# CORSO DI LAUREA IN INFORMATICA
# PROVA SCRITTA DI ALGEBRA (GRUPPI I, II, RECUPERO)
# 26 GENNAIO 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.** $(i)$ Dare la definizione di *divisore* (in $\mathbb{Z}$) di un numero intero.

$(ii)$ Per ogni $m \in \mathbb{Z}$ definire la relazione $\equiv_m$ di congruenza modulo $m$ in $\mathbb{Z}$.

$(iii)$ Per ogni $m, a \in \mathbb{Z}$ descrivere $[a]_{\equiv_m}$.

$(iv)$ Determinare gli $m \in \mathbb{N}$ tali che $[27]_m = [-17]_m$.

**Esercizio 2.** Siano $\mathcal{P} = \mathcal{P}(\mathbb{N}) \setminus \{\varnothing\}$ e $\mathbb{P}$ l'insieme dei numeri primi positivi. Per ogni $X \in \mathcal{P}$, sia $\pi(X) = \{p \in \mathbb{P} \mid (\exists n \in X)(p|n)\}$. Consideriamo l'applicazione $f\colon X \in \mathcal{P} \mapsto \pi(X) \in \mathcal{P}(\mathbb{P})$ ed il suo nucleo di equivalenza $\mathcal{R}_f$.

$(i)$ $f$ è suriettiva? $f$ è iniettiva?

$(ii)$ Trovare un $\bar{Y} \in \mathcal{P}$ tale che $|[\bar{Y}]_{\mathcal{R}_f}| = 1$.

$(iii)$ Verificare: $(\forall X \in \mathcal{P} \setminus \{\bar{Y}\})([X]_{\mathcal{R}_f}$ è infinito$)$.

$(iv)$ Caratterizzare gli $X \in \mathcal{P}$ tali che $|\pi(X)| = 1$.

$(v)$ Dire, di ciascuna delle seguenti formule, se è vera o falsa (e perché):

(a) $(\forall X \in \mathcal{P})(X \text{ infinito} \Rightarrow \pi(X) \text{ infinito})$;

(b) $(\forall X \in \mathcal{P})(\pi(X) \text{ infinito} \Rightarrow X \text{ infinito})$;

(c) $(\forall X, Y \in \mathcal{P})(\pi(X) \cap \pi(Y) \neq \varnothing \Rightarrow X \cap Y \neq \varnothing)$;

(d) $(\forall X, Y \in \mathcal{P})(\pi(X) \cap \pi(Y) = \varnothing \Rightarrow X \cap Y = \varnothing)$;

**Esercizio 3.** Si definisca in $\mathbb{N}$ la relazione d'ordine $\Sigma$ ponendo, per ogni $a, b \in \mathbb{N}$:

$$a \,\Sigma\, b \iff \big((a = b) \vee (\mathrm{rest}(a, 10) < \mathrm{rest}(b, 10) \wedge \mathrm{rest}(a, 5) < \mathrm{rest}(b, 5))\big).$$

$(i)$ Stabilire se $\Sigma$ è totale.

$(ii)$ Determinare, se esistono (o spiegare perché non esistono), gli elementi minimali, massimali, minimo, massimo in $(\mathbb{N}, \Sigma)$.

$(iii)$ Determinare l'insieme dei minoranti di $\{3, 7\}$ in $(\mathbb{N}, \Sigma)$. Esiste, in $(\mathbb{N}, \Sigma)$, $\inf\{3, 7\}$?

$(iv)$ Posto $X = \{0, 1, 3, 6, 7, 9, 17\}$, si stabilisca se $(X, \Sigma)$ è un reticolo.

$(v)$ Di ciascuna delle seguenti parti di $X$ di dica se, ordinata sempre da $\Sigma$, è un reticolo, un reticolo distributivo, un reticolo complementato: $X \setminus \{6\}$, $X \setminus \{7\}$, $X \setminus \{3\}$.

**Esercizio 4.** $(i)$ Determinare gli $a \in \mathbb{Z}_7$ tali che il polinomio $x^2 - a$ sia irriducibile in $\mathbb{Z}_7[x]$.

$(ii)$ Determinare il numero dei polinomi della forma $(x^2 - a)(x^2 - b) \in \mathbb{Z}_7[x]$, con $a, b \in \mathbb{Z}_7$, che siano:

$(\alpha)$ il prodotto di due polinomi irriducibili;

$(\beta)$ il prodotto di tre polinomi irriducibili;

$(\gamma)$ il prodotto di quattro polinomi irriducibili.

**Esercizio 5.** Sia $S = \{n \in \mathbb{N} \mid 1 \leq n \leq 10\}$. Sia $*$ l'operazione binaria definita in $\mathcal{P}(S)$ da:

$$(\forall X, Y \in \mathcal{P}(S))(X * Y = X \triangle Y \triangle \{1\}).$$

$(i)$ $*$ è commutativa? $*$ è associativa?

$(ii)$ determinare (se esiste) l'elemento neutro di $(\mathcal{P}(S), *)$. Nel caso, stabilire quali sono gli elementi simmetrizzabili, descrivendone i corrispondenti simmetrici.

$(iii)$ Che tipo di struttura è $(\mathcal{P}(S), *)$?

$(iv)$ Per ciascuna di $A := \{X \in \mathcal{P}(S) \mid 1 \in X\}$ e $B := \{X \in \mathcal{P}(S) \mid 1 \notin X\}$, si stabilisca se è una parte chiusa e, nel caso, se, munita dell'operazione indotta da $*$, è un gruppo.