CdS in Informatica — a.a. 2007/2008

Esercitazione scritta di **ALGEBRA** (Proff. Cutolo e Rao) venerdì 21 novembre 2008

NOME E COGNOME	MATRICOLA
GRUPPO ☐ *I (Rao)* ☐ *rec. (Cutolo)*	ESAME: mercoledì 26 novembre, ore 15, aula C, DMA

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

- $63845^{684174} \cdot 27263^7 + 97$ è divisibile per 9. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- $(\mathbb{Z}, +)$ è un sottogruppo di $(\mathbb{Q}, +)$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- $(\mathbb{Z}, \cdot\,)$ è un sottogruppo di $(\mathbb{Q}, \cdot\,)$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- La forma $\big((p \Rightarrow (q \vee r)) \wedge (r \Rightarrow \neg p)\big) \Longrightarrow \big(p \Rightarrow q\big)$ è una tautologia. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- A e B sono due algebre di Boole finite e della stessa cardinalità. $A \simeq B$. *vero* ☐ *falso* ☐ *dati insuff.* ☐
- m è un assegnato intero maggiore di 100. Esistono più di dieci applicazioni iniettive da $\mathbb{N}$ a $\mathbb{Z}_m$.
  vero ☐ *falso* ☐ *dati insufficienti* ☐

---

2 Per definizione, una permutazione α su un insieme finito è di classe *pari* se e solo se ....

....

La permutzione $\sigma = (1\ 2\ 4\ 6)(1\ 2)(3\ 4\ 5)(9\ 8\ 7\ 6\ 5\ 4)$ di $\mathbb{S}_9$ è di classe ☐ *pari*, ☐ *dispari*, ☐ *né pari né dispari*, ☐ *sia pari che dispari*. E σ^2 è di classe ☐ *pari*, ☐ *dispari*, ☐ *né pari né dispari*, ☐ *sia pari che dispari.*

---

3 Si consideri la relazione d'ordine σ definita in $\mathbb{N}^{\#}$ ponendo, per ogni $a, b \in \mathbb{N}^{\#}$, $a\ \sigma\ b$ se e solo se il numero dei divisori primi di a è minore del numero dei divisori primi di b. Rispetto a questo ordinamento, $\mathbb{N}^{\#}$ ha massimo? ☐ *no*, oppure: ☐ *sì, esso è* .... ; ha minimo? ☐ *no*, oppure: ☐ *sì, esso è* .... ; ha elementi massimali? ☐ *no*, oppure: ☐ *sì, uno di essi è* .... ; ha elementi minimali? ☐ *no*, oppure: ☐ *sì, uno di essi è* ..... Esiste una parte infinita di $\mathbb{N}^{\#}$ che, rispetto all'ordinamento indotto da σ, sia totalmente ordinata? *sì* ☐ *no* ☐.

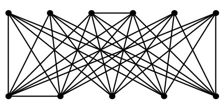
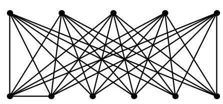
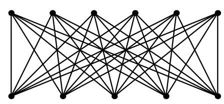
Si consideri $A = \{2^{100}, 10!, 15, 17, 30, 66\}$ ordinato dall'ordinamento indotto da σ. Si disegni a lato il diagramma di Hasse di A e si stabilisca:
$\max A =$ .... , oppure: ☐ $\max A$ *non esiste*;
$\min A =$ .... , oppure: ☐ $\min A$ *non esiste*.
In A, $\inf\{30, 66\} =$ .... , oppure: ☐ $\inf\{30, 66\}$ *non esiste*;
$\sup\{30, 66\} =$ .... , oppure: ☐ $\sup\{30, 66\}$ *non esiste*.
A è un reticolo? *sì* ☐ *no* ☐; nel caso lo sia, è distributivo? *sì* ☐ *no* ☐, complementato? *sì* ☐ *no* ☐, booleano? *sì* ☐ *no* ☐.

---

4 Sia $X = \{n \in \mathbb{Z} \mid -10 \leq n \leq 10\}$ e sia $f\colon x \in X \mapsto [x^2]_3 \in \mathbb{Z}_3$. f è iniettiva? *sì* ☐ *no* ☐, suriettiva? *sì* ☐ *no* ☐. Sia α la relazione binaria in X definita ponendo, per ogni $a, b \in X$, $a\ \alpha\ b \iff a^f = b^f$. Calcolare $|X/\alpha| =$ .... , descrivere esplicitamente $[-6]_\alpha = \{$ .... $\}$, quindi $|[-6]_\alpha| =$ .... , e calcolare $|[7]_\alpha| =$ .... , $|[0]_\alpha| =$ .... e $|[2]_\alpha| =$ .... .

