## Chinese Remainde Theorem :-

Let $m_1, m_2, \ldots, m_k$ be positive integers such that $\gcd(m_i, m_j) = 1$ for $i \neq j$.

(i.e; $m_i$ & $m_j$ are coprime for all $i \neq j$)

Then for any integers $a_1, \ldots, a_k$, the system

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

has a solution.

Moreover, any two solutions of the system are congruent modulo $m_1 m_2 \ldots m_k$.

**Proof :-** (Approach I via Mathematical induction on no. of eqns in the system.

Let there are $k = 2$ eqns.

$$x \equiv a_1 \bmod m_1$$
$$x \equiv a_2 \bmod m_2$$

The eqn. $x \equiv a_1 \bmod m_1$ has a soln since $a_1 + km_1$ satisfies this eqn

for all $k \in \mathbb{Z}$

$x = a_1 + km_1$

$x - a_1 = a_1 + km_1 - a_1 = km_1$ is divisible by $m_1$

Now we need to show that there exist an integer $k_1$ such that

$$a_1 + k_1 m_1 \equiv a_2 \bmod m_2$$

(i.e; for some integer $k_1$, $a_1 + k_1 m_1$ is a solution for both equations).

Equivalent to showing that

$$k_1 m \equiv (a_2 - a_1) \bmod m_2$$

has a solution for $k_1$

Since, $(m_1, m_2) = 1$

$\Rightarrow \exists$ integer $p, q$ such that

$$m_1 p + m_2 q = 1$$

$$\Rightarrow m_1 p = 1 - m_2 q$$

$$\Rightarrow (a_2 - a_1) m_1 p = (a_2 - a_1) - (a_2 - a_1) m_2 q$$

$\Rightarrow [(a_2 - a_1)p]\, m_1 \equiv (a_2 - a_1) \bmod m_2$

Consider $(a_2 - a_1)p = k_1$

Thus we proved

$$k_1 m \equiv (a_2 - a_1) \bmod m_2$$

i.e; we found a solution which satisfy both the equations simultaneously.

Now need to show that any two solns are congruent modulo mn.

Let $c_1$ & $c_2$ be two solns of the system.

i.e; $c_i \equiv a_1 \bmod m_1 \quad i = \{1, 2\}$.

$c_i \equiv a_2 \bmod m_2$

$\Rightarrow c_2 \equiv c_1 \bmod m_1$

$c_2 \equiv c_1 \bmod m_2$

$\Rightarrow m_1 \mid c_2 - c_1 \;,\; m_2 \mid c_2 - c_1$

$\Rightarrow m_1 m_2 \mid c_2 - c_1$

$\Rightarrow$ $c_2 \equiv c_1 \bmod mn$

Proof done for system of 2 eqns.

Now suppose the result is true for a system of $k$ eqns or less.

Now we need to find a soln for $k+1$ eqns

$$x \equiv a_1 \bmod m_1$$
$$x \equiv a_2 \bmod m_2$$
$$\vdots$$
$$x \equiv a_{k+1} \bmod m_{k+1}$$

Considering the first $k$ equations, $\exists$ a solution that is unique modulo $m_1 m_2 m_3 \ldots m_{k+1}$, say $a$.

i.e; for $k$ eqns, we've solution

$$x \equiv a \bmod (m_1 m_2 \ldots m_k)$$

Now $m = m_1 m_2 \ldots m_k$ and $m_{k+1}$ are relatively prime.

i.e; $\gcd(m, m_{k+1}) = 1$

the system

$$x \equiv a \bmod (m_1 m_2 \ldots m_k)$$
$$x \equiv a_{k+1} \bmod (m_{k+1})$$

has a solution that is unique modulo $m_1 m_2 \ldots m_k m_{k+1}$ $(m \cdot m_{k+1})$.

(by the case of 2 eqns)

## Approach 2

Construction of a simultaneous soln of the system of k-congruences:—

Let $m = m_1 m_2 \dots m_k$

Define $M_j = \frac{m}{m_j}$ for $1 \le j \le k$

Claim:- $\forall\ 1 \le j \le k$, $\gcd(m_j, M_j) = 1$

Proof:- Let $\gcd(m_j, M_j) \neq 1 \Rightarrow \exists\ p$ prime such that

$p \mid m_j$ & $p \mid M_j \Rightarrow p \mid m_1 m_2 \dots m_{j-1} m_{j+1} \dots m_k$

(In this $m_j$ is not included.)

