CdL in Informatica — a.a. 2007/2008

Esercitazione scritta di **ALGEBRA** (Proff. Cutolo e Rao) mercoledì 13 febbraio 2008

NOME E COGNOME	MATRICOLA

GRUPPO ☐ *I (Rao)* ☐ *IV (Cutolo)*	ESAME: venerdì 15 febbraio, ore 9, aula D, DMA

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

- La forma proposizionale $\big((p\wedge q)\vee r\big) \Rightarrow \big(p\wedge(q\vee r)\big)$ è una tautologia. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- Esistono insiemi A, B, C tali che $A \subseteq B$, $A \subseteq C$ e $B \cup C \subseteq A$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- La permutazione $(1\,5)(1\,7\,4)(4\,3\,6\,5\,1)$ ha classe pari. *vero* ☐ *falso* ☐ *dati insuff.* ☐
  e manda 1 in se stesso. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- Esistono anelli di cardinalità 16. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- Esistono gruppi di cardinalità 16. *vero* ☐ *falso* ☐ *dati insufficienti* ☐

---

2 Se $*$ è una operazione binaria definita nell'insieme S e $\sim$ è una relazione di equivalenza in S, si dice che $\sim$ è *compatibile con* $*$ se e solo se: ....

....

La relazione di equivalenza α definita in $\mathbb{N}^{\#}$ ponendo, per ogni a, $b \in \mathbb{N}^{\#}$, $a\ \alpha\ b :\Longleftrightarrow a \equiv_3 b$ è compatibile con l'operazione di elevazione a potenza in $\mathbb{N}^{\#}$ (cioè l'operazione binaria interna in $\mathbb{N}^{\#}$ definita come $(x, y) \in \mathbb{N}^{\#} \times \mathbb{N}^{\#} \mapsto x^y \in \mathbb{N}^{\#}$)? *sì* ☐ *no* ☐.

---

3 Sia $S = \{1, 11, 34, 87\}$. Esiste un intero positivo t tale che il reticolo dei divisori di t in $\mathbb{N}$ sia isomorfo al reticolo $(\mathcal{P}(S), \subseteq)$? ☐ *no*, oppure: ☐ *sì, ad esempio* ....

Esiste un sottoreticolo di $(\mathcal{P}(S), \subseteq)$ che non sia booleano? *sì* ☐ *no* ☐

Per definizione, se $(L, \leq)$ è un reticolo una parte $M \neq \varnothing$ di L costituisce un sottoreticolo se e solo se

....

---

4 Sia $n = 2^4 \cdot 7$. Si ha $\varphi(n) =$ ..... . Detto R l'anello $\mathbb{Z}_n$, il numero degli elementi invertibili in R è .... , e quello degli elementi di R che sono divisori dello zero è .... (esprimere questo numero, senza calcolarlo esplicitamente; ciò vale anche per la prossima domanda). Infine, il numero degli elementi cancellabili in R è .....

Quanti sono i numeri interi compresi tra 1 e n (inclusi) che siano coprimi con n? .... Esistono due interi consecutivi che siano entrambi coprimi con n? ☐ *no*, oppure, ☐ *sì, ad esempio* .... *e* ....

Calcolare $25^{49} \bmod n =$ ....

---

5 Sia X l'insieme della parti finite non vuote di $\mathbb{N}$. Si considerino in X le relazioni binarie α, β, γ, δ definite ponendo, per ogni A, $B \in X$,

$$A\ \alpha\ B :\Longleftrightarrow (\exists a \in A)(\exists b \in B)(a < b); \qquad A\ \beta\ B :\Longleftrightarrow \big((\forall b \in B)(b \text{ è un maggiorante di } A) \wedge (A \cap B = \varnothing)\big);$$

$$A\ \gamma\ B :\Longleftrightarrow (\forall a \in A)(\forall b \in B)(a < b); \qquad A\ \delta\ B :\Longleftrightarrow \big((\forall a \in A)(a \text{ è un minorante di } B) \wedge (A \cap B = \varnothing)\big).$$

Quali tra queste sono .... e quali non sono .... relazioni d'ordine? Se ne esistono, se ne fissi una, sia essa ..... Rispetto a questo ordinamento, X è totalmente ordinato? *sì* ☐ *no* ☐, è un reticolo? *sì* ☐ *no* ☐, è un reticolo booleano? *sì* ☐ *no* ☐. Si descrivano in X gli elementi minimali: ☐ *non ne esistono*, oppure: ☐ *ne esistono; sono tutti e soli gli* $A \in X$ *tali che* ....

e quelli massimali: ☐ *non ne esistono*, oppure: ☐ *ne esistono; sono tutti e soli gli* $A \in X$ *tali che* ....
.... $\min X =$ .... , oppure: ☐ $\min X$ *non esiste*.
$\max X =$ .... , oppure: ☐ $\max X$ *non esiste*

---

6 Una foresta G ha esattamente 112378 vertici e due componenti connesse. Quanti lati ha G? . . . .
G ha meno di tre vertici di grado 1? $\square$ *sì*, $\square$ *no*, $\square$ *impossibile stabilirlo.*

---

7 Il periodo di $[2^6]_{65}$ nel gruppo $\mathcal{U}(\mathbb{Z}_{65})$ è . . . . . Di conseguenza, nello stesso gruppo, il periodo di $[2]_{65}$ è . . . . ed il periodo di $[16]_{65}$ è . . . . . Calcolare $16^{24013} \bmod 65 =$ . . . . .

