Tugas Pertemuan 3
Georgia Sugisandhea - 535230080

Kongruensi

4. $2x \equiv 7 \pmod{17}$

Inverse dari 2 modulo 17

$17 = 8 \cdot 2 + 1$ $\rightarrow$ extended euclidian: $1 = 17 - 8 \cdot 2$

$2 = 2 \cdot 1 + 0$ maka inverse dari 2 modulo 17 adalah $-8, 9, 26, \cdots$

$\bar{a} \, a \equiv 1 \pmod{m}$ $\rightarrow$ maka solusi dari $2x \equiv 7 \pmod{17}$

$-8 \cdot 2 \equiv 1 \pmod{17}$ $= 2x \equiv 7 \pmod{17}$

$-16 \equiv 1 \pmod{17}$ $-8 \cdot 2x \equiv -8 \cdot 7 \pmod{17}$

$-16 \bmod 17 \equiv 1 \bmod 17$ $1x \equiv -56 \pmod{17}$

$1 \equiv 1$

$x \bmod 17 \equiv -56 \bmod 17$

$x \bmod 17 \equiv 12$

$x \equiv 12 \pmod{17}$

untuk $x = 12$ maka $2 \cdot 12 = 24 \equiv 7 \pmod{17}$

5. $x \equiv 2 \pmod{3}$ $\rightarrow m = 3 \cdot 4 \cdot 5 = 60$

$x \equiv 1 \pmod{4}$ $M_1 = \dfrac{60}{3} = 20 , M_2 = \dfrac{60}{4} = 15 , M_3 = \dfrac{60}{5} = 12$

$x \equiv 3 \pmod{5}$

$M_1 = 20 \equiv (2 \bmod 3)$ $\rightarrow$ inverse dari 20 mod 3

$20 = 6 \cdot 3 + 2$ $\rightarrow$ extended euclidian $= 2 = 20 - 6 \cdot 3$

$3 = 1 \cdot 2 + 1$ $1 = 3 - 1 \cdot 2$

$2 = 1 \cdot 1 + 1$

$\begin{bmatrix} & & \\ -3 & 0 & 1 \end{bmatrix}$ $[\bar{2}]$ $\begin{bmatrix} 2 & 1 & 1 \\ \frac{3}{2} & 0 & \frac{1}{2} \end{bmatrix}$

$$1 = 3 - 1 \cdot (20 - 6 \cdot 3$$
$$1 = 3 - 1 \cdot 20 + 6 \cdot 3$$
$$1 = 7 \cdot 3 \; \boxed{-1} \; 20$$

maka inverse dari $20 \bmod 3 = -1 + 3 = 2$

$M_2 = 15 \equiv 1 \pmod 4 \to$ inverse dari $15 \bmod 4$

$$15 = 3 \cdot 4 + 3 \qquad \to \text{extended euclidian} =$$
$$4 = 1 \cdot 3 + 1 \qquad\qquad 3 = 15 - 3 \cdot 4$$
$$3 = 3 \cdot 1 + 0 \qquad\qquad 1 = 4 - 1 \cdot 3$$
$$1 = 4 - 1(15 - 3 \cdot 4)$$
$$1 = 4 - 1 \cdot 15 + 3 \cdot 4$$
$$1 = 4 \cdot 4 \; \boxed{-1} \; 15$$

maka inverse dari $15 \bmod 4 = -1 + 4 = 3$

$M_3 = 12 \equiv 3 \pmod 5 \to$ inverse dari $12 \bmod 5$

$$12 = 2 \cdot 5 + 2 \qquad \to 2 = 12 - 2 \cdot 5$$
$$5 = 2 \cdot 2 + 1 \qquad\qquad 1 = 5 - 2 \cdot 2$$
$$2 = 2 \cdot 1 + 0 \qquad\qquad 1 = 5 - 2(12 - 2 \cdot 5)$$
$$1 = 5 - 2 \cdot 12 + 4 \cdot 5$$
$$1 = 5 \cdot 5 \; \boxed{-2} \; 12$$

maka inverse dari $12 \bmod 5 = -2 + 5 = 3$

$$= a_1 \cdot M_1 \cdot Y_1 + a_2 \, M_2 \, V_2 + a_3 \, M_3 \, Y_3$$
$$= 2 \cdot 20 \cdot 2 + 1 \cdot 15 \cdot 3 + 3 \cdot 12 \cdot 3$$
$$= 233 \equiv 53 \pmod{60}$$

Jadi $x = 53$

6. $23^{1002} \bmod 41 = 23^{41-1} = 23^{40} \equiv 1 \pmod{41}$

$$\rightsquigarrow 1002 = 40 \cdot 25 + 2$$
$$23^{1002} = 23^{40 \cdot 25 + 2} = \left(23^{40}\right)^{25} \cdot 23^2$$

$\left(23^{40}\right)^{25} \cdot 23^2 \bmod 41 = \left(\left(\left(23^{40}\right)^{25} \bmod 41\right)(23^2 \bmod 41)\right) \bmod 41$
$$= \left(1^{25} \cdot 529\right) \bmod 41 = 37$$

Jadi $23^{1002} \bmod 41 = 37$