CdS in Informatica — a.a. 2007/2008

Esercitazione scritta di **ALGEBRA** (Proff. Cutolo e Rao) mercoledì 12 marzo 2008

NOME E COGNOME	MATRICOLA

GRUPPO ☐ *I (Rao)* ☐ *IV (Cutolo)*	ESAME: lunedì 17 marzo, ore 15, aula D, DMA

1 Vero o falso? Oppure i dati non sono sufficienti per fornire alcuna delle due risposte?

- Ogni insieme ordinato non vuoto ha elementi massimali. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- Esistono in $\mathbb{S}_9$ due cicli α e β di lunghezza 4 tali che $(1\,2\,3)^2(1\,4\,3\,6\,8) = \alpha^2\beta$. *vero* ☐ *falso* ☐ *dati insuff.* ☐
- $(\exists\, n \in \mathbb{N})(\forall m \in \mathbb{N})(m \leq 100 \Rightarrow n \equiv_m 2)$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- $(\exists\, n \in \mathbb{N})(\forall m \in \mathbb{N})(m \leq 100 \Rightarrow n \equiv_2 m)$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- Siano A, B, C insiemi non vuoti. Si ha $(A \smallsetminus B) \smallsetminus C \neq C$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- La forma proposizionale $\big((p\vee q)\wedge r\big)\vee\big(q\vee(p\wedge r)\big)\vee\big((q\vee p)\wedge r\big)$ è una tautologia. *vero* ☐ *falso* ☐ *dati insuff.* ☐

---

2 Elencare gli elementi dell'insieme $A = \{x \in \mathbb{N} \mid (x+1 \text{ è primo}) \wedge (x \leq 10) \wedge (3|x \Rightarrow x \equiv_3 1)\}$.
$A = \{ \ldots\ldots\ldots\ldots\ldots \}$ e $|A| = \ldots\ldots$ Inoltre $|\mathcal{P}(A) \smallsetminus A| = \ldots\ldots$ e $|\mathcal{P}(A) \smallsetminus \{A\}| = \ldots\ldots$

---

3 Per definizione, un anello $(R, +, \cdot)$ è un *dominio di integrità* se e solo se ....

....

L'anello booleano $(\mathcal{P}(\mathbb{N}), \Delta, \cap)$ è un dominio di integrità? *sì* ☐ *no* ☐. Si fornisca, se possibile, un esempio di:

dominio di integrità finito: ...., oppure: ☐ *non ne esistono*

dominio di integrità infinito: ...., oppure: ☐ *non ne esistono*

anello finito che non sia un dominio di integrità: ...., oppure: ☐ *non ne esistono*

anello infinito che non sia un dominio di integrità: ...., oppure: ☐ *non ne esistono*

dominio di integrità unitario A tale che $A[x]$ non sia integro: ...., oppure: ☐ *non ne esistono*

---

4 Sapendo che $R = (\mathbb{Z}_6 \times \mathbb{Z}_5, \oplus, *)$ è un anello, con le operazioni $\oplus$ e $*$ definite ponendo, per ogni $a, c \in \mathbb{Z}_6$ e $b, d \in \mathbb{Z}_5$,

$$(a,b) \oplus (c,d) = (a+c+1, b+d-1) \qquad \text{e} \qquad (a,b) * (c,d) = (ac+a+c, bd-b-d+2),$$

si stabilisca: R è commutativo? *sì* ☐ *no* ☐, unitario? ☐ *no*, oppure: ☐ *sì, l'unità di R è* $1_R = \ldots\ldots$. Lo zero di R è $0_R = \ldots\ldots$. In R l'opposto di $r = ([0]_6, [3]_5)$ è ...... , oppure ☐ *non esiste*; l'inverso di r è ...... , oppure ☐ *non esiste*.

$\mathcal{U}(R) = \{ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \}$, dunque $|\mathcal{U}(R)| = \ldots\ldots$

---

5 Esistono grafi (semplici) con otto vertici, tutti di grado 3? *sì* ☐ *no* ☐. Nel caso ce ne siano, a meno di isomorfismi, ce ne è ☐ *solo uno*, oppure ☐ *più di uno*?; sono ☐ *tutti connessi*, oppure ☐ *tutti non connessi*, oppure ☐ *ce ne sono alcuni connessi ed alcuni non connessi*. Nel caso sia possibile, disegnare qui esempi di grafi a giustificazione delle risposte date [Suggerimento: *si pensi al grafo completo su quattro vertici*]:

Nel caso in cui in tali grafi esistano, detto G uno di essi, G ha cammini euleriani? *sì* ☐ *no* ☐ *impossibile stabilirlo* ☐. Anche il grafo complementare $\bar{G}$ di G ha tutti i vertici dello stesso grado? ☐ *no*, oppure: ☐ *sì, tutti di grado* . . . , oppure: ☐ *impossibile stabilirlo*. Inoltre, $\bar{G}$ è connesso? *sì* ☐ *no* ☐ *impossibile stabilirlo* ☐, $\bar{G}$ ha cammini euleriani? *sì* ☐ *no* ☐ *impossibile stabilirlo* ☐.

