In any linear congruence $ax \equiv b \pmod{m}$ if gcd of $a, m = 1$ then, an unique solution exists if $\gcd(a, m) = d$ then the linear congruence will have d no. of incongruent solution.

1) Solve a linear Congruence →

$$3x \equiv 6 \pmod{12}$$

$\gcd(3, 12) = 3$

Therefore this linear congruence will have 3 incongruent solutions

Now using inverse modulo we reduce into this form

$x \equiv 2 \pmod{4}$

$x - 4y = 2$

$x = 6$ in a sol

$x = 18$

$x = 6 + 2 \times 12 = 30$

Fermat Little Theorem:—

If p is a prime number and a is an integer which is not divisible by p then Fermat's Little theorem states $a^{p-1} \equiv 1 \pmod{p}$

2) Find the remainder when 7^{222} is divided by 11

⇒ Since 11 is a prime number and 11 does not divide 7 therefore by Fermat's Little Theorem $7^{11-1} \equiv 1 \pmod{11}$

$\Rightarrow 7^{10} \equiv 1 \pmod{11}$

$\Rightarrow (7^{10})^{22} \equiv 1^{22} \pmod{11}$

$\Rightarrow 7^{220} \equiv 1 \pmod{11}$

$\Rightarrow 7^2 \cdot 7^{220} \equiv 7^2 \pmod{11}$

$\Rightarrow 7^{222} \equiv 11 \times 4 + 5 \pmod{11}$

$\Rightarrow 7^{222} \equiv 5 \pmod{11}$

* 15^{222} divided by 13

→

$15^{12} \equiv 1 \pmod{13}$

$\Rightarrow (15^{12})^{18} \equiv 1^{18} \pmod{13}$

$\Rightarrow 15^{216} \equiv 1 \pmod{13}$

$\Rightarrow 15^6 \cdot 15^{216} \equiv 15^6 \pmod{13}$

$\Rightarrow 15^{222} \equiv 12 \pmod{13}$

$15 \equiv 2 \pmod{13}$

$\Rightarrow 15^2 \equiv 4 \pmod{13}$

$\Rightarrow (15^2)^3 \equiv 64 \pmod{13}$

$\Rightarrow 15^6 \equiv 13 \times 4 + 12 \pmod{13}$

$\Rightarrow 15^6 \equiv 12 \pmod{13}$

Q. Find the remainder when $1! + 2! + 3! + \cdots + 100!$ is divided by 12.

$\Rightarrow$ $1! \equiv 1 \pmod{12}$

$2! \equiv 2 \pmod{12}$

$3! \equiv 6 \pmod{12}$

$4! \equiv 0 \pmod{12}$

upto $100!$ it is $\equiv 0 \pmod{12}$

$1! + 2! + 3! + 4! \cdots 100! \equiv 9 \pmod{12}$

Q. Solve the linear congruence $345x \equiv 18 \pmod{\cancel{9}\,12}$

Chinese Remainder Theorem (CRT):-

If a set of Linear Congruence of the form

$x \equiv a_1 \pmod{m_1}$

$x \equiv a_2 \pmod{m_2}$

$x \equiv a_k \pmod{m_k}$

is given where m_1, m_2 until m_k are relatively prime, then there exist an unique solution and by CRT The solution is on the form $x \equiv (a_1 M_1^{-1} M_1 + a_2 M_2^{-1} M_2 + \cdots) \pmod{M}$

where $M = \text{lcm}(m_1, m_2 \cdots m_k)$

here $M_1 = \frac{M}{m_1}$

$M_2 = \frac{M}{m_2}$

$M_k = \frac{M}{m_k}$

Inverse Modulo:- If for any two integers a and m the condition $a^{-1}a \equiv 1 \pmod{m}$ holds then M^{-1} will be the inverse modulo of $a \pmod{m}$

Solve by Chinese Remainder Theorem the set of Linear Congruence

$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$
$$x \equiv 2 \pmod 7$$

⇒ Since the module (3, 5, 7) are relatively prime therefore this set of congruent equations has unique solution.

~~lcm(m,~~

$M = lcm(3, 5, 7) = 105$

$a_1 = 2$
$a_2 = 3$
$a_3 = 2$

$$M_1 = \frac{M}{m_1} = \frac{105}{3} = 35$$

$$M_2 = \frac{M}{m_2} = \frac{105}{5} = 21$$

$$M_3 = \frac{M}{m_3} = \frac{105}{7} = 15$$

$\cancel{M_1^{-1} M_1 \equiv 1 \pmod{105}}$ $\cancel{M_2^{-1} M_2 \equiv 1 \pmod{105}}$ $\cancel{M_3^{-1} M_3 \equiv 1 \pmod{105}}$

$\cancel{\Rightarrow M_1^{-1}\, 35 \equiv 1 \pmod{105}}$ $\cancel{\Rightarrow M_2^{-1}\, 21 \equiv 1 \pmod{105}}$ $\cancel{\Rightarrow M_3^{-1}\, 15 \equiv 1 \pmod{105}}$

⇒

$M^{-1} M \equiv 1 \pmod{3}$ $\quad M_2^{-1}\, 21 \equiv 1 \pmod 5$ $\quad M_3^{-1}\, 15 \equiv 1 \pmod 7$

$\Rightarrow M^{-1}\, 35 \equiv 1 \pmod{3}$ $\quad \Rightarrow M_2^{-1} = 1$ $\quad \Rightarrow M_3^{-1} = 1$

$\Rightarrow M^{-1} = 2$

$$x \equiv (2 \times 2 \times 35 + 3 \times 1 \times 21 + 2 \times 1 \times 15) \pmod{105}$$

$$x \equiv (140 + 63 + 30) \pmod{105}$$

$$x \equiv 233 \pmod{105}$$

$$x \equiv 23 \pmod{105}$$

the unique solution of set of Congruent equation is $x = 23$