CdL in Informatica — a.a. 2006/2007

Esercitazione scritta di **ALGEBRA** (Proff. Cutolo e Rao) venerdì 16 novembre 2007

NOME E COGNOME	MATRICOLA

GRUPPO ☐ *I (Rao)* ☐ *IV (Cutolo)*	ESAME: mercoledì 21 novembre, ore 11, sala riunioni II liv., DMA

1 Vero o falso? Oppure i dati non sono sufficienti per fornire alcuna delle due risposte?

- Esistono $n, m \in \mathbb{N}^{\#}$ tali che esattamente uno tra n e n^m sia multiplo di 23. *vero* ☐ *falso* ☐ *dati insuff.* ☐
- Ogni elemento del monoide $(\mathbb{N}^{\#}, \cdot, 1)$ è cancellabile. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- La forma proposizionale $\big(q \wedge (\neg r)\big) \Rightarrow \big(q \vee (r \Rightarrow p)\big)$ è una tautologia. *vero* ☐ *falso* ☐ *dati insuff.* ☐
- $\{(X, Y) \mid X \subset Y \subseteq \mathbb{Z}\} = \{(A, B) \mid (\forall\, a \in A)(a \in B) \wedge (\forall x \in B)(x \in \mathbb{Z})\}$. *vero* ☐ *falso* ☐ *dati insuff.* ☐
- $25^{7562} \bmod 3971 \geq 3971$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐

---

2 Per definizione, F è una *partizione* dell'insieme S se e solo se ....

....

---

3 Per definizione un anello $(R, +, \cdot)$ è un *campo* se e solo se ....

....

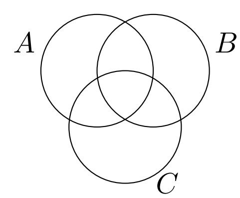
$(\mathbb{N}, +, \cdot)$ è un campo? *sì* ☐ *no* ☐. $(\mathbb{R}[x], +, \cdot)$ è un campo? *sì* ☐ *no* ☐. $(\mathcal{P}(\mathbb{Q}), \Delta, \cap)$ è un campo? *sì* ☐ *no* ☐. $(\mathbb{Z}_8, +, \cdot)$ è un campo? *sì* ☐ *no* ☐.

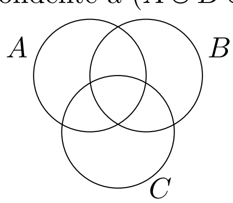
---

4 Sia $S = \{1, 2, 3, 4, 5, 6\}$. Quante sono le relazioni di equivalenza α in S tali che $1 < \big|[6]_\alpha\big| \neq \big|[2]_\alpha\big| = 4$, $1\ \alpha\ 5$ e $2\ \alpha\ 5$? Risposta: .... Se α è una di tali relazioni di equivalenza, $|S/\alpha| =$ ..., oppure: ☐ *non è possibile stabilire quanti elementi ha* S/α.

---

5 Si completino i due diagrammi di Venn tratteggiando a destra l'area corrispondente a $(A \cup B \cup C) \smallsetminus \big(A \smallsetminus (B \cup C)\big)$ e in basso a sinistra quella corrispondente a $(A \cup B \cup C) \smallsetminus \big((A \smallsetminus B) \cup (A \smallsetminus C)\big)$.



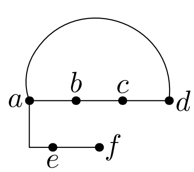


È vero che $(A \cup B \cup C) \smallsetminus \big(A \smallsetminus (B \cup C)\big) = (A \cup B \cup C) \smallsetminus \big((A \smallsetminus B) \cup (A \smallsetminus C)\big)$ per ogni scelta degli insiemi A, B, C? ☐ *sì*, oppure: ☐ *no, un controesempio è fornito dalla terna data da* $A =$ .... , $B =$ .... , $C =$ ....

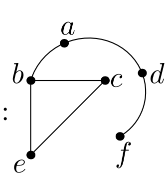
---

6 Tra i tre grafi qui disegnati se ne indichino due tra loro isomorfi: $G =$ ... e $H =$ ..., e si scriva poi (dove indicato) un isomorfismo da G ad H, oppure: ☐ *i grafi disegnati sono a due a due non isomorfi tra loro.*

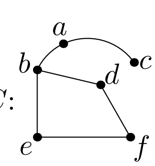
A:



B:



C:



isomorfismo:

$$\begin{pmatrix} a & b & c & d & e & f \\ \_ & \_ & \_ & \_ & \_ & \_ \end{pmatrix}$$

Quanti sono gli isomorfismi da G ad H? ..... Esistono grafi con (esattamente) sei vertici, dei quali uno di grado 1, quattro di grado 2 e uno di grado 3 che non siano isomorfi né ad A, né a B né a C? ☐ *no*, oppure: ☐ *sì, ne disegno uno in basso a sinistra.* Esistono grafi con (esattamente) sei vertici, dei quali uno di grado 1, tre di grado 2 e due di grado 3? ☐ *no*, oppure: ☐ *sì, ne disegno uno in basso a destra.*

7 Si trovi l'insieme (rispettivamente S_1, S_2) di tutte le soluzioni intere di ciascuna delle seguenti equazioni congruenziali:

$129x \equiv_{337} 128, \quad S_1 = \dots\dots\dots\dots\dots\dots$ $\qquad$ $337x \equiv_{129} 128, \quad S_2 = \dots\dots\dots\dots\dots\dots$

Determinare un $a \in \mathbb{Z}$ tale che $129a \equiv_{337} 128$ e $100 < a < 300$. Si ha: $a = \dots\dots$

Calcolare: $(a^2 - a + 1) \bmod 337 = \dots\dots$, $(a^3 + 1) \bmod 337 = \dots\dots$ Il periodo di $[a]_{337} \in \mathcal{U}(\mathbb{Z}_{337})$ è $\dots\dots$

Calcolare $129^{6102} \bmod 337 = \dots\dots$

---

8 Siano $S = \{1, 2, 3\}$ e $\theta\colon X \in \mathcal{P}(S) \mapsto X \cap \{1, 3\} \in \mathcal{P}(S)$. θ è iniettiva? *sì* ☐ *no* ☐, suriettiva? *sì* ☐ *no* ☐. Quante sezioni ha θ? ... E quante retrazioni? ... In $\mathcal{P}(S)$ si considerino le due relazioni binarie σ e ρ definite ponendo, per ogni $X, Y \in \mathcal{P}(S)$,

$$X \,\sigma\, Y :\iff X^\theta \subseteq Y^\theta; \qquad\qquad X \,\rho\, Y :\iff X^\theta \subset Y^\theta.$$

Tra σ e ρ quali sono ...... e quali non sono ...... un ordinamento stretto? Quali sono ...... e quali non sono ...... un ordinamento largo? Se possibile, si indichi una tra σ e ρ che sia un ordinamento: ..., si disegni il relativo diagramma di Hasse e si stabilisca se, rispetto a questo ordinamento:

$\mathcal{P}(S)$ ha minimo? ☐ *no*, oppure: ☐ *sì, esso è* ......
$\mathcal{P}(S)$ ha massimo? ☐ *no*, oppure: ☐ *sì, esso è* ......
$\mathcal{P}(S)$ ha elementi minimali? ☐ *no*, oppure: ☐ *sì, essi sono* ....
$\mathcal{P}(S)$ è un reticolo? *sì* ☐ *no* ☐, un reticolo booleano? *sì* ☐ *no* ☐.

---

9 In $F = \mathrm{Map}(\mathbb{N}, \mathbb{N})$ si considerino le operazioni binarie $*$ e $\oplus$ definite ponendo, per ogni $f, g \in F$,

$$f * g\colon n \in \mathbb{N} \mapsto \max\{n^f, n^g\} \in \mathbb{N}; \qquad\qquad f \oplus g\colon n \in \mathbb{N} \mapsto n^f + n^g \in \mathbb{N}.$$

$*$ è commutativa? *sì* ☐ *no* ☐, associativa? *sì* ☐ *no* ☐. $\oplus$ è commutativa? *sì* ☐ *no* ☐, associativa? *sì* ☐ *no* ☐. $(F, *)$ è un semigruppo? *sì* ☐ *no* ☐, un monoide? *sì* ☐ *no* ☐, un gruppo? *sì* ☐ *no* ☐. $(F, \oplus)$ è un semigruppo? *sì* ☐ *no* ☐, un monoide? *sì* ☐ *no* ☐, un gruppo? *sì* ☐ *no* ☐. Se esistono, indicare gli elementi neutri f_1 di $(F, *)$ e f_0 di $(F, \oplus)$:

$f_1\colon n \in \mathbb{N} \mapsto \dots\dots \in \mathbb{N}$, oppure: ☐ f_1 *non esiste*; $\qquad$ $f_0\colon n \in \mathbb{N} \mapsto \dots\dots \in \mathbb{N}$, oppure: ☐ f_0 *non esiste*.

$(F, \oplus, *)$ è un anello? *sì* ☐ *no* ☐. Nel caso, è booleano? *sì* ☐ *no* ☐, un domino di integrità? *sì* ☐ *no* ☐, un campo? *sì* ☐ *no* ☐. Sia $f\colon n \in \mathbb{N} \mapsto 2n \in \mathbb{N}$. Se esistono, indicare il simmetrico g di f rispetto a $*$ ed il simmetrico h di f rispetto a $\oplus$:

$g\colon n \in \mathbb{N} \mapsto \dots\dots \in \mathbb{N}$, oppure: ☐ g *non esiste*; $\qquad$ $h\colon n \in \mathbb{N} \mapsto \dots\dots \in \mathbb{N}$, oppure: ☐ h *non esiste*.

---

10 Sia $f = x^7 + 6x^5 - x^4 + 9x^3 - 6x^2 - 9 \in \mathbb{Q}[x]$ e sia $g \in \mathbb{Q}[x]$ tale che, in $\mathbb{Q}[x]$, $k := (x^2 + 3)^2$ divida $h := f - xg$ e h divida $g - 2k$. In $\mathbb{Q}[x]$ si calcoli il massimo comun divisore monico d tra f e g [*Suggerimento:* algoritmo euclideo!] e si trovi un divisore t di f di grado 3 con coefficiente direttore 4:

$d = \dots\dots\dots\dots\dots\dots\dots\dots\dots$, $\qquad$ oppure: ☐ *impossibile calcolarlo*

$t = \dots\dots\dots\dots\dots\dots\dots\dots\dots$, $\qquad$ oppure: ☐ *tale t non esiste*
