Chinese Remainder Theorem

To solve the system of congruences:

$$x \equiv a_1 \bmod m_1$$
$$x \equiv a_2 \bmod m_2$$
$$\vdots$$
$$x \equiv a_n \bmod m_n$$

If $g.c.d.(m_i, m_j) = 1$, for $i \neq j$, then there exists a simultaneous solution x and any two solutions are congruent to one another modulo $M = m_1 m_2 \cdots m_r$

Proof:- Let $M_i = \frac{M}{m_i}$

$$= m_1 m_2 \cdots m_{i-1} m_{i+1} \cdots m_r$$

$\Rightarrow$ g.c.d. $(m_i, M_i) = 1$.

$\Rightarrow$ there exists an integer N_i such that $M_i N_i \equiv 1 \pmod{m_i}$

Let $x = \sum_i a_i M_i N_i$.

For each i, all terms of x are congruent to zero except i^{th} term ($\because m_i | M_j$ when $i \neq j$).

$$\therefore x \equiv \sum_i a_i M_i N_i \pmod{m_i}$$

$$\equiv a_i M_i N_i \pmod{m_i}$$

$$\equiv a_i \times 1 \pmod{m_i}$$

$$\equiv a_i \pmod{m_i}$$

Uniqueness:

Let x_1 and x_2 be two solutions.

$$\Rightarrow x = x_1 - x_2 = a_i - a_i \pmod{m_i} \quad \forall i$$

$$\therefore x \equiv 0 \pmod{m_i}, \quad \forall i$$

$$\Rightarrow x_1 \equiv x_2 \pmod{m_i}, \quad \forall i$$

$$\Rightarrow x_1 \equiv x_2 \pmod{M}, \text{ as}$$

g.c.d. $(m_i, m_j) = 1$, for $i \neq j$.

Ex:- $x \equiv 1 \pmod 3$

$x \equiv 2 \pmod 5$

$x \equiv 3 \pmod 7$

$M = 3 \times 5 \times 7 = 105$

$M_1 = \frac{105}{3} = 35$, $M_2 = \frac{105}{5} = 21$,

$$M_3 = \frac{105}{7} = 15.$$

$$\Rightarrow N_1 = M_1^{-1} \pmod 3$$

$$= (35)^{-1} \pmod 3$$

$$= 2^{-1} \pmod 3$$

$$= \underline{2 \pmod 3}$$

$$\Rightarrow N_2 = (21)^{-1} \pmod 5$$

$$\equiv 1^{-1} \pmod 5$$

$$\equiv 1 \pmod 5$$

$$\Rightarrow N_3 = (15)^{-1} \pmod 7$$

$$= 1^{-1} \pmod 7$$

$$\equiv 1 \pmod 7$$

Now $x = \sum a_i M_i N_i$

$$= 1 \times 35 \times 2 + 2 \times 21 \times 1 + 3 \times 15 \times 1$$

$\equiv 157 \pmod{105}$

$\equiv 52 \pmod{105}$

Ex:- $2x \equiv 1 \pmod 5$

$3x \equiv 9 \pmod 6$

$4x \equiv 1 \pmod 7$

$5x \equiv 9 \pmod{11}$

$\Rightarrow \begin{cases} x \equiv 3 \pmod 5 \\ x \equiv 3 \pmod 2 \\ x \equiv 2 \pmod 7 \\ x \equiv 4 \pmod{11} \end{cases}$

$\because 2^{-1} \equiv 3 \pmod 5$

(∵ dividing by 3)

$(\because 4^{-1} \equiv 2 \pmod 7$

$\because \quad 2 \times 5x \equiv 9 \times 2 \pmod{11}$

$-x \equiv 18 \pmod{11}$

$x \equiv -7 \pmod{11}$

$$M = 5 \times 2 \times 7 \times 11 = 770$$

$$M_1 = 154 \Rightarrow N_1 = 4$$

$$M_2 = 385 \Rightarrow N_2 = 1$$

$$M_3 = 110 \Rightarrow N_3 = 3$$

$$M_4 = 70 \Rightarrow N_4 = 3$$

$$\therefore x = 3 \times 154 \times 4 + 3 \times 385 \times 1 + 2 \times 110 \times 3 + 4 \times 70 \times 3$$

$$= 4,503$$

$$\equiv 653 \pmod{770}$$

(HW) Solve:

