

**CORSO DI LAUREA TRIENNALE IN INFORMATICA**  
**PROVA SCRITTA DI ALGEBRA (GRUPPI I, II E III)**  
**15 GENNAIO 2024**

Svolgere i seguenti esercizi,

—————→ *giustificando pienamente tutte le risposte.* ←————

Sui fogli consegnati vanno indicati: **nome, cognome, matricola, gruppo di appartenenza.**

**Non** è necessario consegnare la traccia.

**Esercizio 1.** Scrivere una negazione della formula  $\exists y \left( \forall x \left( (\varphi(x) \wedge \psi(y)) \rightarrow (\psi(y) \rightarrow \theta(x)) \right) \right)$  in cui non appaia il connettivo di implicazione (qui  $\varphi$ ,  $\psi$  e  $\theta$  sono predicati unari).

**Esercizio 2.** Dare una definizione di partizione di un insieme ed enunciare il teorema fondamentale su partizioni e relazioni d'equivalenza. Fornire una partizione di  $\mathbb{Z}$  di cardinalità  $2^{10}$ .

**Esercizio 3.** Determinare i numeri naturali  $n$  tali che  $2^n < n!$ . (Suggerimento: può essere utile fare uso del principio di induzione). Per quali insiemi finiti  $a$  si ha  $|\mathcal{P}(a)| < |\text{Sym}(a)|$ ?

**Esercizio 4.** Si consideri l'operazione  $*$ :  $(a, b) \in \mathbb{Z}_{10} \times \mathbb{Z}_{10} \mapsto \bar{6}a + b \in \mathbb{Z}_{10}$ .

- (i) Decidere se  $*$  è associativa, se è commutativa, se  $(\mathbb{Z}_{10}, *)$  ha elementi neutri a sinistra o a destra e, nel caso la domanda abbia senso, quali suoi elementi sono simmetrizzabili. Che tipo di struttura algebrica è  $(\mathbb{Z}_{10}, *)$ ?
- (ii) Siano  $P = \{\bar{2}a \mid a \in \mathbb{Z}_{10}\}$  e  $D = \mathbb{Z}_{10} \setminus P$ . Per ciascuno di  $P$  e  $D$  decidere se è una parte chiusa rispetto a  $*$  e, nel caso, rispondere, per la corrispondente struttura indotta, alle stesse domande poste al punto precedente per  $(\mathbb{Z}_{10}, *)$ .

**Esercizio 5.**

- (i) Stabilire quali tra  $[2027]_{2024}$ ,  $[1024]_{2024}$ ,  $[-2]_{2024}$  e  $[10001!]_{2024}$  sono invertibili in  $\mathbb{Z}_{2024}$  e quali sono divisori dello zero.
- (ii) Calcolare, utilizzando l'algoritmo euclideo, il massimo comun divisore positivo tra 209 e 165 e trovare quindi tutte le soluzioni delle equazioni congruenziali  $209x \equiv_{165} 14$  e  $165x \equiv_{209} 44$ .

**Esercizio 6.** Siano  $F$  l'insieme delle parti finite non vuote di  $\mathbb{N}$  e  $f$  l'applicazione  $x \in F \mapsto \min x + \max x \in \mathbb{N}$ .

- (i) Spiegare perché  $f$  è ben definita come applicazione;
- (ii) determinare  $\check{f}(\{2\})$  e  $|\check{f}(\{2\})|$ ;
- (iii)  $f$  è iniettiva, suriettiva, biiettiva?
- (iv) Detto  $\sigma$  il nucleo di equivalenza di  $f$ , determinare  $[\{2\}]_\sigma$ .

