CdL in Informatica — a.a. 2004/2005

Esercitazione scritta di **ALGEBRA** (Proff. Cutolo e Rao) venerdì 23 settembre 2005

NOME E COGNOME	MATRICOLA

GRUPPO ☐ *I (Rao)* ☐ *IV (Cutolo)* PREFERENZA PER L'ESAME ☐ *urgenti* ☐ *non urgenti*

1 Il resto modulo 9 di $13265256679856729875 58 \cdot 555555555555$ è . . . . .

---

2 Si calcoli il minimo intero positivo dispari n che sia multiplo di 124 e congruo a 12 modulo 30.
$n =$ . . . . , oppure: ☐ *tale n non esiste.*

---

3 Quali delle seguenti affermazioni sono vere per ogni grafo connesso finito G, se supponiamo che v e w siano due vertici di G, che v abbia grado 16 e w abbia grado 10?

- esiste in G un cammino euleriano di estremi v e w se e solo se in G esistono al più due vertici di grado dispari. *vero* ☐ *falso* ☐
- esiste in G un cammino euleriano di estremi v e w se e solo se ogni vertice di G è pari. *vero* ☐ *falso* ☐
- esiste in G un circuito euleriano se e solo se ogni vertice di G ha grado pari. *vero* ☐ *falso* ☐
- G ha almeno 12 vertici. *vero* ☐ *falso* ☐
- v e w non sono adiacenti. *vero* ☐ *falso* ☐

---

4 Sia $S = \{n \in \mathbb{N} \mid n \leq 20\}$. Si considerino in $\mathcal{P}(S)$ le relazioni binarie ρ e σ definite da: $\forall X, Y \in \mathcal{P}(S)$,

$$X \,\rho\, Y :\iff |X| \equiv_{17} |Y|$$
$$X \,\sigma\, Y :\iff X \cup Y = S$$
$$X \,\tau\, Y :\iff X \subset Y \cup \{1\}.$$

Si completi la tabella a destra.
Quali tra ρ, σ e τ sono equivalenze?
. . . . (o ☐ *nessuna*)
E quali sono ordinamenti (stretti o larghi)? . . . . (o ☐ *nessuno*)

	riflessiva		antiriflessiva		simmetrica		antisimmetrica		transitiva	
	sì	*no*	*sì*	*no*	*sì*	*no*	*sì*	*no*	*sì*	*no*
ρ è										
σ è										
τ è										

Se una tra ρ, σ e τ è una equivalenza, chiamiamola ε (scegliamo dunque $\varepsilon =$ . . .), si dica quanti sono gli elementi di $\mathcal{P}(S)/\varepsilon$ e quanti quelli della ε-classe di equivalenza di $\{11\}$:

$|\mathcal{P}(S)/\varepsilon| =$ . . . . $|[\{11\}]_\varepsilon| =$ . . . .

Se una tra ρ, σ e τ è un ordinamento, chiamiamolo η (scegliamo dunque $\eta =$ . . . ; si tratta di un ordinamento ☐ *largo* oppure ☐ *stretto*?), si dica quanti sono gli elementi minimali in $\mathcal{P}(S)$, ordinato secondo η (sono . . . .), se $(\mathcal{P}(S), \eta)$ è un reticolo (*sì* ☐ *no* ☐), se è un reticolo booleano (*sì* ☐ *no* ☐), e si calcoli poi, sempre con riferimento a η,

$\sup\{X \subset S \mid |X| = 3\} =$ . . . . , oppure: ☐ $\sup\{X \subset S \mid |X| = 3\}$ *non esiste.*

---

5 Si considerino le operazioni binarie:
$\alpha\colon (a,b) \in \mathbb{Z} \times \mathbb{Z} \longmapsto b - a \in \mathbb{Z}$ $\beta\colon (a,b) \in \mathbb{Z} \times \mathbb{Z} \longmapsto b + a \in \mathbb{Z}$
$\gamma\colon (a,b) \in \mathbb{N} \times \mathbb{N} \longmapsto a^b \in \mathbb{N}$ $\delta\colon (a,b) \in \mathbb{N} \times \mathbb{N} \longmapsto a^b + b^a \in \mathbb{N}$
α è associativa? *sì* ☐ *no* ☐, β è associativa? *sì* ☐ *no* ☐, γ è associativa? *sì* ☐ *no* ☐, δ è associativa? *sì* ☐ *no* ☐.

