MAT2440, Classwork41, Spring2025

ID:______________________________ Name:______________________________

1. Solve for $ax \equiv 1 (\text{mod } m)$ in General.

   Step1. Use the Euclidean Algorithm to show $\gcd(a, m) = 1$.

   Step2. Reverse the steps to find Bézout coefficient s, t, such that

$$s \cdot a + t \cdot m = \gcd(a, m) = 1.$$

   Step3. Then s is the **inverse of *a* modulo *m***:

Since $s \cdot a + t \cdot m \equiv 1 \text{ mod } m$

$sa \ (\text{mod } m) + \underbrace{tm \ (\text{mod } m)}_{} \overset{\text{"}0\text{"}}{} \equiv 1 \ (\text{mod } m)$

$\Rightarrow sa \ (\text{mod } m) \equiv 1 \ (\text{mod } m)$

$\Rightarrow sa \equiv 1 \ (\text{mod } m) \Rightarrow s$ is the inverse of a modulo m.

2. Find an inverse of 7 modulo 32. (That is, solve $7x \equiv 1 (\text{mod } 32)$)

Sol: Step1 (by Euclidean Algorithm)

$\gcd(7, 32) = \gcd(7, \underline{32 \text{ mod } 7})$ | $32 = 4 \times 7 + 4$

$= \gcd(7, 4)$

$= \gcd(\underline{7 \text{ mod } 4}, 4)$ | $7 = 4 \times 1 + 3$

$= \gcd(3, 4)$

$= \gcd(3, \underline{4 \text{ mod } 3})$ | $4 = 3 \times 1 + 1$

$= \gcd(3, 1) = 1$

Step2:

$\boxed{1} = 4 - \underline{3} \times 1 = 4 - (7 - 4 \times 1) \times 1 = 4 - 7 \times 1 + 4 \times 1$

$= 4 \times 2 - 7 \times 1 = (32 - 4 \times 7) \times 2 - 7 \times 1$

$4 = 32 - 4 \times 7$

$= 32 \times 2 - 8 \times 7 - 7 \times 1 = \boxed{32 \times 2 - 9 \times 7}$

$\Rightarrow 1 = \underset{s}{(-9)} \times \underset{a}{7} + \underset{t}{2} \times \underset{m}{32}$

Step 3. the inverse of 7 modulo 32 is -9

$-9+32=23$

$$\begin{array}{r} 32 \\ \times\ 5 \\ \hline 160 \end{array}$$

$\underline{\underline{-9}}\times 7 = -63 \pmod{32} = 1$

$23\times 7 = 161 \pmod{32} = 1$

$$\begin{array}{r} 161 \\ -160 \\ \hline 1 \end{array}$$

Either -9 or 23 will work,

In fact, $s = -9 + n\cdot 32$ or $s \equiv -9 \pmod{32}$

3. Find an inverse of 22 modulo 41. (That is, solve $22x \equiv 1 \pmod{41}$)

Step1: $\gcd(22,41) = \gcd(22, 41 \bmod 22)$ | $41 = 1 \times 22 + 19$ — ①

$= \gcd(22, 19) = \gcd(22 \bmod 19, 19)$ | $22 = 1 \times 19 + 3$ — ②

$= \gcd(3, 19) = \gcd(3, 19 \bmod 3)$ | $19 = 6 \times 3 + 1$ — ③

$= \gcd(3, 1) = 1$

from ② $3 = 22 - 1 \times 19$

step2: from ③ $1 = 19 - 6 \times 3 = 19 - 6 \times (22 - 1 \times 19) = 19 - 6 \times 22 + 6 \times 19$

$= 7 \times 19 - 6 \times 22$

from ① $41 - 1 \times 22 = 19$

$= 7 \times (41 - 1 \times 22) - 6 \times 22$

$= (-13) \times 22 + 7 \times 41$

$\underset{s}{(-13)} \times \underset{a}{22} + \underset{t}{7} \times \underset{m}{41}$

$\Rightarrow$ (-13) is the inverse of 22 modulo 41.

4. Solve Linear Congruences $ax \equiv b \pmod{m}$:

(a) Solve $7x \equiv 5 \pmod{32}$

① Find the inverse of 7 modulo 32 (solve $7\bar{a} \equiv 1 \pmod{32}$)

from Q2. $\bar{a} = -9$.

② Then solve $7x \equiv 5 \bmod 32$

$\underbrace{-9 \cdot 7}_{1 \pmod{32}} x \equiv -9 \cdot 5 \pmod{32}$

$1x \equiv -45 \pmod{32} \Rightarrow x \equiv 19 \pmod{32}$

(b) Solve $22x \equiv 3 \pmod{41}$

① Find the inverse of 22 mod 41 (solve $22\bar{a} \equiv 1 \pmod{41}$)

$\bar{a} = -13$

② Then solve $22x \equiv 3 \pmod{41}$

$\underbrace{-13 \cdot 22}_{1} x \equiv -13 \cdot 3 \pmod{41}$

$\Rightarrow 1x \equiv -39 \pmod{41}$

$\Rightarrow x \equiv 2 \pmod{41}$