CdL in Informatica — a.a. 2006/2007

Esercitazione scritta di **ALGEBRA** (Proff. Cutolo e Rao) lunedì 17 dicembre 2007

NOME E COGNOME	MATRICOLA

GRUPPO ☐ *I (Rao)* ☐ *IV (Cutolo)*	ESAME: giovedì 20 dicembre, ore 11, aula D, DMA

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

- La forma proposizionale $\big(p \Rightarrow (q \Rightarrow r)\big) \vee \big(p \Rightarrow (r \Rightarrow q)\big)$ è una tautologia. *vero* ☐ *falso* ☐ *dati insuff.* ☐
- L'applicazione $f\colon n \in \mathbb{Z} \mapsto \begin{cases} n+1, & \text{se } n \in \mathbb{N} \\ 3-n, & \text{se } n \notin \mathbb{N} \end{cases} \in \mathbb{N}^{\#}$ è iniettiva. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- $\{X \in \mathcal{P}(\mathbb{N}) \mid (3 \in X) \wedge (7 \notin X)\} = \{A \in \mathcal{P}(\mathbb{Z}) \mid (A \subseteq \mathbb{N}) \wedge (A \cap \{3,7\} = \{3\})\}$. *vero* ☐ *falso* ☐ *dati insuff.* ☐
- Esistono interi a, b, c, nessuno dei quali multiplo di 11, tali che 11 divida a^4bc^7. *vero* ☐ *falso* ☐ *dati insuff.* ☐
- La permutazione $(1\,2)(1\,3)(1\,2\,3)^2 \in \mathbb{S}_5$ è l'elemento neutro di $\mathbb{S}_5$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- È assegnato un anello $(R, +, \cdot)$. $(R, \cdot)$ è un semigruppo . *vero* ☐ *falso* ☐ *dati insufficienti* ☐

---

2 Per definizione, se A è un anello commutativo unitario, un polinomio $f \in A[x]$ è *irriducibile* se e solo se:

. . . .

Si esibiscano:

un polinomio di grado 11 irriducibile in $\mathbb{Q}[x]$: . . . . , oppure: ☐ *non ne esistono*

un polinomio di grado 11 irriducibile in $\mathbb{R}[x]$: . . . . , oppure: ☐ *non ne esistono*

un polinomio f di grado 8 irriducibile in $\mathbb{Z}_6[x]$ tale che $f([2]_6) = [0]_6$: . . . . , oppure: ☐ *non ne esistono*

---

3 Si forniscano esempi di:

un semigruppo non commutativo: . . . . , oppure:☐ *non ne esistono*

un monoide che non è un gruppo: . . . . , oppure:☐ *non ne esistono*

un gruppo non abeliano: . . . . , oppure:☐ *non ne esistono*

un anello non integro: . . . . , oppure:☐ *non ne esistono*

un dominio di integrità che non è un campo: . . . . , oppure:☐ *non ne esistono*

---

4 Per ogni $n \in \mathbb{Z}$ si ponga $\bar{n} = [n]_{17}$. Si consideri l'operazione binaria $*$ definita in $\mathbb{Z}_{17}$ ponendo $a*b = a+b+\bar{4}$ per ogni $a, b \in \mathbb{Z}_{17}$. Questa operazione è commutativa? *sì* ☐ *no* ☐, associativa? *sì* ☐ *no* ☐. Ammette elemento neutro? ☐ *no*, oppure: ☐ *sì, esso è* . . . . .

L'elemento $\bar{6}$ è simmetrizzabile in $(\mathbb{Z}_{17}, *)$? ☐ *no*, oppure: ☐ *sì, il suo simmetrico è* . . . . . L'elemento $\bar{9}$ è cancellabile in $(\mathbb{Z}_{17}, *)$? ☐ *no* ☐ *sì*. Esistono in $(\mathbb{Z}_{17}, *)$ elementi non cancellabili? ☐ *no*, oppure: ☐ *sì, ad esempio* . . . . . Esistono in $(\mathbb{Z}_{17}, *)$ elementi idempotenti? ☐ *no*, oppure: ☐ *sì, ad esempio* . . . . .

$(\mathbb{Z}_{17}, *)$ è un semigruppo? *sì* ☐ *no* ☐, un monoide? *sì* ☐ *no* ☐, un gruppo? *sì* ☐ *no* ☐, un gruppo abeliano? *sì* ☐ *no* ☐.

---

5 Si considerino le relazioni binarie α, β, γ, δ definite nell'insieme $S = \{n \in \mathbb{N} \mid n < 20\}$ ponendo, per ogni $a, b \in S$,

$$a\ \alpha\ b :\Longleftrightarrow\ a^2 \equiv_8 b; \qquad a\ \beta\ b :\Longleftrightarrow\ a \equiv_5 b+1;$$

$$a\ \gamma\ b :\Longleftrightarrow\ (a^2 \equiv_7 b^2 \wedge a \le b); \qquad a\ \delta\ b :\Longleftrightarrow\ a^2+4 \equiv_{10} b^2-6.$$

α è una equivalenza? ☐ *sì*, oppure: ☐ *no, perché non è* . . . . *, in quanto* . . . . ,

β è una equivalenza? ☐ *sì*, oppure: ☐ *no, perché non è* . . . . *, in quanto* . . . . ,

γ è una equivalenza? ☐ *sì*, oppure: ☐ *no, perché non è* . . . . *, in quanto* . . . . ,

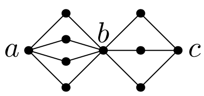
δ è una equivalenza? ☐ *sì*, oppure: ☐ *no, perché non è* . . . . *, in quanto* . . . .

