Linear Congruence

Monday, September 15, 2025 9:01 AM

Recall: Modular Arithmetic

Missing

100 # 1, 5, 6, 7, 10, 14, 15, 17, sec 2

Ex # 217 on 9/8

Soln # 3, 6, 11, 14, 19, 29

1] E.g- **a.** Add 17 to 27 in Z_{14}.
b. Subtract 43 from 12 in Z_{13}.
c. Multiply 123 by −10 in Z_{19}.

Soln

a) $17 + 27 \pmod{14}$

$\equiv 7 + (-1)$

$\equiv 2 \pmod{14}$

b) $12 - 43 \pmod{13}$

$\equiv (-1) - (+1)$

$\equiv -5$

$\equiv 8 \pmod{13}$

c) $123 \cdot (-10) \pmod{19}$

$\equiv 9 \cdot 9$

$\equiv 81$

$\equiv 5 \pmod{19}$

2] Finding Multiplicative Inverse $a^{-1} \pmod{n}$

a has a multiplicative inverse iff $\gcd(a, n) = 1$

by EEA, $1 = s \cdot n + t \cdot a$

$\Rightarrow 1 \equiv t \cdot a \pmod{n}$

$\therefore a^{-1} \equiv t \pmod{n}$ in $\mathbb{Z}_n$

3] e.g. Find $11^{-1} \pmod{26}$

$26 = 2 \cdot 11 + 4$ — (1)

$11 = 2 \cdot 4 + 3$ — (2)

$4 = 1 \cdot 3 + 1$ — (3) ← gcd

by (3)

$1 = 4 - 1 \cdot 3$

$= 4 - 1(11 - 2 \cdot 4)$

$= -1 \cdot 11 + 3 \cdot 4$

$= -1 \cdot 11 + 3(26 - 2 \cdot 11)$

$= 3 \cdot 26 - 7 \cdot 11$

$\therefore \quad \gcd = 1 = 3 \cdot 26 + (-7) \cdot 11$

$\Rightarrow 1 = 3 \cdot 26 - 7 \cdot 11 \pmod{26}$

$\Rightarrow 1 = (-7) \cdot 11$

$\therefore 11^{-1} \equiv (-7) \equiv 19 \pmod{26}$

4] e.g. Find $23^{-1} \pmod{100}$

$100 = 4 \cdot 23 + 8$

$23 = 2 \cdot 8 + 7$

$8 = 1 \cdot 7 + 1$ ← gcd

$1 = 8 - 1 \cdot 7$

$= 8 - 1(23 - 2 \cdot 8)$

$= -1 \cdot 23 + 3 \cdot 8$

$= -1 \cdot 23 + 3(100 - 4 \cdot 23)$

$= 3 \cdot 100 - 13 \cdot 23$

$\therefore 23^{-1} \equiv -13 \equiv 87 \pmod{100}$

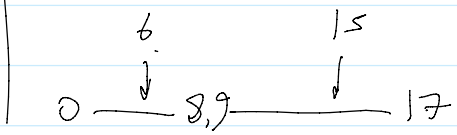
5] Solving Linear congruences (See slides p02)

$ax \equiv b \pmod{n}$

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

e.g. Solve:

$$14x \equiv 12 \pmod{18}$$



Soln.

Since 14 has no inverse in mod 18, simplify it.

Simplify: divide by $\gcd(14, 18) = 2$

<u>div by 2:</u> $7x \equiv 6 \pmod{9}$

$$x \equiv 6 \cdot 7^{-1}$$

$$\equiv 6 \cdot 4 \equiv 6 \quad (9) \implies 6, 15, 24, \ldots$$

$$\therefore x \equiv 6, 15 \pmod{18}$$

6] Examples:

$$3x + 4 \equiv 6 \pmod{13}$$

Soln

$$3x \equiv 2 \pmod{13}$$

$$\implies x \equiv 2 \cdot 3^{-1}$$

$$\equiv 2 \cdot (-4)$$

$$\equiv -8 \equiv 5 \quad (13)$$

$$= 2 \cdot 9 \equiv 18$$

$$\equiv 5 \quad (13)$$

7] e.g.

Solve the set of following three equations:

$$3x + 5y + 7z \equiv 3 \pmod{16}$$
$$x + 4y + 13z \equiv 5 \pmod{16}$$
$$2x + 7y + 3z \equiv 4 \pmod{16}$$

Soln

$$\begin{bmatrix} 3 & 5 & 7 \\ 1 & 4 & 13 \\ 2 & 7 & 3 \end{bmatrix} \cdot \begin{bmatrix} x \\ y \\ z \end{bmatrix} = \begin{bmatrix} 3 \\ 5 \\ 4 \end{bmatrix} \checkmark \pmod{16}$$

$$A \cdot X = B$$

$$\Rightarrow X = A^{-1} \cdot B \pmod{16}$$

$$\Rightarrow X = \begin{bmatrix} 15 \\ 4 \\ 14 \end{bmatrix} \Rightarrow$$

Solution

$x \equiv 15 \pmod{16}$,
$y \equiv 4 \pmod{16}$,
$z \equiv 14 \pmod{16}$.

To verify

$$\begin{bmatrix} 3 & 5 & 7 \\ 1 & 4 & 13 \\ 2 & 7 & 3 \end{bmatrix} \cdot \begin{bmatrix} 15 \\ 4 \\ 14 \end{bmatrix} = \begin{bmatrix} -3 & +4 & +2 \end{bmatrix} = \begin{bmatrix} 3 \\ 5 \checkmark \\ 5 \checkmark \end{bmatrix} \pmod{16}$$

(HW)

3×3 $\quad$ 3×1