CdL in Informatica — a.a. 2007/2008

Esercitazione scritta di **ALGEBRA** (Proff. Cutolo e Rao) martedì 15 gennaio 2008

NOME E COGNOME	MATRICOLA

GRUPPO ☐ *I (Rao)* ☐ *IV (Cutolo)*	PREFERENZA PER L'ESAME ☐ *merc. 16/1* ☐ *ven. 18/1*

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

- $1234567! + 1 \equiv_{11111} 7654321! - 1$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- La forma proposizionale $(q \Rightarrow p) \vee (r \Rightarrow \neg p)$ è una tautologia. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- La forma proposizionale $\big(p \wedge (r \vee \neg q)\big) \Rightarrow \big((q \Rightarrow p) \vee (r \Rightarrow \neg p)\big)$ è una tautologia. *vero* ☐ *falso* ☐ *dati insuff.* ☐
- Esistono $s, t \in \mathbb{Z}$ tali che $2^{12}7^5 13^{80} s + 2^7 5^{13} 11^{17} 41 t = 320$ *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- L'applicazione $f\colon A \in \mathcal{P}(\mathbb{N}) \smallsetminus \{\varnothing\} \mapsto \min A \in \mathbb{N}$ è iniettiva. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- È assegnata $\sigma \in \mathbb{S}_{10}$. σ^{10} ha classe pari. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- Posto, $S = \{i \in \mathbb{N} \mid i < 11\}$, $\{X \subseteq S \mid 3 < |S \smallsetminus X| < 5\} \subseteq \mathcal{P}_7(\mathbb{N})$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐

---

2 Per definizione, se X è un insieme, P è una *partizione* di X se e solo se . . . .

. . . .

Esiste Y tale che $\pi = \big\{\mathbb{N} \smallsetminus \{12, 4567, 10^7\}, Y\big\}$ sia una partizione di $\mathbb{N}$? ☐ *no*, oppure: ☐ *sì, ad esempio* $Y =$ . . . . , inoltre, ☐ *questa è l'unica scelta possibile per Y affinché π sia una partizione*, oppure: ☐ *ce ne sono altre.*

---

3 Il Teorema di Ruffini stabilisce che, se A è un anello commutativo unitario e $f \in A[x]$ allora, ...

. . . .

Si fornisca un esempio di polinomio $f \in \mathbb{Z}[x]$ tale che f abbia grado otto e -4, -3, 0, 7 siano radici di f ma 1 non ne sia radice:

$f =$ . . . . , oppure: ☐ *tale f non esiste.*

Si fornisca poi un esempio di polinomio $g \in \mathbb{Z}[x]$ di grado 17 di cui 1 sia radice e che sia irriducibile in $\mathbb{Q}[x]$:

$g =$ . . . . , oppure: ☐ *tale g non esiste.*

---

4 Si consideri in $\mathcal{P}(\mathbb{Z})$ l'operazione binaria $\star$ definita ponendo $A \star B = B \cap \mathbb{N}$ per ogni $A, B \subseteq \mathbb{Z}$.

$\star$ è commutativa? *sì* ☐ *no* ☐, associativa? *sì* ☐ *no* ☐, ammette elemento neutro a sinstra? ☐ *no*, oppure: ☐ *sì, uno è* . . . . ; ammette elemento neutro a destra? ☐ *no*, oppure: ☐ *sì, uno è* . . . . ; ammette elemento neutro? ☐ *no*, oppure: ☐ *sì, esso è* . . . . Esiste in $(\mathcal{P}(\mathbb{Z}), \star)$ qualche elemento idempotente? ☐ *no*, oppure: ☐ *sì, uno è* . . . . Sia $X = \{n \in \mathbb{Z} \mid n < 4000\}$. $\mathcal{P}(X)$ è una parte stabile in $(\mathbb{Z}, \star)$? ☐ *sì*, oppure: ☐ *no, perché* . . . .

In $(\mathbb{Z}, \star)$, X è cancellabile a sinistra? ☐ *sì*, oppure: ☐ *no, perché* . . . . ; X è cancellabile a destra? ☐ *sì*, oppure: ☐ *no, perché* . . . .

---

5 Sia $G = (V, L)$ un albero tale che $|V| = 6$. Si ha allora $|L| =$ . . . , oppure: ☐ *non è possibile stabilire quanto vale $|L|$*. Dei sei vertici di G, esattamente tre hanno grado 1 e almeno uno ha grado 3. Che grado hanno i due rimanenti vertici? . . . e . . . , oppure: ☐ *impossibile stabilirlo.*

A meno di isomorfismi, quanti sono gli alberi con queste proprietà? . . . . Disegnarne quanti più possibile, a due a due non isomorfi tra loro.