---

6 Si calcolino i possibili valori di verità della formula proposizionale $(p \Rightarrow p) \Longrightarrow \big(p \vee (\neg p)\big)$. Se p si assume vera, il valore della formula è ☐ *vero* ☐ *falso*. Se p si assume falsa, il valore della formula è ☐ *vero* ☐ *falso*.

---

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

$1770x \equiv_{2570} 110$. $S_1 = \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$

$1770x \equiv_{257} 110$. $S_2 = \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$

$177x \equiv_{25} 110$. $S_3 = \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$

L'anello $\mathbb{Z}_{257}$ è un dominio di integrità? *sì* □ *no* □, è un campo? *sì* □ *no* □. È un sottoanello di $\mathbb{Z}$? *sì* □ *no* □. È un anello booleano? *sì* □ *no* □. Sapendo che il gruppo $\mathcal{U}(\mathbb{Z}_{257})$ è generato da $[3]_{257}$ e che $[177]_{257} = [3]_{257}^{4\cdot 597\cdot 173\cdot 49}$, qual è il periodo di $[3]_{257}$? . . . . E qual è il periodo di $[177]_{257}$? . . . . E quello di $[177]_{257}^{-1}$? . . . . Calcolare $3^{102610251982} \bmod 257 =$ . . . .

Il polinomio $f = [256256198]_{257} + [177]_{257}x$ è irriducibile nell'anello $\mathbb{Z}_{257}[x]$? *sì* □ *no* □. f ammette qualche radice in $\mathbb{Z}_{257}$? *sì* □ *no* □. Se sì, quali? . . . .

---

8 Dati in $\mathbb{Q}[x]$ i polinomi $f = x^8 + 2x^7 - 15x^6 - 24x^5 + 84x^4 + 96x^3 - 208x^2 - 128x + 192$ e $g = x^4 + 2x^3 - 4x^2 - 2x + 3$,

si trovino il massimo comun divisore *monico* d di f e g, i quozienti $f_1 = f/d$ e $g_1 = g/d$, il massimo comun divisore *monico* d_1 di f_1 e g_1, il massimo comun divisore *monico* d_2 di f_1^2 e g_1^2, gli insiemi $C_1 = \{c \in \mathbb{Q} \mid f_1(c) = 0 = g_1(c)\}$ e $C = \{c \in \mathbb{Q} \mid f(c) = 0 = g(c)\}$.

$d = \dots\dots\dots\dots\dots\dots$

$f_1 = \dots\dots\dots\dots\dots\dots$, $g_1 = \dots\dots\dots\dots\dots\dots$

$d_1 = \dots\dots\dots\dots\dots\dots$, $d_2 = \dots\dots\dots\dots\dots\dots$

$C_1 = \dots\dots\dots\dots\dots\dots$, $C = \dots\dots\dots\dots\dots\dots$

Si decompongano poi d, f e g in prodotto di polinomi monici irriducibili nell'anello $\mathbb{Q}[x]$:

$d = \dots\dots\dots\dots\dots\dots$

$f = \dots\dots\dots\dots\dots\dots$, $g = \dots\dots\dots\dots\dots\dots$

Infine, riguardati i polinomi f e g a coefficienti in $\mathbb{Z}_3$, si trovino nell'anello $\mathbb{Z}_3[x]$ le fattorizzazioni in prodotto di polinomi monici irriducibili del massimo comun divisore monico d_3 e del minimo comune multiplo monico m_3 di f e di g:

$d_3 = \dots\dots\dots\dots\dots\dots$, $m_3 = \dots\dots\dots\dots\dots\dots$

---

9 Si spieghi (sul questo foglio) perché ogni intero della forma $645a - 3465 + 195b$, dove $a, b \in \mathbb{Z}$, è divisibile per 15.
