CdL e CdD in Informatica — a.a. 2002/2003
Esercitazione scritta di **ALGEBRA** (Prof. Rao) martedì 25 febbraio 2003

NOME E COGNOME	MATRICOLA

1 A e B sono due insiemi tali che $|A \cap B| = 11$, $|A| = 111$, $|A \cup B| = 1111$. Quanto vale $|B|$? Vale . . . . , oppure ☐ *dati insufficienti per decidere.*

---

2 La forma proposizionale $\Big(\big((\neg q) \Rightarrow r\big) \Rightarrow \big(p \Rightarrow r\big)\Big) \Longrightarrow \Big(p \Rightarrow (\neg q)\Big)$
è: ☐ *una tautologia,* ☐ *contingente,* ☐ *una contraddizione.*

Invece, la forma proposizionale $\Big(p \Rightarrow (\neg q)\Big) \Longrightarrow \Big(\big((\neg q) \Rightarrow r\big) \Rightarrow \big(p \Rightarrow r\big)\Big)$
è: ☐ *una tautologia,* ☐ *contingente,* ☐ *una contraddizione.*

---

3 [*Riportare i calcoli relativi a questo esercizio e le motivazioni alle risposte sul retro di questo foglio*]
Dati in $\mathbb{Q}[x]$ i polinomi $f = x^6 + 9x^5 + 25x^4 + 26x^3 + 3x^2 - 11x - 5$ e $g = x^5 + 7x^4 + 11x^3 + 3x^2 - 12x - 10$, con l'algoritmo euclideo si trovino il massimo comun divisore *monico* d di f e g e dei polinomi u_0, $v_0 \in \mathbb{Q}[x]$ tali che $d = u_0 f + v_0 g$. Si trovino poi l'insieme C delle radici razionali comuni a f e g e si calcolino i quozienti $g_1 = g/d$ e $f_1 = f/d$.

[Risposte: $d =$ . . . .

$u_0 =$ . . . . $v_0 =$ . . . .

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

$g_1 =$ . . . . $f_1 =$ . . . .]

Infine si decompongano i polinomi d, g ed f nel prodotto di polinomi *monici irriducibili* in $\mathbb{Q}[x]$:

$d =$ . . . . $g =$ . . . .

$f =$ . . . .

Siano $A := \{(u, v) \in \mathbb{Q}[x] \times \mathbb{Q}[x] \mid uf + vg = d\}$, $B := \{(h, k) \in \mathbb{Q}[x] \times \mathbb{Q}[x] \mid hf_1 + kg_1 = 1\}$ e si consideri l'applicazione $\varphi : h \in \mathbb{Q}[x] \mapsto (u_0 + g_1 h, v_0 - f_1 k) \in \mathbb{Q}[x] \times \mathbb{Q}[x]$. L'insieme A è vuoto? *sì* ☐ *no* ☐. L'insieme B è vuoto? *sì* ☐ *no* ☐. L'applicazione φ è ben definita? *sì* ☐ *no* ☐. Quali delle seguenti affermazioni sono vere?

☐ $A \subset B$, ☐ $B \subset A$, ☐ $A \not\subseteq B$, ☐ $B \not\subseteq A$, ☐ $A \neq B$, ☐ $A = B$;
☐ *φ è iniettiva,* ☐ *φ è suriettiva,* ☐ $\mathrm{im}(\varphi) \neq A$, ☐ $\mathrm{im}(\varphi) = A$, ☐ *l'insieme A è finito,* ☐ *l'insieme A è infinito;*
☐ *tutte,* ☐ *nessuna.*

Calcolare: $\min\{\deg(uv) \mid (u, v) \in A\} =$ . . . .

Siano $H := \{uf + vg \mid (u, v) \in \mathbb{Q}[x] \times \mathbb{Q}[x]\}$ e $K := \{dk \mid k \in \mathbb{Q}[x]\}$. Quali delle seguenti affermazioni sono vere?

