Chinese Remainder Theorem:

Let $n_1, n_2, \cdots, n_r$ be positive integers such that $\gcd(n_i, n_j) = 1$ for $i \neq j$. Then the system of linear congruences

$$x \equiv a_1 \pmod{n_1}$$
$$x \equiv a_2 \pmod{n_2}$$
$$\vdots$$
$$x \equiv a_r \pmod{n_r}$$

$\boxed{x \equiv a_k \bmod n_k}$

has a simultaneous solution which is unique modulo the integer $n_1 n_2 \cdots n_r$.

Proof: Form the product $n = n_1 n_2 \cdots n_r$.

Consider $N_k = \dfrac{n}{n_k} = \dfrac{n_1 n_2 \cdots n_r}{n_k}$, $k = 1, 2, \cdots, r$

$$\therefore N_k = n_1 n_2 \cdots n_{k-1} n_{k+1} \cdots n_r$$

now, since n_i's are relatively prime in pairs

i.e $\gcd(n_i, n_j) = 1$

$\Rightarrow \gcd(n_k, n_j) = 1 \quad k \neq j, \; j = 1, 2, \cdots r$

$\Rightarrow \gcd(n_k, n_1 n_2 \cdots n_{k-1} n_{k+1} \cdots n_r) = 1$

$\Rightarrow \gcd(n_k, N_k) = 1$ but n_k / N_i, $k \neq i$

$\therefore$ according to the theory of single linear congruence, $N_k x \equiv 1 \bmod n_k$ has unique sol^n.

say $x = x_k$

our aim: To prove that

$x^* = a_1 N_1 x_1 + a_2 N_2 x_2 + \cdots + a_r N_r x_r$ is a simultaneous solution of the given system.

First, observe that $N_i \equiv 0 \bmod n_k \; (i \neq k)$ because n_k / N_i in this case $\therefore x^* = a_1 N_1 x_1 + a_2 N_2 x_2 + \cdots + a_r N_r x_r$

$x^* \equiv a_k N_k x_k \pmod{n_k}$,

but x_k to satisfy $N_k x_k \equiv 1 \bmod n_k \Rightarrow x^* \equiv a_k \bmod n_k$ which is sol^n of (*) $\forall k = 1, 2, \cdots r$

$\therefore$ simultaneous sol^n x^* of (*) exist.

System of congruences

$$(*)\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases} \qquad \begin{matrix} x \equiv a_1 \bmod n_1 \\ x \equiv a_2 \bmod n_2 \\ x \equiv a_3 \bmod n_3 \end{matrix}$$

Since $n = n_1 n_2 n_3 = (3)(5)(7) = 105$

$N_K = \frac{n}{n_K}$

$N_1 = \frac{n}{n_1} = \frac{105}{3} = 35$

$N_2 = \frac{n}{n_2} = \frac{105}{5} = 21$

$N_3 = \frac{n}{n_3} = \frac{105}{7} = 15$

now the linear congruences

$N_K x_K \equiv 1 \pmod{n_K}$ call the unique solution x_K

$\therefore$ $N_1 x_1 \equiv 1 \bmod n_1 \Rightarrow 35 x_1 \equiv 1 \bmod 3 \Rightarrow x_1 = 2$

$N_2 x_2 \equiv 1 \bmod n_2 \Rightarrow 21 x_2 \equiv 1 \bmod 5 \Rightarrow x_2 = 1$

$N_3 x_3 \equiv 1 \bmod n_3 \Rightarrow 15 x_3 \equiv 1 \bmod 7 \Rightarrow x_3 = 1$

hence solution of the system is given by

$x = a_1 N_1 x_1 + a_2 N_2 x_2 + \cdots + a_r N_r x_r \bmod n$

$\therefore x = a_1 N_1 x_1 + a_2 N_2 x_2 + a_3 N_3 x_3 \bmod n$

$x = (2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1) \bmod 105$

$x = (140 + 63 + 30) \bmod 105$

$x = 233 \bmod 105$

$x = 23 \bmod 105$

$\therefore$ we get the unique solution $x = 23 \bmod 105$ of the system $(*)$.

Remember Steps to solve Chinese Remainder Theorem

(i) write $n = n_1 n_2 n_3 \cdots n_r, a_1, a_2, a_3 \cdots a_r$

(ii) find $N_K = \frac{n}{n_K}$, $K = 1, 2, \cdots r$

(iii) find unique soln x_K s.t $N_K x_K \equiv 1 \bmod n_K$, $K = 1, 2, \cdots r$

(iv) soln of $(*)$ is $x = \sum_{K=1}^{r} x_K a_K N_K \pmod n$

Uniqueness:- suppose x' is any other integer that satisfies these congruences, then

$x^* \equiv a_k \bmod n_k$ and $x' \equiv a_k \bmod n_k \; \forall k = 1, 2, \ldots r$

so $n_k / x^* - x' \quad \forall k$

$n_1 / x^* - x'$
$n_2 / x^* - x'$
$\vdots$
$n_r / x^* - x'$

and $\gcd(n_i, n_j) = 1$

$\Rightarrow n_1 n_2 \cdots n_r / x^* - x'$

$\Rightarrow n / x^* - x'$

$\Rightarrow x^* \equiv x' \bmod n$

$\therefore$ x' is congruent to $x^* \bmod n$

so simultaneous solution x^* of $x_k \equiv a_k \bmod n_k$ is unique.

Exercise:- Apply Chinese Remainder Thoorom.

find simultaneous solution of

(1) $x \equiv 0 \bmod 3$
$x \equiv 1 \bmod 4$
$17x \equiv 9 \bmod 23$

Ans $x \equiv 33 \bmod 276$

(2) $x \equiv 1 \bmod 3$
$x \equiv 2 \bmod 5$
$x \equiv 3 \bmod 7$

(3) $x \equiv 5 \bmod 6$
$x \equiv 4 \bmod 11$
$x \equiv 3 \bmod 17$