CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II, RECUPERO)
7 SETTEMBRE 2015

Svolgere i seguenti esercizi, ***giustificando pienamente tutte le risposte***. Sui fogli consegnati vanno indicati: ***nome***, ***cognome***, ***matricola*** e ***gruppo di appartenenza***. Non è necessario consegnare la traccia.

Esercizio 1. Si dia la definizione di *grafo* (semplice) e quella di *grafo connesso.*

Esercizio 2. Indicato con $\mathbb{P}$ l'insieme degli interi positivi primi, e posto $X = \{10, 25, 26\}$, elencare gli elementi di ciascuno degli insiemi:

$A = \{p \in \mathbb{P} \mid (\forall x \in X)(p|x)\}$,
$B = \{p \in \mathbb{P} \mid (\exists x \in X)(x|p)\}$,
$C = \{p \in \mathbb{P} \mid (\forall x \in X)(p|x \vee p < x)\}$,
$D = \{p \in \mathbb{P} \mid p < 20 \wedge (\forall x \in X)(p|x \Rightarrow p = 2)\}$,
$E = \{p \in \mathbb{P} \mid p > 8 \Rightarrow (\exists x \in X)(p|x)\}$.

Esercizio 3. Nell'insieme $S = \{1, 2, 3\}$ si consideri la relazione binaria α di grafico

$$\{(1, 1), (1, 3), (2, 2), (3, 1), (3, 3)\}.$$

α una relazione di equivalenza? Nel caso lo sia, elencare le classi di equivalenza in S/α.

Esercizio 4. Si considerino le relazioni binarie $\mathcal{S}$ e $\mathcal{R}$ definite in $\mathbb{N}$ ponendo, per ogni $a, b \in \mathbb{N}$,

$$a\ \mathcal{S}\ b \iff (a \leq b \vee \mathrm{rest}(a, 3) \mid \mathrm{rest}(b, 3)); \qquad a\ \mathcal{R}\ b \iff (a \leq b \wedge \mathrm{rest}(a, 3) \mid \mathrm{rest}(b, 3)).$$

(*i*) $\mathcal{S}$ non è né d'ordine né di equivalenza; perché?
(*ii*) Invece $\mathcal{R}$ è d'ordine. Determinare gli eventuali elementi minimali, massimali, minimo e massimo in $(\mathbb{N}, \mathcal{R})$.
(*iii*) Quali dei seguenti sono reticoli, e quali no? Per quelli che lo sono, specificare se sono reticoli distributivi e se sono reticoli complementati: $(\mathbb{N}, \mathcal{R})$, $(3\mathbb{N} + 1, \mathcal{R})$, $(A, \mathcal{R})$, $(B, \mathcal{R})$, dove $A = \{n \in \mathbb{N} \mid n \leq 9\}$ e $B = \{1, 7, 18, 23, 31, 300\}$. Nel rispondere, disegnare i diagrammi di Hasse di $(A, \mathcal{R})$ e $(B, \mathcal{R})$.
(*iv*) In $(\mathbb{N}, \mathcal{R})$, determinare, se esistono, $\inf\{59, 61\}$ e $\sup\{59, 61\}$.
(*v*) Spiegare perché non esistono in $(\mathbb{N}, \mathcal{R})$ quattro elementi a due a due non confrontabili tra loro.

Esercizio 5. Si consideri l'applicazione $f\colon (a, b) \in \mathbb{Z}_{12} \times \mathbb{Z}_{12} \mapsto ab \in \mathbb{Z}_{12}$.

(*i*) f è suriettiva?
(*ii*) Determinare gli elementi dell'insieme $A = \{a \in \mathbb{Z}_{12} \mid (\exists b \in \mathbb{Z}_{12} \smallsetminus \{\bar{0}\})((a, b) \in \overleftarrow{f}(\{\bar{0}\}))\}$.
(*iii*) Determinare gli elementi dell'insieme $B = \{a \in \mathbb{Z}_{12} \mid (\exists b \in \mathbb{Z}_{12})((a, b) \in \overleftarrow{f}(\{\bar{1}\}))\}$.
(*iv*) $\mathcal{F} := \{A, B\}$ è una partizione di $\mathbb{Z}_{12}$? (Giustificare la risposta in tutti i dettagli).
(*v*) Indicata, per ogni $a \in \mathbb{Z}_{12}$, con f_a l'applicazione: $b \in \mathbb{Z}_{12} \mapsto ab \in \mathbb{Z}_{12}$, dire per quali $a \in \mathbb{Z}_{12}$ f_a è iniettiva e per quali f_a è suriettiva.
(*vi*) Determinare, se possibile, l'applicazione inversa di $f_{\bar{7}}$ (utilizzare e risolvere a questo scopo un'opportuna equazione congruenziale).

Esercizio 6.

(*i*) Senza effettuare prodotti, si spieghi perché in $\mathbb{Z}_5[x]$ si ha $x^5 - x = x(x - \bar{1})(x - \bar{2})(x - \bar{3})(x - \bar{4})$.
(*ii*) Si costruisca un polinomio $g \in \mathbb{Z}_5[x]$ di grado 5 che non ammetta radici in $\mathbb{Z}_5$.

Per ogni primo p, sia f_p il polinomio $x^5 - x \in \mathbb{Z}_p[x]$.

(*iii*) Per ogni p, si giustifichi il fatto che f_p è prodotto, in $\mathbb{Z}_p[x]$, di fattori di grado 1 se e solo se $x^2 + \bar{1}$ ha radici in $\mathbb{Z}_p$
(*iv*) Si trovi un primo p tale che f_p abbia, in $\mathbb{Z}_p[x]$, un fattore irriducibile di grado 2.
(*v*) Esiste un primo p tale che f_p abbia, in $\mathbb{Z}_p[x]$, un fattore irriducibile di grado 3?