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

$160x \equiv_{650} 10$; $\qquad$ $16x \equiv_{650} 20$; $\qquad$ $32x \equiv_{130} 5$;

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

---

8 Sia $A = \{n \in \mathbb{N} \mid n < 8\}$ e sia $P = \mathcal{P}(A)$. Allora $|P| =$ . . . . . Vale $A \in P$? *sì* $\square$ *no* $\square$. Sia, poi, $B = \{n \in A \mid n > 4\}$, dunque $|B| =$ . . . . e $|\operatorname{InjMap}(A, B)| =$ . . . . . Si considerino le relazioni binarie α, β e γ definite in P come segue: per ogni $X, Y \in P$,

$$X\ \alpha\ Y :\iff \big((X \cap B = Y \cap B) \wedge (|X \smallsetminus B| = |Y \smallsetminus B|)\big); \qquad X\ \beta\ Y :\iff |X \cap B| = |Y \cap B|;$$
$$X\ \gamma\ Y :\iff \big((X \cap B = Y \cap B) \vee (|X \smallsetminus B| = |Y \smallsetminus B|)\big).$$

α è una equivalenza? $\square$ *sì, e si ha* $|P/\alpha| =$ . . . . , oppure: $\square$ *no, perché non è* . . . . , *in quanto* . . . . β è una equivalenza? $\square$ *sì, e si ha* $|P/\beta| =$ . . . . , oppure: $\square$ *no, perché non è* . . . . , *in quanto* . . . . γ è una equivalenza? $\square$ *sì, e si ha* $|P/\gamma| =$ . . . . , oppure: $\square$ *no, perché non è* . . . . , *in quanto* . . . .

---

9 Siano f e g le applicazioni da $\mathbb{N}$ a $\mathbb{N}$ così definite:

$$f\colon n \in \mathbb{N} \mapsto \begin{cases} 3n, & \text{se } n \text{ è pari;} \\ 2n, & \text{se } n \text{ è dispari} \end{cases} \in \mathbb{N} \qquad g\colon n \in \mathbb{N} \mapsto \begin{cases} 2n, & \text{se } n \text{ è pari;} \\ 5n, & \text{se } n \text{ è dispari} \end{cases} \in \mathbb{N}.$$

f è iniettiva? *sì* $\square$ *no* $\square$, f è suriettiva? *sì* $\square$ *no* $\square$. $\qquad$ g è iniettiva? *sì* $\square$ *no* $\square$, g è suriettiva? *sì* $\square$ *no* $\square$.

Esiste $n \in \mathbb{N}$ tale che f^n sia l'applicazione identica in $\mathbb{N}$? *sì* $\square$ *no* $\square$ *impossibile stabilirlo* $\square$ (la potenza f^n è definita rispetto all'operazione di prodotto operativo).
g ha qualche sezione? $\square$ *no*, $\square$ *sì, esattamente una*, $\square$ *sì, più di una.*
g ha qualche retrazione? $\square$ *no*, $\square$ *sì, esattamente una*, $\square$ *sì, più di una.*
g ha qualche sezione che mandi 12 in 44? *sì* $\square$ *no* $\square$. g ha qualche retrazione che mandi 12 in 44? *sì* $\square$ *no* $\square$.

---

10 Il resto della divisione in $\mathbb{Q}[x]$ del polinomio $f = \sum_{i=0}^{100} x^i$ per $x + 1$ è . . . .

Tenendo presente che 4567 è primo, è vero che, scelto comunque un insieme S formato da 10000 interi consecutivi, esiste $n \in S$ tale che il polinomio $2x^9 + 4567^2x^5 + n$ sia irriducibile in $\mathbb{Q}[x]$? *sì* $\square$ *no* $\square$.

Siano, in $\mathbb{Q}[x]$, $a = x^8 + 1$, $b = x^5 + 1$, $f = 800a$ e $g = 2a - b$. Si calcoli il massimo comun divisore monico d tra f e g. Si ha $d =$ . . . .

Esiste un massimo comun divisore tra f e g che abbia coefficiente direttore $-1/2$? $\square$ *no*, $\square$ *sì, esattamente uno, cioè* . . . . , $\square$ *sì, più di uno, ad esempio* . . . . *e* . . . .
