CORSO DI LAUREA TRIENNALE IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I E II)
12 LUGLIO 2019

Svolgere i seguenti esercizi,

$\longrightarrow$ **giustificando pienamente tutte le risposte.** $\longleftarrow$

Sui fogli consegnati vanno indicati: **nome**, **cognome**, **matricola**, **gruppo di appartenenza**.
Non è necessario consegnare la traccia.

Esercizio 1. Dare la definizione di *differenza simmetrica* $X \vartriangle Y$ tra due insiemi X e Y.
Siano $A = \{n \in \mathbb{Z} \mid n^2 < 25 \wedge n \equiv_3 1\}$ e $B = \{n \in \mathbb{N} \mid n < 6\}$. Elencare gli elementi di A e quelli di $C := A \vartriangle B$.

Esercizio 2. Sia $*$ l'operazione binaria definita in $S := \mathbb{Z}_{25} \times \mathbb{Z}_{25}$ ponendo, per ogni $a, b, c, d \in \mathbb{Z}_{25}$,

$$(a, b) * (c, d) = (\bar{3}ac, b).$$

(*i*) $*$ è commutativa? $*$ è associativa?
(*ii*) Facendo uso di un'opportuna equazione congruenziale, determinare tutti gli elementi $(x, y) \in S$ tali che in S si abbia $(x, y) * (\bar{3}, \bar{5}) = (\bar{6}, \bar{6})$.
(*iii*) Determinare tutti gli (eventuali) elementi neutri a destra, neutri a sinistra, neutro in $(S, *)$ e decidere se $(S, *)$ è o non è un semigruppo, un monoide, un gruppo.
(*iv*) Siano $T_1 = \mathbb{Z}_{25} \times \{\bar{9}\} \subseteq S$ e $T_2 = \{\bar{9}\} \times \mathbb{Z}_{25} \subseteq S$. Per ciascuna di T_1 e T_2 decidere se è una parte chiusa in $(S, *)$ e, nel caso lo sia, studiare la struttura indotta su essa da $(S, *)$, decidendo se si tratta di un semigruppo, un monoide, un gruppo, commutativa o meno, e, nel caso la domanda abbia senso, determinandone gli elementi simmetrizzabili.

Esercizio 3. Si consideri l'applicazione $f\colon n \in \mathbb{N}^* \mapsto |\tau(n)| \in \mathbb{N}$, dove, per ogni $n \in \mathbb{N}^*$ indichiamo con $\tau(n) = \{p \in \mathbb{P} \mid p \leq n\}$ l'insieme dei numeri naturali primi minori o uguali ad n.
(*i*) f è iniettiva? f è suriettiva?
(*ii*) Vero o falso? Per ogni $n, m \in \mathbb{N}^* \ldots$
  (a) $\ldots n < m \implies |\tau(n)| \leq |\tau(m)|$;
  (b) $\ldots n < m \implies |\tau(n)| < |\tau(m)|$.
(*iii*) Detto $\sim$ il nucleo di equivalenza di f, determinare $[1]_\sim$ e $[9]_\sim$.

Sia ora σ la relazione d'ordine definita in $\mathbb{N}^*$ ponendo, per ogni $n, m \in \mathbb{N}^*$,

$$n \,\sigma\, m \iff \big(n = m \vee (|\tau(n)| \neq |\tau(m)| \wedge |\tau(n)| \text{ divide } |\tau(m)|)\big).$$

(*iv*) Stabilire se σ è una relazione totale.
(*v*) Determinare in $(\mathbb{N}^*, \sigma)$ eventuali minimo, massimo, elementi minimali, elementi massimali.
(*vi*) In $(\mathbb{N}^*, \sigma)$, descrivere gli insiemi dei minoranti e dei maggioranti di $\{3, 4\}$ individuando poi, se esistono, $\inf\{3, 4\}$ e $\sup\{3, 4\}$.
(*vii*) $(\mathbb{N}^*, \sigma)$ è un reticolo? Se lo è, è distributivo? È complementato?

Esercizio 4. Sia $f = x^4 - \bar{4} \in \mathbb{Z}_{13}[x]$.
(*i*) f si può rappresentare nella forma $(x^2 - a)(x^2 + a)$. Per quali valori di $a \in \mathbb{Z}_{13}$? f ha radici in $\mathbb{Z}_{13}$? È irriducibile in $\mathbb{Z}_{13}[x]$?
(*ii*) Spiegare perché un polinomio monico di grado due non irriducibile in $\mathbb{Z}_{13}[x]$ ha necessariamente la forma $(x - u)(x - v)$ per opportuni elementi $u, v \in \mathbb{Z}_{13}$.
(*iii*) Quanti sono i polinomi monici di secondo grado e non irriducibili in $\mathbb{Z}_{13}[x]$? E quanti quelli, sempre monici di secondo grado, irriducibili?
(*iv*) Descrivere i polinomi in $\mathbb{Z}_{13}[x]$ che abbiano grado 13 ed ammettano tutti gli elementi di $\mathbb{Z}_{13}$ come radici.