CdL in Informatica — a.a. 2006/2007

Esercitazione scritta di **ALGEBRA** (Proff. Cutolo e Rao) martedì 10 luglio 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?

- Un certo $f \in \mathbb{Z}_{111}[x]$ ha un fattore di primo grado. f ha radici in $\mathbb{Z}_{111}$. *vero* ☐ *falso* ☐ *dati insuff.* ☐
- $\mathbb{Z}_2$ è un anello booleano. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- Dati gli insiemi A, B, C, D si ha $(A \cup B) \cap (C \cap D) \cap A = D \cap A \cap C$. *vero* ☐ *falso* ☐ *dati insuff.* ☐
- Esiste $n \in \mathbb{N}$ tale che $10^{100} < n < 10^{1000}$ e $n \equiv_{195372} 2487$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- Esiste un intero n che, modulo 3, non sia congruo a 0, né a 10 né a 50. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- La somma dei primi 111 interi positivi è pari. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- $\big\{A \in \mathcal{P}(\mathbb{Z}) \,\big|\, |A| < 1\big\} = \{\varnothing\}$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐

---

2 Siano $U = \{n \in \mathbb{N}^{\#} \mid n \leq 8\}$ e $V = \{n \in \mathbb{N}^{\#} \mid n \leq 20\}$. Si considerino le applicazioni $f\colon x \in U \mapsto 2x \in V$ e $g\colon V \to U$ definita da

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 \\ 3 & 7 & 2 & 2 & 8 & 4 & 1 & 3 & 7 & 6 & 7 & 1 & 4 & 5 & 1 & 8 & 2 & 4 & 1 & 1 \end{pmatrix}.$$

Quante sezioni ha f? . . . e quante retrazioni? . . . . Quante sezioni ha g? . . . e quante retrazioni? . . .
Sia $\alpha := fg$. Allora α ha dominio . . . . e codominio . . . . , ed è descritta da:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \_ & \_ & \_ & \_ & \_ & \_ & \_ & \_ \end{pmatrix}$$

α è una permutazione? *sì* ☐ *no* ☐. Se lo è la si scriva come prodotto di cicli disgiunti: $\alpha =$ . . . . , se ne calcoli il periodo: . . . . e si stabilisca se è di classe ☐ *pari* o ☐ *dispari*. Se $\beta := gf$ è una permutazione si faccia lo stesso per β: $\beta =$ . . . . ha periodo . . . . ed è di classe ☐ *pari* ☐ *dispari*, oppure: ☐ *β non è una permutazione.*

---

3 Sia $g\colon V \to U$ l'applicazione definita nell'esercizio 2. Si considerino in V le relazioni binarie α, β, γ , δ così definite: per ogni $x, y \in V$,

$$x\,\alpha\,y :\iff y^g \equiv_{10} x^g; \quad x\,\beta\,y :\iff y^g - x^g \in \mathbb{N}; \quad x\,\gamma\,y :\iff y \equiv_{22} x; \quad x\,\delta\,y :\iff y^g - x^g \in \mathbb{N}^{\#}.$$

Quali tra α, β, γ e δ sono: . . . . e quali non sono: . . . . equivalenze? Quali sono: . . . . e quali non sono: . . . . relazioni d'ordine (stretto o largo)?

Se possibile, si scelga una relazione di equivalenza ρ tra α, β, γ e δ che non sia anche d'ordine (dunque $\rho =$ . .), si calcoli $|V/\rho| =$ . . . . e si descriva esplicitamente

$$[12]_\rho = \{\,.\,.\,.\,.\,.\,.\,.\,.\,.\,.\,.\,.\,.\,.\,.\,.\,.\,\} \qquad (\text{dunque } \big|[12]_\rho\big| = \,.\,.\,.\,).$$

Se possibile, si scelga un ordinamento σ tra α, β, γ e δ che non sia anche un'equivalenza (dunque $\sigma =$ . . è un ordinamento, ☐ *largo* o ☐ *stretto*?). Rispetto a questo ordinamento, V è totalmente ordinato? *sì* ☐ *no* ☐, è un reticolo? *sì* ☐ *no* ☐. $\min V =$ . . . , oppure ☐ $\min V$ *non esiste*. L'insieme dei minoranti di $\{4, 5, 6\}$ in V è $\{$. . . . .$\}$. $\sup\{6, 13\} =$ . . . . , oppure: ☐ $\sup\{6, 13\}$ *non esiste*. Per ogni $T \in \mathcal{P}(V)$ indichiamo con σ_T l'ordinamento indotto da σ su T. Esiste $T \in \mathcal{P}(V)$ tale che $|T| = 4$ e (T, σ_T) sia un reticolo booleano? ☐ *no*, oppure: ☐ *sì, un esempio è* $T = \{$. . . . .$\}$. Esiste $T \in \mathcal{P}(V)$ tale che $|T| = 14$ e (T, σ_T) sia un reticolo booleano? ☐ *no*, oppure: ☐ *sì, un esempio è* $T = \{$. . . . .$\}$.

---

4 In accordo con il teorema di Bézout, se K è un campo e $f, g \in K[x]$, l'insieme $\{uf + vg \mid u, v \in K[x]\}$ coincide con l'insieme dei . . . .

