

Algebra per Informatica

Esercitazione guidata dicembre 2023

Svolgere i seguenti esercizi motivando chiaramente le risposte.

Esercizio 1. Sia dato l'insieme $A = \{(1, 2), (2, 1), (2, 2), (2, 3), (2, 4), (4, 3), (5, 3)\}$.

- Si consideri A come sottoinsieme del poset $(\mathbb{N} \times \mathbb{N}, \leq \times \leq)$ e si determinino (se esistono) massimo, minimo, estremo inferiore, ed estremo superiore di A . Determinare l'insieme dei maggioranti e l'insieme dei minoranti di A .
- Si consideri A come sottoinsieme del poset $(\mathbb{N} \times \mathbb{N}, \text{LEX})$ e si determinino (se esistono) massimo, minimo, estremo inferiore, ed estremo superiore di A . Determinare l'insieme dei maggioranti e l'insieme dei minoranti di A .

Esercizio 2. Trovare la classe di equivalenza x che soddisfa le seguenti uguaglianze:

- $\bar{3} \cdot x = \bar{5}$ in \mathbb{Z}_7 ;
- $\bar{70} \cdot x = \bar{183}$ in \mathbb{Z}_9 .

Esercizio 3. Si consideri l'insieme \mathbb{Z}_{36} .

- Quali tra le classi $\bar{8}, \bar{21}$ e $\bar{35}$ sono invertibili? In tal caso qual è il loro inverso?
Suggerimento: rappresentare la classe con un numero negativo.
- Quanti sono gli elementi invertibili rispetto al prodotto?
- Quanto fa $\bar{5}^{50}$?

Esercizio 4. Si consideri \mathbb{Z}_{35} e la funzione

$$\begin{aligned} f : \mathbb{Z}_{35} &\longrightarrow \mathbb{Z}_{35} \\ \bar{x} &\mapsto \bar{3} \cdot \bar{x} \end{aligned}$$

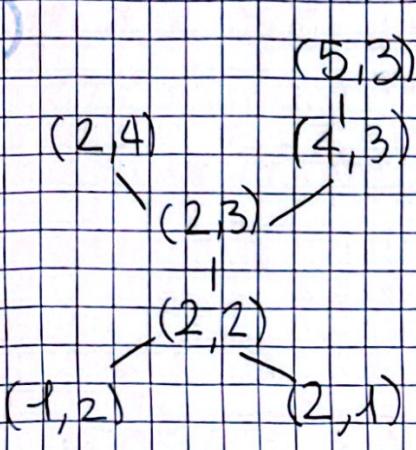
- Calcolare $(f(\bar{1}))^{303}$.
- Determinare se f è iniettiva e/o surgettiva.
- Trovare (se esiste) l'inversa di f nel monoide $(X^X, \circ, \text{Id}_X)$, dove $X = \mathbb{Z}_{35}$.

ESERCITAZIONE DICEMBRE 2023

Esercizio 1)

$$A = \{(1,2), (2,1), (2,2), (2,3), (2,4), (4,3), (5,3)\}$$

- 1) Si consideri A come sottoinsieme del poset $(\mathbb{N} \times \mathbb{N}, \leq \times \leq)$ e si determinino massimo, minimo, estremo inferiore e superiore. Determinare l'insieme dei maggioranti e minoranti
- 2) Si consideri A come sottoinsieme del poset $(\mathbb{N} \times \mathbb{N}, \leq \times \leq)$ e si determinino massimo, minimo, estremo inferiore e superiore, maggioranti e minoranti



