Linear Congruences

Saturday, January 24, 2026 8:19 PM

1] Linear Congruences:

$$ax \equiv b \pmod{n}$$

e.g. $3x \equiv 5 \pmod{11}$

Soln. $x \equiv 9 \pmod{11}$

2] Solving Linear Congruences:

$$ax \equiv b \pmod{n}$$

① if a has an inverse $(\bmod n)$, then

$$x \equiv b \cdot \bar{a}^{1} \pmod{n}$$

e.g. $3x \equiv 5 \pmod{11}$

$$\Rightarrow x \equiv 5 \cdot 3^{-1}$$
$$\equiv 5 \cdot 4 \equiv 20 \equiv 9 \pmod{11}$$

e.g. $4x \equiv 6 \pmod{13}$

$$\Rightarrow x \equiv 6 \cdot 4^{-1} \pmod{13}$$
$$\equiv 6 \cdot 10 \xrightarrow{\equiv} 6(-3) \equiv -18 \equiv 8 \pmod{13}$$
$$\equiv 60 \equiv 8 \pmod{13}$$

4(-3)
12 — 13
26
40 — 39
52

② What if a has no inverse?

In general,

If $\gcd(a, n) = d \geq 1$, then

if $d \mid b$ then x has d solutions (by simplification)

else no solution.

e.g. $d = 1 \Rightarrow a$ has a inverse (see Part ①)

e.g. $d = 2$:

$$4x \equiv 6 \pmod{10} \Rightarrow \gcd(4,10) = d = 2 \mid 6$$
$$\Rightarrow 2 \text{ solutions}$$

Simplify (divide by $d = 2$)

$$\Rightarrow 2x \equiv 3 \pmod 5 \Rightarrow \gcd = 1$$

$$\Rightarrow x \equiv 3 \cdot 2^{-1} \pmod 5$$
$$\equiv 3 \cdot 3 \equiv 9 \equiv 4 \pmod 5$$

$$\therefore x \equiv 4, \ 4+5 = 9 \pmod{10}$$

3] e.g.

① $10x \equiv 2 \pmod{15}$

Soln. $d = \gcd(10, 15 = 5 \nmid 2 \Rightarrow$ No solution

② $18x \equiv 15 \pmod{24}$

Simplify: Can we div. by $\Rightarrow$ No solution

Can we div by 3? Yes, but it is useless

$$\Rightarrow 6x \equiv 5 \pmod 8$$

6 has no inverse modulo 8

③ $30x \equiv 45 \pmod{75}$

div. by $d = 5$ ✗ $\Rightarrow 6x \equiv 9 \pmod{15}$

$\Rightarrow$ Simplify again? not a good idea!

how many soln?

div. by $d = \gcd(30, 75) = 15$

$\Rightarrow 2x \equiv 3 \pmod 5$ $\Rightarrow$ we have 15 solutions

$\Rightarrow x \equiv 3 \cdot 2^{-1} \pmod 5$

$\equiv 3 \cdot 3 \equiv 9 \equiv 4 \pmod 5$

$\therefore x \equiv 4, \quad 4+5 = 9,$

$4 + 2 \cdot 5 = 14,$

$4 + 3 \cdot 5 = 19,$

$4 + 4 \cdot 5 = 24,$

$\vdots$

$4 + k \cdot 5$. for $k = 0 \cdots (d-1) = 0 \cdots 14$

4] Solving a system of linear Congruences

Given $\underset{(n \times n)}{A} \cdot \underset{(n \times 1)}{X} = \underset{(n \times 1)}{B} \pmod n$

Sol^n : $\underset{(n \times 1)}{X} = \underset{(n \times n)}{A^{-1}} \cdot \underset{(n \times 1)}{B}$