CdS in Informatica — a.a. 2008/2009

Esercitazione scritta di **ALGEBRA** (Proff. Cutolo e Rao) venerdì 15 maggio 2009

NOME E COGNOME	MATRICOLA
GRUPPO ☐ *I (Rao)* ☐ *rec. (Cutolo)*	ESAME: martedì 19 maggio, ore 9, aula D, DMA

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

- Esiste $f \in \mathbb{Q}[x]$ tale che $f \neq 0$ e ogni intero n tale che $n^2 < 10^{16}$ sia radice di f. *vero* ☐ *falso* ☐ *dati insuff.* ☐
- Il numero delle terne ordinate di numeri naturali minori di 5 è pari. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- L'applicazione $x \in \mathbb{Z} \mapsto \mathbb{N} \cup \{x\} \in \mathcal{P}(\mathbb{Z})$ è iniettiva. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- $(\mathcal{P}(\mathbb{N}), \cup)$ è un gruppo. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- È assegnata, ma non specificata, $\sigma \in \mathbb{S}_9$. Posto $\alpha = \sigma^{13!}$, si ha $4^\alpha = 4$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- $\{u \in \mathbb{Z} \mid 32 \text{ divide } u + 8\} \subseteq 4\mathbb{Z}$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐

---

2 Dato un insieme X, due permutazioni α e β di X sono, per definizione, *disgiunte* se e solo se: ....

....

Se α e β sono disgiunte, cosa possiamo dire sui prodotti $\alpha\beta$ e $\beta\alpha$?: ....

In $\mathbb{S}_7$, le permutazioni $(1\,2\,3)(1\,3\,7)$ e $(3\,4\,5\,6)$ sono disgiunte? *sì* ☐ *no* ☐ *impossibile stabilirlo* ☐

---

3 Per ogni $n \in \mathbb{N}$ sia $A_n = \{1, 2, 3, 8, 12, 33, n\}$ e siano p_n la proposizione '$(\forall x \in A_n)(x < 5 \Rightarrow x \leq 3)$' e s_n la proposizione '$(\forall x \in A_n)(x > 6 \Rightarrow x \geq 10)$'. Sia poi, per fissate proposizioni q e r, Φ_n la proposizione '$\big(q \Rightarrow (p_n \vee q)\big) \wedge \big(p_n \Rightarrow s_n\big) \wedge \big((\neg r) \vee ((q \wedge p_n) \Rightarrow r)\big)$'. Si stabiliscano, ove possibile, i valori di verità di:

Φ_2: ☐ *vero* ☐ *falso* ☐ *impossibile stabilirlo*; Φ_4: ☐ *vero* ☐ *falso* ☐ *impossibile stabilirlo*;

Φ_7: ☐ *vero* ☐ *falso* ☐ *impossibile stabilirlo*; Φ_9: ☐ *vero* ☐ *falso* ☐ *impossibile stabilirlo*.

---

4 Si considerino le relazioni binarie α, β, γ in $\mathbb{Z}$ definite ponendo per ogni a, $b \in \mathbb{Z}$,

$$a \,\alpha\, b :\iff \big((ab \geq 0 \Rightarrow a \mid b) \wedge (ab < 0 \Rightarrow a < b)\big)$$
$$a \,\beta\, b :\iff \big((a < 0 < b) \vee \big((0 \leq ab) \wedge (a \mid b)\big)\big)$$
$$a \,\gamma\, b :\iff \big((ab \geq 0 \Rightarrow a \mid b) \wedge (ab < 0 \Rightarrow a < 0)\big)$$

α è una relazione d'ordine? *sì* ☐ *no* ☐, β è una relazione d'ordine? *sì* ☐ *no* ☐, γ è una relazione d'ordine? *sì* ☐ *no* ☐. Nel caso almeno una delle tre sia una relazione d'ordine, se ne scelga una, la si chiami ρ (dunque $\rho = \ldots$) e si risponda alle domande che seguono. *Rispetto all'ordinamento* ρ,

$\min \mathbb{Z} = \ldots$, oppure: ☐ $\min \mathbb{Z}$ *non esiste*; $\max \mathbb{Z} = \ldots$, oppure: ☐ $\max \mathbb{Z}$ *non esiste*.

In $(\mathbb{Z}, \rho)$, $\inf \mathbb{N}^\# = \ldots$, oppure: ☐ $\inf \mathbb{N}^\#$ *non esiste*; $\sup \mathbb{N}^\# = \ldots$, oppure: ☐ $\sup \mathbb{N}^\#$ *non esiste*;

$\inf(\mathbb{Z} \smallsetminus \mathbb{N}) = \ldots$, oppure: ☐ $\inf(\mathbb{Z} \smallsetminus \mathbb{N})$ *non esiste*; $\sup(\mathbb{Z} \smallsetminus \mathbb{N}) = \ldots$, oppure: ☐ $\sup(\mathbb{Z} \smallsetminus \mathbb{N})$ *non esiste*.

Si consideri l'ordinamento indotto da ρ su $X := \{n \in \mathbb{Z} \,\big|\, |n| < 4\}$.

Si disegni a lato il diagramma di Hasse di questo ordinamento; rispetto ad esso, X è un reticolo? *sì* ☐ *no* ☐, nel caso, è complementato? *sì* ☐ *no* ☐, distributivo? *sì* ☐ *no* ☐, booleano? *sì* ☐ *no* ☐.

$\min X = \ldots$, oppure ☐ $\min X$ *non esiste*;

$\max X = \ldots$, oppure ☐ $\max X$ *non esiste*.