Sia ora  $\tau$  la relazione d'ordine in  $F$  definita da:

$$\forall x, y \in F \quad (x \tau y \iff (x = y \vee f(x) \text{ è un divisore proprio di } f(y))).$$

- (v) Determinare in  $(F, \tau)$  eventuali elementi minimali, massimali, minimo, massimo.  $(F, \tau)$  è un reticolo?
- (vi) Posto  $M = \{\{1\}, \{2\}, \{2, 3, 4\}, \{1, 3, 5, 7\}, \{5, 6, 7\}, \{9\}, \{10, 11, 15, 60, 62\}\}$ , disegnare un diagramma di Hasse di  $(M, \tau)$ , verificare se questo è un reticolo e, nel caso, se è distributivo, complementato, booleano.
- (vii) Determinare in  $(M, \tau)$  una catena massimale  $C$  ed un sottoreticolo booleano massimale  $B$ .

**Esercizio 7.** Per ogni primo positivo  $p$ , si consideri il polinomio  $f_p = (\bar{4}x^3 + x^2 - \bar{2}x - \bar{4})(x + \bar{1}) \in \mathbb{Z}_p[x]$ .

- (i) Determinare l'insieme  $X$  dei primi  $p$  tali che il resto della divisione tra  $f_p$  e  $x - \bar{2}$  sia  $\bar{0}$ .
- (ii) Posto  $p = \max X$ , decomporre  $f_p$  in prodotto di polinomi irriducibili in  $\mathbb{Z}_p[x]$ .
- (iii)  $f_p$  ha un divisore irriducibile monico di grado 2? In caso di risposta affermativa, dire quanti ne ha ed esibirne almeno uno.

# GEN-24 ES 1

Esercizio 1. Scrivere una negazione della formula  $\exists y (\forall x ((\varphi(x) \wedge \psi(y)) \rightarrow (\psi(y) \rightarrow \theta(x))))$  in cui non appaia il connettivo di implicazione (qui  $\varphi$ ,  $\psi$  e  $\theta$  sono predicati unari).

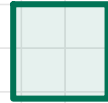
$$\exists y \left( \forall x \left( (\varphi(x) \wedge \psi(y)) \rightarrow (\psi(y) \rightarrow \theta(x)) \right) \right)$$

$$\forall y \neg \left( \forall x \left( (\varphi(x) \wedge \psi(y)) \rightarrow (\psi(y) \rightarrow \theta(x)) \right) \right)$$

$$\forall y \left( \exists x \neg \left( (\varphi(x) \wedge \psi(y)) \rightarrow (\psi(y) \rightarrow \theta(x)) \right) \right)$$

$$\forall y \left( \exists x \left( (\varphi(x) \wedge \psi(y)) \wedge \neg (\psi(y) \rightarrow \theta(x)) \right) \right)$$

$$\forall y \left( \exists x \left( (\varphi(x) \wedge \psi(y)) \wedge (\psi(y) \wedge \neg \theta(x)) \right) \right)$$



# GEN-24 ES 2

**Esercizio 2.** Dare una definizione di partizione di un insieme ed enunciare il teorema fondamentale su partizioni e relazioni d'equivalenza. Fornire una partizione di  $\mathbb{Z}$  di cardinalità  $2^{10}$ .

Def. Partizione:

$X \subseteq A$  è una partizione di  $A$  se e solo se:

- $\forall a \in X (a \neq \emptyset)$
- $\forall a, b \in X (a \neq b \Rightarrow a \cap b = \emptyset)$
- $\bigcup X = A$

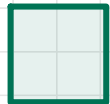
Teorema fondamentale su partizioni e rel. equivalenti

Per ogni insieme  $A$  esiste una funzione biettiva  $f$  definita

$$f: m \in EQ(A) \mapsto a/m \in \text{PART}(A)$$

PARTIZIONE

$$\mathbb{Z}_{2^{10}}$$



# GEN 24 ES 3

i) Vale per tutti gli  $n \geq 4$

ii) PER INDUZIONE

$$n=4$$

$$2^4 < 4! = 16 < 24$$

?

# GEN-ZH ES 4

**Esercizio 4.** Si consideri l'operazione  $*$ :  $(a, b) \in \mathbb{Z}_{10} \times \mathbb{Z}_{10} \mapsto \bar{6}a + b \in \mathbb{Z}_{10}$ .