(1) $17x \equiv 3 \pmod 2$

$17x \equiv 3 \pmod 3$

$17x \equiv 3 \pmod 5$

$17x \equiv 3 \pmod 7$

(2) $x \equiv 5 \pmod 6$

$x \equiv 4 \pmod{11}$

$x \equiv 3 \pmod{17}$

Ex:- Obtain 3 consecutive integers, each having a square factor.

Let a, $a+1$, $a+2$ be the required 3 integers.

We find a such that

$$\begin{cases} a \equiv 0 \pmod{2^2} \\ a+1 \equiv 0 \pmod{3^2} \\ a+2 \equiv 0 \pmod{5^2} \end{cases}$$

(4, 3, 5 are relatively prime)

Chinese remainder theorem (CRT) $\Rightarrow$

$$a \equiv 0 \pmod 4$$

$$a \equiv -1 \pmod 9$$

$$a \equiv -2 \pmod{25}$$

$$M = 4 \times 9 \times 25 = 900$$

$$\left.\begin{aligned} M_1 &= 225 \\ M_2 &= 100 \\ M_3 &= 36 \end{aligned}\right\} \quad \begin{aligned} N_1 &= 1 \\ N_2 &= 1 \\ N_3 &= -9 \equiv 16 \end{aligned}$$

$$\begin{cases} 99 \equiv -1 \pmod{25} \\ 9 \times 11 \equiv -1 \pmod{25} \\ -9 \times 11 \equiv 1 \pmod{25} \end{cases}$$

$$\therefore a = 0 + (-1) \times 100 \times 1 + (-2) \times 36 \times 16$$

$\equiv -1252 \pmod{900}$

$\equiv -352 \pmod{900}$

$\equiv 548 \pmod{900}$

$\therefore$ 548 549 550 are the required 3 consecutive integers

EX: A band of 17 pirates stole a sack of gold coins. When they tried to divide the fortune into equal portions, 3 coins remained. In the ensuing brawl over who should get the extra coins, one pirate was killed. The wealth was redistributed, but this time an equal division left 10 coins. Again an argument developed in which another pirate was killed. But now the total fortune was evenly distributed among the survivors. What was the least number of coins that could have been stolen?

$x \equiv 3 \pmod{17}$

$x \equiv 10 \pmod{16}$

$x \equiv 0 \pmod{15}$

$M = 17 \times 16 \times 15 = 4080$

$M_1 = 240 \Rightarrow N_1 \equiv 9 \pmod{17}$

$M_2 = 255 \quad N_2 \equiv -1 \pmod{16}$

$M_3 = 272 \quad N_3 =$

$\therefore x = 3 \times 240 \times 9 + 10 \times 255 \times (-1) + 0$

$\equiv 3930 \pmod{4080}$

$\therefore$ Minimum coins $= 3930$

EX:- When eggs in a basket are removed 2, 3, 4, 5, 6 at a time there remain, respectively, 1, 2, 3, 4, 5 eggs. When they are taken out 7 at a time, none are left over. Find the smallest number of eggs that could have been contained in the basket.

$x \equiv 1 \pmod{2} \rightarrow (1)$

$x \equiv 2 \pmod{3} \rightarrow (2)$

$x \equiv 3 \pmod{4} \rightarrow (3)$

$x \equiv 4 \pmod{5} \rightarrow (4)$

$x \equiv 5 \pmod{6} \rightarrow (5)$

$x \equiv 0 \pmod 7 \longrightarrow (6)$.

$(3) \Rightarrow x \equiv 3 \pmod 4$

$\Rightarrow x = 4k+3 = 4k+2+1$

$= 2(2k+1)+1$

$\Rightarrow x \equiv 1 \pmod 2$

$\Rightarrow$ We eliminate (1).

(2) and (5) $\Rightarrow$ $\left.\begin{array}{l} x \equiv 2 \pmod 3 \\ x \equiv 5 \pmod 6 \end{array}\right\}$

g.c.d. $(3,6) = 3 \neq 1$.

