

i)  $77x \equiv 1 \pmod{5}$

ii)  $55x \equiv 1 \pmod{7}$

iii)  $35x \equiv 1 \pmod{11}$

i)  $77x \equiv \overset{b}{1} \pmod{5}$

$\text{HCD}(77, 5) = 1$

$$\left. \begin{array}{l} 77 = 5 \cdot 15 + 2 \\ 5 = 2 \cdot 2 + 1 \\ 2 = 1 \cdot 2 + 0 \end{array} \right\}$$

$$\begin{aligned} 1 &= 5 + (-2) \cdot 2 = 5 + (-2)(77 + (-15) \cdot 5) = \\ &= \underline{(-2)} \cdot 77 + (31) \cdot 5 \end{aligned}$$

$S = b \cdot u = 1 \cdot (-2) = -2 \equiv 3 \pmod{5}$

ii)  $55x \equiv \textcircled{1} \pmod{7}$

$\text{HCD}(7, 55) = 1$

$$\left. \begin{array}{l} 55 = \textcircled{7} \cdot 7 + 6 \\ 7 = \textcircled{6} \cdot 1 + 1 \\ 6 = 1 \cdot 6 + 0 \end{array} \right\}$$

$$\begin{aligned} 1 &= 7 + (-1) \cdot 6 = 7 + (-1)(55 + (-7) \cdot 7) = \\ &= \textcircled{(-1)} 55 + 8 \cdot 7 \end{aligned}$$

$S_2 = 1 \cdot (-1) = -1 \equiv 6 \pmod{7}$

iii)  $35x \equiv \underline{1} \pmod{11}$

$\text{HCD}(35, 11) = 1$

$$\left. \begin{array}{l} 35 = 11 \cdot 3 + 2 \\ 11 = 2 \cdot 5 + 1 \\ 2 = 1 \cdot 2 + 0 \end{array} \right\}$$

$$\begin{aligned} 1 &= 11 + (-5) \cdot 2 = 11 + (-5)(35 + (-3) \cdot 11) = \\ &= 11 + (-5) \cdot 35 + (15) \cdot 11 = \\ &= (16) \cdot 11 + \underline{(-5)} \cdot 35 \end{aligned}$$

$S_3 = (-5) \cdot 1 = -5 \equiv 6 \pmod{11}$

## ESERCIZIO

$$\begin{cases} X \equiv 3 \pmod{5} \\ X \equiv 3 \pmod{7} \\ X \equiv 9 \pmod{11} \end{cases}$$

1) Risolvo  $X \equiv 3 \pmod{5} \rightarrow X = 3 + 5k, k \in \mathbb{Z}$

2) Sostituisco nella seconda:

$$3 + 5k \equiv 3 \pmod{7} \Rightarrow 5k \equiv 3 - 3 \pmod{7}$$

$$5k \equiv 0 \pmod{7} \Rightarrow k = 0$$

3) k nella prima mi dà  $X = 3 \Rightarrow S = [3]_{35}$  "soluzione parziale"

$$\Rightarrow \text{Solvo } X \in S \Rightarrow X = 3 + 35 \cdot t, t \in \mathbb{Z}$$

4) Sostituisco nella III

$$3 + 35t \equiv 9 \pmod{11}$$

$$35t \equiv 6 \pmod{11}$$

$$2t \equiv 6 \pmod{11} \quad (\text{perché } 35 \equiv 2 \pmod{11})$$

$$\begin{cases} 35 \equiv 2 \pmod{11} \\ 35t \equiv 2t \pmod{11} \end{cases} \quad \text{lemma}$$

$$\left. \begin{array}{l} 11 = 2 \cdot 5 + 1 \\ 2 = 1 \cdot 2 + 0 \end{array} \right\} 1 = 11 + (-5)2$$

$$\Rightarrow t = (-5) \cdot 6 = -30 \equiv 3 \pmod{11} \quad (\text{perché } -30 + 3 \cdot 11 = 3)$$

5) Sostituisco:  $X = 3 + 35 \cdot 3 = 108$

$$S = [108]_{385}$$

## ESERCITAZIONE

①  $25x \equiv 24 \pmod{16}$

$$\text{HCD}(25, 16) = 1$$

$$\begin{cases} 25 = 16 \cdot 1 + 9 \\ 16 = 9 \cdot 1 + 7 \\ 9 = 7 \cdot 1 + 2 \\ 7 = 2 \cdot 3 + 1 \\ 2 = 1 \cdot 2 + 0 \end{cases}$$

$$1 = 7 - 2 \cdot 3 = 7 - (9 - 7) \cdot 3 = 7 + (-3)9 + 3 \cdot 7 = 4 \cdot 7 + (-3)9$$

$(a-b)c = ac - bc = 9 \cdot 3 - 7 \cdot 3$   
 $-(9 \cdot 3 - 7 \cdot 3) = -9 \cdot 3 + 7 \cdot 3 = (-3)9 + (3)7$

$$= 4(16 - 9) + (-3)9 =$$

$$= 4 \cdot 16 + (-4)9 + (-3)9 = 4 \cdot 16 + (-7)9$$

$$= 4 \cdot 16 + (-7)(25 - 16) =$$

$$= 4 \cdot 16 + (-7)25 + (+7)16 = 11 \cdot 16 + (-7)25$$

$$S = (-7) \cdot 24 = -168 \equiv 8 \pmod{16}$$

$$S = [8]_{16}$$

(b)  $20x \equiv 30 \pmod{26}$

(f)  $24x \equiv 8 \pmod{9}$

$\text{HCD}(20, 26) = 2$  perché  $2 \mid 30$ , l'equazione <sup>(b)</sup> ha soluzione

$\text{gcd}(20, 26) = 2$  perché  $2 \mid 30$ , l'equazione ha soluzione

$\text{gcd}(24, 9) = 3$  perché  $3 \nmid 8$ , l'equazione (P) non ha soluzione

(b)  $10x \equiv 15 \pmod{13}$   $\text{gcd}(13, 10) = 1$

$$\begin{array}{l} 13 = 10 \cdot 1 + 3 \\ 10 = 3 \cdot 3 + 1 \\ 3 = 1 \cdot 3 + 0 \end{array} \left. \vphantom{\begin{array}{l} 13 = 10 \cdot 1 + 3 \\ 10 = 3 \cdot 3 + 1 \\ 3 = 1 \cdot 3 + 0 \end{array}} \right\} 1 = 10 + (-3) \cdot 3 = 10 + (-3)(13 + (-1)10) =$$
$$= 10 + (-3)13 + (+3)10$$
$$= (4)10 + (-3)13$$

$$S = 4 \cdot 15 = 60$$

$$S = [60]_{13} = [9]_{13} = \left[ 9 + \frac{26}{2} \right]_{26} \cup [9]_{26} \cup$$