CdL in Informatica — a.a. 2005/2006

Esercitazione scritta di **ALGEBRA** (Proff. Cutolo e Rao) venerdì 24 novembre 2006

NOME E COGNOME	MATRICOLA

GRUPPO ☐ *I (Rao)* ☐ *IV (Cutolo)* PREFERENZA PER L'ESAME ☐ *urgenti* ☐ *non urgenti*

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

- $(\forall\, n, m \in \mathbb{Z})(n \equiv_{159128} m \Longrightarrow n \equiv_4 m)$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- $(\forall\, n, m \in \mathbb{Z})(n \equiv_4 m \Longrightarrow n \equiv_{159128} m)$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- 3 divide $10^6 + 10^3$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- L'applicazione $n \in \mathbb{Z} \mapsto n \in \mathbb{Q}$ è suriettiva. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- La forma $\big((p \Rightarrow \neg r) \Rightarrow (p \Rightarrow q)\big) \Rightarrow \big(p \Rightarrow (\neg r \Rightarrow q)\big)$ è una tautologia. *vero* ☐ *falso* ☐ *dati insuff.* ☐
- Scelti comunque insiemi A, B, C, D, si ha $A \cap C \subseteq (B \cup C) \cap (A \cup D)$. *vero* ☐ *falso* ☐ *dati insuff.* ☐
- Sia S un insieme tale che $|S| = 1000$. In S esistono almeno 1000 relazioni di equivalenza distinte.
  vero ☐ *falso* ☐ *dati insufficienti* ☐

---

2 Sia $(S, *)$ è una struttura algebrica in cui $*$ un'operazione binaria e sia $a \in S$. Per definizione a si dice *neutro* in $(S, *)$ se e solo se ....

....

---

3 Sia R l'insieme delle stringhe di lunghezza due composte da una lettera dell'alfabeto italiano scelta nell'insieme $\{a, b, c, d, e, f, g, h, i, l, m, n, o, p\}$ e da una cifra (cioè un intero compreso tra 0 e 9), ad esempio $a7, h6, t0 \in R$. Indichiamo con "$\preceq$" la relazione di "precedenza o uguaglianza" tra le lettere in ordine alfabetico (dunque: $a \preceq a \preceq b \preceq c \preceq \cdots \preceq p$). Tra le relazioni ρ_1 e ρ_2 definite come segue in R, esattamente una è un ordinamento, quale? [*Risposta:* . . . .]. Si tratta di un ordinamento ☐ *stretto* o ☐ *largo*?

$$(\forall xr, ys \in R) \qquad xr\ \rho_1\ ys :\Longleftrightarrow\ (x \preceq y\ \wedge\ r \leq s)$$
$$xr\ \rho_2\ ys :\Longleftrightarrow\ (x \preceq y\ \vee\ r \leq s)$$

Indicata con ρ quella tra ρ_1 e ρ_2 che è un ordinamento, si consideri la parte $S = \{a0, b3, b5, c0, f2, l4, m3, p5\}$ di R ordinata dall'ordinamento indotto su essa da ρ.

Se ne disegni a fianco il diagramma di Hasse. Si determinino:

$\max S =$ . . . . , oppure: ☐ $\max S$ *non esiste*,

$\min S =$ . . . . , oppure: ☐ $\min S$ *non esiste*,

$\inf\{b5, f2, l4\} =$ . . . . , oppure: ☐ $\inf\{b5, f2, l4\}$ *non esiste*,

$\sup\{b5, f2\} =$ . . . . , oppure: ☐ $\sup\{b5, f2\}$ *non esiste*,

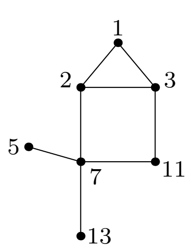
(S, ρ) è un reticolo? *sì* ☐ *no* ☐, nel caso è distributivo? *sì* ☐ *no* ☐, complementato *sì* ☐ *no* ☐, booleano *sì* ☐ *no* ☐?

Si individui in (S, ρ) una parte totalmente ordinata T della cardinalità massima possibile.

$$T = \{ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \}$$

---

4 Sia $V = \{1, 2, 3, 5, 7, 11, 13\}$. Si considerino i tre grafi $G_A = (V, A)$, $G_B = (V, B)$ e $G_C = (V, C)$ così descritti: avendo posto $X_B = \{2, 3, 5, 7, 8, 22, 26, 77, 143\}$ e $X_C = \{6n \mid n \in V\}$, siano $B = \big\{\{n, m\} \mid n, m \in V\ \wedge\ nm \in X_B\big\}$ e $C = \big\{\{n, m\} \mid n, m \in V\ \wedge\ nm \in X_C\big\}$, e sia invece G_A come disegnato a fianco. Tra G_A, G_B e G_C due sono isomorfi tra loro (ma non al terzo). Quali? Descrivere esplicitamente un isomorfismo tra questi due grafi (da . . . . a . . . .):



$$\begin{pmatrix} 1 & 2 & 3 & 5 & 7 & 11 & 13 \\ - & - & - & - & - & - & - \end{pmatrix}$$

Questo è l'unico isomorfismo esistente tra i due grafi? *sì* ☐ *no* ☐.