- due elementi minimi $(1,2)$ e $(2,1)$, quindi $\inf A = (1,1)$
- due elementi massimali $(2,4)$ e $(5,3)$, quindi $\sup A = (5,4)$
- insieme dei maggioranti: $\{(x,y) \in \mathbb{N}^2 : x \geq 5 \text{ e } y \geq 4\}$
quindi $\sup A = (5,4)$.
- insieme dei minoranti: $\{(x,y) \in \mathbb{N}^2 : x \leq 1 \text{ e } xy \leq 1\}$

$$\text{Quindi } \inf A = (1,1)$$

$$(1,2) \leq (2,1) \leq (2,2) \leq (2,3) \leq (2,4) \leq (4,3) \leq (5,3)$$

- $\min A = \inf A = (1,1)$ e $\max A = \sup A = (5,3)$
- I maggioranti di A sono $\{(x,y) \in \mathbb{N}^2 : x \geq 5 \text{ o } (x=5 \text{ e } y \geq 3)\}$
- I minoranti di A sono $\{(x,y) \in \mathbb{N}^2 : x \leq 1 \text{ o } (x=1 \text{ e } y \leq 2)\} = \{(0,x) : x \in \mathbb{N}\} \cup \{(1,0), (1,1), (1,2)\}$

Esercizio 2)

Trovare la classe di equivalenza \bar{x} che soddisfa le seguenti uguaglianze:

$$1) \bar{3} \cdot \bar{x} = \bar{5} \text{ in } \mathbb{Z}_7$$

$$2) \bar{70} \cdot \bar{x} = \bar{183}$$

L'equazione $\overline{3} \cdot \overline{x} = 5$ in \mathbb{Z}_7 è equivalente diofantea $3x = 5 + 7k$ in \mathbb{Z} . Dobbiamo determinare quindi due interi x, k tali che $3x - 7k = 5$.

$$(x, k) = (4, 1), \text{ infatti } 3 \cdot 4 - 7 \cdot 1 = 5$$

$$\text{Quindi } \overline{x} = \overline{4}$$

2)

$$\overline{70} = \overline{7} \text{ e } \overline{183} = \overline{3} \text{ in } \mathbb{Z}_9$$

Quindi l'equazione da risolvere diventa $\overline{7} \cdot \overline{x} = \overline{3}$ in \mathbb{Z}_9 , quindi $\overline{7}x = \overline{3} + 9k$ in \mathbb{Z} .

Dobbiamo quindi trovare due interi x, k tali che $\overline{7}x - 9k = 3$

$$(x, k) = (3, 2), \text{ infatti } \overline{7} \cdot 3 - 9 \cdot 2 = 3$$

$$\text{Quindi } \overline{x} = \overline{3}$$

Esercizio 3)

Si consideri l'insieme \mathbb{Z}_{36}

- 1) Quali tra le classi $\overline{8}, \overline{21}$ e $\overline{35}$ sono invertibili? In tal caso qual è il loro inverso?
- 2) Quanti sono gli elementi invertibili rispetto al prodotto?
- 3) Quanto fa $\overline{5}^{50}$?

1)

$$\text{MCD}(8, 36)$$

$$\begin{aligned} 36 &= 4 \cdot 8 + 4 \\ 8 &= 2 \cdot 4 + 0 \end{aligned}$$

$$\text{MCD}(21, 36)$$

$$\begin{aligned} 36 &= 1 \cdot 21 + 15 \\ 21 &= 1 \cdot 15 + 6 \\ 15 &= 2 \cdot 6 + 3 \\ 6 &= 2 \cdot 3 \end{aligned}$$

$$\text{MCD}(35, 36)$$

$$36 = 1 \cdot 35 + 1$$

$$\text{MCD}(8, 36) = 4 \neq 1 \quad \text{MCD}(21, 36) = 3 \neq 1$$

non invertibili in \mathbb{Z}_{36}

$$\overline{35} = \overline{-1}$$

l'inverso di $\overline{35}$
è $\overline{35}$

2)

$$|\text{U}(\mathbb{Z}_{36})| = \varphi(36) \quad 36 = 2^2 \cdot 3^2$$

$$\overline{35} \cdot \overline{35} = (-1) \cdot (-1) = 1$$

$$\varphi(36) = 36 \cdot \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) = 36 \cdot \frac{1}{2} \cdot \frac{2}{3} = 12$$