6 Sapendo che $3 \cdot 7 \cdot 19 = 399$, $3 \cdot 7 \cdot 23 = 483$ e $3 \cdot 7 \cdot 19 \cdot 23 = 9177$, si disegni a destra il diagramma di Hasse dell'insieme $A = \{1, 3, 7, 19, 21, 23, 399, 483, 9177\}$ ordinato per divisibilità. $(A, |)$ è totalmente ordinato? *sì* ☐ *no* ☐, è un reticolo? *sì* ☐ *no* ☐. Se lo è, è un reticolo distributivo? *sì* ☐ *no* ☐, complementato? *sì* ☐ *no* ☐, booleano? *sì* ☐ *no* ☐. Calcolare:
$\sup\{7, 19\} = \ldots$, oppure: ☐ $\sup\{7, 19\}$ *non esiste.*;
$\inf\{23, 399\} = \ldots$, oppure: ☐ $\inf\{23, 399\}$ *non esiste.*

---

7 Si completi la tabella a destra, riferita alle relazioni binarie definite in $\mathbb{Z}$ ponendo, per ogni $n, m \in \mathbb{Z}$,

$$n \,\alpha\, m \iff (n, m) \neq (1, 2)$$
$$n \,\beta\, m \iff \big((n \neq 2) \vee (m = 2)\big)$$
$$n \,\gamma\, m \iff 2n^3 + 3 \equiv_9 2m^3 - 6$$
$$n \,\delta\, m \iff 3n^3 + 3 \equiv_9 3m^3 + 6.$$

la relazione è	α sì	α no	β sì	β no	γ sì	γ no	δ sì	δ no
riflessiva								
antiriflessiva								
simmetrica								
antisimmetrica								
transitiva								
di ordine stretto								
di ordine largo								
di equivalenza								

Se tra queste relazioni ne esiste almeno una che sia di equivalenza se ne scelga una, la si chiami ρ, dunque $\rho = \ldots$, e si indichi:
$|\mathbb{Z}/\rho| = \ldots$; $[0]_\rho$ è ☐ *finito* o ☐ *infinito*?;
$[14]_\rho \cap \{n \in \mathbb{Z} \mid -10 < n < 0\} = \{\ldots\}$.

---

8 Determinare gli insiemi $S = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid 197x + 14y = 1\}$ e $T = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid 197x - 6y = 1\}$.

$S = \{\ldots\}$; $T = \{\ldots\}$.

Sapendo che 197 non è multiplo di alcun intero compreso tra 2 e 100, che $6^3 \equiv_{197} 19$ e che $6^4 \equiv_{197} -83$, si calcoli $|\mathcal{U}(\mathbb{Z}_{197})| = \ldots$, e si determinino i periodi nel gruppo $\mathcal{U}(\mathbb{Z}_{197})$ di $[14]_{197}$ (risposta: $\ldots$) e di $[-6]_{197}$ (risposta: $\ldots$). Calcolare poi $(14^{38673} - 4)(-6)^{21715} \bmod 197 = \ldots$

---

9 Siano $h = x^6 - x^5 + 4x^4 - x^3 + x^2 + 2x - 6$ e $k = 2x^5 - 2x^4 + 5x^3 - 5x^2 + 2x - 2$, polinomi in $\mathbb{Q}[x]$. Posto $f = h(k^5 + 1)$ e $g = 10^9 k$, si calcoli il massimo comun divisore monico d tra f e g:

$$d = \ldots$$

Esistono $s, t \in \mathbb{Q}[x]$ tali che $sf + tg = d^2 + hd$? *sì* ☐ *no* ☐ *impossibile stabilirlo* ☐.

Si decompongano d, h e g come prodotto di un'eventuale costante e di polinomi monici irriducibili:

$d = \ldots$ $h = \ldots$

$g = \ldots$

Si determini, se esiste, il minimo numero naturale primo p tale che h_p, cioè h riguardato come polinomio a coefficienti in $\mathbb{Z}_p$, sia prodotto di polinomi di primo grado: ☐ *tale* p *non esiste*, oppure: $p = \ldots$ e h_p si decompone in prodotto di fattori irriducibili in $\mathbb{Z}_p[x]$ come:

$$h_p = \ldots$$

h_p è divisibile in $\mathbb{Z}_p[x]$ per un polinomio irriducibile di secondo grado? *sì* ☐ *no* ☐

Quali e quante sono, in $\mathbb{Z}_p$, le radici di h_p? Le radici sono $\ldots$; il loro numero è $\ldots$
