Algebra 1 – Pre-prova Intermedia – 11.11.11

Rispondere alle domande su questo foglio giustificando brevemente ma esaurientemente tutte le risposte.

1. Sia $f : X \to Y$ un'applicazione e sia $f^* : \mathcal{P}(Y) \to \mathcal{P}(X)$ la funzione definita da $f^*(B) = f^{-1}(B) = \{a \in X | f(a) \in B\}$. Dimostrare che

   (a) L' applicazione f^* è iniettiva se e solo se f è suriettiva.

   (b) L'applicazione f^* è suriettiva se e solo se f è iniettiva.

(a) *Dimostriamo che se f^* è iniettiva allora f è suriettiva. Se per assurdo, f non fosse suriettiva, allora $Im(f)$ e Y sarebbero due insiemi distiniti tali che $f^*(Y) = f^*(Im(f)) = X$ e quindi f^* non sarebbe iniettiva, assurdo. Ora supponiamo che f sia suriettiva e dimostriamo che f^* è iniettiva. Quindi supponiamo che A, B siano due sottoinsiemi diversi di Y e dimostriamo che $f^*(A) \neq f^*(B)$. Possiamo supporre che esista $a \in A$ tale che $a \notin B$. Dato che f è suriettiva, allora $f^*(\{b\}) \neq \emptyset$ ed è un sottoinsieme di $f^*(A)$ ma non di $f^*(B)$ che quindi sono diversi.*

(b) *Notiamo che se $f : X \to Y$ e $g : Y \to Z$, allora $(gf)^* = f^*g^*$, $f^* = id$ se e solo se $f = id$ e ogni mappa fra gli insiemi delle parti è indotta da una mappa fra gli insiemi. Ma allora f è iniettiva se e solo se esiste un inversa g tale che $gf = id$, se e solo se $(gf)^* = id^*$ cioè, per quando detto sopra, $f^*g^* = id$ quindi se e solo se f^* è suriettiva.*

2. Si consideri l'insieme $\mathbb{Z} \times \mathbb{Z}$ e siano ρ e η le relazioni binarie definite da

$$(a_1, b_1)\rho(a_2, b_2) \qquad \text{se } a_1 < a_2 \text{ oppure } a_1 = a_2 \text{ e } b_1 \leq b_2$$

$$(a_1, b_1)\eta(a_2, b_2) \qquad \text{se } a_1 \leq a_2 \text{ e } b_1 \leq b_2$$

   (a) Mostrare che la relazione ρ è una relazione d'ordine. È totale?

   (b) Mostrare che la relazione η è una relazione d'ordine. È totale?

(a) *L'ordinamento considerato è detto "lessicografico" (si pensi a come sono ordinate le parole su un dizionario). Per provare che ρ è una relazione d'ordine, devono essere verificate le proprietà riflessiva, antisimmetrica e transitiva. La riflessività è ovvia (infatti $a_1 = a_1$ e $b_1 \leq b_1$). Proviamo l'antisimmetricità. La condizione $(a_1, b_1)\rho(a_2, b_2)$ significa che vale $(*)$ $a_1 < a_2$ oppure $(**)$ $a_1 = a_2$ e $b_1 \leq b_2$, mentre $(a_2, b_2)\rho(a_1, b_1)$ significa $(+)$ $a_2 < a_1$ oppure $(++)$ $a_2 = a_1$ e $b_2 \leq b_1$. Evidentemente non valgono $(*)$ e $(+)$ contemporaneamente; anche $(*)$ e $(++)$ sono incompatibili, così come $(**)$ e $(+)$. Dunque valgono $(**)$ e $(++)$, da cui $a_1 = a_2$ e $b_1 = b_2$. Per quanto riguarda la transitività, supponiamo $(a_1, b_1)\rho(a_2, b_2)$ e $(a_2, b_2)\rho(a_3, b_3)$. La prima condizione significa che vale $(*)$ $a_1 < a_2$ oppure $(**)$ $a_1 = a_2$ e $b_1 \leq b_2$, mentre la seconda significa $(+)$ $a_2 < a_3$ oppure $(++)$ $a_2 = a_3$ e $b_2 \leq b_3$. Se valgono $(*)$ e $(+)$, oppure $(*)$ e $(++)$, o ancora $(**)$ e $(+)$, allora abbiamo $a_1 < a_3$, da cui $(a_1, b_1)\rho(a_3, b_3)$. Se invece valgono $(**)$ e $(++)$, allora abbiamo $a_1 = a_3$ e $b_1 \leq b_3$, da cui ancora la conclusione voluta. Infine, scelti due elementi (a_1, b_1) e (a_2, b_2), se $a_1 \neq a_2$ vale una tra $a_1 < a_2$ oppure $a_2 < a_1$, da cui rispettivamente $(a_1, b_1)\rho(a_2, b_2)$ o $(a_2, b_2)\rho(a_1, b_1)$. Se invece $a_1 = a_2$, poiché vale una tra $b_1 \leq b_2$ oppure $b_2 \leq b_1$, concludiamo che vale rispettivamente $(a_1, b_1)\rho(a_2, b_2)$ o $(a_2, b_2)\rho(a_1, b_1)$. Si tratta dunque di un ordinamento totale.*

