

CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II, RECUPERO)
22 GENNAIO 2016

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. Assegnati tre interi a, b, m , con $m \neq 0$, si consideri l'equazione congruenziale

$$ax \equiv_m b. \quad (*)$$

- (i) Cosa significa dire che l'intero u è soluzione di $(*)$?
- (ii) Fornire una condizione necessaria e sufficiente affinché $(*)$ abbia almeno una soluzione in \mathbb{Z} .
- (iii) Se $u \in \mathbb{Z}$ è una soluzione di $(*)$, come si può descrivere, in generale, l'insieme di *tutte* le soluzioni di $(*)$ in \mathbb{Z} ?

Esercizio 2. Per ogni intero positivo n , indichiamo con $C(n)$ la somma delle cifre di n (quando n sia scritto in base 10. Ad esempio, $C(3049) = 3 + 0 + 4 + 9 = 16$). Consideriamo la relazione d'ordine σ definita in $S := \{n \in \mathbb{N} \mid 1 \leq n \leq 100001\}$ ponendo, per ogni $a, b \in S$,

$$a \sigma b \iff (a = b \vee C(a) < C(b)).$$

- (i) Si determinino in (S, σ) , gli eventuali elementi minimali, massimali, minimo, massimo.
- (ii) σ è totale?
- (iii) (S, σ) è un reticolo?
- (iv) Disegnare il diagramma di Hasse di (T, σ) , dove $T = \{5, 21, 32, 44, 101, 771, 906, 2000, 11111\}$.
 (T, σ) è un reticolo?
- (v) Determinare, se possibile (o spiegare perché non esiste) una parte K di T tale che $|K| = 5$ e (K, σ) sia un reticolo distributivo non totalmente ordinato.

Esercizio 3. Per ogni polinomio $f \in \mathbb{Z}_5[x]$, sia $R(f) = \{a \in \mathbb{Z}_5 \mid f(a) = \bar{0}\}$, l'insieme delle radici di f in \mathbb{Z}_5 .

- (i) Determinare (o spiegare perché non esiste) un $f \in \mathbb{Z}_5[x]$ tale che $R(f) = \{\bar{1}, \bar{3}\}$.
- (ii) Verificare che per ogni $X \subseteq \mathbb{Z}_5$ esiste $f \in \mathbb{Z}_5[x]$ tale che $R(f) = X$.

Sia ora F l'applicazione $f \in \mathbb{Z}_5[x] \mapsto R(f) \in \mathcal{P}(\mathbb{Z}_5)$.

- (iii) F è iniettiva? F è suriettiva?

Detta poi \sim la relazione binaria definita in $\mathbb{Z}_5[x]$ ponendo, per ogni $f, g \in \mathbb{Z}_5[x]$, $f \sim g \iff R(f) = R(g)$,

- (iv) spiegare perché \sim è una relazione di equivalenza;
- (v) decidere se $\bar{1} \sim x^2 + \bar{2}$ e se $\bar{1} \sim (x^2 + \bar{2})^{500}$;
- (vi) calcolare $|\mathbb{Z}_5[x]/\sim|$.
- (vii) Esiste $f \in \mathbb{Z}_5[x]$ tale che $[f]_\sim$ sia finito?

Esercizio 4. Considerare, in $M := \mathbb{Z}_{10} \times \mathbb{Z}_{10} \times \mathbb{Z}_{10}$, l'operazione binaria $*$ definita da:

$$(a_1, b_1, c_1) * (a_2, b_2, c_2) = (a_1 a_2, a_1 b_2 + b_1 c_2, c_1 c_2)$$

per ogni $a_1, b_1, c_1, a_2, b_2, c_2 \in \mathbb{Z}_{10}$.

- (i) $*$ è associativa? È commutativa?
- (ii) $(M, *)$ ha elemento neutro?
- (iii) Descrivere l'insieme degli elementi invertibili in $(M, *)$, specificandone anche gli inversi.
- (iv) Stabilire se, in $(M, *)$, l'elemento $(\bar{3}, \bar{5}, \bar{3})$ ha inverso, e nel caso calcolare questo inverso.
- (v) Spiegare perché, scelti comunque $u, v \in \mathbb{Z}$, se $u \equiv_{10} v$, allora si ha: u è pari se e solo se v è pari.
- (vi) Posto $D = \{\bar{b} \in \mathbb{Z}_{10} \mid b \text{ è un intero dispari}\}$ e $P = \{\bar{b} \in \mathbb{Z}_{10} \mid b \text{ è un intero pari}\}$, per ciascuna delle parti $A := \mathbb{Z}_{10} \times D \times \mathbb{Z}_{10}$ e $B := \mathbb{Z}_{10} \times P \times \mathbb{Z}_{10}$ si dica se è o meno chiusa in $(M, *)$.