- (i) Decidere se  $*$  è associativa, se è commutativa, se  $(\mathbb{Z}_{10}, *)$  ha elementi neutri a sinistra o a destra e, nel caso la domanda abbia senso, quali suoi elementi sono simmetrizzabili. Che tipo di struttura algebrica è  $(\mathbb{Z}_{10}, *)$ ?
- (ii) Siano  $P = \{2a \mid a \in \mathbb{Z}_{10}\}$  e  $D = \mathbb{Z}_{10} \setminus P$ . Per ciascuno di  $P$  e  $D$  decidere se è una parte chiusa rispetto a  $*$  e, nel caso, rispondere, per la corrispondente struttura indotta, alle stesse domande poste al punto precedente per  $(\mathbb{Z}_{10}, *)$ .

i) ASSOCIATIVITA' ? SI

$$\forall x, y, z \in \mathbb{Z}_{10} \left( x * (y * z) = (x * y) * z \right)$$

$$\bar{6}x + \bar{6}y + z = \bar{6}(\bar{6}x + y) + z$$

$$\bar{6}x + \bar{6}y + z = \bar{36}x + \bar{6}y + z$$

$$\bar{6}x + \bar{6}y + z = \bar{6}x + \bar{6}y + z$$

COMMUTATIVITA' ? NO

$$\forall x, y \in \mathbb{Z}_{10} \left( x * y = y * x \right)$$

$$\bar{6}x + y = \bar{6}y + x \text{ è falso}$$

ELEMENTO NEUTRO ? NO

$$\forall x \quad x * e = x \quad \text{NESSUNO}$$

$$\forall x \quad e * x = x \quad \text{SÌ, } 0 \quad \bar{6} \cdot 5 + x = \bar{30} + x = x \quad \bar{6} \cdot 0 + x = x$$

STRUTTURA ALGEBRA? SEMIGRUPPO

i i.1)

$$P = \{ \bar{a} \mid a \in \mathbb{Z}_{10} \}$$

PARTI CHIUSA? SI

$$\forall x, y \in P (x * y \in P)$$

$\bar{6}x + y$  è poi, perché addizione e moltiplicazione sono parti chiuse

ASSOCIATIVA? SI

Uguale a prima

COMMUTATIVA? SI

$$\bar{6}x + y = \bar{6}y + x$$

$$x=2 \quad y=4$$

$$6 \cdot 2 + 8 = 6 \cdot 8 + 2$$

$$12 + 8 = 48 + 2$$

ELEMENTO NEUTRO? 0

$$\bar{6}x: 0 \quad 6 \cdot 0 + x = x$$

$$\bar{6}x: 0 \quad 6 \cdot x + 0 = x$$

SIMMETRIZZABILI? SI

$$x * l = 0 \Rightarrow \bar{6}x + l = \bar{0}$$

$$\bar{x}=2 \quad \bar{2} * l = \bar{0} \quad \bar{6} \cdot \bar{2} * \bar{8} = \bar{0}$$

STRUTTURA ALGEBRA? GRUPPO ABELIANO

i i.2)

$$D: \mathbb{Z}_{10} \setminus P$$

PARTE CHIUSA? SI

$$\forall x, y \in P (x \cdot y \in P)$$

$\overline{6}x + y$  è poi, perché addizione e moltiplicazione sono parte chiuse

ASSOCIATIVA? SI

Uguale a prima

COMMUTATIVA? SI (PER IL POTERE DELL'AMORE DI CRISTO)

$$\overline{6}x + y = \overline{6}y + x \quad \begin{array}{l} x=5, y=3 \\ \overline{6} \cdot 5 \quad \quad \overline{6} \cdot 3 \\ 30 + 3 = 18 + 5 \end{array}$$

