CdS in Informatica — a.a. 2009/2010

Esercitazione scritta di **ALGEBRA** (Proff. Cutolo e Rao) venerdì 17 dicembre 2010

NOME E COGNOME	MATRICOLA

GRUPPO ☐ *I (Rao)* ☐ *rec. (Cutolo)*	ESAME: lunedì 20 dicembre, ore 9, aula D, DMA

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

- Per ogni coppia A, B di parti di un insieme S si ha: $(A \smallsetminus B) \cup (B \smallsetminus A) \subseteq S \smallsetminus (A \cap B)$. *vero* ☐ *falso* ☐ *dati insuff.* ☐
- Per ogni applicazione $f\colon A \to B$ esiste almeno un'applicazione g di dominio B tale che il prodotto fg sia un'applicazione biettiva. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- Per ogni insieme A ed ogni quoziente $\bar{A}$ di A esiste un'applicazione suriettiva $A \twoheadrightarrow \bar{A}$. *vero* ☐ *falso* ☐ *dati insuff.* ☐
- Il numero dei divisori di 10^{15} in $\mathbb{N}$ è una potenza di 2. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- $[1345]_{3^{200}}$ è invertibile in $\mathbb{Z}_{3^{200}}$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- Sia p un intero positivo primo e sia n un intero positivo minore di p. Il periodo di $[p+n]_n$ in $\mathcal{U}(\mathbb{Z}_n)$ divide $\varphi(n)$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- $\mathbb{N}$ è una parte stabile di $(\mathbb{Z}, +)$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- Sono dati due 3-cicli disgiunti $\alpha, \beta \in \mathbb{S}_8$. Si ha $(\alpha\beta)^{26} = \alpha^2$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐

---

2 Per definizione, $(G, *)$ è un *gruppo abeliano* se e solo se .....

.....

Si forniscano, ove possibile, esempi di:

un gruppo non abeliano: ....., oppure: ☐ *non ne esistono;*

un gruppo abeliano finito: ....., oppure: ☐ *non ne esistono;*

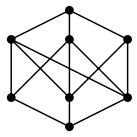
un gruppo abeliano infinito: ....., oppure: ☐ *non ne esistono.*

---

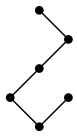
3 La forma proposizionale $\big(p \wedge q \wedge (\neg p)\big) \implies \big((p \vee q) \Rightarrow p\big)$ è ☐ *una tautologia*, ☐ *contingente*, ☐ *una contraddizione.*

---

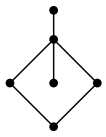
4 Si considerino gli insiemi ordinati A, B, C e D rappresentati dai seguenti diagrammi di Hasse e si completino le tabelle sottostanti.



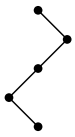
A



B



C



D

	è una catena		è un reticolo		è un reticolo distributivo		è un reticolo complementato		è un reticolo booleano		ha minimo		ha massimo	
	sì	*no*	*sì*	*no*	*sì*	*no*	*sì*	*no*	*sì*	*no*	*sì*	*no*	*sì*	*no*
A														
B														
C														
D														

Nella tabella a destra si inserisca il numero di elementi minimali e di elementi massimali di ciascuno degli insiemi ordinati considerati.

	A	B	C	D
minimali				
massimali				

---

5 Esiste in $\mathbb{Z}[x]$ un polinomio non nullo del quale siano radici tutti gli interi pari compresi tra -100 e 1000 (inclusi)? ☐ *no* ☐ *sì, ed un tale polinomio è:*

. . . . . .

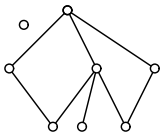
Ne esiste uno che abbia grado minore di 500? ☐ *no* ☐ *sì*

Esiste in $\mathbb{Z}_{24}[x]$ un polinomio non nullo di grado minore di 500 del quale sia radice $[n]_{24}$ per ogni intero n tale che $-100 \leq n \leq 1000$? ☐ *no* ☐ *sì, ed un tale polinomio è:*

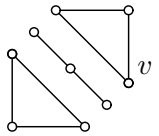
. . . . . .

---

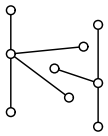
6 Si considerino i grafi A, B, C qui sotto rappresentati. Il grado del vertice v di B è . . . . .