---

5 Siano $V = \{n \in \mathbb{N} \mid n \leq 10\}$, $L_1 = \big\{\{a, b\} \subseteq V \mid a + b \text{ è pari}\big\}$ e $L_2 = \big\{\{a, b\} \subseteq V \mid a + b \text{ è dispari}\big\}$. (V, L_1) è un grafo? *sì* ☐ *no* ☐. (V, L_2) è un grafo? *sì* ☐ *no* ☐. Se possibile, si scelga e si chiami L uno tra L_1 e L_2 in modo che $G = (V, L)$ sia un grafo: $L =$ .... , e si indichi con una freccia quale dei seguenti disegni rappresenti G:

oppure: ☐ *nessuno dei disegni rappresenta G.* G è planare? *sì* ☐ *no* ☐

---

6 Si consideri l'insieme $R = \mathbb{Z}_4 \times \mathbb{Z}_3$. Allora $|R| = \ldots\ldots$ e $|R \cup R| = \ldots\ldots$. In R si definiscano le operazioni $\oplus$ e $*$ ponendo, per ogni $a, c \in \mathbb{Z}_4$ e $b, d \in \mathbb{Z}_3$:

$$(a, b) \oplus (c, d) = (a + c + [1]_4, b + d + [2]_3) \qquad \text{e} \qquad (a, b) * (c, d) = (a + c + ac, b + d - bd).$$

Si ha che $(R, \oplus, *)$ è un anello (non effettuare la verifica). Per stabilirlo occorrerebbe e basterebbe verificare che:

☐ $(R, \oplus)$ è un gruppo e $(R, *)$ è un monoide; ☐ $\oplus$ e $*$ sono associative e commutative;
☐ $(R, \oplus)$ è un gruppo e $*$ è distributiva rispetto a $\oplus$; ☐ nessuna delle risposte precedenti è corretta

$(R, \oplus, *)$ è commutativo? *sì* ☐ *no* ☐, unitario? ☐ *no*, oppure: ☐ *sì, e l'unità è* $1_R = (\ldots\ldots, \ldots\ldots)$. Lo zero di R è $0_R = (\ldots\ldots, \ldots\ldots)$. Se $a = ([0]_4, [1]_3)$, $b = ([1]_4, [1]_3)$, $c = ([2]_4, [0]_3)$, in questo anello a è invertibile? ☐ *no*, oppure: ☐ *sì, l'inverso di a è:* $\ldots\ldots$; b è invertibile? ☐ *no*, oppure: ☐ *sì, l'inverso di b è:* $\ldots\ldots$; c è invertibile? ☐ *no*, oppure: ☐ *sì, l'inverso di c è:* $\ldots\ldots$; a ha un opposto? ☐ *no*, oppure: ☐ *sì, esso è:* $\ldots\ldots$; a è idempotente? *sì* ☐ *no* ☐; b è un divisore dello zero? *sì* ☐ *no* ☐.

L'applicazione $[n]_{12} \in \mathbb{Z}_{12} \mapsto ([n-1]_4, [1-n]_3) \in R$ è ben definita? *sì* ☐ *no* ☐. Nel caso, è un omorfismo da $(\mathbb{Z}_{12}, +)$ a $(R, \oplus)$? *sì* ☐ *no* ☐; un omorfismo da $(\mathbb{Z}_{12}, +)$ a $(R, *)$? *sì* ☐ *no* ☐; un omorfismo di anelli? *sì* ☐ *no* ☐, un omomorfismo di anelli unitari? *sì* ☐ *no* ☐, un isomorfismo di anelli? *sì* ☐ *no* ☐.

Si determinino gli invertibili di R: $|\mathcal{U}(R)| = \ldots\ldots$ e

$$\mathcal{U}(R) = \{\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\}.$$

R è un anello booleano? *sì* ☐ *no* ☐, un dominio di integrità? *sì* ☐ *no* ☐, un campo? *sì* ☐ *no* ☐

---

7 Sia $n = (25^{6731376} + 25^{7731377} + 25^{8731378} + 25^{9731379})^{313}$. Calcolare $n \bmod 313 = \ldots\ldots$. Determinare l'insieme (risp. S_1, S_2, S_3) di tutte le soluzioni intere di ciascuna delle seguenti equazioni congruenziali:

$5^3 x \equiv_{5\cdot 313} 5$; $\qquad 5x \equiv_{5\cdot 313} 5^2$; $\qquad 5^7 x \equiv_{5\cdot 313} 5$;

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

---

8 Si considerino in $\mathbb{Q}[x]$ i polinomi $f = x^8 + 1$ e $g = x^6 - 1$. Calcolare, in $\mathbb{Q}[x]$:

Il massimo comun divisore monico d tra f e g: $\quad d = \ldots\ldots\ldots\ldots\ldots\ldots$

Il massimo comun divisore d_1 tra $f+g$ e $2g$ che abbia coefficiente direttore 3: $d_1 = \ldots\ldots\ldots\ldots$

Il massimo comun divisore d_2 tra $f+g$ e fg che abbia coefficiente direttore 5: $d_2 = \ldots\ldots\ldots\ldots$

Trovare, se esistono, $h, k \in \mathbb{Q}[x]$ tali che $hf + kg = x^{100} + 1$:

$h = \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \qquad k = \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$

oppure: ☐ *non esistono tali h e k.*

Trovare, se esiste, $a \in \mathbb{Q}[x]$ tale che $(\forall b, c \in \mathbb{Q}[x])(a \neq bf + cg)$:

$$a = \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

oppure: ☐ *non esiste un tale a.*