$(2) \Rightarrow x \equiv 2 \pmod 3$

$\Rightarrow 2x \equiv 4 \pmod 6$

$(5) \Rightarrow x \equiv 5 \pmod 6$ $\Big\}$

Subtracting $\Rightarrow x \equiv -1 \pmod 6$

$\Rightarrow x \equiv 5 \pmod 6$

∴ We can eliminate (2)

∴ We have:

$x \equiv 3 \pmod 4 \rightarrow (3)$

$x \equiv 4 \pmod 5 \rightarrow (4)$

$x \equiv -1 \pmod 6 \rightarrow (5)$

$x \equiv 0 \pmod 7 \rightarrow (6)$

Now, g.c.d. $(4, 6) \neq 1$

$(3) \times 3 \Rightarrow 3x \equiv 9 \pmod{12}$

$(5) \times 2 \Rightarrow 2x \equiv -2 \pmod{12}$

Subtracting $\Rightarrow x \equiv 11 \pmod{12}$

We can replace (3) & (5) by this new congruence.

$$\therefore \quad \left.\begin{aligned} x &\equiv 4 \pmod 5 \\ x &\equiv 11 \pmod{12} \\ x &\equiv 0 \pmod 7 \end{aligned}\right\}$$

C.R.T. $\Rightarrow$ $x \equiv 119 \pmod{420}$

$\therefore$ 119 eggs. (Ans.)

Theorem

The system of linear congruences

$ax + by \equiv r \pmod n$

$cx + dy \equiv s \pmod n$

has a unique solution modulo n whenever $\gcd(ad - bc, n) = 1$.

Proof. Let us multiply the first congruence of the system by d, the second congruence by b, and subtract the lower result from the upper.

These calculations yield $(ad - bc)x \equiv dr - bs \pmod n$..... (1)

The assumption $\gcd(ad - bc, n) = 1$ ensures that the congruence $(ad - bc)z \equiv 1 \pmod n$ posseses a unique solution; denote the solution by t.

When congruence (1) is multiplied by t, we obtain

$x \equiv t(dr - bs) \pmod n$

A value for y is found by a similar elimination process.

That is, multiply the first congruence of the system by c, the

second one by a, and subtract to end up with
(ad − bc)y ≡ as − cr (mod n) ..... (2)
Multiplication of this congruence by t leads to
y ≡ t(as − cr) (mod n)
.....

Ex:- $5x+3y \equiv 1 \pmod 7 \rightarrow (1)$

$3x+2y \equiv 4 \pmod 7 \rightarrow (2)$

(1) × 2 $\Rightarrow 10x+6y \equiv 2 \pmod 7$

(2) × 3 $\Rightarrow 9x+6y \equiv 12 \pmod 7$

Subtracting,

$x \equiv -10 \pmod 7$

$\Rightarrow x \equiv -3 \pmod 7$

$\Rightarrow x \equiv 4 \pmod 7$

$\Rightarrow 5x \equiv 20 \pmod 7$

$\Rightarrow 5x \equiv -1 \pmod 7$

From ① $\Rightarrow -1 + 3y \equiv 1 \pmod 7$

$\Rightarrow 3y \equiv 2 \pmod 7$

$\Rightarrow 2 \times 3y \equiv 4 \pmod 7$

$\Rightarrow 6y \equiv 4 \pmod 7$

$\Rightarrow -y \equiv 4 \pmod 7$

$\Rightarrow y \equiv -4 \pmod 7$

$\Rightarrow y \equiv 3 \pmod 7$

$\therefore x \equiv 4 \pmod 7$

$y \equiv 3 \pmod 7$

Ex:- $7x + 3y \equiv 6 \pmod{11}$

$4x + 2y \equiv 9 \pmod{11}$

Ex:- $11x + 5y \equiv 7 \pmod{20}$

$6x + 3y \equiv 8 \pmod{20}$

Ex:- Find the smallest integer which leaves a remainder of 1 when divided by 11, a remainder 2 when divided by 12, and a remainder of 3 when divided by 13.