CdL in Informatica — a.a. 2005/2006

Esercitazione scritta di **ALGEBRA** (Proff. Cutolo e Rao) venerdì 15 dicembre 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?

- Siano $n = 11 + 2^5 \cdot 3^{14}$ e $m = 2n$. Allora:
  - ogni divisore dispari di m divide n. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
  - ogni divisore dispari di n divide m. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- Il polinomio $x^7 - 3x^4 + 1 \in \mathbb{Z}_{15}[x]$ è invertibile in $\mathbb{Z}_{15}[x]$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- $927342619814^{178732398}$ è multiplo di 3. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- Esistono 14 trasposizioni $\sigma_1, \dots, \sigma_{14} \in \mathbb{S}_8$ tali che $\sigma_1\sigma_2\cdots\sigma_{14} = (1\,4\,3)$. *vero* ☐ *falso* ☐ *dati insuff.* ☐
- Esistono 14 trasposizioni $\sigma_1, \dots, \sigma_{14} \in \mathbb{S}_8$ tali che $\sigma_1\sigma_2\cdots\sigma_{14} = (7\,1\,4\,3)$. *vero* ☐ *falso* ☐ *dati insuff.* ☐

---

2 Sia Φ la forma proposizionale $(p \Rightarrow \neg q) \wedge \big((p \vee q) \Rightarrow r\big)$. Si determini il valore di verità assunto da Φ in ciascuno dei seguenti casi:

[p vero, q vero, r vero]: ☐ V ☐ F; [p falso, q vero, r falso]: ☐ V ☐ F; [p vero, q falso, r falso]: ☐ V ☐ F

Φ è ☐ *una tautologia*, ☐ *contingente*, ☐ *una contraddizione*, ☐ *nessuna delle tre*

Sia Ψ un'altra forma proposizionale. Allora la forma proposizionale $\Phi \Rightarrow (\Psi \Rightarrow \Phi)$ è:
☐ *una tautologia*, ☐ *contingente*, ☐ *una contraddizione*, ☐ *impossibile stabilirlo (dipende da Ψ)*

---

3 Sia $S = \{A, B, C, D, E, F\}$, dove

$$A = \{n \in \mathbb{Z} \mid (\exists m \in \mathbb{N})(n + m = 4)\}, \qquad B = \{n \in \mathbb{Z} \mid (\forall m \in \mathbb{N})(n + m = 4)\},$$
$$C = \{n \in \mathbb{Z} \mid (\exists m \in \mathbb{N})(n + 4 = m)\}, \qquad D = \{n \in \mathbb{Z} \mid (\exists m \in \mathbb{Z})(n + 4 = m)\},$$
$$E = \{n \in \mathbb{Z} \mid 17^{4n+3} > 11^{n^2} \cdot 13 \Rightarrow n = n\}, \qquad F = \{n \in \mathbb{Q} \mid n \neq |n| \ \wedge\ n^3 > 0\}.$$

Si indichi la cardinalità (eventualmente infinita) di ciascuno degli insiemi: $|S| = \dots$, $|A| = \dots$, $|B| = \dots$, $|C| = \dots$, $|D| = \dots$, $|E| = \dots$, $|F| = \dots$, $|A \cap C| = \dots$, $|A \times F| = \dots$, $|\mathrm{SurjMap}(E, B)| = \dots$.

Ordinato S per inclusione, se ne disegni a fianco il diagramma di Hasse.
$(S, \subseteq)$ è un reticolo? *sì* ☐ *no* ☐, nel caso, è booleano? *sì* ☐ *no* ☐. $(S, \subseteq)$ è totalmente ordinato? *sì* ☐ *no* ☐. Esiste $X \in S$ tale che $(S \setminus \{X\}, \subseteq)$ sia una catena? ☐ *no*, oppure: ☐ *sì, un tale X è* ...

---

4 Si consideri l'operazione binaria $\diamond$ definita in $\mathcal{P}(\mathbb{Z})$ ponendo, per ogni $X, Y \in \mathcal{P}(\mathbb{Z})$, $X \diamond Y = (X \cup Y) \cap \mathbb{N}$.
$\diamond$ è associativa? *sì* ☐ *no* ☐, commutativa? *sì* ☐ *no* ☐, ha elemento neutro? *sì* ☐ *no* ☐, quanti sono in $\mathcal{P}(\mathbb{Z})$ gli elementi cancellabili rispetto a $\diamond$? ..... In $\big(\mathcal{P}(\mathbb{Z}), \diamond\big)$:

$\mathcal{P}(\mathbb{N})$ è stabile? *sì* ☐ *no* ☐. Nel caso, $\big(\mathcal{P}(\mathbb{N}), \diamond\big)$ ha elementi neutri? *sì* ☐ *no* ☐, è un gruppo? *sì* ☐ *no* ☐.

$\mathcal{P}(\mathbb{Z} \setminus \mathbb{N})$ è stabile? *sì* ☐ *no* ☐. Nel caso, $\big(\mathcal{P}(\mathbb{Z} \setminus \mathbb{N}), \diamond\big)$ ha elementi neutri? *sì* ☐ *no* ☐, è un gruppo? *sì* ☐ *no* ☐.

$\{\varnothing, \{3\}\}$ è stabile? *sì* ☐ *no* ☐. Nel caso, $\big(\{\varnothing, \{3\}\}, \diamond\big)$ ha elementi neutri? *sì* ☐ *no* ☐, è un gruppo? *sì* ☐ *no* ☐.

