Esercizio

$$15x + 9 \equiv 0 \mod 36$$

Soluzione

$$15x \equiv \underset{\substack{\| \\ -9 \mod 36}}{27} \mod 36$$

- Calcolo MCD(36, 15):

$$36 = 2 \cdot 15 + 6$$
$$15 = 6 \cdot 2 + \boxed{3} = \text{MCD}$$
$$6 = 3 \cdot 2$$

$$\text{MCD}(36,15) = 3 \mid 27$$
$$\Rightarrow \exists \text{ soluzioni}$$

- Divido per 3:

$$15x \equiv 27 \mod 36$$
$$\Rightarrow \boxed{5x \equiv 9 \mod 12}$$

- Euclide (12, 5):

$$12 = 5 \cdot 2 + 2$$
$$5 = 2 \cdot 2 + \boxed{1} \quad \text{MCD}(12,5)$$

- Bézout:

$$1 = 5 - 2 \cdot 2$$
$$= 5 - 2(12 - 2 \cdot 5)$$
$$= 5 \cdot 5 - 2 \cdot 12$$

$$\rightarrow 1 \equiv 5 \cdot 5 - \underbrace{\cancel{2 \cdot 12}}_{= 0 \mod 12} \mod 12$$

$$\Rightarrow 1 \equiv 5 \cdot 5 \mod 12$$
$$\rightarrow \boxed{9 \equiv 45 \cdot 5 \mod 12}$$
$$x$$
$$\Rightarrow \boxed{45 \equiv 9 \mod 12} \Rightarrow x = 9 \quad \text{rappresentante canonico}$$

Ho trovato una soluzione $(x = 9)$

$$\text{Soluzioni} = \{9 + 12k \mid k \in \mathbb{Z}\} = [9]_{12}$$

Esercizio (esame)

2) (3 pt) Quale è ciclico? $\mathbb{Z}_2 \times \mathbb{Z}_5$ / $\mathbb{Z}_2 \times \mathbb{Z}_6$ / $\mathbb{Z}_2 \times \mathbb{Z}_{10}$

3) (4 pt) $14x \equiv 6 \mod 20$

Soluzione

2) L'unico gruppo ciclico è $\mathbb{Z}_2 \times \mathbb{Z}_5$

infatti: $\underbrace{([1]_2, [1]_5)}_{=g}$ genera $\mathbb{Z}_2 \times \mathbb{Z}_5$

$\boxed{\text{MODO 1}}$ Elenco le prime 10 potenze di g e mostro che ricoprono tutto $\mathbb{Z}_2 \times \mathbb{Z}_5$

in realtà sarebbe $([1]_2, [1]_5)$

perché ho $G(\mathbb{Z}, +, 0)$ e $g \in G$

$g = (\bar{1}, \bar{1})$ $\quad g+g = (\bar{0}, \bar{2})$ $\quad g+g+g = (\bar{1}, \bar{3})$

$4g = (\bar{0}, \bar{4})$ $\quad 5g = (\bar{1}, \bar{0})$ $\quad 6g = (\bar{0}, \bar{1})$

$7g = (\bar{1}, \bar{2})$ $\quad 8g = (\bar{0}, \bar{3})$ $\quad 9g = (\bar{1}, \bar{4})$

$10g = (\bar{0}, \bar{0})$ $\quad$ ho ricoperto tutto ✓

$\boxed{\text{MODO 2}}$ se $\underbrace{per(g)}_{\text{PERIODO DELL'ELEMENTO } g \in G \; = |\langle g \rangle|} = \underbrace{|G|}_{\text{ORDINE DEL GRUPPO} = \text{numero dei suoi elementi}} \Rightarrow G$ ciclico

se $g \in (G, +, 0) \Rightarrow \min\{k \text{ t.c. } k \cdot g = 0\}$

se $g \in (G, \cdot, 1) \Rightarrow \min\{k \text{ t.c. } g^k = 1\}$

$|G| = |\mathbb{Z}_2 \times \mathbb{Z}_5| = 10$

Ricordo che se n, m sono <u>co-primi</u> $\Rightarrow per(g) = n \cdot m$ in $\mathbb{Z}_n \times \mathbb{Z}_m$

$\Rightarrow per(g) = 2 \cdot 5 = 10$ ✓

se non lo fossero, $per(g) = mcm(n, m)$ in $\mathbb{Z}_n \times \mathbb{Z}_m$

Perché gli altri sono falsi? (non è richiesto)

- $\mathbb{Z}_2 \times \mathbb{Z}_6$

  $|\mathbb{Z}_2 \times \mathbb{Z}_6| = 2 \cdot 6 = 12$

  $per(g) = mcm(2,6) = 6 \neq 12 \Rightarrow$ NON CICLICO

- $|\mathbb{Z}_2 \times \mathbb{Z}_{10}| = 2 \cdot 10 = 20 \neq per(g) = mcm(2,10) = 10$

b) $14x \equiv 6 \mod 20$

$MCD(20,14) = 2$

$20 = 14 \cdot 1 + 6$
$14 = 6 \cdot 2 + 2$
$6 = 2 \cdot 3$

$\Rightarrow \quad 7x \equiv 3 \mod 10$

Euclide: $10 = 1 \cdot 7 + 3$
$7 = 3 \cdot 2 + 1$

Bezout: $1 = 7 - 3 \cdot 2 = 7 - 2 \cdot (10 - 7) = 3 \cdot 7 - 10$

$1 \equiv 3 \cdot 7 \mod 10 \Rightarrow 3 \equiv 7 \cdot \underbrace{9}_{x} \mod 10$

$\Longrightarrow \quad x = [9]_{20}$