CdL e CdD in Informatica — a.a. 2002/2003
Esercitazione scritta di **ALGEBRA** (Prof. Rao) lunedì 16 giugno 2003

NOME E COGNOME	MATRICOLA

1 La forma proposizionale $\Big(\big(r \Rightarrow (\neg q)\big) \Rightarrow \big(r \Rightarrow \neg(p \vee q)\big)\Big) \Longrightarrow \Big(r \Rightarrow (\neg p)\Big)$
è: ☐ *una tautologia,* ☐ *contingente,* ☐ *una contraddizione.*

Invece, la forma proposizionale $\Big(r \Rightarrow (\neg p)\Big) \Longrightarrow \Big(\big(r \Rightarrow (\neg q)\big) \Rightarrow \big(r \Rightarrow \neg(p \vee q)\big)\Big)$
è: ☐ *una tautologia,* ☐ *contingente,* ☐ *una contraddizione.*

---

2 Sia $H = \big\{[2n]_{30} \mid n \in \mathbb{Z}\big\}$, una parte dell'anello $\mathbb{Z}_{30}$. H è un sottoanello di $\mathbb{Z}_{30}$? *sì* ☐ *no* ☐. Ne è un ideale? *sì* ☐ *no* ☐. Quanti elementi ha? $|H| =$ . . . . .

Si considerino in H le operazioni binarie $\oplus$ e $\odot$ definite da: $\forall\, n, m \in \mathbb{Z}$,

$$[2n]_{30} \oplus [2m]_{30} := [2(n+m)]_{30} \qquad\qquad [2n]_{30} \odot [2m]_{30} := [4nm]_{30}$$

$(H, \oplus, \odot)$ è un anello? *sì* ☐ *no* ☐; nel caso, è commutativo? *sì* ☐ *no* ☐.

Si consideri l'applicazione $\varphi : [n]_{15} \in \mathbb{Z}_{15} \mapsto [16n]_{30} \in \mathbb{Z}_{30}$. Questa applicazione φ è ben definita?

☐ *sì, perché:* $\forall n, m \in \mathbb{Z} \quad n \equiv_{15} m \Longrightarrow 16n \equiv_{30} 16m$

☐ *sì, perché:* $\forall n \in \mathbb{Z} \quad 16n \equiv_{15} n$

Quali delle seguenti valgono?

$\operatorname{im}\varphi \subseteq H$	$\operatorname{im}\varphi \subset H$	$\operatorname{im}\varphi = H$	φ è iniettiva	φ è suriettiva	φ è un omomorfismo di anelli
sì ☐ no ☐	sì ☐ no ☐	sì ☐ no ☐	sì ☐ no ☐	sì ☐ no ☐	sì ☐ no ☐

Quali tra i seguenti coincidono con $\varphi\big([2]_{15}\big)$? ☐ $[2]_{30}$, ☐ $[3]_{30}$, ☐ $[12]_{30}$, ☐ $[6]_{30}$, ☐ nessuno dei precedenti.

$(H, \oplus, \odot)$ è isomorfo a $\mathbb{Z}_{15}$? *sì* ☐ *no* ☐. Nel caso, un isomorfismo è (completare):

$$[n]_{15} \in \mathbb{Z}_{15} \longmapsto \; . \; . \; . \; . \; . \; . \; . \; . \; . \; . \; . \; . \; . \; . \; . \; . \; . \; . \quad \in H$$

$(H, \oplus, \odot)$ è un anello unitario? *sì* ☐ *no* ☐; nel caso, la sua unità è: . . . . . $(H, \oplus, \odot)$ è un dominio di integrità? *sì* ☐ *no* ☐, è un campo? *sì* ☐ *no* ☐.

L'applicazione $[t]_{30} \in H \mapsto [t]_{15} \in \mathbb{Z}_{15}$ è un isomorfismo? *sì* ☐ *no* ☐ Quali tra i seguenti sono cancellabili in $(H, \oplus, \odot)$? ☐ $[6]_{30}$, ☐ $[8]_{30}$, ☐ $[16]_{30}$, ☐ nessuno dei precedenti.

---

3 Determinare l'insieme delle soluzioni in $\mathbb{Z}$ di ciascuna delle seguenti equazioni congruenziali. *[Trascrivere il procedimento effettuato sul retro di questo foglio.]*

$2076x \equiv 1692 \pmod{843}$ *insieme delle soluzioni:* . . . .

$480x \equiv 80 \pmod{210}$ *insieme delle soluzioni:* . . . .

$480x \equiv 90 \pmod{210}$ *insieme delle soluzioni:* . . . .

Calcolare il resto di $n := 90001 \cdot 17^{8954285785} + (25 \cdot 6)^{14} + (-17)^{678678}$ modulo 90. $n \bmod 90 =$ . . . . .