$\Rightarrow \exists\ m_i$ such that

$p \mid m_i$

i.e; $\gcd(m_j, m_i) \neq 1$ because $p \mid m_i$ & $p \mid m_j$

Contradiction to the fact that $\gcd(m_i, m_j) = 1$

Now, we've for each $1 \le j \le k$,

$$\gcd(m_j, M_j) = 1$$

$\Rightarrow M_j x_j + m_j y_j = 1$ for some integers $x_j$ & $y_j$

Considering mod $m_j$, we'll get

$$M_j x_j \equiv 1 \bmod m_j$$

Consider sum $x = a_1 M_1 x + \ldots + a_k M_k x_k$

Claim:- $x$ is a simultaneous soln of the system of k-congruences.

If $i \neq j$

then $M_i = m_1 m_2 \ldots m_j m_{j+1} \ldots m_{i-1} m_{i+1} \ldots m_k$

(means in $M_i$ we will have $m_j$ term but not $m_i$)

$\Rightarrow m_j \mid M_i$

i.e; $M_i \equiv 0 \bmod m_j$

$\Rightarrow M_i x_i \equiv 0 \bmod m_j$

If $(i=j)$ $\quad M_j x_j \equiv 1 \bmod m_j$

$\Rightarrow a_j M_j x_j \equiv a_j \bmod m_j$

$\Rightarrow x \equiv a_j M_j x_j \equiv a_j \bmod m_j$

for each $1 \leq j \leq k$

$\therefore x = a_1 M_1 x_1 + \ldots + a_k M_k x_k$ is a solution for the system of k congruences

We're claiming this sum as a simultaneous soln because, for instance, suppose you're considering

1st eqn. $x \equiv a_1 \bmod m_1$

then replacing $x$ with $a_1 M_1 x_1 + \dots + a_k M_k x_k$

$j \neq 1$ for that case

$M_j x_j \equiv 0 \bmod m_1$

and same thing for other eqns.

for understanding only

---

For uniqueness :- Let $x$ and $y$ both simultaneous solutions of the system of $k$ congruences.

$\Rightarrow x \equiv y \bmod m_j \quad \forall \quad 1 \leq j \leq k.$

Now, $m = m_1 m_2 \dots m_k$ (prime factorization)

Let $p^t \mid m$ but $p^{t+1} \nmid m$ for some $t \in \mathbb{Z}^+$

Also, $(m_i, m_j) = 1 \quad \forall \quad 1 \leq i < j \leq k$

$\Rightarrow p^t \mid m_j$ for only one mod $m_j$

$\Rightarrow p^t \mid (x-y) \Rightarrow m \mid (x-y)$

$\Rightarrow x \equiv y \bmod m$

$\therefore$

By Fundamental theorem of Arithmatic (which says that every integer greater than 1 can be represented uniquely a product of prime no.)

Q:-8 Determine the number of n-digit quaternary (0,1,2,3) sequences in which there is never a 3 anywhere to the right of 0.

Soln:- Let $a_n$ denote the no. of such sequences of n-digits.

Now for (n+1)-digit sequences:

Case I:- Sequences of length n that end in 3.

Total no. of such sequence will be $3^n$ for (n+1) length.

Case II:- Sequences of length n that end in 0,1,2

No. of such seq. will be $3a_n$ because for last place we've only 3 choices

i.e; $$\boxed{a_{n+1} = 3a_n + 3^n}$$

This is required recursive relation (Non-homogeneous)

Now, $a_n^{(h)} = A.3^n$

$a_n^{(p)} = Bn\,3^n$

$\Rightarrow B(n+1).3^{n+1} = 3.Bn.3^n + 3^n$

$\Rightarrow 3B(n+1) - 3Bn + 1$

$\Rightarrow B = 1/3$

$\Rightarrow a_n = A \cdot 3^n + n\,3^{n-1}$

$a_0 = 1$

$a_1 = 4$

$\Rightarrow A = 1$

$\Rightarrow \boxed{a_n = 3^n + n\,3^{n-1}, \quad n \geq 0}$