CdS in Informatica — a.a. 2009/2010

Esercitazione scritta di **ALGEBRA** (Proff. Cutolo e Rao) giovedì 24 giugno 2010

NOME E COGNOME	MATRICOLA

GRUPPO ☐ *I (Rao)* ☐ *rec. (Cutolo)*	ESAME: martedì 29 giugno, ore 9, aula C

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

- 10000000000020000000000300000000000000000000000 è multiplo di 18. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- 20! divide $\sum_{i=50}^{2000} i!$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- La forma proposizionale $\big((p\wedge q)\vee(r\wedge\neg s)\big) \Longrightarrow \big((r\wedge q)\Rightarrow(q\vee\neg p)\big)$ è una tautologia. *vero* ☐ *falso* ☐ *dati insuff.* ☐
- $\{n\in\mathbb{Z} \mid n\equiv_3 1 \Rightarrow n\equiv_3 2\} = \varnothing$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- Lo zero è l'unico elemento non cancellabile nell'anello $\mathbb{Z}_{13}$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- L'anello delle matrici 2×2 sul campo dei numeri reali è commutativo. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- È assegnata una permutazione $\sigma\in\mathbb{S}_7$ tale che $2^\sigma = 4$ e $4^\sigma = 6$. σ ha classe pari. *vero* ☐ *falso* ☐ *dati insuff.* ☐

---

2 Si eunuci il criterio di irriducibilità di Eisenstein: sia $f = b_0 + b_1x + \cdots + b_nx^n$ un polinomio a coefficienti in $\mathbb{Z}$, con $b_n \neq 0$. Se .....

.....

allora .....

---

3 Sia $X = \{n\in\mathbb{N} \mid n < 9\}$, dunque $|X| = \ldots$, $\big|\{A\subset X \,\big|\, |A| = 3\}\big| = \ldots\ldots$ e $|\mathcal{P}_6(X)| = \ldots\ldots$. Si consideri in X l'operazione binaria $*$ definita ponendo, per ogni $a, b\in X$, $a*b = 2ab \bmod 9$. Allora $6*7 = \ldots$. L'operazione $*$ è commutativa? *sì* ☐ *no* ☐, associativa? *sì* ☐ *no* ☐. X ha elemento neutro rispetto a $*$? ☐ *no*, oppure: ☐ *sì, esso è* .... $(X,*)$ è un semigruppo? *sì* ☐ *no* ☐, un monoide? *sì* ☐ *no* ☐, un gruppo? *sì* ☐ *no* ☐. In $(X,*)$, 1 è invertibile? ☐ *no*, oppure: ☐ *sì, il suo inverso è* ...; 0 è cancellabile? *sì* ☐ *no* ☐. Si elenchino gli elementi invertibili in $(X,*)$: .....

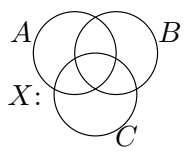
---

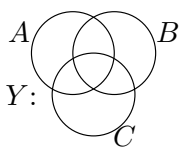
4 Sia X l'insieme $\{1, 3, 12, 20, 21, 60, 84, 210^2\}$ ordinato per divisibilità. Se ne disegni a lato il diagramma di Hasse. Questo insieme ordinato è un reticolo? *sì* ☐ *no* ☐. Nel caso, esso è distributivo? *sì* ☐ *no* ☐, complementato? *sì* ☐ *no* ☐, booleano? *sì* ☐ *no* ☐. In questo insieme ordinato si calcoli:
$\inf\{84, 20\} = \ldots$, oppure: ☐ $\inf\{84, 20\}$ *non esiste*;
$\sup\{12, 21\} = \ldots$, oppure: ☐ $\sup\{12, 21\}$ *non esiste*.
X è un sottoreticolo di $(\mathbb{N}, |\,)$ (il reticolo dei naturali ordinati per divisibilità)? *sì* ☐ *no* ☐.

Esistono $a, b\in\mathbb{N}$ tali che $X\cup\{a, b\}$ sia un sottoreticolo di $(\mathbb{N}, |)$? ☐ *no*, oppure: ☐ *sì, ad esempio,* $a = \ldots$, $b = \ldots$.

---

5 Si completino i due diagrammi di Venn, tratteggiando le aree corrispondenti a $X = (B\smallsetminus C)\cup\big((A\cap C)\smallsetminus B\big)$ e $Y = \big((A\cap B)\cup(A\cap C)\big)\smallsetminus(B\cap C)$.





È vero che $X\subseteq Y$ per ogni scelta degli insiemi A, B, C? ☐ *sì*, oppure: ☐ *no, un controesempio è dato da* $A = \ldots$, $B = \ldots$, $C = \ldots$. È vero che $Y\subseteq X$ per ogni scelta degli insiemi A, B, C? ☐ *sì*, oppure: ☐ *no, un controesempio è dato da* $A = \ldots$, $B = \ldots$, $C = \ldots$.