---

5 Esiste un grafo $G = (V, L)$ tale che $|V| = 12$, $|L| = \binom{12}{2} - 1$ e G non abbia sottografi isomorfi al grafo completo su 4 vertici? *sì* ☐ *no* ☐. (Se no, perché ....).
Nel caso, disegnarne uno qui sotto. Esistono due siffatti grafi tra loro non isomorfi? *sì* ☐ *no* ☐

---

6 Il Teorema di Bézout garantisce che, se f, g e h sono polinomi a coefficienti in un campo K, esistono $s, t \in K[x]$ tali che $fs + gt = h$ se e solo se ....

---

7 Sia $A = \{u, v, w\}$ in modo che $|A| = 3$ e si considerino $\sigma \in \mathrm{Corr}(A, \mathbb{N})$ e $\tau \in \mathrm{Corr}(\mathbb{N}, A)$ definite dai grafici:

$$\sigma^{\#} = \{(u,2),(u,4),(v,100),(w,n) \mid n \in \mathbb{N} \text{ e } n \text{ è dispari}\}$$
$$\tau^{\#} = \{(2n,u) \mid 30 > n \in \mathbb{N}^{\#}\} \cup \{(2n+1,v) \mid n \in \mathbb{N}\} \cup \{(50n,w) \mid n \in \mathbb{N}\}$$

(dunque τ fa corrispondere ad ogni $a \in \mathbb{N}$ l'elemento u se a è pari e minore di 60, v se a è dispari, w se a è multiplo di 50). σ è un'applicazione? *sì* □ *no* □, τ è un'applicazione? *sì* □ *no* □. Sia ρ la corrispondenza composta $\sigma\tau$ (dunque $\rho \in \mathrm{Corr}(A, A) = \mathrm{Rel}(A)$ e $\rho^{\#} = \sigma^{\#}\tau^{\#}$). Scrivere esplicitamente gli elementi di $\rho^{\#}$:

$$\rho^{\#} = \{\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\}, \qquad |\rho^{\#}| = \ldots\ldots\ldots$$

ρ è un'applicazione? *sì* □ *no* □. Se no, perché?.......................... Se sì, è iniettiva? *sì* □ *no* □, suriettiva? *sì* □ *no* □.

Come relazione binaria in A, ρ è riflessiva? *sì* □ *no* □, antiriflessiva? *sì* □ *no* □, simmetrica? *sì* □ *no* □, antisimmetrica? *sì* □ *no* □, transitiva? *sì* □ *no* □. È una equivalenza? *sì* □ *no* □. Se lo è descrivere A/ρ, elencando esplicitamente gli elementi di ciascuna classe di equivalenza modulo ρ:

$$A/\rho = \{\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\}, \quad |A/\rho| = \ldots$$

e dire quanti sono i numeri interi strettamente compresi tra 48756786 e 508278790677 che abbiano esattamente $|[u]_\rho|^{12} + 12^{|[w]_\rho|}$ divisori primi (sono esattamente ....).

---

8 Posto $n = 9^{1000} + 9^{1001} + 9^{1002} + 9^{1003} + 9^{1004} + 9^{1005}$, si ha: $n \bmod 61 = \ldots$, $9^{-1} \bmod 61 = \ldots$, $(-9)^{-1} \bmod 61 = \ldots$.

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

$90x \equiv_{610} 50$. $\quad S_1 = \ldots\ldots\ldots\ldots$ $\qquad$ $90x \equiv_{610} -50$. $\quad S_2 = \ldots\ldots\ldots\ldots$

$50x \equiv_{610} 90$. $\quad S_3 = \ldots\ldots\ldots\ldots$ $\qquad$ $50x \equiv_{610} -90$. $\quad S_4 = \ldots\ldots\ldots\ldots$

---

9 In $\mathbb{Q}[x]$, il massimo comun divisore *monico* dei polinomi $f = x^5 + 14x^4 + 76x^3 + 200x^2 + 256x + 128$ e $g = 5x^4 + 56x^3 + 228x^2 + 400x + 256$ è il polinomio $d = \ldots\ldots\ldots\ldots\ldots$.

Come si può descrivere l'insieme $S = \{k \in \mathbb{Q}[x] \mid (k|f \ \wedge \ k|g) \wedge (\forall h \in \mathbb{Q}[x])((h|f \ \wedge \ h|g) \Rightarrow h|k))\}$?

È $S = \ldots\ldots\ldots\ldots\ldots\ldots\ldots$

Se $C := \{c \in \mathbb{Q}[x] \mid f(c) = 0 = g(c)\}$, si ha $C = \ldots\ldots\ldots$. Si decompongano d, f e g nel prodotto di un elemento invertibile e di polinomi *monici* irriducibili:

$$d = \ldots\ldots\ldots\ldots\ldots , \qquad g = \ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$f = \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots .$$

Il polinomio $p = (x^3 + 2)(x^2 + 4)$ è irriducibile in $\mathbb{Q}[x]$? *sì* □ *no* □ *impossibile stabilirlo* □

In $\mathbb{Q}[x]$, qual è il massimo comun divisore *monico* d_1 dei polinomi $f_1 = p^3 f$ e $g_1 = (x + 4)p^2 g$?

$$d_1 = \ldots\ldots\ldots\ldots\ldots\ldots$$

Infine, detti f_3 e g_3 i polinomi f e g riguardati come polinomi a coefficienti in $\mathbb{Z}_3[x]$, si scrivano f_3 e g_3 come prodotti di un elemento invertibile e di polinomi monici irriducibili in $\mathbb{Z}_3[x]$:

$$f_3 = \ldots\ldots\ldots\ldots\ldots , \qquad g_3 = \ldots\ldots\ldots\ldots\ldots$$

e se ne indichino il massimo comun divisore monico d_3 ed il minimo comune multiplo m_3:

$$d_3 = \ldots\ldots\ldots\ldots\ldots , \qquad m_3 = \ldots\ldots\ldots\ldots\ldots$$