5 Si consideri la forma proposizionale $\Phi = \big((p \wedge q) \Rightarrow p\big) \wedge \big((s \vee t) \Rightarrow r\big)$. Questa è ☐ *una tautologia*, ☐ *una contraddizione*, ☐ *contingente*, ☐ *nessuna delle tre*. Si esprima il valore di verità assunto da Φ in ciascuno dei casi indicati: p, q, r, s, t veri: Φ è ☐ *vera* ☐ *falsa* p, q, r, s, t falsi: Φ è ☐ *vera* ☐ *falsa*
p, q, r, s veri, t falso: Φ è ☐ *vera* ☐ *falsa* p, s veri, q, r, t falsi: Φ è ☐ *vera* ☐ *falsa*
r vera, gli altri valori non sono noti: Φ è ☐ *vera* ☐ *falsa* ☐ *impossibile stabilirlo*
p falsa, gli altri valori non sono noti: Φ è ☐ *vera* ☐ *falsa* ☐ *impossibile stabilirlo*

---

6 Si considerino i grafi (semplici) $G = (V, L)$ tali che $|V| = 9$ e G abbia due vertici di grado 1, quattro di grado 2, due di grado 3 e uno di grado 6. Per un tale grafo si ha $|L| =$ . . . , oppure: ☐ *è impossibile stabilirlo.* A meno di isomorfismi, quanti di tali grafi esistono? ☐ *nessuno*, ☐ *esattamente uno (e lo disegno in basso)*, ☐ *più di uno (e ne disegno in basso due non isomorfi).* Esiste un tale grafo G che sia un albero? *sì* ☐ *no* ☐ (nel caso, disegnarne uno a sinistra).

---

7 Si consideri l'operazione binaria $*$ definita in $S = \mathbb{Z}_{10} \times \mathbb{Z}$ ponendo, per ogni $(a, b), (a', b') \in S$,

$$(a, b) * (a', b') = (aa' + 3a + 3a' + 6, bb').$$

$*$ è commutativa? *sì* ☐ *no* ☐, associativa? *sì* ☐ *no* ☐. Esiste in $(S, *)$ un elemento neutro? ☐ *no*, oppure: ☐ *sì, esattamente uno, esso è* . . . . , o, ancora: ☐ *sì, uno è* . . . . , *ma ce ne sono altri.*

$(S, *)$ è un semigruppo? *sì* ☐ *no* ☐, un monoide? *sì* ☐ *no* ☐, un gruppo? *sì* ☐ *no* ☐. Nel caso in cui la domanda abbia senso, quanti elementi invertibili ha $(S, *)$? . . . . . Se questi sono meno di dieci, elencarli:

. . . .

$\mathcal{U}(S)$ munito dell'operazione indotta da $*$ è un gruppo? *sì* ☐ *no* ☐, un gruppo abeliano? *sì* ☐ *no* ☐.
Se $(6, -1) \in \mathcal{U}(S)$, se ne calcoli l'inverso . . . . e il periodo . . . , oppure: ☐ $(6, -1) \notin \mathcal{U}(S)$.
Se $(1, 1) \in \mathcal{U}(S)$, se ne calcoli l'inverso . . . . e il periodo . . . , oppure: ☐ $(1, 1) \notin \mathcal{U}(S)$.

---

8 Calcolare: $1019^{-1} \bmod 1021 =$ . . . . , $1021^{-1} \bmod 1019 =$ . . . . , $374^{-1} \bmod 1021 =$ . . . . , $374^{374} \bmod 1021 =$ . . . . .

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

$1019x \equiv_{1021} 10$. $\big[S_1 = \;......\big]$. $1021x \equiv_{1019} 10$. $\big[S_2 = \;......\big]$. $374x \equiv_{1021} 10$. $\big[S_3 = \;......\big]$.

Calcolare il minimo intero positivo m e il massimo intero negativo n tali che $374m \equiv_{1021} 10$ e $374n \equiv_{1021} 10$.
☐ *m non esiste*, oppure: ☐ *m esiste e $m =$* . . . . . ☐ *n non esiste*, oppure: ☐ *n esiste e $n =$* . . . . .

---

9 In $\mathbb{Q}[x]$ si considerino $p = x^{10} + 2$, $a = 2x^6 + x^5 + 5x^3 + 2x^2 + 2$ e $b = 2x^5 + 3x^4 + 5x^3 + 3x^2 + x + 2$.

p è irriducibile in $\mathbb{Q}[x]$? *sì* ☐ *no* ☐. p è irriducibile in $\mathbb{R}[x]$? *sì* ☐ *no* ☐. Qual è il polinomio monico h del minimo grado possibile che sia multiplo di p ed abbia -2 come radice? $h =$ . . . .

Qual è il massimo comun divisore monico d_1 tra $f := a^2p$ e $ap + 1$? $d_1 =$ . . . .
Si calcoli il massimo comun divisore monico d tra f e $g := b^2(ap + 1)$, quindi si indichino le radici (in $\mathbb{Q}$) comuni a f e g, infine si fattorizzi f in $\mathbb{Q}[x]$ come prodotto di un polinomio invertibile e di polinomi monici irriducibili.

$d =$ . . . . $\{c \in \mathbb{Q} \mid f(c) = g(c) = 0\} =$ . . . .

$f =$ . . . .
