CdS in Informatica — a.a. 2009/2010

Esercitazione scritta di **ALGEBRA** (Proff. Cutolo e Rao) venerdì 22 gennaio 2010

NOME E COGNOME	MATRICOLA

GRUPPO ☐ *I (Rao)* ☐ *rec. (Cutolo)*	ESAME: 26 gennaio, ore 9, aula D, DMA

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

- 18^{1000} divide $2^{1200}3^{1300}5^{1500}7^{1700}$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- 18^{1000} divide $2^{2000}3^{3000}5^{5000}7^{7000}+18$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- $876853759465840737547967666934752087 5! - 2$ è un numero primo. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- $\mathbb{N}$, munito della consueta operazione di addizione, costituisce un gruppo. *vero* ☐ *falso* ☐ *dati insuff.* ☐
- L'anello di polinomi $\mathbb{Z}_{11}[x]$ è finito. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- Per ogni scelta degli insiemi A, B, C si ha $\big(C \smallsetminus (A \smallsetminus B)\big) \smallsetminus C = \varnothing$. *vero* ☐ *falso* ☐ *dati insuff.* ☐
- In $\mathbb{S}_9$, la permutazione $\big((1\,2\,3\,8)(1\,7\,3\,5\,4\,9)(6\,2)(4\,2\,3)\big)^6$ ha classe pari. *vero* ☐ *falso* ☐ *dati insuff.* ☐
- In $\mathbb{S}_9$, $\big((1\,2\,3\,8)(1\,7\,3\,5\,4\,9)(6\,2)(4\,2\,3)\big)^{9!}$ è la permutazione identica. *vero* ☐ *falso* ☐ *dati insuff.* ☐

---

2 Un anello A è, per definizione, un *dominio di integrità* se e solo se: . . . . . .

. . . . . .

Per due elementi a e b di un anello R vale la formula $(a+b)^2 = a^2+2ab+b^2$ ☐ *sempre*, oppure: non sempre, ma ☐ *se l'anello R è unitario*, ☐ *se l'anello R è commutativo*, ☐ *se l'anello R è finito*, ☐ *se a e b commutano*.

---

3 Si considerino le forme proposizionali $A\colon \big(p \Rightarrow (q \vee r)\big) \Longrightarrow (q \wedge r)$ e $B\colon (q \iff r) \wedge \big((\neg p) \Rightarrow q\big)$.
Calcolare il valore di verità assunto da A in ciascuno dei due casi:
per p vero, q vero, r falso, A vale ☐ *vero* ☐ *falso*; per p falso, q vero, r falso, A vale ☐ *vero* ☐ *falso*.
La forma $A \Longrightarrow B$ è ☐ *una tautologia*, ☐ *una contraddizione*, ☐ *contingente*.
La forma $B \Longrightarrow A$ è ☐ *una tautologia*, ☐ *una contraddizione*, ☐ *contingente*.
La forma $A \Longleftrightarrow B$ è ☐ *una tautologia*, ☐ *una contraddizione*, ☐ *contingente*.

---

4 Sia S l'insieme dei divisori (in $\mathbb{N}$) pari di 84, ordinato per divisibilità. Se ne disegni a destra il diagramma di Hasse. Rispetto a questo ordinamento, S è un reticolo? *sì* ☐ *no* ☐, un reticolo complementato? *sì* ☐ *no* ☐, distributivo? *sì* ☐ *no* ☐, booleano? *sì* ☐ *no* ☐.
$\min S =$ . . . , oppure: ☐ $\min S$ *non esiste*.
$\inf\{n \in S \mid 4 \text{ divide } n\}$ ☐ *esiste ed è* . . . , oppure: ☐ *non esiste*.
12 ha complementi in S? ☐ *no*, oppure: ☐ *sì, esattamente uno, cioè* . . . , oppure: ☐ *sì, più di uno, ad esempio* . . . *e* . . .
Quante sono le parti X di S tali che $|X| = 4$ e X sia totalmente ordinato dall'ordinamento indotto da S? . . .

---

5 In $A = \{n \in \mathbb{N} \mid n < 9\}$ si consideri l'operazione binaria associativa $*$ definita ponendo, per ogni $a, b \in A$,

$$a * b = (a + b - 5ab) \bmod 9$$

Questa operazione è commutativa? *sì* ☐ *no* ☐. Si stabilisca se, in $(A, *)$,
esiste un elemento neutro: ☐ *no*, oppure: ☐ *sì, esso è* . . ;
3 è invertibile? ☐ *no*, oppure: ☐ *sì, il suo inverso è* . . *e il suo periodo è* . . ; 3 è cancellabile? ☐ *no* ☐ *sì*.
8 è invertibile? ☐ *no*, oppure: ☐ *sì, il suo inverso è* . . *e il suo periodo è* . . ; 8 è cancellabile? ☐ *no* ☐ *sì*.

