Linear Congruences:-

An equation of the form $ax \equiv b \mod n$ is called a linear congruence and by a soln of $ax \equiv b \mod n$ means the integer x_0 satisfying $ax_0 \equiv b \mod n$.

Definition of congruence gives info that

$$\boxed{ax_0 \equiv b \mod n \text{ if and only if } n / ax_0 - b}$$

Or

$ax_0 \equiv b \mod n$ iff $ax_0 - b = ny_0$ for some $y_0 \in \mathbb{Z}$

Remark: ① $ax_0 \equiv b \mod n \Leftrightarrow ax_0 - b = ny_0 \Leftrightarrow ax_0 - ny_0 = b$

$\therefore$ solving linear congruence $ax \equiv b \mod n$ is equivalent to solving linear Diophantine equation
$ax - ny = b$.

Remark ② Treat two solutions of $ax \equiv b \mod n$, equal if they are congruent modulo n, even though they are not equal in the usual sense.

Ex: $3x \equiv 9 \mod 12$

$x = 3$ s.t $3(3) \equiv 9 \mod 12$

$x = -9$ s.t. $3(-9) \equiv 9 \mod 12$

$\therefore x = 3$ and $x = -9$ are two sol's.

but $-9 \equiv 3 \mod 12$

so $x = 3$ and $x = -9$ are equal under congruent modulo 12.

we refer to find the number of incongruent mod n solutions

Theorem: The linear congruence $ax \equiv b \bmod n$ has a solution if and only if d/b, where $d = \gcd(a,n)$.
If d/b, then it has d mutually incongruent solutions modulo n.

Proof:
$$ax \equiv b \bmod n$$
$$\Leftrightarrow ax - b = ny \text{ for some } y \in \mathbb{Z}$$
$$\Leftrightarrow ax - ny = b,\ y \in \mathbb{Z} \text{ which is linear diophantine equation.}$$
$$\Leftrightarrow \text{has a sol}^n \text{ iff } \gcd(a,n)/b \Leftrightarrow d/b.$$

Moreover if it is solvable and x_0, y_0 is one specific solution, then other solutions are

$$\left.\begin{aligned} x &= x_0 + \left(\frac{-n}{d}\right)t = x_0 - \frac{n}{d}t \\ y &= y_0 - \left(\frac{a}{d}\right)t \end{aligned}\right\} t \in \mathbb{Z}$$

Or $\boxed{x = x_0 + \frac{n}{d}t, \quad y = y_0 + \frac{a}{d}t}$ for some choice of t.

consider $t = 0, 1, 2, \ldots, d-1$

$\therefore$
$$x = x_0$$
$$x = x_0 + \frac{n}{d}$$
$$x = x_0 + \frac{2n}{d}$$
$$\ldots$$
$$x = x_0 + \frac{(d-1)n}{d}$$

claim: the integers
$$x_0,\ x_0 + \frac{n}{d},\ x_0 + \frac{2n}{d},\ \ldots,\ x_0 + \frac{(d-1)n}{d}$$
are incongruent modulo n and all others are congruent to some one of them.

If so, $x_0 + \frac{n}{d}t_1 \equiv x_0 + \frac{n}{d}t_2 \pmod n$
where $0 \le t_1 < t_2 \le d-1$ or $\boxed{0 < t_2 - t_1 < d-1}$ (1)

then $\frac{n}{d}t_1 \equiv \frac{n}{d}t_2 \pmod n$

since $\gcd\left(\frac{n}{d}, n\right) = \frac{n}{d}$

$$\Rightarrow t_1 \equiv t_2 \bmod \left(\frac{n}{n/d}\right)$$
$$\Rightarrow t_1 \equiv t_2 \bmod d \Rightarrow d / t_1 - t_2$$
$$\Rightarrow\Leftarrow \because (1) \text{ holds.}$$

Theorem: If $ca \equiv cb \bmod n$ then $a \equiv b \bmod \left(\frac{n}{d}\right)$ where $d = \gcd(c,n)$

$\therefore \forall\ 0 \le t_1 < t_2 \le d-1$, $\boxed{x_0 + \frac{n}{d}t_1 \not\equiv x_0 + \frac{n}{d}t_2}$ ✓

now only thing is to show that for $t \notin [0,1,2,\ldots,d-1]$ other solution $x = x_0 + \left(\frac{n}{d}\right)t$ is congruent modulo n to one of the d integers listed above.

by division algorithm,

$$t = qd + r, \quad 0 \le r \le d-1$$

$$\therefore x_0 + \frac{n}{d}t = x_0 + \frac{n}{d}[qd+r]$$

$$= x_0 + nq + \frac{n}{d}r$$

$$\boxed{x_0 + \frac{n}{d}t \equiv x_0 + \frac{n}{d}r \bmod n}$$

Since $x_0 + \frac{n}{d}r$, $0 \le r \le d-1$ is one of our d selected sol's

Note ① If x_0 is any solution of $ax \equiv b \pmod{n}$ then $d = \gcd(a,n)$ incongruent solutions are

$$x = x_0, \quad x_0 + \frac{n}{d}, \quad x_0 + \frac{2n}{d}, \ldots, \quad x_0 + (d-1)\frac{n}{d}$$

② If $\gcd(a,n) = 1 = d$ then $ax \equiv b \bmod n$ has unique solution modulo n. and this solution $x = x^*$ is sometimes called multiplicative inverse of a modulo n.

Example: $18x \equiv 30 \bmod 42$. ①

$\because \gcd(18,42) = 6$ and $6/30$ $\therefore$ ① has 6 incongruen sol's modulo 42.

by inspection, $x_0 = 4$,

other six solutions are

$$x \equiv 4 + \frac{42}{6}t \equiv 4 + 7t \bmod 42, \quad t = 0,1,2,3,4,5$$

$$\therefore x \equiv 4, 11, 18, 25, 32, 39 \pmod{42}$$