Se almeno una tra α, β, γ e δ è un'equivalenza, detta essa $\sim$ (dunque $\sim$ = . . .), si ha $|S/{\sim}|$ = ... , $[1]_\sim = \{$ . . . . $\}$ e $[5]_\sim = \{$ . . . . $\}$.

---

6 Si disegni a destra il diagramma di Hasse dell'insieme ordinato (S, σ), dove $S = \{-2, 0, 1, 7, 15, 42, (7 \cdot 15)^2, 30^4\}$ e σ è l'ordinamento indotto su S dalla divisibilità in $\mathbb{Z}$. In questo ordinamento:
$\min S = \ldots\ldots$, oppure: $\square$ $\min S$ *non esiste;*
$\max S = \ldots\ldots$, oppure: $\square$ $\max S$ *non esiste;*
$\inf\{0, 15, 42\} = \ldots\ldots$, oppure: $\square$ $\inf\{0, 15, 42\}$ *non esiste.*
(S, σ) è un reticolo? *sì* $\square$ *no* $\square$, un reticolo complementato? *sì* $\square$ *no* $\square$, distributivo? *sì* $\square$ *no* $\square$, booleano? *sì* $\square$ *no* $\square$. La sua parte $\{0, 1, 7, 15\}$ è totalmente ordinata? *sì* $\square$ *no* $\square$

---

7 

Sia G il grafo disegnato a sinistra. Per ogni $n, m \in \mathbb{Z}$ siano $X_n = \{n, -n\}$ e $Y_{n,m} = \{x \in \mathbb{Z} \mid n \leq x \leq m\}$; sia poi $V = \{\mathbb{N}, X_1, X_2, X_3, X_4, X_7, X_8, X_9, Y_{-5,-1}, Y_{-9,-7}\}$. Definiamo i grafi $G_1 = (V, L_1)$, $G_2 = (V, L_2)$ e $G_3 = (V, L_3)$ ponendo:
$L_1 = \big\{\{A, B\} \in \mathcal{P}_2(V) \mid A \cap B = \varnothing\big\}$, $L_2 = \big\{\{A, B\} \in \mathcal{P}_2(V) \mid A \cap B \neq \varnothing\big\}$, $L_3 = \big\{\{A, B\} \in \mathcal{P}_2(V) \mid A \neq B\big\}$. Tra questi tre grafi, quali non sono: $\ldots\ldots\ldots$ e quali sono: $\ldots\ldots\ldots$ isomorfi a G? Se qualcuno di essi è isomorfo a G, sceglierne uno: $\ldots$; esiste un isomorfismo da G a questo grafo che manda il vertice b in $\ldots\ldots$

In G esistono cammini euleriani? *sì* $\square$ *no* $\square$, esistono circuiti euleriani? *sì* $\square$ *no* $\square$. Quanti sono i cammini da a a c? $\ldots\ldots$ Quanti tra questi sono euleriani? $\ldots\ldots$

---

8 Sapendo che 1033 è primo, $\mathcal{U}(\mathbb{Z}_{1033}) = \langle [5]_{1033} \rangle$ e che $5^{1032/3} \bmod 1033 = 837$, $5^{1032/4} \bmod 1033 = 678$, quali sono, in $\mathcal{U}(\mathbb{Z}_{1033})$, i periodi di $[837]_{1033}$: $\ldots\ldots$ e di $[678]_{1033}$: $\ldots\ldots$?

Calcolare $(837 \cdot 678)^{924} \bmod 1033 = \ldots\ldots$, $(837)^{-1} \bmod 1033 = \ldots\ldots$, $(678)^{-1} \bmod 1033 = \ldots\ldots$

Si trovi l'insieme (rispettivamente S_1, S_2, S_3) di tutte le soluzioni intere di ciascuna delle seguenti equazioni congruenziali:

$837 \cdot 678x \equiv_{1033} 5$; $\qquad$ $5x \equiv_{1033} 3$; $\qquad$ $10x \equiv_{2066} 3$;

$S_1 = \ldots\ldots\ldots\ldots\ldots\ldots$; $\qquad$ $S_2 = \ldots\ldots\ldots\ldots\ldots\ldots$; $\qquad$ $S_3 = \ldots\ldots\ldots\ldots\ldots\ldots$;

---

9 Siano, in $\mathbb{Q}[x]$, $f = x^{11} + x^{10} + x + 1$ e $g = x^8 + x^7 - x - 1$. Si calcolino, in $\mathbb{Q}[x]$, i massimi comuni divisori monici: d tra f e $7g$; d_1 tra $189f$ e $f + g$; d_2 tra $8f^2$ e $(f - g)^2$.

$d = \ldots\ldots\ldots\ldots\ldots\ldots$; $\qquad$ $d_1 = \ldots\ldots\ldots\ldots\ldots\ldots$; $\qquad$ $d_2 = \ldots\ldots\ldots\ldots\ldots\ldots$

f ha qualche radice in $\mathbb{Q} \setminus \mathbb{Z}$? $\square$ *no*, oppure: $\square$ *sì, una è* $\ldots$
$(x^2 - 5)f + 3g$ è irriducibile in $\mathbb{Q}[x]$? $\square$ *no, perché* $\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$,
oppure: $\square$ *sì, perché* $\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$
