Chinese Remainder Theorem.

Find x such that

$x \% 3 = 2$,
$x \% 4 = 3$,
$x \% 5 = 1$

Or using the congruence notation,

$x \equiv 2 \bmod 3$
$x \equiv 3 \bmod 4$
$x \equiv 1 \bmod 5$

Here the 3 divisors 3, 4, 5 have to be mutually prime i.e.

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

One possible x is $x = 11$.
But how do we find x?

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

~~where $M = M_1 * M_2 * M_3 * \cdots * M_n$~~

where $M = m_1 * m_2 * m_3 * \cdots * m_n$.

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

X_i = multiplicative inverse of M_i
ie $M_i X_i \equiv 1 \bmod m_i$

$M = 3 * 4 * 5 = 60$

$M_1 = \frac{M}{m_1} = \frac{60}{3} = 20$

$M_2 = \frac{M}{m_2} = \frac{60}{4} = 15$

$M_3 = \frac{m}{m_3} = \frac{60}{5} = 12$

~~$(20 X_1) \bmod 20 = 1$~~

$(20 * X_1) \bmod 3 \equiv 1$

$X_1 = 2 \therefore 40 \bmod 3 = 1.$

$(15 * X_2) \bmod 4 \equiv 1$

~~$X_2 = 1$~~ $X_2 = 3 \therefore 45 \bmod 4 = 1$

$(12 * X_3) \bmod 5 \equiv 1$

$X_3 = 3 \therefore 36 \bmod 5 = 1$

$X = (20 * 3 * 2 + 15 * 3 * 3 + 12 * 3 * 1) \bmod 60$

$= (120 + 135 + 36) \bmod 60$

$= 291 \bmod 60$

$= 51.$

$\begin{array}{r} 291 \\ 240 \\ \hline 51 \end{array}$

Find x such that

$x \equiv 1 \bmod 5$
$x \equiv 1 \bmod 7$
$x = 3 \bmod 11$

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

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

$M = m_1 * m_2 * m_3$
$= 5 * 7 * 11$
$= 385$

$M_1 = \frac{M}{m_1} = \frac{385}{5} = 77$

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

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

$M_1 X_1 = 1 \bmod m_1$
$77 * X_1 = 1 \bmod 5$

$(77 \times 1) \% 5 = 2$
$(77 \times 2) \% 5 = 4$
$(77 \times 3) \% 5 = 1$
$\therefore X_1 = 3$

Similarly

$(55 \times 1) \bmod 7 = 6$

$(55 \times 2) \bmod 7 = 110 \% 7 = 5$

$(55 \times 3) \bmod 7 = (165 \% 7) = 4$

$(55 \times 4) \bmod 7 = (220 \% 7) = 3$

$(55 \times 5) \bmod 7 = (275 \% 7) = 2$

$(35 \times 6) \bmod 7 = (330 \% 7) = 1$

$X_2 = 6$

$(35 \times 1) \bmod 11 = 2$

$(35 \times 2) \bmod 11 = 4$

$(35 \times 3) \bmod 11 = 6$

$(35 \times 4) \bmod 11 = 8$

$(35 \times 5) \bmod 11 = 10$

$(35 \times 6) \bmod 11 = 1$

$X_3 = 6$

$$x = (m_1 x_1 a_1 + m_2 x_2 a_2 + m_3 x_3 a_3) \bmod M$$

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

$$= 1191 \bmod 385$$

$$= 36.$$

Verify

$36 \bmod 5 = 1$

$36 \bmod 7 = 1$

$36 \bmod 11 = 3$

$x \equiv a_1 \bmod m_1$

$x = a_2 \bmod m_2$

$\vdots$

$x = a_n \bmod m_n$

where

$(m_1, m_2 \cdots m_n)$ are mutually prime

~~$x = M_1 x_1$~~

$x = (M_1 a_1 y_1 + M_2 a_2 y_2 + \cdots M_n a_n y_n) \bmod M$

where

$M = m_1 \cdot m_2 \cdot \cdots * M_n$

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

y_i = multiplicative inverse of M_i

$\Rightarrow M_i y_i \bmod m_i = 1$

eg ~~Ex~~

$x \equiv a_1 \bmod m_1$

$x = a_2 \bmod m_2$

$\vdots$

$x = a_n \bmod m_n$

where

$(m_1, m_2 \cdots m_n)$ are mutually prime

~~$x = M_1 x_1$~~

$x = (M_1 a_1 Y_1 + M_2 a_2 Y_2 + \cdots M_n a_n Y_n) \bmod M$

where

$M = m_1 \cdot m_2 \cdot \cdots * M_n$

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

Y_i = multiplicative inverse of M_i

$\Rightarrow M_i Y_i \bmod m_i = 1$

eg ~~Ftan~~

eg 2 Find x such that

$x \equiv 1 \bmod 5$

$x \equiv 2 \bmod 6$

$x \equiv 3 \bmod 7$

$M = 5 \times 6 \times 7 = 210.$

$M_1 = \frac{210}{5} = 42 \quad M_2 = \frac{210}{6} = 35 \quad M_3 = \frac{210}{7} = 30$

$a_1 = 1 \quad a_2 = 2 \quad a_3 = 3.$

$m_1 = 5 \quad m_2 = 6 \quad m_3 = 7$

$y_1 \Rightarrow (42 * y_1) \bmod 5 = 1$

$(~~43 * 7~~) \bmod 5 = ~~301~~ \overset{126}{} \bmod 5 = 1$

$y_1 = 3$

$(35 * y_2) \bmod 6 = 1$

$35 \times 3 = 105/6 = 42 \quad (3)$

$35 \times 4 \% 6 = 140 \% 6, \quad (2)$

$35 \times 5 = 175 \% 6 = 2 \quad (1)$

$y_2 = 5$

$(30 \times y_3) \bmod 7 = 1$

$(30 \times 4) \% 7 \quad 120 \% 7 = 119 \equiv 1$

$y_3 = 4$

$x = (42 * 1 * 3 + 35 * 2 * 5 + 30 * 3 * 4) \bmod 210$

$= 836 \bmod 210 = 206$

check

206 % 5 = 1
206 % 6 = 2
206 % 7 = 3

eg 3

$$\left.\begin{aligned} x &\equiv 3 \pmod 4 \\ x &\equiv 0 \pmod 6 \end{aligned}\right\} \text{ no solution}$$

$x \equiv 3 \pmod 4$ can be written as
$x = 3 + 4t$

Substituting this in second gives

$3 + 4t \equiv 0 \pmod 6$

$4t = -3 \pmod 6$

But gcd(4,6) cannot be -3
∴ No solution !

Another way:
First congruence implies x is odd
Second congruence implies x is even

That is a contradiction ∴ no solution

eg4 Solve the following

$x \equiv 1 \pmod 5$
$x \equiv 2 \pmod 7$
$x \equiv 3 \pmod 9$
$x \equiv 4 \pmod{11}$

Solution

$x = 1731$

eg5 Find x such that

$$3x \equiv 7 \pmod{10}$$

- Multiplicative inverse of $3 \pmod{10}$ is defined as.

$3^{\phi(10)-1}$

$\phi(10) = 4$ { Fermat's theorem }

$3^{4-1} = 3^3 = 27 \equiv 7 \pmod{10}$

∴ Multiply both sides of the equation by 7

$7 \times 3x = 7 \times 7 \pmod{10}$
$21 \cdot x = 49 \bmod 10$
$21 \bmod 10 = 1$
$x = 9 \pmod{10}$

check

$3 \times 9 = 27 = 7 \pmod{10}$