Chinese Remainder Theorem:

Sun - Tsu's puzzle : $x \equiv 1 \pmod 3$
$x \equiv 2 \pmod 5$
$x \equiv 3 \pmod 7$

- used to find solution of a ~~base~~ system of linear congruence.
- There can be ∞'ly many solutions
- Solving method:
  1. Iteration.
  2. Using chinese Remainder theorem

Statement: The linear system of congruences $x \equiv a_i \pmod{m_i}$ — ①
where moduli are pairwise prime and $1 \le i \le k$ has
a unique sol'n modulo $m_1 m_2 \dots m_k$.

PROOF: consists of ② parts:

1st: construct a solution

2nd: show the solution has unique modulo $m_1 m_2 \dots m_k$

Let $M = m_1 m_2 \dots m_k$ and $M_i = \frac{M}{m_i}$ where $1 \le i \le k$

Given, the moduli are pairwise prime

$\Rightarrow (M_i, m_i) = 1$

Also, $\Rightarrow$ Inverse exists for M_i such that $M_i (M_i)^{-1} \equiv 1 \pmod{m_i}$

And Also, $M_i \equiv 0 \pmod{m_j}$ for $i \neq j$ — ②

1st: construct a sol'n to the linear system:

Given $(M_i, m_i) = 1$ where $1 \le i \le k$

So, $M_i (M_i)^{-1} \equiv 1 \pmod{m_i}$ — ③ has unique solution $(M_i)^{-1}$

Now,

Take $x = a_1 M_1 (M_1)^{-1} + a_2 M_2 (M_2)^{-1} + \dots + M_k (M_k)^{-1} a_k$

to prove: x is a solution of ①

$x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + \dots + a_k M_k y_k \pmod{m_1}$

$= a_1 M_1 y_1 \pmod{m_1} + a_2 M_2 y_2 \pmod{m_1}$

$+ \dots + a_k M_k y_k \pmod{m_1}$

$= a_1 M_1 y_1 \pmod{m_1} + 0 + \dots + 0$ [from ②]

$x = a_1 M_1 y_1 \pmod{m_1}$

$x \equiv a_1 \times 1 \pmod{m_1}$ [from ③]

$x \equiv a_1 \pmod{m_1}$

Similarly, we can prove

$x \equiv a_2 \pmod{m_2}$

$\vdots$

$x \equiv a_k \pmod{m_k}$

Generalized:

To show that x is a solution of the linear system.

we have

$x = \sum_{i=1}^{k} a_i M_i y_i + a_j M_j y_j$ → from ③

$\equiv \sum_{i \neq j} a_i \cdot 0 \cdot y_i + a_j \cdot 1 \cdot \pmod{m_j}$

↳ from ②

$\equiv 0 + a_j \pmod{m_j}$

$x \equiv a_j \pmod{m_j}$ where $1 \leq j \leq k$

2nd: Show that unique modulo M exists

Suppose there are two solutions x_0 and x_1.

Then $x_0 \equiv a_1 \pmod{m_1}$ and $x_1 \equiv a_1 \pmod{m_1}$

$x_0 \equiv a_2 \pmod{m_2}$ $\quad$ $x_1 \equiv a_2 \pmod{m_2}$

$\vdots$ $\quad$ $\vdots$

$x_0 \equiv a_k \pmod{m_k}$ $\quad$ $x_1 \equiv a_k \pmod{m_k}$

~~Then~~ ~~$m_1 \mid x_1 - x_0$~~

~~$m_2 \mid x_1 - x_0$~~

Then $x_1 - x_0 \equiv 0 \pmod{m_1}$

$x_1 - x_0 \equiv 0 \pmod{m_2}$

$\vdots$

$x_1 - x_0 \equiv 0 \pmod{m_k}$

i.e. $m_1 \mid x_1 - x_0$ $\quad$ $m_2 \mid x_1 - x_0$ $\dots$ $m_k \mid x_1 - x_0$

Since $m_1, m_2, \ldots, m_k$ are relatively prime.

Then $m_1 m_2 \ldots m_k \mid x_1 - x_0$

$\Rightarrow \quad M \mid x_1 - x_0$

$\Rightarrow \quad x_1 \equiv x_0 \pmod M$

$\therefore$ The sol'n is unique.

<u>Generalized:</u>

Let x_0 and x_1 be two solutions of the system.

we should show that $x_0 \equiv x_1 \pmod M$

Since, $x_0 \equiv a_j \pmod{m_j}$ and $x_1 \equiv a_j \pmod{m_j}$ for $1 \le j \le k$

$x_1 - x_0 \equiv 0 \pmod{m_j}$

i.e. $m_j \mid x_1 - x_0$ for every j btw $1 \le j \le k$

$\Rightarrow$ Since ~~$m_1, m_2, \ldots$~~ m_j for $1 \le j \le k$ are RP.

Then $m_1 m_2 \ldots m_k \mid x_1 - x_0$

~~$M \mid M$~~

$\Rightarrow \quad M \mid x_1 - x_0$

So, $x_1 - x_0 \equiv 0 \pmod M$

Thus, any two solutions of the linear system are congruent modulo M.

So, the solution has unique modulo M.

Q: Solve $x \equiv 1 \pmod 3$ $x \equiv 2 \pmod 4$ $x \equiv 3 \pmod 5$

~~Here, the unique solution is are~~ $\cancel{M_1 y_1 \equiv 1 \pmod 3}$

$\cancel{M_2 y_2 \equiv 1 \pmod 4}$

$\cancel{M_3 y_3 \equiv 1 \bmod}$

From CRT, $x \equiv \sum_{i=1}^{3} a_i M_i y_i \pmod M$ where $M = m_1 m_2 m_3$

Here $m_1 = 3$ $m_2 = 4$ $m_3 = 5$

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

$M_1 = 20$ $M_2 = 15$ $M_3 = 12$

and $M_1 y_1 \equiv 1 \pmod{m_1}$ $M_2 y_2 \equiv 1 \pmod{m_2}$ $M_3 y_3 \equiv 1 \pmod{m_3}$

$20 y_1 \equiv 1 \pmod 3$ $15 y_2 \equiv 1 \pmod 4$ $12 y_3 \equiv 1 \pmod 5$

$y_1 = 2$ $y_2 = 3$ $y_3 = 3$

Thus $x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 \pmod M$

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

$= 40 + 90 + 108 \pmod{60}$

$= 238 \pmod{60}$

$= 58 \pmod{60}$