---

5 Siano $S = \{n \in \mathbb{N} \mid n \leq 9\}$ e $T = \{0, 3, 7\}$. In $\mathcal{P}(S)$ si considerino le relazioni binarie α, β, γ definite ponendo, per ogni X, $Y \in \mathcal{P}(S)$,

$$X \,\alpha\, Y :\iff X \cap Y = T; \qquad X \,\beta\, Y :\iff (T \subseteq X \iff T \subseteq Y); \qquad X \,\gamma\, Y :\iff |X \cap T| = |Y|.$$

Quali tra le tre sono: ...... e quali non sono: ...... relazioni di equivalenza? Se almeno una lo è, se ne scelga una e la si chiami ρ (dunque, $\rho = \ldots$) e si calcoli: $|S/\rho| = \ldots$, $|[\varnothing]_\rho| = \ldots\ldots$, $|[T]_\rho| = \ldots\ldots$.

---

6 Si consideri l'operazione binaria $\diamond$ definita nell'insieme $\mathbb{Z}_{15}$ ponendo, per ogni $a, b \in \mathbb{Z}_{15}$,

$$a \diamond b = \left(a^3 b^3 + 4(a^3 + b^3) - 3\right)^3.$$

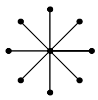
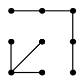
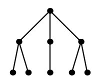
[*Suggerimento:* Nel rispondere alle domande che seguono, tenere presente che per ogni $n \in \mathbb{Z}$ si ha $n^9 \equiv_{15} n$. Questo fatto permette di calcolare facilmente radici cubiche in $\mathbb{Z}_{15}$: se $u, v \in \mathbb{Z}_{15}$ e $u^3 = v$ allora $u = v^3$].

$\diamond$ è commutativa? *sì* □ *no* □, associativa? *sì* □ *no* □. $\mathbb{Z}_{15}$ ha elemento neutro rispetto a $\diamond$? □ *no*, oppure: □ *sì, esso è:* . . . . . $(\mathbb{Z}_{15}, \diamond)$ è un semigruppo? *sì* □ *no* □, un monoide? *sì* □ *no* □, un gruppo? *sì* □ *no* □.

Scrivendo, per ogni $n \in \mathbb{Z}$, $\bar{n}$ per $[n]_{15}$, in $(\mathbb{Z}_{15}, \diamond)$: $\bar{0}$ è invertibile? □ *no*, oppure: □ *sì, il suo inverso è:* . . . . ; $\bar{1}$ è invertibile? □ *no*, oppure: □ *sì, il suo inverso è:* . . . . ; $\bar{4}$ è invertibile? □ *no*, oppure: □ *sì, il suo inverso è:* . . . . . $\bar{0}$ è cancellabile? *sì* □ *no* □; $\bar{1}$ è cancellabile? *sì* □ *no* □; $\bar{4}$ è cancellabile? *sì* □ *no* □. $\bar{0}$ è idempotente? *sì* □ *no* □; $\bar{1}$ è idempotente? *sì* □ *no* □; $\bar{4}$ è idempotente? *sì* □ *no* □.

---

7 Il grafo K_9 (cioè, si ricorda, il grafo completo su nove vertici) ha circuiti euleriani? *sì* □ *no* □. Ha sottoalberi massimali? *sì* □ *no* □. Quanti lati ha? . . . . . Si considerino K_8 ed i grafi A, B e C qui disegnati:

A:  B:  C: 

Tra questi *quattro* grafi, quali sono: . . . . e quali non sono . . . . isomorfi ad un sottoalbero massimale di K_9? Ce ne sono due isomorfi tra loro? □ *no*, oppure: □ *sì, ad esempio* . . . *e* . . . .

---

8 Sia $n = 44^{6944796} + 44^{7944797} + 44^{8944798} + 44^{9944799}$. Calcolare $(3n + n^3) \bmod 447 =$ . . . . ,
$|U(\mathbb{Z}_{447})| =$ . . . . , il periodo di $[44]_{447} \in U(\mathbb{Z}_{447})$ è: . . . .

Determinare l'insieme (risp. S_1, S_2, S_3, S_4) di tutte le soluzioni intere di ognuna delle seguenti equazioni congruenziali:

$500x + 449 \equiv_{447} 9x - 444$, $S_1 =$ . . . . ; $450x - 6 \equiv_{447} 142$, $S_2 =$ . . . . ;
$146x + 6 \equiv_{447} 50 - 2x$, $S_3 =$ . . . . ; $258x - 6 \equiv_{447} 142 + 4x$, $S_4 =$ . . . . ;

Descrivere esplicitamente l'insieme $A := \{a \in \mathbb{Z} \mid (\exists c \in \mathbb{Z})(132c \equiv_{447} a + 1)\}$:

$A =$ . . . .

---

9 Si calcoli il massimo comun divisore monico d in $\mathbb{Q}[x]$ tra $f := x^5 - x^4 + 3x^3 - 3x^2 + 2x - 2$ e $g := x^5 - x^4 + x^3 - x^2 - 2x + 2$; si scrivano poi f e g come prodotto di polinomi monici irriducibili in $\mathbb{Q}[x]$:

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

Quante: . . . e quali: . . . . sono le radici comuni a f e g?

Detti infine 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 irriducibili in $\mathbb{Z}_3[x]$ e si indichino il massimo comun divisore monico d_3 ed il minimo comune multiplo non monico m_3 in $\mathbb{Z}_3[x]$ tra f_3 e g_3:

$f_3 =$ . . . . ; $g_3 =$ . . . .

$d_3 =$ . . . . ; $m_3 =$ . . . .
