CdS in Informatica — a.a. 2009/2010

Esercitazione scritta di **ALGEBRA** (Proff. Cutolo e Rao) venerdì 19 marzo 2010

NOME E COGNOME	MATRICOLA

GRUPPO ☐ *I (Rao)* ☐ *rec. (Cutolo)*	ESAME: martedì 23 marzo, ore 15, studio 88, DMA

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

- L'insieme dei numeri reali non negativi, con le consuete operazioni $+$ e $\cdot$ è un campo. *vero* ☐ *falso* ☐ *dati insuff.* ☐
- Nessun polinomio f di grado 7 in $\mathbb{Z}_{33}[x]$ ha più di 7 radici in $\mathbb{Z}_{33}$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- L'operazione $\diamond$ in $\mathcal{P}(\mathbb{Z})$, data da $(\forall X, Y \in \mathcal{P}(\mathbb{Z}))(X \diamond Y = (X \cup Y) \smallsetminus \mathbb{N})$, è associativa. *vero* ☐ *falso* ☐ *dati insuff.* ☐
- Esistono insiemi distinti A, B tali che $A \smallsetminus B = A \cup B$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- La forma proposizionale $\big(((p \Rightarrow q) \Rightarrow r) \Rightarrow (p \Rightarrow q)\big) \iff (p \Rightarrow q)$ è una tautologia. *vero* ☐ *falso* ☐ *dati insuff.* ☐
- $127548! \equiv_{1290!} 87345!$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- $\{a \in \mathbb{R} \mid a^2 < 0 \Rightarrow a^2 > a^2 + 1\} = \mathbb{R}$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐

---

2 Si enunci il *principio di identità dei polinomi*: se A è un anello unitario che sia ....

.... , e $f, g \in A[x]$, allora ....

....

---

3 In $\mathbb{S}_{10}$ si scriva $\alpha = (1\,6\,8)(2\,7\,3\,9\,4\,5)(1\,2\,4)(3\,5\,6\,8\,10)(7\,9)$ come prodotto di cicli a due a due disgiunti: $\alpha =$ .... , oppure: ☐ *non esiste una tale fattorizzazione.*

Il periodo di α è .... ; α è di classe ☐ *pari*, ☐ *dispari*, ☐ *nessuna delle due*, ☐ *entrambe.*

Si calcoli α^{-1}: .... Esiste $\beta \in \mathbb{S}_{10}$ tale che $\alpha\beta = (1\,2\,9\,4)$? *sì* ☐ *no* ☐.

Esiste $\beta \in \mathbb{S}_{10}$ tale che $\alpha\beta^2 = (3\,2\,8\,7)$? *sì* ☐ *no* ☐.

---

4 Siano $A = \{n \in \mathbb{N} \mid n \leq 10\}$ e $B = \{a, b, c, d, e, f, g\}$ tale che $|B| = 7$. Indicare $|\operatorname{InjMap}(A, B)| =$ .... , $|\operatorname{InjMap}(B, A)| =$ .... , $|\mathcal{P}(A \times B)| =$ .... . Sia $\varphi \colon A \to B$ l'applicazione definita da

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ f & a & c & b & c & e & b & a & d & e & g \end{pmatrix}.$$

φ è iniettiva? *sì* ☐ *no* ☐, suriettiva? *sì* ☐ *no* ☐, ha sezioni? *sì* ☐ *no* ☐, ha retrazioni? *sì* ☐ *no* ☐.

Siano ρ e σ le relazioni binarie in B definite ponendo, per ogni $x, y \in B$,

$$x\ \rho\ t \iff (\forall n, m \in A)\big(((n^\varphi = x) \wedge (m^\varphi = y)) \Rightarrow n < m\big); \quad x\ \sigma\ t \iff (\exists n, m \in A)\big((n^\varphi = x) \wedge (m^\varphi = y) \wedge (n < m)\big).$$

ρ è un ordinamento? *sì* ☐ *no* ☐; σ è un ordinamento? *sì* ☐ *no* ☐. Se possibile, si scelga una tra le due che sia un ordinamento (specificare quale: ...) e se ne disegni a fianco il diagramma di Hasse. B, così ordinato, è un reticolo? *sì* ☐ *no* ☐; nel caso, è distributivo? *sì* ☐ *no* ☐, complementato? *sì* ☐ *no* ☐, booleano? *sì* ☐ *no* ☐.

