Chinese Reminder theorem:

Pairwise relatively Prime Positive integers:

$m_1, m_2, m_3 \text{ ---- } m_K$

any integers: $a_1\ a_2\ a_3 \text{ ----- } a_K$

then congruences equation using these values:

$$\left.\begin{array}{l} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ x \equiv a_3 \pmod{m_3} \\ \vdots \\ x \equiv a_K \pmod{m_K} \end{array}\right]$$

have a solution and the solution is unique Modulo M where

$M = m_1 \cdot m_2 \text{ --- } m_K$

Solution:

$$\boxed{x = (M_1 X_1 a_1 + M_2 X_2 a_2 \text{ --- } M_K X_K a_K) \bmod M}$$

eq. (1) $\quad M_i = \dfrac{M}{m_i}$

eq. (2) $\quad M_i X_i \equiv 1 \pmod{m_i}$

chinese reminder theorem state that there always exists an x that satisfy the given congruence equ.

$$x \equiv a_1 \pmod{m_1}$$
$$x \equiv a_2 \pmod{m_2}$$
$$\vdots$$

where $m_1 m_2 \cdots$ all must be coprime to one another.

$$\gcd(m_1, m_2) = 1 = \gcd(m_2, m_3)$$

Exa ① $x \equiv 1 \bmod 5$

$x \equiv 1 \bmod 7$

$x \equiv 3 \bmod 11$

Solve the simultaneous congruences using chinese reminder theorem.

Sol: $\cancel{x} = (M_1 X_1 a_1 + M_2 X_2 a_2 + M_3 X_3 a_3) \pmod{M}$

given $a_1 = 1$ $\quad m_1 = 5$

$a_2 = 1$ $\quad m_2 = 7$

$a_3 = 3$ $\quad m_3 = 11$

$m = m_1 \cdot m_2 \cdot m_3$

$= 5 \times 7 \times 11$

$= 385$

$$M_1 = \frac{m}{m_1} = \frac{385}{5} = \underline{\underline{77}}$$

$$M_2 = \frac{M}{m_2} = \frac{385}{7} = 55$$

$$M_3 = \frac{M}{m_3} = \frac{385}{11} = 35$$

X_1 : equation: $M_i X_i \equiv 1 (\mathrm{mod}\ m_1)$

$$M_1 \cdot X_1 \equiv 1 (\mathrm{mod}\ m_1)$$

$$77 \cdot X_1 \equiv 1 (\mathrm{mod}\ 5)$$

$$(77 \cdot X_1)(\mathrm{mod}\ 5) \equiv 1 (\mathrm{mod}\ 5)$$

$$\underline{77 (\mathrm{mod}\ 5)} \cdot X_1 (\mathrm{mod}\ 5) \equiv 1 (\mathrm{mod}\ 5)$$

$\downarrow$

$$2 \cdot X_1 (\mathrm{mod}\ 5) \equiv 1 (\mathrm{mod}\ 5)$$

$1 \quad 5 \,)\, 77 \,(\, 15$

$2 \cdot x_1 (\bmod 5) = \ldots$

multiply 3 both side

$$
\begin{array}{r}
5\overline{)77}(15 \\
5 \\
\hline
27 \\
25 \\
\hline
2
\end{array}
$$

$2 \times 3 \cdot x_1 (\bmod 5) \equiv 1 (\bmod 5)$

$6 x_1 \bmod 5 \equiv 3 \cdot 1 (\bmod 5)$

$\underbrace{6 (\bmod 5)} \cdot x_1 (\bmod 5) \equiv 3 (\bmod 5)$

$1 \cdot x_1 (\bmod 5) \equiv 3 (\bmod 5)$

$x_1 = 3$

x_2:

$\underline{m_2} x_2 \equiv 1 (\bmod m_2)$

$55 \cdot x_2 \equiv 1 (\bmod 7)$

$55 (\bmod 7) \cdot x_2 \equiv 1 (\bmod 7)$

$$
\begin{array}{r}
7\overline{)55}(7 \\
49 \\
\hline
6
\end{array}
$$

$6 \cdot x_2 (\bmod 7) \equiv 1$

multiply both side 6

$6 \cdot 6 x_2 \equiv 6 \cdot 1 (\bmod 7)$

$36 \cdot x_2 \equiv 6 (\bmod 7)$

$36 \cdot X_2 \equiv 6 \pmod 7$

$36 \pmod 7 \cdot X_2 \equiv 6 \pmod 7$ $\qquad 7 \overline{)36}(5$, 35, $\overline{1}$

$1 \cdot X_2 \equiv 6 \pmod 7$

$\boxed{X_2 = 6}$

X_3:

$m_3 X_3 \equiv 1 \pmod{m_3}$

$35 X_3 \equiv 1 \pmod{11}$

$35 \pmod{11} \cdot X_3 \equiv 1 \pmod{11}$

$2 \cdot X_3 \equiv 1 \pmod{11}$

multiply both side by 6

$12 \cdot X_3 \equiv 1 \cdot 6 \pmod{11}$

$12 \pmod{11} \cdot X_3 \equiv 6 \pmod{11}$

$1 \cdot X_3 \equiv 6 \pmod{11}$

$$\boxed{X_3 = 6}$$

Now $x = (m_1 X_1 y_1 + m_2 X_2 y_2 + M_3 X_3 y_3) \bmod M$

$= (77 \cdot 3 \cdot 1 + 55 \cdot 6 \cdot 1 + 77 \cdot 6 \cdot 3) \bmod 385$

$x =$

Exa. $X \equiv 2 \pmod 3$

$X \equiv 3 \pmod 5$

$X \equiv 2 \pmod 7$