TUTORIAL 6 SOLUTIONS

1) Bezout coefficients of a, m = integers s, t : $as + mt = \gcd(a, m)$

a) $a = 34$, $m = 55$

$55 = 34 \cdot 1 + 21$ — $1 = 3 + 2 \cdot (-1)$

$34 = 21 \cdot 1 + 13$ — $= 3 + (5 - 3 \cdot 1)(-1) = 5 \cdot (-1) + 3 \cdot 2$

$21 = 13 \cdot 1 + 8$ — $= 5 \cdot (-1) + (8 - 5 \cdot 1) \cdot 2 = 8 \cdot 2 + 5 \cdot (-3)$

$13 = 8 \cdot 1 + 5$ — $= 8 \cdot 2 + (13 - 8 \cdot 1) \cdot (-3) = 13 \cdot (-3) + 8 \cdot 5$

$8 = 5 \cdot 1 + 3$ — $= 13 \cdot (-3) + (21 - 13 \cdot 1) \cdot 5 = 21 \cdot 5 + 13 \cdot (-8)$

$5 = 3 \cdot 1 + 2$ — $= 21 \cdot 5 + (34 - 21 \cdot 1)(-8) = 34 \cdot (-8) + 21 \cdot 13$

$3 = 2 \cdot 1 + 1$ — $= 34 \cdot (-8) + (55 - 34 \cdot 1) \cdot 13 = 55 \cdot 13 + 34 \cdot (-21)$

$2 = 1 \cdot 2 + 0$ — (b·t, a·s)

$\therefore 34 \cdot (-21) + 55 \cdot 13 = 1$

(b) $a = 117$, $m = 213$

$213 = 117 \cdot 1 + 96$ — $3 = 12 + 9 \cdot (-1)$

$117 = 96 \cdot 1 + 21$ — $= 12 + (21 - 12 \cdot 1) \cdot (-1) = 21 \cdot (-1) + 12 \cdot 2$

$96 = 21 \cdot 4 + 12$ — $= 21 \cdot (-1) + (96 - 21 \cdot 4) \cdot 2 = 96 \cdot 2 + 21 \cdot (-9)$

$21 = 12 \cdot 1 + 9$ — $= 96 \cdot 2 + (117 - 96 \cdot 1) \cdot (-9) = 117 \cdot (-9) + 96 \cdot 11$

$12 = 9 \cdot 1 + 3$ — $= 117 \cdot (-9) + (213 - 117 \cdot 1) \cdot 11 = 213 \cdot 11 + 117 \cdot (-20)$

$9 = 3 \cdot 3 + 0$

$\therefore 117 \cdot (-20) + 213 \cdot 11 = 3$

c) $a = 3454,\ b = 4666$

$4666 = 3454 \cdot 1 + 1212$

$3454 = 1212 \cdot 2 + 1030$

$1212 = 1030 \cdot 1 + 182$

$1030 = 182 \cdot 5 + 120$

$182 = 120 \cdot 1 + 62$

$120 = 62 \cdot 1 + 58$

$62 = 58 \cdot 1 + 4$

$58 = 4 \cdot 14 + 2$

$4 = 2 \cdot 2 + 0$

$2 = 58 + 4 \cdot (-14)$

$= 58 + (62 - 58 \cdot 1) \cdot (-14)$

$= 62 \cdot (-14) + 58 \cdot 15$

$= \dots$

$= 4666 \cdot (-835) + 3454 \cdot 1128$

m . t a . s

Conclusion :

$4666 \cdot (-835) + 3454 \cdot 1128 = 2$

2) a) $34x \equiv 3 \pmod{55}$ (1)

$\gcd(34, 55) = 1 \mid 3$. By 1a

$34 \cdot (-21) + 55 \cdot 13 = 1 \xrightarrow{\%55} 34 \cdot (-21) \equiv 1 \pmod{55}$

$34^{-1} \bmod 55 = -21 \bmod 55 = 34$

Multiply both sides of (1) by $34 = 34^{-1} \bmod 55$:

$x \equiv 3 \cdot 34 = 102 \pmod{55} \Rightarrow x \equiv 47 \pmod{55}$

Equivalently, $x = 47 + 55k$ for any $k \in \mathbb{Z}$.

b) $117x \equiv 5 \pmod{213}$

$\gcd(117, 213) = \gcd(3^2 \cdot 13, 3 \cdot 71) = 3 \nmid 5 \rightarrow$ no solution.

c) $3454x \equiv 2 \pmod{4666}$: $\gcd(3454, 4666) = 2 \mid 2$.