☐ $H = K$, ☐ $H \neq K$, ☐ $H \not\subseteq K$, ☐ $K \not\subseteq H$, ☐ $H \subset K$, ☐ $K \subset H$, ☐ *tutte,* ☐ *nessuna.*

H è un ideale di $\mathbb{Q}[x]$? *sì* ☐ *no* ☐. K è un ideale di $\mathbb{Q}[x]$? *sì* ☐ *no* ☐. Se sì, K è un ideale proprio massimale di $\mathbb{Q}[x]$? *sì* ☐ *no* ☐. Se K è un ideale, l'anello quoziente $\mathbb{Q}[x]/K$ è un campo? *sì* ☐ *no* ☐. Se K è un ideale, l'applicazione $\psi : h \in \mathbb{Q}[x] \mapsto h + K \in \mathbb{Q}[x]/K$ è un omomorfismo di anelli? *sì* ☐ *no* ☐. È un epimorfismo? *sì* ☐ *no* ☐. È un isomorfismo? *sì* ☐ *no* ☐.

Siano f_5 e g_5 rispettivamente f e g riguardati come polinomi in $\mathbb{Z}_5[x]$, e sia d_5 il loro massimo comun divisore monico in $\mathbb{Z}_5[x]$. Si decompongano (nell'ordine) f_5, g_5 e d_5 nel prodotto di polinomi monici irriducibili in $\mathbb{Z}_5[x]$:

$f_5 =$ . . . . $g_5 =$ . . . .

$d_5 =$ . . . .

---

4 Si consideri l'anello $(A,+,\cdot)$ di sostegno l'insieme $A := \{x \in \mathbb{Z} \mid 0 \leq x < 8\}$, con addizione e moltiplicazione definite da: $\forall\, x, y \in A$,

$$x + y := (x+y) \bmod 8 \qquad\qquad x \cdot y := (xy) \bmod 8$$

(cioè, resti della divisione per 8, rispettivamente, della somma e del prodotto usuali degli interi x, y).

$(A,+,\cdot)$ è isomorfo all'anello $\mathbb{Z}_8$? *sì* ☐ *no* ☐. Se sì, un isomorfismo è l'applicazione (completare):

$$\varphi : x \in A \longmapsto \ldots\ldots\ldots\ldots\ldots \in \mathbb{Z}_8$$

$(A,+,\cdot)$ è commutativo? *sì* ☐ *no* ☐; è un dominio di integrità? *sì* ☐ *no* ☐; è un campo? *sì* ☐ *no* ☐. In $(A,+,\cdot)$ quali sono *tutti* gli elementi:

idempotenti ...., nilpotenti ....,

cancellabili ...., invertibili ....,

divisori non nulli dello zero ....

Calcolare (in A), se esistono: $(3+7)^{-1} = \ldots.$ oppure: ☐ *non esiste*; $(3\cdot 7)^{-1} = \ldots.$ oppure: ☐ *non esiste*.
Quanti e quali sono gli ideali non banali di $(A,+,\cdot)$? *Non ne esistono* ☐, oppure: *ve ne sono* ... *ed hanno per elementi*:

....

Si considerino le applicazioni: $f : z \in \mathbb{Z} \mapsto z \bmod 8 \in A$ e $g : a \in A \mapsto 3a \in \mathbb{Z}$.

l'applicazione	f		g		fg		gf	
è	sì	no	sì	no	sì	no	sì	no
iniettiva								
suriettiva								
biettiva								
una permutazione di $\mathbb{Z}$								
una permutazione di A								
un omomorfismo di anelli								
un isomorfismo di anelli								

Si calcolino:

$f(-642) = \ldots,$

$f^{-1}(\{0\}) = \ldots\ldots\ldots\ldots\ldots,$

$g(A) = \ldots\ldots\ldots\ldots\ldots,$

$(fg)(-5) = \ldots,$

$(gf)(5) = \ldots.$

Si compili la tabella a sinistra.

