CdL in Informatica — a.a. 2006/2007
Esercitazione scritta di **ALGEBRA** (Proff. Cutolo e Rao) venerdì 18 maggio 2007

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?

- Esiste una partizione ψ di $\mathbb{Z}$ con la proprietà che $\{1,2,4,5,6\} \in \psi$ e $[84]_5 \in \psi$. *vero* ☐ *falso* ☐ *dati insuff.* ☐
- Supponiamo assegnata una partizione ω di $\mathbb{Z}$ con la proprietà che $\{-10,2,14,506\} \in \omega$. Esiste $\alpha \in \mathrm{Eq}(\mathbb{Z})$ tale che $\mathbb{Z}/\alpha = \omega$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- La congruenza modulo 134 è compatibile con l'operazione di sottrazione in $\mathbb{Z}$. *vero* ☐ *falso* ☐ *dati insuff.* ☐
- $\big(\mathcal{P}(\mathbb{N}), \cup, \cap\big)$ è un anello. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- Il coefficiente binomiale $\binom{799431896}{799431895}$ è 799431896. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- Esistono $n, m \in \mathbb{N}$ tali che $3 \mid 2^n 5^m 7^{n+m}$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- Sia $\alpha = (1\,5)(1\,2\,3\,4)(1\,3\,7)(1\,5\,6) \in \mathbb{S}_7$. Allora α è di classe pari. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
  Inoltre $\alpha^7 = 1$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- Se p è una proposizione vera, q, r e s proposizioni false, allora la proposizione
  $\big((p \Rightarrow q) \Rightarrow \neg r\big) \Longrightarrow \big(((\neg s) \vee r) \Rightarrow (q \iff \neg p)\big)$ è vera. *vero* ☐ *falso* ☐ *dati insufficienti* ☐

---

2 Ricordando che $\mathcal{P}_f(\mathbb{N})$ è l'insieme delle parti finite di $\mathbb{N}$, si considerino le applicazioni

$$f\colon x \in \mathbb{N} \mapsto x^4 + 5 \in \mathbb{N} \qquad h\colon X \in \mathcal{P}(\mathbb{N}) \smallsetminus \mathcal{P}_f(\mathbb{N}) \mapsto \min X \in \mathbb{N}$$

$$g\colon x \in \mathbb{N} \mapsto \{n \in \mathbb{N} \mid n \le x\} \in \mathcal{P}_f(\mathbb{N}) \qquad k\colon X \in \mathcal{P}(\mathbb{Z}) \mapsto \begin{cases} X \cup \{-13\} & \text{se } X \subseteq \mathbb{N} \\ \{-x \mid x \in X\} & \text{se } X \not\subseteq \mathbb{N} \end{cases} \in \mathcal{P}(\mathbb{Z}).$$

f è iniettiva? ☐ *sì*, o: ☐ *no, perché:* . . . . , suriettiva? ☐ *sì*, o: ☐ *no, perché:* . . . .

g è iniettiva? ☐ *sì*, o: ☐ *no, perché:* . . . . , suriettiva? ☐ *sì*, o: ☐ *no, perché:* . . . .

h è iniettiva? ☐ *sì*, o: ☐ *no, perché:* . . . . , suriettiva? ☐ *sì*, o: ☐ *no, perché:* . . . .

k è iniettiva? ☐ *sì*, o: ☐ *no, perché:* . . . . , suriettiva? ☐ *sì*, o: ☐ *no, perché:* . . . .

---

3 Per ogni intero positivo n si ponga $\widehat{n} := \{p \in \mathbb{N} \mid p \text{ è primo e } p \mid n\}$. Sia ρ la relazione d'ordine stretto in $S := \{n \in \mathbb{N}^{\#} \mid n \le 30\}$ definita da: $(\forall\, a,b)(a \;\rho\; b :\iff \widehat{a} \subset \widehat{b})$. Si descrivano esplicitamente, in (S,ρ):

l'insieme A dei minoranti di $\{20,24,30\}$: $A = \{$ . . . . $\}$;

l'insieme B dei maggioranti di $\{3,8,9\}$: $B = \{$ . . . . $\}$;

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

(S,ρ) è un reticolo? *sì* ☐ *no* ☐. Nel caso, è distributivo? *sì* ☐ *no* ☐, complementato? *sì* ☐ *no* ☐, booleano? *sì* ☐ *no* ☐. Siano $X = \{1,8,9,12,16,30\}$ e $Y = X \cup \{18\}$. Si disegnino qui i diagrammi di Hasse di (X,ρ_X) e (Y,ρ_Y), dove ρ_X e ρ_Y sono gli ordinamenti indotti da ρ:

(X,ρ_X) (Y,ρ_Y)

(X,ρ_X) è un reticolo? *sì* ☐ *no* ☐. Nel caso, è distributivo? *sì* ☐ *no* ☐, complementato? *sì* ☐ *no* ☐, booleano? *sì* ☐ *no* ☐, $\{1,8,9,30\}$ è un sottoreticolo di (X,ρ_X)? *sì* ☐ *no* ☐.

(Y,ρ_Y) è un reticolo? *sì* ☐ *no* ☐. Nel caso, è distributivo? *sì* ☐ *no* ☐, complementato? *sì* ☐ *no* ☐, booleano? *sì* ☐ *no* ☐, $\{1,8,9,30\}$ è un sottoreticolo di (Y,ρ_Y)? *sì* ☐ *no* ☐.