Divide all terms by 2:

$1727x \equiv 1 \pmod{2333}$ (2)

By 1c:

$3454 \cdot 1128 + 4666 \cdot (-835) = 2$

$\div 2$

$1727 \cdot 1128 + 2333 \cdot (-835) = 1 \Rightarrow 1727^{-1} \bmod 2333 = 1128$

Multiply both sides of (2) by 1128:

$x \equiv 1128 \pmod{2333}$

3) $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$

a) How many $x \in \mathbb{Z}_{93} = \{0, 1, \ldots, 92\}$ satisfy

$$36x \equiv 9 \pmod{93}$$

$\gcd(36, 93) = 3 \mid 9$. Divide all terms by 3:

$$12x \equiv 3 \pmod{31} \quad (*)$$

$31 = 12 \cdot 2 + 7$

$12 = 7 \cdot 1 + 5$

$7 = 5 \cdot 1 + 2$

$5 = 2 \cdot 2 + 1$

$2 = 1 \cdot 2 + 0$

$1 = 5 + 2 \cdot (-2)$

$= 5 + (7 - 5 \cdot 1) \cdot (-2) = 7 \cdot (-2) + 5 \cdot 3$

$= 7 \cdot (-2) + (12 - 7) \cdot 3 = 12 \cdot 3 + 7 \cdot (-5)$

$= 12 \cdot 3 + (31 - 12 \cdot 2) \cdot (-5) = 31 \cdot (-5) + 12 \cdot 13$

$12^{-1} \bmod 31 = 13$

Multiply $(*)$ by 13: $x \equiv 39 \pmod{31} \Leftrightarrow x \equiv 8 \pmod{31}$

Hence $x = 8 + 31k$. For $x \in \{0, 1, \ldots, 92\}$, we have $k = 0, 1, 2$:

$$x \in \{\underbrace{8 + 31 \cdot 0}_{(8)}, \underbrace{8 + 31 \cdot 1}_{(39)}, \underbrace{8 + 31 \cdot 2}_{(70)}\}$$

$\therefore$ There are 3 possible values of x in $\{0, \ldots, 92\}$.

(b) Given $d = \gcd(a, m) \mid b$.

How many solutions $x \in \mathbb{Z}_m = \{0, 1, \ldots, m-1\}$:

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

Write $a = da_1$, $b = db_1$, $m = dm_1$. Divide all terms by d:

$$a_1 x \equiv b_1 \pmod{m_1}$$

$$x \equiv b_1 a_1^{-1} \pmod{m_1} \Leftrightarrow x \equiv c \pmod{m_1},$$

where $c = b_1 a_1^{-1} \bmod m_1 \in \{0, 1, \ldots, m_1 - 1\}$. Equivalently

$$x = c + k m_1 \text{ for any } k \in \mathbb{Z}$$

For $x \in \{0, 1, \ldots, dm_1 - 1\}$, we have $k \in \{0, 1, \ldots, d-1\}$

$$x \in \{c, c + m_1, \ldots, c + (d-1) m_1\}$$

$\therefore$ There are $d = \gcd(a, m)$ solutions in $\mathbb{Z}_m = \{0, \ldots, m-1\}$.

c) Find # solutions $x \in \mathbb{Z}_m$ to $ax \equiv b \pmod{m}$:

(i) $25x \equiv 2 \pmod{15}$: $\gcd(25, 15) = 5 \nmid 2$ → no solution

(ii) $25x \equiv 10 \pmod{15}$: $\gcd(25, 15) = 5 \mid 10$

$\therefore$ 5 solutions.

(iii) $55x \equiv 121 \pmod{187}$: $\gcd(55, 187) = 11 \mid 121$.

$\therefore$ 11 solutions.

4) Solve $\begin{cases} 2x \equiv 5 \pmod 9 & (1) \\ 16x \equiv 6 \pmod{70} & (2) \end{cases}$

$2 \cdot 1 = 2,\ 2 \cdot 2 = 4,\ 2 \cdot 3 = 6$
$2 \cdot 4 = 8,\ 2 \cdot 5 = 10 \equiv 1 \pmod 9$

Multiply both sides of (1) by $2^{-1} \bmod 9 = 5$:

$$x \equiv 25 \pmod 9 \equiv 7 \pmod 9$$

$$x = 7 + 9y \text{ for } y \in \mathbb{Z} \quad (*)$$

Divide all terms of (2) by 2: $8x \equiv 3 \pmod{35}$

$$8(7+9y) \equiv 3 \pmod{35} \quad (\text{by } (*))$$

$$56 + 72y \equiv 3 \pmod{35}$$

$$72y \equiv -53 \pmod{35} \quad (\%\,35)$$

$$2y \equiv 17 \pmod{35}$$

$2 \cdot 18 \equiv 1 \pmod{35}$

Multiply both sides by $2^{-1} \bmod 35 = 18$:

$$y \equiv 306 \pmod{35} \equiv 26 \pmod{35}$$

$$y = 26 + 35k \text{ for any } k \in \mathbb{Z} \quad (**)$$

By (*) and (**):

$$x = 7 + 9(26 + 35k) = 241 + 315k \text{ for any } k \in \mathbb{Z}$$

Equivalently $x \equiv 241 \pmod{315}$.