---

5 Calcolare (se esistono):

$100^3 \bmod 657 =$ ...... , oppure: ☐ *non esiste*; $(-100)^3 \bmod 657 =$ ...... , oppure: ☐ *non esiste*

$100^4 \bmod 657 =$ ...... , oppure: ☐ *non esiste*; $(\sum_{i=0}^{2^{10}} 100^{10^i}) \bmod 657 =$ ...... , oppure: ☐ *non esiste*

$2^{-1} \bmod 657 =$ ...... , oppure: ☐ *non esiste*; $3^{-1} \bmod 657 =$ ...... , oppure: ☐ *non esiste*;

$5^{-1} \bmod 657 =$ ...... , oppure: ☐ *non esiste.*

---

6 Sia $V = \{n \in \mathbb{N} \mid n < 10\}$ e siano $A = \big\{\{a,b\} \in \mathcal{P}(V) \mid a+b \equiv_4 2\big\}$, $B = \big\{\{a,b\} \in \mathcal{P}(V) \mid a+b \equiv_5 3\big\}$, $C = \big\{\{a,b\} \in \mathcal{P}(V) \mid a+b \equiv_6 3\big\}$. Quali tra $G_A = (V, A)$, $G_B = (V, B)$ e $G_C = (V, C)$ sono: . . . . e quali non sono: . . . . grafi (semplici)? Se possibile, se ne scelga uno che lo è e lo si chiami G (dunque, $G =$ . . .) e si risponda alle domande che seguono. Quante componenti connesse ha G? . . . ; G è un albero *sì* ☐ *no* ☐, una foresta?, *sì* ☐ *no* ☐ha cammini euleriani?, *sì* ☐ *no* ☐circuiti euleriani? *sì* ☐ *no* ☐. Senza modificare l'insieme dei vertici, è possibile:

(1) aggiungere a G un numero m di lati in modo che:
G diventi un albero? *sì* ☐ *no* ☐, nel caso, a questo scopo, il minimo valore possibile per m è . . .
G diventi una foresta? *sì* ☐ *no* ☐, nel caso, a questo scopo, il minimo valore possibile per m è . . .
G abbia circuiti euleriani? *sì* ☐ *no* ☐, nel caso, a questo scopo, il minimo valore possibile per m è . . .
G abbia cammini euleriani? *sì* ☐ *no* ☐, nel caso, a questo scopo, il minimo valore possibile per m è . . .

(2) cancellare da G un numero n di lati in modo che:
G diventi un albero? *sì* ☐ *no* ☐, nel caso, a questo scopo, il minimo valore possibile per n è . . .
G diventi una foresta? *sì* ☐ *no* ☐, nel caso, a questo scopo, il minimo valore possibile per n è . . .
G abbia circuiti euleriani? *sì* ☐ *no* ☐, nel caso, a questo scopo, il minimo valore possibile per n è . . .
G abbia cammini euleriani? *sì* ☐ *no* ☐, nel caso, a questo scopo, il minimo valore possibile per n è . . .

Si disegnino, ove possibile, grafi con cammini euleriani ottenuti come in (1) e in (2) per i valori minimi di m ed n (al più un grafo per tipo).

---

7 Sia, ancora, $V = \{n \in \mathbb{N} \mid n < 10\}$. Si considerino in V le tre relazioni binarie α, β, γ definite ponendo, per ogni $a, b \in V$,

$$a \,\alpha\, b :\iff a + 2b \equiv_6 2, \qquad a \,\beta\, b :\iff (5 \mid a \iff 5 \mid b), \qquad a \,\gamma\, b :\iff 125 \mid a + b.$$

α è antisimmetrica? *sì* ☐ *no* ☐, β è transitiva? *sì* ☐ *no* ☐, γ è riflessiva? *sì* ☐ *no* ☐, γ è antiriflessiva? *sì* ☐ *no* ☐. Se almeno una delle tre è di equivalenza, detta questa ρ (dunque $\rho =$ . . .) si indichino $|V/\rho| =$ . . . e $[9]_\rho = \{$ . . . . $\}$. Quante sono le relazioni di equivalenza σ in V tali che $[3]_\sigma = [3]_\rho$? . . .

---

8 In $\mathbb{Q}[x]$, sia $f = x^7 - 4x^5 - 6x^4 + 3x^3 + 24x^2 - 18$ e, posto $S = \{c \in \mathbb{Q} \mid f(c) = 0\}$, sia $g = \prod_{c \in S}(x - c)$. Indicare il massimo comun divisore monico d_1 tra f e g: $d_1 =$ . . . . Sia ora $h = x^6 - 2x^5 - 2x^4 - 2x^3 + 12x^2 + 12x - 24$; si calcolino il massimo comun divisore monico d_2 tra $2f$ e $3h + f$ ed il massimo comun divisore monico d_3 tra $4g$ e h:

$d_2 =$ . . . . ; $d_3 =$ . . . .

Si scriva f come prodotto di polinomi monici irriducibili in $\mathbb{Q}[x]$: $f =$ . . . . ; Sia f_7 il polinomio f riguardato come polinomio a coefficienti in $\mathbb{Z}_7$. Si scriva f_7 come prodotto di polinomi monici irriducibili in $\mathbb{Z}_7[x]$: $f_7 =$ . . . .