---

4 Sia $(S,\cdot)$ un semigruppo commutativo e siano $a,\, b \in S$. Per definizione, a divide b in $(S,\cdot)$ se e solo se

. . . .

---

5 Di un grafo (semplice) G sappiamo che ha esattamente 1000 vertici e 10 componenti connesse. Indicare: il minimo possibile numero, m, di lati di G. $m =$ . . . . . È possibile che G abbia $\binom{1000}{2}$ lati? *sì* □ *no* □.

Se G ha esattamente m lati, cosa possiamo dire su G? [*Risposta:* che G è . . . .] Se G ha esattamente $m+1$ lati, quante componenti connesse di G sono alberi? . . . . .

---

6 Si considerino le relazioni binarie α, β e γ definite in $\mathbb{N}^{\#}$ ponendo per ogni $a, b \in \mathbb{N}^{\#}$:

$$a\ \alpha\ b :\iff (\forall i \in \mathbb{N})(10^i < a \iff 10^i < b)$$

$a\ \beta\ b :\iff$ nella usuale rappresentazione in base 10, a e b hanno lo stesso numero di cifre

$$a\ \gamma\ b :\iff (\forall n \in \mathbb{N})(a \le 10^n \iff b \le 10^n)$$

Quali tra α, β e γ sono: . . . . e quali non sono: . . . . equivalenze? Se possibile, si scelga una relazione di equivalenza ρ tra α, β e γ (dunque $\rho =$ . . .) e si ponga $Q = \mathbb{N}^{\#}/\rho$. Si indichino: $[4]_\rho = \{$ . . . . $\}$, $\big|[465]_\rho\big| =$ . . . . , $\big|[12]_\rho \times [85]_\rho\big| =$ . . . . , $|Q| =$ . . . .

Esiste una relazione di equivalenza τ su $\mathbb{N}^{\#}$ tale che $\tau \ne \rho$ e $\mathbb{N}^{\#}/\tau = Q$? *sì* □ *no* □

Si consideri la relazione binaria σ definita in Q ponendo, per ogni $X, Y \in Q$,

$$X\ \sigma\ Y :\iff (X \text{ e } Y \text{ sono entrambi infiniti, oppure sono entrambi finiti e } |X| \equiv_6 |Y|).$$

σ è una relazione di equivalenza? *sì* □ *no* □. Nel caso lo sia, calcolare $|Q/\sigma| =$ . . . . e $\big|\big[[3]_\rho\big]_\sigma\big| =$ . . . . .

---

7 Una stringa di caratteri si dice *palindroma* se si legge allo stesso modo da sinistra verso destra e da destra verso sinistra (ad esempio, *xyaabaayx* è palindroma). Avendo a disposizione un alfabeto di 6 caratteri, quante stringhe palindrome di lunghezza 5 possiamo ottenere? . . . . . E quante di lunghezza 6? . . . .

---

8 Calcolare: $28^2 \bmod 157 =$ . . . . , $28^3 \bmod 157 =$ . . . . , $28^4 \bmod 157 =$ . . . . , $157^2 \bmod 29 =$ . . . . , $157^3 \bmod 29 =$ . . . . , $157^4 \bmod 29 =$ . . . . , $28^{156} \bmod 157 =$ . . . . , $28^{156156} \bmod 157 =$ . . . . , $157^{28} \bmod 29 =$ . . . . , $157^{2828} \bmod 29 =$ . . . . .

Per ognuna delle seguenti equazioni congruenziali, si trovi poi l'insieme (rispettivamente S_1, S_2, S_3, S_4, S_5, S_6) di tutte le soluzioni intere:

$12x \equiv_{29} 157$. $S_1 =$ . . . . $157x \equiv_{29} 12$. $S_2 =$ . . . .

$29x \equiv_{157} 186$. $S_3 =$ . . . . $186x \equiv_{157} 29$. $S_4 =$ . . . .

$2x \equiv_{29\cdot 157} 2$. $S_5 =$ . . . . $2x \equiv_{29\cdot 157} 1$. $S_6 =$ . . . .

---

9 Si considerino in $\mathbb{Q}[x]$ i polinomi $f = x^{20} - 1$, $g = x^5 + x^3 + 2x^2 + 3$, $h = (x^7+1)g$ e $k = (x^7+1)(g+1)$. In $\mathbb{Q}[x]$ si determini il massimo comun divisore monico d tra f, h e k, nonché, se possibile, un massimo comun divisore d_5, sempre tra f, h e k che abbia coefficiente direttore 5.

$d =$ . . . .

$d_5 =$ . . . . oppure □ *un tale* d_5 *non esiste.*

Esistono $a,\, b \in \mathbb{Q}[x]$ tali che $(x+4)d^2 = 12(x^7+1)a - bf$? *sì* □ *no* □ *impossibile stabilirlo* □

Si determini l'insieme delle radici razionali comuni ad h e k:

$$\{q \in \mathbb{Q} \mid h(q) = k(q) = 0\} = \text{. . . . .}$$

f ha radici in $\mathbb{Q}$ che non siano intere? *sì* □ *no* □ *impossibile stabilirlo* □