Se esiste, si scelga una permutazione di A, $\alpha \in \{f, g, fg, gf\}$: $\alpha = \ldots.$ Si decomponga α in prodotto di cicli disgiunti: $\alpha = \ldots\ldots\ldots\ldots\ldots\ldots$.
Di che classe è α? *pari* ☐, *dispari* ☐, *nessuna delle due* ☐. Qual è il periodo di α? ..... Qual è la decomposizione di α^{-1} in prodotto di cicli disgiunti? $\alpha^{-1} = \ldots\ldots\ldots\ldots\ldots\ldots$

Quante sono le applicazioni iniettive di $\mathcal{P}_3(A)$ in $\mathcal{P}_5(A)$? .... E quante le applicazioni suriettive di $\mathcal{P}_5(A)$ in $\mathcal{P}_3(A)$? ....

---

5 Determinare l'insieme delle soluzioni in $\mathbb{Z}$ di ciascuna delle seguenti equazioni congruenziali. *[Trascrivere il procedimento effettuato sul retro di questo foglio.]*

$1902x \equiv 1704 \pmod{849}$ *insieme delle soluzioni:* ....

$600x \equiv 390 \pmod{210}$ *insieme delle soluzioni:* ....

$600x \equiv 380 \pmod{210}$ *insieme delle soluzioni:* ....

Calcolare il resto di $n := 9^{12345665} + 9100(1 + 2^{222})$ modulo 91. $n \bmod 91 = \ldots.$

Calcolare $|\mathcal{U}(\mathbb{Z}_{91})| = \ldots\ldots\ldots$ Qual è il periodo di $u := [9]_{91}$ nel gruppo $\mathcal{U}(\mathbb{Z}_{91})$? .... E qual è l'inverso di u? $u^{-1} = \ldots\ldots\ldots$ È vero che $u^{-1} = [n]_{91}$? ☐ *sì,* ☐ *no,* ☐ *non lo si può decidere.*

---

6 Sia A un albero con 1000 vertici e sia G il grafo ottenuto da A sopprimendo sei lati a due a due non incidenti. G è: ☐ *un albero,* ☐ *una foresta,* ☐ *di altro tipo.* Quante sono le componenti connesse di G? .... , oppure: ☐ *non lo si può decidere.* Quanti sono i lati di G? .... , oppure: ☐ *non lo si può stabilire.*

---

7 Nell'insieme $S := \{1,2,3,4,5,6,7,8\}$ si considerino le relazioni binarie ρ, σ, τ di grafici rispettivamente

$$\rho^{\#} := \Delta_S \cup \{(1,2),(2,1),(2,3),(3,4),(4,5),(5,4),(5,6),(6,7),(7,6)\};$$
$$\sigma^{\#} := \Delta_S \cup \{(2,3),(3,2),(4,6),(4,8),(5,7),(6,4),(6,8),(7,5),(8,4),(8,6)\};$$
$$\tau^{\#} := \Delta_S \cup \{(3,7),(4,7),(5,7),(6,7),(8,3),(8,4),(8,5),(8,6),(8,7)\};$$

dove $\Delta_S := \{(x,x) \mid x \in S\}$. Si compili la tabella:

la relazione	ρ		σ		τ	
è di	sì	no	sì	no	sì	no
equivalenza						
ordine largo						
ordine stretto						

Si scelga tra ρ, σ e τ una equivalenza: . . . . Quanti elementi ha il corrispondente insieme quoziente? . . . . . Si scrivano le corrispondenti classi di equivalenza, elencandone esplicitamente gli elementi:

. . . .

Tra ρ, σ e τ si scelga ora un ordinamento (largo o stretto): . . . . . Disegnarne su questo foglio, in basso, il diagramma di Hasse.

Con questo ordinamento,
S è un reticolo? *sì* □ *no* □. Ha minimo? *sì* □ *no* □ (è . . .), ha massimo? *sì* □ *no* □ (è . . .);
ha elementi minimali? *sì* □ *no* □ (sono . . . .); ha elementi massimali? *sì* □ *no* □ (sono . . . .);
$\sup\{1,2\}$ non esiste □, oppure è . . ?

Sia θ l'ordinamento indotto da quello scelto per S su $T := S - \{1,2\}$. (T,θ) è un reticolo? *sì* □ *no* □, un reticolo distributivo? *sì* □ *no* □, un reticolo complementato? *sì* □ *no* □, un reticolo booleano? *sì* □ *no* □.