Chinese Remainder theorem.

eg $x \equiv 1 \bmod 5$

$x \equiv 3 \bmod 7$

5 & 7 are co prime

GCD(5, 7) = 1

eg $x \equiv 2 \bmod 3$

$x \equiv 3 \bmod 4$

$x = 1 \bmod 5$

gcd(3,4) = gcd(4,5), gcd(3,5) = 1

$x \equiv a_1 \pmod{m_1}$

$x \equiv a_2 \pmod{m_2}$

$x \equiv a_3 \pmod{m_3}$

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

ie all co prime.

$x = (M_1 X_1 a_1 + M_2 X_2 a_2 + M_3 X_3 a_3 \cdots + M_n X_n a_n) \bmod M$

$M = m_1 * m_2 * m_3$

$M_i = \frac{M}{m_i}$

$M_1 = \frac{M}{m_1} = \frac{m_1 \times m_2 \times m_3}{m_1}$, $M_2 = \frac{M}{m_2}$

$= \frac{m_1 \times m_2 \times m_3}{m_2}$

$M_1 = m_2 m_3$

$M_2 = m_1 m_3$

$M_3 = m_1 m_2$

TO calculate X_i (multiplicate Inverse of M_i)

$M_i X_i \equiv 1 \bmod m_i$

Example

To find x ?

$x \equiv 1 \pmod 5$

$x \equiv 1 \pmod 7$

$x \equiv 3 \pmod{11}$

$x \equiv a_i \bmod (m_i)$

$a_1 = 1,\ a_2 = 1,\ a_3 = 3$

$m_1 = 5,\ m_2 = 7,\ m_3 = 11$

Solution

5, 7, 11 all are relatively prime to one another

So we can find x.

ie $\gcd(5,7) = \gcd(7,11) = \gcd(11,5) = 1$

$M = m_1 * M_2 \times m_3 = 5 \times 7 \times 11 = 385$

$M = 385$

$M_1 = m_2 \times m_3 = 7 \times 11 = 77$

$M_2 = m_1 \times m_3 = 5 \times 11 = 55$

$M_3 = m_1 \times m_2 = 5 \times 7 = 35$

Calculate x_i value

$M_1 x_1 \equiv 1 \pmod{m_1}$ ie $M_1 x_1 \pmod{m_1} = 1$

$77 \cdot x_1 \pmod 5 = 1$

$\frac{77}{5}$ = Remainder 2

$2 \cdot x_1 \pmod 5 = 1$

$\therefore x_1 = 3$

$M_2 x_2 \equiv 1 \pmod{m_2}$

$M_2 x_2 \pmod{m_2} = 1$

$55 \cdot x_2 \pmod 7 = 1$

$\frac{55}{7} = 6$

$6 \cdot x_2 \pmod 7 = 1$

$x_2 = 6$

$M_3 \cdot X_3 \equiv 1 \pmod{m_3}$

$M_3 \cdot X_3 \pmod{m_3} = 1$

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

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

$\boxed{X_3 = 6}$

$\frac{35}{11} = 2$

now

$a_1 = 1, \quad a_2 = 1, \quad a_3 = 3$

$m_1 = 5, \quad m_2 = 7, \quad m_3 = 11$

$M_1 = 77, \quad M_2 = 55 \quad M_3 = 55$

$x_1 = 3, \quad x_2 = 6, \quad x_3 = 6$

$x = (77 \times 3 \times 1 + 55 \times 6 \times 1 + 35 \times 6 \times 3) \bmod 385$

$x = 1191 \bmod 385$

$\boxed{x = 36}$

we can verify :-

$36 \bmod 5 = 1$

$36 \bmod 7 = 1$

$36 \bmod 11 = 3$