6 Siano A e B due insiemi tali che $|A| = 8$ e $|B| = 12$. Si indichino (senza calcolarle) le cardinalità:
$|A \times B| =$ . . . . , $|\operatorname{Map}(A, B)| =$ . . . . , $|A \smallsetminus (A \cup B)| =$ . . . . , $|\mathcal{P}(B)| =$ . . . . , $|\mathcal{P}_5(A)| =$ . . . . ,
$|\operatorname{InjMap}(A, B)| =$ . . . . , $|\operatorname{SurMap}(A, B)| =$ . . . .

Quante sono le corrispondenze da A a B? . . . . E quelle da B ad A? . . . .

---

7 Si consideri la relazione binaria σ definita nell'insieme $S = \{x \in \mathbb{Z} \mid 0 < x < 15\}$ ponendo, per ogni $a, b \in S$,

$$a \,\sigma\, b :\iff \big(\exists\, u, v \in \mathbb{Z} \smallsetminus (2\mathbb{Z} \cup 7\mathbb{Z})\big)(a \equiv_{14} bu \ \wedge\ b \equiv_{14} av)$$

σ è un'equivalenza? ☐ *sì*, oppure: ☐ *no, perché non è* . . . . , *in quanto* . . . .

Se σ è un'equivalenza, si ha $|S/\sigma| =$ . . . . , $[1]_\sigma = \{$. . . . .$\}$, $[2]_\sigma = \{$. . . . .$\}$ $[3]_\sigma = \{$. . . . .$\}$, $[7]_\sigma = \{$. . . . .$\}$.

---

8 Sia $S = \{n \in \mathbb{N}^{\#} \mid n < 9\}$. Allora $|S| =$ . . . . Si determini l'unico $x \in S \times S$ tale che

$$G = \Delta_S \cup \{x\} \cup \big\{(1,2),(1,5),(2,5),(3,2),(3,5),(3,6),\\ (4,1),(4,2),(4,3),(4,5),(4,7),(4,8),(6,5),(7,5),(7,6),(8,5),(8,6),(8,7)\big\}$$

sia il grafico di una relazione di ordine largo in S. $x =$ . . . . Detta ρ questa relazione, si disegni a fianco il diagramma di Hasse di (S, ρ).

Rispetto all'ordinamento ρ, $\min S =$ . . . . , oppure: ☐ $\min S$ *non esiste;*
$\max S =$ . . . . , oppure: ☐ $\max S$ *non esiste;*
$\inf\{2, 6, 7\} =$ . . . . , oppure: ☐ $\inf\{2, 6, 7\}$ *non esiste.*
S è un reticolo? *sì* ☐ *no* ☐. Nel caso, è un reticolo complementato? *sì* ☐ *no* ☐,
distributivo? *sì* ☐ *no* ☐, booleano? *sì* ☐ *no* ☐.

---

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

$2007x \equiv_{2008} 2003$; $\qquad$ $2006x \equiv_{2008} 2003$; $\qquad$ $160x \equiv_{2008} 24$;

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

Sapendo che 251 è primo, qual è il periodo di $[20]_{251} \in \mathcal{U}(\mathbb{Z}_{251})$? . . . . Calcolare: $20^2 \bmod 251 =$ . . . . ; $20^4 \bmod 251 =$ . . . . ; $20^5 \bmod 251 =$ . . . . ; $20^{-1} \bmod 251 =$ . . . . ; $20^{1234567} \bmod 251 =$ . . . . .

---

10 In $\mathbb{Q}[x]$ si calcoli il massimo comun divisore monico d tra $f = x^7 + 3x^5 + 2x^4 + 6x^3 + 6x^2 + 12$ e $g = x^6 + 2x^4 + 3x^2 - 6$.

$d =$ . . . .

L'insieme S delle radici comuni a f e g è . . . . (dunque $|S| =$ . . . .).

Si scrivano le fattorizzazioni di f e g come prodotti di irriducibili monici in $\mathbb{Q}[x]$:

$f =$ . . . . ; $\quad$ $g =$ . . . .

Siano ora f_5 e g_5, nell'ordine, f e g riguardati come polinomi a coefficienti in $\mathbb{Z}_5$. Si scrivano le fattorizzazioni di f_5 e g_5 come prodotti di irriducibili monici in $\mathbb{Z}_5[x]$:

$f_5 =$ . . . . ; $\quad$ $g_5 =$ . . . .

Si calcolino un massimo comun divisore $\bar{d}$ ed un minimo comune multiplo $\bar{m}$ tra f_5 e g_5 in $\mathbb{Z}_5[x]$:

$\bar{d} =$ . . . . ; $\quad$ $\bar{m} =$ . . . .
