CHINESE REMAINDER THEOREM

Let $n_1, n_2, \ldots, n_r$ be relatively prime positive integers. Let $a_1, a_2, \ldots, a_r$ be integers. The Chinese remainder theorem is a method to find an integer $x \pmod{n_1 n_2 \cdots n_r}$ such that

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_r \pmod{n_r}. \end{aligned}$$

Method to find x: Let $N := n_1 n_2 \cdots n_r$. A solution is always given by

$$x \equiv a_1 w_1 + a_2 w_2 + \cdots + a_r w_r \pmod{N}$$

as long as

$$w_i \equiv \begin{cases} 1 \pmod{n_j} & \text{if } i = j, \\ 0 \pmod{n_j} & \text{if } i \neq j, \end{cases}$$

for all $1 \leq i, j \leq r$. We may choose $\boxed{w_i = \frac{N}{n_i}\left(\left(\frac{N}{n_i}\right)^{-1} \pmod{n_i}\right).}$

Example: Solve for x:

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

Solution We want to find w_1, w_2, w_3 such that $x = 2w_1 + 3w_2 + 5w_3$ and where

$$\begin{array}{lll} w_1 \equiv 1 \pmod{3}, & w_1 \equiv 0 \pmod{5}, & w_1 \equiv 0 \pmod{7}, \\ w_2 \equiv 0 \pmod{3}, & w_2 \equiv 1 \pmod{5}, & w_2 \equiv 0 \pmod{7}, \\ w_3 \equiv 0 \pmod{3}, & w_3 \equiv 0 \pmod{5}, & w_3 \equiv 1 \pmod{7}. \end{array}$$

We may choose

$$\begin{aligned} w_1 &= 5 \cdot 7 \cdot \left(35^{-1} \pmod{3}\right) = 70, \\ w_2 &= 3 \cdot 7 \cdot \left(21^{-1} \pmod{5}\right) = 21, \\ w_3 &= 3 \cdot 5 \cdot \left(15^{-1} \pmod{7}\right) = 15. \end{aligned}$$

We obtain:

$$x = 2{\cdot}70 + 3{\cdot}21 + 5{\cdot}15 = 140 + 63 + 75 \equiv 278 \pmod{3{\cdot}5{\cdot}7} \equiv 278 \pmod{105} = 68.$$

So $\boxed{\boxed{x = 68}}$ is the solution.