ELEMENTO NEUTRO? S

$$\overline{6}e + x = x \quad \overline{5} \quad \overline{6} \cdot \overline{5} = \overline{30} = 0$$

$$\overline{6}x + 5 = x \quad \text{potere magico di numeri}$$

SIMMETRIZZABILI? SI

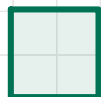
$$\overline{6}x + l = 5$$

$$\begin{array}{l} 1, -1(9) \quad 9, (-9)(1) \\ \overline{6} \cdot 1 + 9 = 5 \quad \overline{6} \cdot 9 + 1 = 5 \end{array}$$

$$\begin{array}{l} 5, -5(5) \\ \overline{6} \cdot 5 + 5 = 5 \end{array}$$

$$\begin{array}{l} 3, -3(7) \quad 7, -7(3) \\ \overline{6} \cdot 3 + 7 = 5 \quad \overline{6} \cdot 7 + 3 = 5 \end{array}$$

STRUTTURA ALGEBRA? GRUPPO ABELIANO



# GEN - 2h PS S

## Esercizio 5.

- (i) Stabilire quali tra  $[2027]_{2024}$ ,  $[1024]_{2024}$ ,  $[-2]_{2024}$  e  $[10001]_{2024}$  sono invertibili in  $\mathbb{Z}_{2024}$  e quali sono divisori dello zero.
- (ii) Calcolare, utilizzando l'algoritmo euclideo, il massimo comun divisore positivo tra 209 e 165 e trovare quindi tutte le soluzioni delle equazioni congruenziali  $209x \equiv_{165} 14$  e  $165x \equiv_{209} 44$ .

$$209 = 165 \cdot 1 + 44$$

$$44 = 209 + 165 \cdot (-1)$$

$$165 = 44 \cdot 3 + 33$$

$$33 = 165 + 44 \cdot (-3)$$

$$44 = 33 \cdot 1 + 11$$

$$11 = 44 + 33 \cdot (-1)$$

$$33 = 11 \cdot 3 + 0$$

$$209x \equiv_{165} 14 \quad \text{non ammette soluzioni}$$

$$165x \equiv_{209} 44 \quad \text{non ci sono soluzioni}$$





# GEN-24 ES 6

$$F = \mathcal{P}(\mathbb{N}) \setminus \emptyset \quad f: x \in F \mapsto \min x + \max x \in \mathbb{N}$$

i) È una suriezione perché ogni elemento del dominio ha una immagine nel codominio

$$\text{ii)} \quad \tilde{f}(\{2\}) = \{\{1\}, \{0, 2\}, \{0, 1, 2\}\}$$

$$|\tilde{f}(\{2\})| = 3$$

iii) INIEZIONE: NO

$$\forall x, y \in F \quad (f(x) = f(y) \Rightarrow x = y)$$

$$\text{FALSO} \quad f(\{1\}) = 2$$

$$f(\{0, 2\}) = 2$$

SURIEZIONE: SI

$$\forall y \in \mathbb{N} \quad \exists x \in F \quad (y = f(x))$$

Tutti gli elementi di  $F$  con cardinalità 2 e con 0 come elemento nel  $\{0\}$  coprono tutto  $\mathbb{N}$

BIIEZIONE: NO

$$\text{iv)} \quad [\{2\}]_f = \{\{0, 2\}, \{1\}, \{0, 1, 2\}\}$$

$\tau: \forall x, y \in F (x \tau y \iff x=y \vee f(x) \text{ è un div. proprio di } f(y))$

v) Reticolo:

- Riflessiva: SI, vale per  $x=y$

- Transitività:

vi)  $M = \left\{ \overset{A}{\underbrace{\{1\}}_2}, \overset{B}{\underbrace{\{2\}}_4}, \overset{C}{\underbrace{\{2,3,4\}}_6}, \overset{D}{\underbrace{\{1,3,5,7\}}_8}, \overset{E}{\underbrace{\{5,6,7\}}_{12}}, \overset{F}{\underbrace{\{9\}}_{18}}, \overset{G}{\underbrace{\{10,11,15,60,62\}}_{72}} \right\}$