Per il teorema di Eulero, abbiamo che se \bar{x} è invertibile in \mathbb{Z}_{36} , allora $\bar{x}^{\varphi(36)} = \bar{1}$, cioè $\bar{x}^{12} = \bar{1}$

La classe $\bar{5}$ è invertibile perché $\text{MCD}(5, 36) = 1$

$$\bar{5}^{12} = \bar{1} \text{ per calcolare } \bar{5}^{50}, \text{ scriviamo}$$

$$50 = 48 + 2 = 4 \cdot 12 + 2, \text{ quindi}$$

$$\bar{5}^{50} = \bar{5}^{4 \cdot 12 + 2} = (\bar{5}^{12})^4 \cdot \bar{5}^2 = \bar{1}^4 \cdot \bar{5}^2 = \bar{5}^2 = \bar{25}$$

Esercizio 4)

Si consideri \mathbb{Z}_{35} e la funzione

$$f: \mathbb{Z}_{35} \rightarrow \mathbb{Z}_{35}$$
$$\bar{x} \mapsto \bar{3} \cdot \bar{x}$$

1) Calcolare $(f(\bar{x}))^{303}$

2) Determinare se f è iniettiva e/o surgettiva

3) Trovare l'inversa di f nel monoide $(\mathbb{X}^*, \circ, \text{Id})$,
dove $\mathbb{X} = \mathbb{Z}_{35}$

1) $f(\bar{x}) = \bar{3} \cdot \bar{x} = \bar{3}$, quindi dobbiamo calcolare $\bar{3}^{303}$
in \mathbb{Z}_{35}

$$\varphi(35) = (3-1)(7-1) = 4 \cdot 6 = 24$$

Quindi $\bar{x}^{24} = \bar{1}$ e in particolare $\bar{3}^{24} = \bar{1}$

L'operazione euclidea di 303 per 24 è
 $303 = 12 \cdot 24 + 15$, quindi

$$\begin{aligned}\bar{3}^{303} &= \bar{3}^{12 \cdot 24 + 15} = (\bar{3}^{24})^{12} \cdot \bar{3}^{15} = \bar{1}^{12} \cdot \bar{3}^{15} = \\ &= \bar{3}^{15} = \bar{3}^4 \cdot \bar{3}^4 \cdot \bar{3}^4 \cdot \bar{3}^3 = \bar{81} \cdot \bar{81} \cdot \bar{81} \cdot \bar{27} = \\ &= \bar{11} \cdot \bar{11} \cdot \bar{11} \cdot \bar{27} = \bar{121} \cdot \bar{11} \cdot \bar{27} = \bar{16} \cdot \bar{11} \cdot \bar{27} = \\ &= \bar{176} \cdot \bar{27} = \bar{1} \cdot \bar{27} = \bar{27}\end{aligned}$$

2) iniettività

Siano $\bar{x}, \bar{a} \in \mathbb{Z}_{35}$ tali che $f(\bar{x}) = f(\bar{a})$, cioè

$\bar{3} \cdot \bar{x} = \bar{3} \cdot \bar{a}$. Moltiplicando entrambi i membri per

$\bar{12} \in \mathbb{Z}_{35}$ si ottiene $\bar{12} \cdot \bar{3} \cdot \bar{x} = \bar{12} \cdot \bar{3} \cdot \bar{a}$

e quindi $\bar{x} = \bar{a}$. Quindi f è iniettiva

• Surgettività

Sia $\bar{a} \in \mathbb{Z}_{35}$. Scegliamo $\bar{x} = \bar{12} \cdot \bar{a} \in \mathbb{Z}_{35}$

$f(\bar{x}) = f(\bar{12} \cdot \bar{a}) = \bar{3} \cdot \bar{12} \cdot \bar{a} = \bar{a}$, quindi f è surgettiva

3)

L'inversa di f è

$$g: \mathbb{Z}_{35} \rightarrow \mathbb{Z}_{35}$$

$$\bar{x} \mapsto \bar{12} \cdot \bar{x}$$