---

5 Siano $A = \{n \in \mathbb{Z} \mid 12 < n \leq 347 \ \wedge\ 100|n \ \wedge\ 3 \nmid n^2\}$, $B = \{n \in \mathbb{N} \mid n \neq 100 \Rightarrow n = 200\}$, $C = \{n \in \mathbb{N} \mid n \neq 200 \Rightarrow n = 100\}$. Allora, $|B| =$ . . . . . Quali delle seguenti valgono:
☐ $A = B$, ☐ $A \neq B$, ☐ *nessuna delle due precedenti*, ☐ *entrambe*.
☐ $A = C$, ☐ $A \neq C$, ☐ *nessuna delle due precedenti*, ☐ *entrambe*.
☐ $B = C$, ☐ $B \neq C$, ☐ *nessuna delle due precedenti*, ☐ *entrambe*.

---

6 Per ogni $n \in \mathbb{Z} \setminus \{0\}$ si indichi con $\tilde{n}$ la massima potenza di 2 che divide n (ad esempio, se $m = 2^4 \cdot 3^5 \cdot 11^3$ allora $\widetilde{m} = 2^4$) e sia $\tilde{0} = 0$. Si calcolino $\tilde{1} =$ . . . . e $\widetilde{900} =$ . . . . . È vero che $\widetilde{ab} = \tilde{a}\tilde{b}$ per ogni $a, b \in \mathbb{Z}$? *sì* ☐ *no* ☐. L'applicazione $n \in \mathbb{Z} \mapsto \tilde{n} \in \mathbb{Z}$ è un omomorfismo dal monoide $(\mathbb{Z}, \cdot)$ in sé? *sì* ☐ *no* ☐.

Si consideri l'operazione binaria $*$ definita in $\mathbb{Z}$ ponendo, per ogni $a, b \in \mathbb{Z}$, $a * b = \tilde{a}b$. Si stabilisca se $*$ è commutativa *sì* ☐ *no* ☐; associativa *sì* ☐ *no* ☐. In $(\mathbb{Z}, *)$ esistono elementi neutri a sinistra? *sì* ☐ *no* ☐, nel caso fornire un esempio: . . . . , esso è unico? *sì* ☐ *no* ☐, ce ne sono in numero ☐ *finito* o ☐ *infinito*? Similmente, in $(\mathbb{Z}, *)$ esistono elementi neutri a destra? *sì* ☐ *no* ☐, nel caso fornire un esempio: . . . . , esso è unico? *sì* ☐ *no* ☐, ce ne sono in numero ☐ *finito* o ☐ *infinito*?

$(\mathbb{Z}, *)$ è un semigruppo? *sì* ☐ *no* ☐, un monoide? *sì* ☐ *no* ☐, un gruppo? *sì* ☐ *no* ☐. $(\mathbb{Z}, +, *)$ è un anello? *sì* ☐ *no* ☐. Nel caso lo sia, è commutativo *sì* ☐ *no* ☐, unitario *sì* ☐ *no* ☐, un dominio di integrità *sì* ☐ *no* ☐, un campo *sì* ☐ *no* ☐? Nel caso invece non lo sia, perché non lo è?

. . . .

---

7 Calcolare: $32^2 \bmod 205 =$ . . . . , $32^{-1} \bmod 205 =$ . . . . , $32^{206} \bmod 205 =$ . . . .
Trovare l'insieme (rispettivamente S_1, S_2, S_3, S_4) di tutte le soluzioni intere di ciascuna delle seguenti equazioni congruenziali:

$32x \equiv_{205} 1$. $S_1 =$ . . . . $32x \equiv_{205} 32$. $S_2 =$ . . . .

$82x \equiv_{205} 64$. $S_3 =$ . . . . $64x \equiv_{205} 82$. $S_4 =$ . . . .

Quanti sono gli elementi invertibili dell'anello $\mathbb{Z}_{205}$? . . . . . . $\mathbb{Z}_{205}$ è un campo? ☐ *sì*, ☐ *no*, ☐ *impossibile stabilirlo*; è un dominio di integrità? ☐ *sì*, ☐ *no*, ☐ *impossibile stabilirlo*.

---

8 Si considerino i polinomi $f = x^4 - 8x^3 + 18x^2 - 16x + 5$ e $g = x^3 - 6x^2 + 9x - 4$. Si calcoli il massimo comun divisore monico d di f e g in $\mathbb{Q}[x]$:

$d =$ . . . .

e si fattorizzino d, g, f in prodotto di eventuali invertibili e fattori irriducibili monici in $\mathbb{Q}[x]$:

$d =$ . . . . , $g =$ . . . .

$f =$ . . . .

Trovare il minimo numero primo p tale che, detti rispettivamente f_p e g_p i polinomi f e g riguardati su $\mathbb{Z}_p$, un minimo comune multiplo di f_p e g_p in $\mathbb{Z}_p[x]$ abbia grado maggiore di 2. $p =$ . . . . , oppure: ☐ *tale p non esiste*.
