since m_i and m_k are relatively prime if $i \neq k$, it follows that gcd $(m_k, M_k) = 1$. Therefore, there exist integers r_k and s_k such that $m_k r_k + M_K s_k = 1$. By Bezout's Theorem,

$$m_k r_k + M_k s_k \equiv 1 \pmod{m_k}$$

But $m_k r_k \equiv \pmod{m_k}$. Therefore

$$M_k s_k \equiv 1 \pmod{m_k}$$

We call s_k an inverse of $M_k \pmod{m_k}$ since their product is 1. So, we know that for $j = 1, 2, \ldots, n$, there exists integers $s_1, s_2, \ldots, s_n$ such that $M_j s_j \equiv 1 \pmod{m_j}$. Now we form the theorem:

$$x = a_1 M_1 s_1 + a_2 M_2 s_2 + \cdots + a_n M_n s_n$$

and we will show that x is a solution to all n linear congruences. Since $M_j \equiv 0 \pmod{m_k}$ for $j \neq k$, all terms except the k^{th} in the sum are $\equiv 0 \pmod{m_k}$. Because $M_k s_k \equiv 1 \pmod{m_k}$ we see that

$$x \equiv a_k M_k s_k \equiv a_k \pmod{m_k} \text{ for } k = 1, 2, \ldots, n$$

Thus, x is a solution to all n linear congruences.

Example 1: The Chinese mathematician Sun-Tsu, in the 1st century AD asked: when a number is divided by 3, the remainder is 2; when dividing by 5, the remainder is 3; and when dividing by 7, the remainder is 2. What is the number?
So, we have the following system of linear congruences:

$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 2 \pmod 7$$

Let $m = 3 \times 5 \times 7 = 105$,

$$M_1 = \frac{m}{3} = \frac{105}{3} = 35$$

$$M_2 = \frac{m}{5} = \frac{105}{5} = 21$$

$$M_3 = \frac{m}{7} = 15$$

By inspection, 2 is an inverse of $M_1 = 35 \pmod 3$ since $2 \times 35 = 70 \equiv 1 \pmod 3$; 1 is an inverse of $M_2 = 21 \pmod 5$ since $1 \equiv 21 \pmod 5 \rightarrow 1 \times 21 \equiv 1 \pmod 5$; $M_3 = 15 \rightarrow 15 \times s_3 \equiv 1 \pmod 7 \rightarrow s_3 = 1$ also since $15 \times 1 = 15 \equiv 1 \pmod 7$.

$$x = a_1 M_1 s_1 + a_2 M_2 s_2 + a_3 M_3 s_3$$

$$x = (2 \times 35 \times 2) + (3 \times 21 \times 1) + (2 \times 15 \times 1) = 233 \equiv 23 \pmod{105}$$

$$23 \equiv 2 \pmod 3 \text{ because } 23 - 2 = 21 \equiv 0 \pmod 3$$
$$23 \equiv 3 \pmod 5 \text{ because } 23 - 3 = 20 \equiv 0 \pmod 5$$
$$23 \equiv 2 \pmod 7 \text{ because } 23 - 2 = 21 \equiv 0 \pmod 7$$

Example 2: Solve the system:

$$x \equiv 1 \pmod 2$$
$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 4 \pmod{11}$$

$$m = 2 \times 3 \times 5 \times 11 = 330$$
$$M_1 = \frac{330}{2} = 165$$
$$M_2 = \frac{330}{3} = 110$$
$$M_3 = \frac{330}{5} = 66$$
$$M_4 = \frac{330}{11} = 33$$

$165s_1 \equiv 1 \pmod 2 \rightarrow s_1 = 1$ since $165 - 1 \equiv 0 \pmod 2$

$110s_2 \equiv 1 \pmod 3 \rightarrow s_2 = 2$ since $220 - 1 = 119$ and $3 \times 73 = 219$

$66s_3 \equiv 1 \pmod 5 \rightarrow s_3 = 1$ since $66 - 1 = 65$ and $5 \times 13 = 65$

$30s_4 \equiv 1 \pmod{11} \rightarrow s_4 = -4$ since $-120 - 1 = -121 \equiv 0 \pmod{11}$

Therefore:

$$x = (1 \times 165 \times 1) + (2 \times 110 \times 2) + (3 \times 66 \times 1) + (4 \times 30 \times -4)$$

$$x = 323$$

$$x \equiv -7 \pmod{330} \equiv 323$$

$$323 \equiv 1 \pmod 2$$
$$323 \equiv 2 \pmod 3$$
$$323 \equiv 3 \pmod 5$$
$$323 \equiv 4 \pmod{11}$$

Fermat's Little Theorem

Let p be a prime such that $p \mid a$, $a \in \mathbb{Z}$. Then

$$a \equiv 1 \pmod{p}$$

Furthermore, there exists $a \in \mathbb{Z}$ such that

$$a^p \equiv a \pmod{p}$$

Proof: Consider $\{a, 2a, 3a, \ldots, (p-1)a\}$. Since p is a prime, only 1 and p divide p and so $\{1, 2, 3, \ldots, p-1\}$ are all relatively prime to p. Can $ai \equiv aj \pmod{p}$? That would require

$$ai - aj \equiv 0 \pmod{p} \rightarrow a(i-j) \equiv 0 \pmod{p}$$

Now, $p \nmid a$ by hypothesis and $1 \leq i - j \leq p - 2$ so that $p \nmid i - j$. Therefore, $\{a, 2a, 3a, \ldots, (p-1)a\}$ consists of $p-1$ integers all relatively prime to each other and therefore each one belongs to a unique congruence class $\pmod{p}$, namely $\{1, 2, 3, \ldots, p-1\}$. Therefore

$$a(2a)(3a)\ldots((p-1)a) \equiv (p-1)! \pmod{p}$$

$$a^{p-1}(p-1)! \equiv (p-1)! \pmod{p}$$

$$a^{p-1} \equiv 1 \pmod{p}$$

$$a \cdot a^{p-1} \equiv a \cdot 1 = a \pmod{p} \text{ if } p \nmid a$$

$$a^p \equiv a \pmod{p} \text{ if } p \nmid a$$

What if $p \mid a$? Then $a^p \equiv 0 \equiv a \pmod{p}$. Hence

$$a^p \equiv a \pmod{p}$$

whether or not $p \mid a$.