---

6 Si considerino le applicazioni $f\colon n \in \mathbb{Z} \mapsto [n^2+1]_8 \in \mathbb{Z}_8$ e $g\colon [n]_8 \in \mathbb{Z}_8 \mapsto [3n]_{12} \in \mathbb{Z}_{12}$. Cosa si intende quando si dice che g è "ben definita" e cosa va verificato per provarlo? . . . . . .

. . . . . .

f è iniettiva? *sì* ☐ *no* ☐, suriettiva? *sì* ☐ *no* ☐; g è iniettiva? *sì* ☐ *no* ☐, suriettiva? *sì* ☐ *no* ☐; fg è iniettiva? *sì* ☐ *no* ☐, suriettiva? *sì* ☐ *no* ☐. Siano σ e ρ, nell'ordine, i nuclei di equivalenza di g e di fg. Allora $|\mathbb{Z}_8/\sigma| = \ldots$ e $|\mathbb{Z}/\rho| = \ldots$. $\big[[3]_8\big]_\sigma = \{\ldots\ldots\ldots\ldots\ldots\ldots\}$. $[178]_\rho$ è ☐ *finito* o ☐ *infinito*?

---

7 Consideriamo grafi (semplici) G con esattamente 7 lati e 6 vertici, dei quali uno abbia grado 5 ed un altro grado 3. Esiste un tale grafo? *sì* ☐ *no* ☐. Nel caso, è necessariamente connesso? *sì* ☐ *no* ☐. Ne esiste uno con almeno tre vertici di grado 1? *sì* ☐ *no* ☐. È comunque possibile stabilire quali sono i gradi dei quattro vertici restanti? ☐ *no*, oppure: ☐ *sì, questi gradi sono:* $\ldots, \ldots, \ldots$ *e* $\ldots$. Se possibile, disegnare a fianco un tale grafo. Ne esistono almeno due tra loro non isomorfi? *sì* ☐ *no* ☐. Con riferimento al grafo disegnato, chiamiamolo X, si stabilisca: X è un albero? *sì* ☐ *no* ☐, è planare? *sì* ☐ *no* ☐, qual è la massima distanza tra due suoi vertici? $\ldots$. Quanti sono gli isomorfismi da X a X? $\ldots$.

---

8 Calcolare: $106^2 \bmod 199 = \ldots\ldots$, $106^3 \bmod 199 = \ldots\ldots$, $2^{-1} \bmod 199 = \ldots\ldots$, $2^{199}(100 + 106^{1234} + 100 + 106^{2345} + 100 + 106^{3456}) \bmod 199 = \ldots\ldots$.

Determinare gli insiemi (risp. S_1, S_2, S_3) di tutte le soluzioni intere di ognuna delle seguenti equazioni congruenziali:

$$106x - 106^2 \equiv_{199} 398 \qquad 106^2x - 106 \equiv_{199} 597 \qquad 106^3x - 106 \equiv_{199} 796$$

$S_1 = \ldots\ldots\ldots\ldots$ $S_2 = \ldots\ldots\ldots\ldots$ $S_3 = \ldots\ldots\ldots\ldots$

---

9 In $\mathbb{Q}[x]$ si considerino i polinomi $a = x^{10}-1$, $b = x^6+1$, $u = \prod_{i=1}^{11}(x-i)$, $v = \prod_{i=11}^{21}(x-i)$. Quante e quali sono le radici in $\mathbb{Q}$ di u? [*Risposta:* $S := \{c \in \mathbb{Q} \mid u(c) = 0\} = \{\ldots\ldots\ldots\ldots\ldots\ldots\}$ e $|S| = \ldots$]. Si calcolino il massimo comun divisore monico d_1 tra a e b, e poi, senza usare l'algoritmo euclideo, il massimo comun divisore monico d_2 tra u e v ed il massimo comun divisore monico d_3 tra av e bu:

$d_1 = \ldots\ldots\ldots\ldots$; $d_2 = \ldots\ldots\ldots\ldots$; $d_3 = \ldots\ldots\ldots\ldots$.

Siano ora $\bar a$, $\bar b$, $\bar u$ e $\bar v$, nell'ordine, i polinomi a, b, u, v visti come polinomi a coefficienti in $\mathbb{Z}_{11}$. Quante e quali sono le radici in $\mathbb{Z}_{11}$ di $\bar a$? [*Risposta:* $T := \{c \in \mathbb{Z}_{11} \mid \bar a(c) = 0\} = \ldots\ldots\ldots\ldots\ldots\ldots$ e $|T| = \ldots$]. In $\mathbb{Z}_{11}[x]$ si determinino:

il massimo comun divisore monico tra $\bar a$ e $\bar b$: $\ldots\ldots\ldots\ldots$
il massimo comun divisore monico tra $\bar a$ e $\bar u$: $\ldots\ldots\ldots\ldots$
il massimo comun divisore monico tra $\bar u$ e $\bar v$: $\ldots\ldots\ldots\ldots$

Esiste in $\mathbb{Z}_{11}[x]$ un polinomio di grado 1111 che divida $\bar u - \bar v$? *sì* ☐ *no* ☐.