A



B



C

Indicare, se è il caso, quali tra questi grafi sono isomorfi:
A è isomorfo a B *sì* ☐ *no* ☐; A è isomorfo a C *sì* ☐ *no* ☐; B è isomorfo a C *sì* ☐ *no* ☐.
A è un albero? *sì* ☐ *no* ☐, una foresta? *sì* ☐ *no* ☐, ha un cammino euleriano? *sì* ☐ *no* ☐.
B è un albero? *sì* ☐ *no* ☐, una foresta? *sì* ☐ *no* ☐, ha un cammino euleriano? *sì* ☐ *no* ☐.
C è un albero? *sì* ☐ *no* ☐, una foresta? *sì* ☐ *no* ☐, ha un cammino euleriano? *sì* ☐ *no* ☐.
Esiste un grafo connesso di cui B è un sottografo? *sì* ☐ *no* ☐ *impossibile stabilirlo* ☐

---

7 Determinare un $x \in \mathbb{Z}$ tale che $x \equiv_{379} 300$ e $|x| \leq 189$. ☐ *Tale x non esiste*, oppure ☐ *esiste ed è* . . . .

Calcolare $51^{-1} \bmod 379 =$ . . . . , $51^2 \bmod 379 =$ . . . . , $(3 \cdot 17)^{223456789} \bmod 379 =$ . . . . .

Trovare il minimo intero non negativo n che sia soluzione dell'equazione congruenziale $51x \equiv_{379} 5$. ☐ *Tale x non esiste*, oppure ☐ *esiste ed è* . . . . In ogni caso, qual è l'insieme S di tutte le soluzioni intere dell'equazione? $S =$ . . . . . .

Il numero $2^{379} - 2$ è multiplo di 379? *sì* ☐ *no* ☐ *impossibile stabilirlo* ☐

---

8 Siano $A = \{n \in \mathbb{Z} \mid (|n| < |10|) \wedge (n \equiv_4 1)\}$, $B = \{n \in \mathbb{N} \mid n \leq 8\}$ e $C = \{n \in A \mid n > 0\}$; si consideri poi l'insieme $F = \mathrm{Map}(A, B)$ delle applicazioni da A a B. Si indichino: $|A| =$ . . . . , $|B| =$ . . . . , $|C| =$ . . . . , $|F| =$ . . . . . Quante sono le applicazioni iniettive da A a B? . . . . . .

Si considerino in F le relazioni binarie ρ, σ e τ così definite: per ogni f, $g \in F$,

$$f \,\rho\, g \iff (\exists a \in A)(a^f \neq a^g)$$
$$f \,\sigma\, g \iff \text{almeno una tra } f \text{ e } g \text{ è iniettiva}$$
$$f \,\tau\, g \iff \text{la restrizione di } f \text{ a } C \text{ coincide con la restrizione di } g \text{ a } C$$

ρ è un'equivalenza? *sì* ☐ *no* ☐, σ è un'equivalenza? *sì* ☐ *no* ☐, τ è un'equivalenza? *sì* ☐ *no* ☐.
Se almeno una delle tre è una equivalenza, detta questa η (dunque $\eta =$ . . .), stabilire $|F/\eta| =$ . . . . . .
Sia $f\colon a \in A \mapsto 0 \in B$. Si indichi $\left|[f]_\eta\right| =$ . . . . . e si descriva, se possibile, un'applicazione $g\colon A \to B$ tale che $f \,\eta\, g$ e $f \neq g$: ☐ *tale g non esiste*, oppure ☐ *esiste, un esempio è*

$$g = \begin{pmatrix} — & — & — & — & — & — & — & — & — & — & — & — \\ — & — & — & — & — & — & — & — & — & — & — & — \end{pmatrix}$$

(per descrivere l'applicazione si inseriscano gli elementi di A nella prima riga e le corrispondenti immagini nella seconda; ignorare gli spazi in eccesso rispetto al numero di elementi di A).

---

9 Dati in $\mathbb{Q}[x]$ i polinomi $f = (x^3-1)(x^3-x^2+3x-3)$ e $g = (x^3-1)(x^3-2x^2-x+2)$, si calcoli il massimo comun divisore *monico* d di f e g e l'insieme delle radici razionali comuni a f e g:

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

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

$f =$ . . . . . , $g =$ . . . . . .

È vero che f ha infiniti divisori di primo grado in $\mathbb{Q}[x]$? ☐ *sì* ☐ *no*.