(b) *Per quanto riguarda la relazione η, le tre proprietà dell'ordinamento sono ovviamente verificate. Ovvio anche che non si tratta di un ordinamento totale, poiché ad esempio $(1, 2)$ e $(2, 1)$ non sono elementi confrontabili.*

3. Dimostrare per induzione che per ogni $n \geq 2$ il numero $n^3 - n$ è divisibile per 3.

3. *Si verifica che per* $n = 2$, $n^3 - n = 8 - 2 = 6$ *è divisibile per* 3. *Supponiamo ora vero per* n *che* $n^3 - n$ *sia divisibile per* 3, *e per* $n + 1$*:*

$$(n+1)^3 - (n+1) = n^3 + 3n^2 + 3n + 1 - n - 1 = (n^3 - n) + 3(n^2 + n)$$

che è somma di numeri divisibili per 3 *e quindi è divisibile per* 3.

4. Sia $k > 1$ un numero naturale. Si consideri la congruenza $(k^2 - k)x \equiv_{k^2-1} 6$, e si determinino i valori di k per cui essa ha soluzioni. In corrispondenza di tali valori, si determinino tutte le soluzioni.

4. *Condizione necessaria e sufficiente affinché una congruenza del tipo* $ax \equiv_n b$ *abbia soluzioni è che* $d = \mathrm{MCD}(a, n)$ *sia un divisore di* b*: se questo accade, detta* x_0 *una soluzione, l'insieme delle soluzioni (modulo* n*) è* $\{x_0 + \frac{n}{d}t \ : \ t \in \{0, 1, ..., d-1\}\}$. *Nel nostro caso, l'MCD tra* $k^2 - k = k(k-1)$ *e* $k^2 - 1 = (k+1)(k-1)$ *è* $k - 1$ *(infatti,* k *e* $k + 1$ *sono coprimi). Allora* $k - 1$ *dovrà essere un divisore di* 6, *e poiché i divisori positivi di* 6 *sono* $1, 2, 3, 6$, *deve essere* $k \in \{2, 3, 4, 7\}$. *Si ottengono rispettivamente le seguenti congruenze:* (a) $2x \equiv_3 6 \equiv_3 0$, (b) $6x \equiv_8 6$, (c) $12x \equiv_{15} 6$, (d) $42x \equiv_{48} 6$. *Come soluzioni particolari troviamo rispettivamente:* 0, 1, 3, 7 *(le prime due sono ovvie, le altre si trovano osservando che una soluzione di* $4x \equiv_5 2$ *lo è anche di* (c), *mentre una soluzione di* $7x \equiv_8 1$ *lo è anche di* (d)). *Le soluzioni generali sono dunque, rispettivamente,* $\{0\}$, $\{1, 5\}$, $\{3, 8, 13\}$, $\{7, 15, 23, 31, 39, 47\}$.

