14 The Chinese Remainder Theorem

The Chinese Remainder Theorem is a structure theorem for the ring $\mathbb{Z}_n$. It is arguably the most important theorem in all of number theory!

The Chinese Remainder Theorem - CRT

Theorem 14.1. *Let $m_1, m_2, \ldots, m_n$ be pairwise relatively prime integers greater than 1, and let $a_1, a_2, \ldots, a_n$ be any integers. Then there is a solution x to the following system of simultaneous congruences:*

$$\begin{aligned} x &\equiv a_1 \pmod{n_1}, \\ x &\equiv a_2 \pmod{n_2}, \\ &\vdots \\ x &\equiv a_n \pmod{n_n}. \end{aligned}$$

Furthermore, if x and x' are two solutions to the system, then

$$x \equiv x' \pmod{M},$$

where $M = n_1 n_2 \ldots n_n$ is the product of the modulo.

The **Chinese Remainder Theorem** states that if we have a system of congruences:

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_k \pmod{n_k} \end{aligned}$$

where $n_1, n_2, \ldots, n_k$ are pairwise coprime, then there exists a unique solution modulo M,

Steps to Solve Using CRT

1. Compute $M = n_1 \times n_2 \times \cdots \times n_k$.

2. Compute $m_i = \frac{M}{n_i}$ for each i.

3. Find the modular x_i such that:

$$x_i \equiv m_i^{-1} \pmod{n_i}$$

4. Compute:

$$x = \sum_{i=1}^{k} x_i \cdot m_i \cdot a_i \pmod{M}$$

If $i = 2$, Then

$$x = x_1 m_1 a_1 + x_2 m_2 a_2 \pmod{M}$$

where

$x_1 \equiv m_1^{-1} \pmod{n_1}$, $m_1 = \frac{M}{n_1}$, $x_2 \equiv m_2^{-1} \pmod{n_2}$, $m_2 = \frac{M}{n_2}$, and $M = n_1 n_2$

Example 14.1. Solve the system:

$$x \equiv 2 \pmod{3}$$

$$x \equiv 3 \pmod{4}$$

Step 1: Compute M

$$M = 3 \times 4 = 12$$

Step 2: Compute $m_i = \frac{M}{n_i}$

$$m_1 = \frac{12}{3} = 4, \quad m_2 = \frac{12}{4} = 3$$

Step 3: Compute the Modular Inverses

Find x_i such that $x_i \equiv m_i^{-1} \pmod{n_i}$:

$$x_1 \equiv 4^{-1} \pmod 3 \quad \Rightarrow \quad x_1 = 1$$

$$x_2 \equiv 3^{-1} \pmod 4 \quad \Rightarrow \quad x_2 = 3$$

Step 4: Compute x

$$x = x_1 m_1 a_1 + x_2 m_2 a_2 \pmod M$$

$$x = (1 \times 4 \times 2) + (3 \times 3 \times 3) \pmod{12}$$

$$x = (8) + (27) \pmod{12}$$

$$x = 35 \pmod{12}$$

$$x \equiv 11 \pmod{12}$$

Thus, the solution is:

$$x \equiv 11 \pmod{12}$$

Example 14.2. Solve the system:

$$x \equiv 2 \pmod 3$$

$$x \equiv 3 \pmod 4$$

$$x \equiv 1 \pmod 5$$

Step 1: Compute M

$$M = 3 \times 4 \times 5 = 60$$

Step 2: Compute $m_i = \frac{M}{n_i}$

$$m_1 = \frac{60}{3} = 20, \quad m_2 = \frac{60}{4} = 15, \quad M_3 = \frac{60}{5} = 12$$

Step 3: Compute the Modular Inverses

Find x_i such that $x_i \equiv m_i^{-1} \pmod{n_i}$:

$$x_1 \equiv 20^{-1} \pmod 3 \quad \Rightarrow \quad x_1 = 2$$

$$x_2 \equiv 15^{-1} \pmod 4 \quad \Rightarrow \quad x_2 = 3$$

$$x_3 \equiv 12^{-1} \pmod 5 \quad \Rightarrow \quad x_3 = 3$$

Step 4: Compute x

$$x = (2 \times 20 \times 2) + (3 \times 15 \times 3) + (1 \times 12 \times 3) \pmod{60}$$

$$x = (80) + (135) + (36) \pmod{60}$$

$$x = 251 \pmod{60}$$

$$x \equiv 11 \pmod{60}$$

Thus, the solution is:

$$x \equiv 11 \pmod{60}$$

Exercises

1. Find x satisfying:

$$x \equiv 3 \pmod{5}$$

$$x \equiv 4 \pmod{7}$$

2. Find x satisfying:

$$x \equiv 2 \pmod{3}$$

$$x \equiv 3 \pmod{4}$$

$$x \equiv 1 \pmod{5}$$

3. Find x satisfying:

$$x \equiv 1 \pmod{6}$$

$$x \equiv 3 \pmod{7}$$

4. Find x satisfying:

$$x \equiv 2 \pmod{4}$$

$$x \equiv 3 \pmod{5}$$

$$x \equiv 4 \pmod{6}$$

5. Solve the following system:

$$x \equiv 5 \pmod{9}$$

$$x \equiv 7 \pmod{11}$$

$$x \equiv 3 \pmod{13}$$

$$x \equiv 1 \pmod{17}$$