

Recall: Extended Euclidean Algorithm

Missing:

500 # 5, 8, 13

~~+B#12~~1] Exer: $63^{-1} \pmod{101}$

$$\equiv 106$$

$$\equiv 93 \equiv -8$$

$$\equiv 8 \quad \checkmark$$

$$101 = 1 \cdot 63 + 38$$

$$63 = 1 \cdot 38 + 25$$

$$38 = 1 \cdot 25 + 13$$

$$25 = 1 \cdot 13 + 12$$

$$13 = 1 \cdot 12 + 1 \leftarrow \text{gcd}$$

$$1 = 13 - 1 \cdot 12$$

$$= 13 - 1(25 - 1 \cdot 13)$$

$$= -1 \cdot 25 + 2 \cdot 13$$

$$= -1 \cdot 25 + 2(38 - 1 \cdot 25)$$

$$= +2 \cdot 38 - 3 \cdot 25$$

$$= +2 \cdot 38 - 3(63 - 1 \cdot 38)$$

$$= -3 \cdot 63 + 5 \cdot 38$$

$$= -3 \cdot 63 + 5(101 - 1 \cdot 63)$$

$$= +5 \cdot 101 - 8 \cdot 63$$

$$\therefore 63^{-1} = -8 \equiv 93 \pmod{101}$$

2] Solving Linear Congruences (See Slide P03)

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

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

e.g. $63x \equiv 2 \pmod{101}$

$$\Rightarrow x \equiv 2 \cdot 63^{-1}$$

$$\equiv 2 \cdot 93$$

$$\equiv 2(-8)$$

$$\equiv -16 \equiv 85 \pmod{101}$$

3] What if a has no inverse (modulo n)?

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

check if $d = \gcd(a, n) \mid b$ then simplify
and we get d solutions

e.g. $14x \equiv 12 \pmod{18}$

Solⁿ. $\gcd(14, 18) = 2$

Simplify by 2

$$\Rightarrow 7x \equiv 6 \pmod{9}$$

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

$$\equiv 6 \cdot 4 \equiv 6 \pmod{9}$$

$$4 \cdot 7 \equiv 28 \equiv 1 \pmod{9}$$

$$\therefore x \equiv 6, 6 + 9 = 15 \pmod{18}$$

$$\left[\begin{array}{r} 6 \overline{) 17} \\ \underline{18} \\ 17 \end{array} \right]$$

4] Exer.

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

$$\Rightarrow 3x \equiv 6 - 4 \equiv 2 \pmod{13}$$

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

$$\equiv 2(-4) \equiv -8 \equiv \pmod{13}$$

13

26

39

:

5]

Example 2.38

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.

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

$$A \cdot X \equiv B \pmod{16}$$

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

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

$$\Rightarrow X = \begin{bmatrix} 15 \\ 4 \\ 14 \end{bmatrix} \Rightarrow \begin{aligned} x &\equiv 15 \pmod{16} \\ y &= 4 \pmod{16} \\ z &= 14 \pmod{16} \end{aligned}$$

To verify:

$$\begin{bmatrix} 3 & 5 & 7 \\ 1 & 4 & 13 \\ 2 & 7 & 3 \end{bmatrix} \cdot \begin{bmatrix} 15 \\ 4 \\ 14 \end{bmatrix} = \begin{bmatrix} -3+4-41 \\ \\ \end{bmatrix} = \begin{bmatrix} 3 \\ \\ \end{bmatrix} \pmod{16}$$

6] Divisibility:

by 3: Add the digits

$$\begin{aligned} 1245 &= 1 \cdot 10^3 + 2 \cdot 10^2 + 4 \cdot 10^1 + 5 \\ &\equiv 1 \cdot (1)^3 + 2 \cdot 1^2 + 4 \cdot 1 + 5 \pmod{3} \\ &\equiv 1 + 2 + 4 + 5 \\ &= 12 \equiv 1+2 \equiv 0 \pmod{3} \end{aligned}$$

by 9: Add the digits

$$\begin{aligned} 1245 &= 1 \cdot 10^3 + 2 \cdot 10^2 + 4 \cdot 10^1 + 5 \\ &\equiv 1 \cdot (1)^3 + 2 \cdot 1^2 + 4 \cdot 1 + 5 \pmod{9} \\ &\equiv 1 + 2 + 4 + 5 \\ &= 12 \equiv 1+2 \equiv 3 \pmod{9} \end{aligned}$$

by 4: take last

$$\begin{aligned} 1245 &\equiv 1 \cdot 10^3 + 2 \cdot 10^2 + 45 \\ &\equiv 0 + 0 + 45 \\ &\equiv 1 \pmod{4} \end{aligned}$$