5. Sia $G = \{a + ib \in \mathbb{C} \ : \ a, b \in \mathbb{Z} \ , \ a \equiv_{29} 12b\}$, e sia $\cdot$ l'ordinario prodotto tra numeri complessi. Si dica se $(G, \cdot)$ è un semigruppo, e se è un monoide.

5. *Il prodotto di numeri complessi su* $\mathbb{C}$ *è un'operazione commutativa, bisogna controllare che succede restringendo a* G. *Siano* $a_1 + ib_1$ *e* $a_2 + ib_2$ *due elementi di* G *e vediamo se il prodotto appartiene ancora a* G. *Sappiamo* $a_1 = 12b_1 + 29k_1$ *e* $a_2 = 12b_2 + 29k_2$ *allora*

$$(a_1 + ib_1) \cdot (a_2 + ib_2) = (a_1a_2 - b_1b_2) + i(a_1b_2 + a_2b_1)$$

e sostituendo da sopra troviamo

$$(12b_1 + 29k_1)(12b_2 + 29k_2) - b_1b_2 + i((12b_1 + 29k_2)b_1 + (12b_2 + 29k_2)b_2)$$

e raccogliendo 29 *a sinistra e destra*

$$(143b_1b_2 + 29k_3) + i(24b_1b_2 + 29k_4)$$

che é un elemento ancora in G *visto che* $143 - 24 \cdot 12 = (-5) \cdot 29$ *e quindi* $143 \equiv_{29} 24 \cdot 12$. *L'identità del prodotto* $1 = 1 + i0$ *non appartiene a* G *visto che* $1 \not\equiv_{29} 0$ *e quindi* G *non può essere un monoide.*

6. Risolvere il seguente sistema di congruenze.

$$\begin{cases} x \equiv_5 2 \\ x \equiv_9 16 \\ x \equiv_{14} 4 \end{cases}$$

6. *Essendo i moduli delle congruenze due a due coprimi, il Teorema Cinese del Resto garantisce che il sistema ammetta una e una sola soluzione modulo* $5 \cdot 9 \cdot 14$. *Utilizziamo la prima congruenza: questa significa* $(*)$ $x = 5k_1 + 2$ *per qualche* $k_1 \in \mathbb{Z}$. *Sostituendo nella seconda congruenza:* $5k_1 + 2 \equiv_9 16 \equiv_9 7$, *ovvero* $5k_1 \equiv_9 5$, *ovvero* $k_1 \equiv_9 1$, *ovvero esiste* $k_2 \in \mathbb{Z}$ *tale che* $k_1 = 9k_2 + 1$. *Tornando a* $(*)$, *otteniamo* $(**)$ $x = 5(9k_2 + 1) + 2 = (5 \cdot 9)k_2 + 7$. *Sostituiamo ora nella terza congruenza:* $(5 \cdot 9)k_2 + 7 \equiv_{14} 4$, *ovvero* $3k_2 \equiv_{14} 11$, *ovvero (moltiplicando per* 5, *inverso di* 3 *modulo* 14, *entrambi i membri)* $k_2 \equiv_{14} 55 \equiv_{14} 13$, *da cui* $k_2 = 14k_3 + 13$ *per qualche* $k_3 \in \mathbb{Z}$. *Tornando infine a* $(**)$*:* $x = 5 \cdot 9(14k_3 + 13) + 7 = 5 \cdot 9 \cdot 14 + 592$. *La soluzione (modulo* $5 \cdot 9 \cdot 14$*) è dunque* 592. *Alternativamente, ma equivalentemente, si risolvono le tre congruenze* $9 \cdot 14a \equiv_5 1$, $5 \cdot 14b \equiv_9 1$ *e* $5 \cdot 9c \equiv_{14} 1$ *e e soluzioni sono* $2 \cdot 9 \cdot 14 \cdot a + 16 \cdot 5 \cdot 14 \cdot b + 4 \cdot 5 \cdot 9 \cdot c + 5 \cdot 9 \cdot 14k$.