Calcolare $|\mathcal{U}(\mathbb{Z}_{90})| =$ . . . . Qual è il periodo di $u := [-17]_{90}$ nel gruppo $\mathcal{U}(\mathbb{Z}_{90})$? . . . . E qual è l'inverso di u? $u^{-1} =$ . . . . È vero che $u^{-1} = [n]_{90}$? ☐ *sì,* ☐ *no,* ☐ *non lo si può decidere.*

---

4 Vero o falso? Per ogni intero positivo n, esiste almeno un grafo (semplice) con $n(n-1)/2$ lati.
☐ *vero,* ☐ *falso,* ☐ *dati insufficienti per stabilirlo.*

Se esiste, un tale grafo è necessariamente connesso. ☐ *vero,* ☐ *falso,* ☐ *dati insufficienti per stabilirlo.*

---

5 Siano X un insieme di 9 elementi e Y insieme di 12 elementi. Se $|X \cap Y| = 5$ allora esistono esattamente . . . . applicazioni da $X \cup Y$ a X, ed esistono esattamente . . . . applicazioni iniettive da $X \cup Y$ a $X \cap Y$. Si ha $(X \cup Y) \smallsetminus Y = X \smallsetminus Y$? *sì* ☐ *no* ☐ *i dati non sono sufficienti per stabilirlo* ☐

Il numero delle parti di Y equipotenti a X è . . . .

---

6 Nell'insieme $S := \{1,2,3,4,5,6,7,8\}$ si considerino le relazioni binarie ρ, σ, τ di grafici rispettivamente

$$\rho^{\#} := \Delta_S \cup \{(1,4),(1,7),(2,4),(2,7),(3,4),(3,7),(6,1),(6,2),(6,3),(6,4),(6,7),(7,4)\};$$
$$\sigma^{\#} := \Delta_S \cup \{(1,4),(1,7),(2,4),(2,7),(3,4),(4,2),(4,3),(6,1),(6,2),(6,3),(6,4),(6,7)\};$$
$$\tau^{\#} := \Delta_S \cup \{(1,6),(1,7),(2,3),(2,4),(3,2),(3,4),(4,2),(4,3),(6,1),(6,7),(7,1),(7,6)\};$$

dove $\Delta_S := \{(x,x) \mid x \in S\}$. Si compili la tabella:

la relazione	ρ		σ		τ	
è di	sì	no	sì	no	sì	no
equivalenza						
ordine largo						
ordine stretto						

Si scelga tra ρ, σ e τ una equivalenza: . . . . Quanti elementi ha il corrispondente insieme quoziente? . . . . . Si scrivano le corrispondenti classi di equivalenza, elencandone esplicitamente gli elementi:

. . . .

Tra ρ, σ e τ si scelga ora un ordinamento (largo o stretto): . . . . . Disegnarne su questo foglio, a destra della tabella in alto, il diagramma di Hasse.

Con questo ordinamento,

S è un reticolo? *sì* ☐ *no* ☐. Ha minimo? *sì* ☐ *no* ☐ (è . . .), ha massimo? *sì* ☐ *no* ☐ (è . . .);
ha elementi minimali? *sì* ☐ *no* ☐ (sono . . . .); ha elementi massimali? *sì* ☐ *no* ☐ (sono . . . .);
$\sup\{5,8\}$ non esiste ☐, oppure è . . ?

Sia θ l'ordinamento indotto da quello scelto per S su $T := S - \{5,8\}$. (T,θ) è un reticolo? *sì* ☐ *no* ☐, un reticolo distributivo? *sì* ☐ *no* ☐, un reticolo complementato? *sì* ☐ *no* ☐, un reticolo booleano? *sì* ☐ *no* ☐.

---

7 [*Riportare i calcoli relativi a questo esercizio e le motivazioni alle risposte sul retro di questo foglio*]
Dati in $\mathbb{Q}[x]$ i polinomi $f = x^6 - x^5 - 15x^4 - 24x^3 - 7x^2 + 9x + 5$ e $g = x^5 - 3x^4 - 9x^3 - 7x^2 + 8x + 10$, con l'algoritmo euclideo si trovino il massimo comun divisore *monico* d di f e g e dei polinomi u_0, $v_0 \in \mathbb{Q}[x]$ tali che $d = u_0 f + v_0 g$. Si trovino poi l'insieme C delle radici razionali comuni a f e g e si calcolino i quozienti $g_1 = g/d$ e $f_1 = f/d$.

[Risposte: $d =$ . . . .

$u_0 =$ . . . . $v_0 =$ . . . .

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

$g_1 =$ . . . . $f_1 =$ . . . .]

Infine si decompongano i polinomi d, g ed f nel prodotto di polinomi *monici irriducibili* in $\mathbb{Q}[x]$:

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

$f =$ . . . .

Siano f_5 e g_5 rispettivamente f e g riguardati come polinomi in $\mathbb{Z}_5[x]$, e sia d_5 il loro massimo comun divisore monico in $\mathbb{Z}_5[x]$. Si decompongano (nell'ordine) f_5, g_5 e d_5 nel prodotto di polinomi monici irriducibili in $\mathbb{Z}_5[x]$:

$f_5 =$ . . . . $g_5 =$ . . . .

$d_5 =$ . . . .