Si considerino le applicazioni $f\colon a \in A \mapsto 3 * a \in A$ e $g\colon a \in A \mapsto a * 8 \in A$. f è iniettiva? *sì* ☐ *no* ☐, suriettiva? *sì* ☐ *no* ☐. g è iniettiva? *sì* ☐ *no* ☐, suriettiva? *sì* ☐ *no* ☐. Se f è biettiva, il suo periodo in $\operatorname{Sym} A$ è . . ; se g è biettiva, il suo periodo in $\operatorname{Sym} A$ è . . .
$(A, *)$ è un semigruppo? *sì* ☐ *no* ☐, un monoide? *sì* ☐ *no* ☐, un gruppo? *sì* ☐ *no* ☐, un anello? *sì* ☐ *no* ☐, un anello booleano? *sì* ☐ *no* ☐.

---

6 Sia $X = \{2, 3\}$. Si definiscano in $\mathbb{Z}$ le relazioni binarie α, β, γ e δ ponendo, per ogni $a, b \in \mathbb{Z}$,

$a \,\alpha\, b : \iff (\forall\, x \in X)\big((x \mid a) \wedge (x \mid b)\big)$; $\quad a \,\gamma\, b : \iff (\forall\, x \in X)\big((x \mid a) \Rightarrow (x \mid b)\big)$

$a \,\beta\, b : \iff (\forall\, x \in X)\big((x \mid a) \vee (x \mid b)\big)$; $\quad a \,\delta\, b : \iff (\forall\, x \in X)\big((x \mid a) \iff (x \mid b)\big)$.

Si dica tra queste quali sono . . . . . e quali non sono . . . . . relazioni di equivalenza. Se possibile, se ne scelga una che lo è, la si chiami ρ (dunque, $\rho =$ . .) e si descrivano in modo esplicito $[6]_\rho =$ . . . . . e $\mathbb{Z}/\rho =$ . . . . . .

---

7 Sia S un insieme finito e sia $\sim$ la relazione binaria in $\mathcal{P}(S)$ definita ponendo, per ogni X, $Y \in \mathcal{P}(S)$, $X \sim Y$ se e solo se $|X \cap Y|$ è dispari e $|X \cup Y|$ è pari. Si decida se $\sim$ definisce una struttura di grafo (semplice) con insieme di vertici $\mathcal{P}(S)$ e $\sim$ come relazione di adiacenza: $\square$ *sì, qualunque sia S, perché* $\sim$ è . . . . . , oppure: $\square$ *no, non necessariamente, perché* . . . . . .

Nel primo caso, si chiami $G(S)$ questo grafo; posto $A = \{1, 2, 3\}$ e $B = \{1, 2, 3, 4\}$, si disegni qui a destra $G(A)$ e si risponda alle domande che seguono.

Quante componenti connesse ha $G(A)$? . . . $G(A)$ è planare? *sì* $\square$ *no* $\square$. $G(A)$ ha cammini euleriani? *sì* $\square$ *no* $\square$. $G(A)$ ha circuiti euleriani? *sì* $\square$ *no* $\square$. Quante componenti connesse ha $G(B)$? . . .

---

8 Determinare, se possibile, una coppia di interi u, v tali che $0 < u - v < 250$ e $491u + 101v = 1$. Una tale coppia: $\square$ *non esiste*, $\square$ *esiste ed è* $u =$ . . . . , $v =$ . . . . . In tal caso determinare l'insieme (risp. S_1, S_2, S_3, S_4) di tutte le soluzioni intere di ognuna delle seguenti equazioni congruenziali:

(1) $101x \equiv_u 1$ $\quad S_1 =$ . . . . . ; $\qquad$ (2) $491x \equiv_v 1$ $\quad S_2 =$ . . . . . ;

(3) $ux \equiv_{101} vx + 1$ $\quad S_3 =$ . . . . . ; (4) $ux - 1 \equiv_{491} vx$ $\quad S_4 =$ . . . . . .

Infine, sapendo che $(u - v)^{40} + 6 \equiv_{101} 0$, calcolare $(u - v)^{40000} \bmod 101 =$ . . . . .

---

9 Si considerino, in $\mathbb{Q}[x]$, i polinomi $f := x^6 + 2x^5 + 4x^4 + 6x^3 + 6x^2 + 4x + 1$ e $g := x^4 + x^3 + 3x^2 + 2x + 2$. Si calcolino i massimi comuni divisori monici (in $\mathbb{Q}[x]$): d, tra f e g; d_1, tra $2f^2$ e $2g^2$; d_2, tra $gf + x$ e $12g$:

$d =$ . . . . . ; $d_1 =$ . . . . . ; $d_2 =$ . . . . . .

Si ha $\{a \in \mathbb{Q} \mid f(a) = 0 = g(a)\} =$ . . . . . Si scrivano f e g come prodotti di polinomi monici irriducibili in $\mathbb{Q}[x]$:

$f =$ . . . . . ; $\quad g =$ . . . . . .

Siano, rispettivamente, f_3 e g_3 i polinomi f e g riguardati come polinomi a coefficienti in $\mathbb{Z}_3$. Si scrivano f_3 e g_3 come prodotti di polinomi monici irriducibili in $\mathbb{Z}_3[x]$:

$f_3 =$ . . . . . ; $\quad g_3 =$ . . . . . ;

si calcolino il massimo comun divisore monico $\bar{d}$ ed il minimo comune multiplo $\bar{m}$ tra f_3 e g_3 in $\mathbb{Z}_3[x]$:

$\bar{d} =$ . . . . . ; $\quad \bar{m} =$ . . . . . ;
