$\odot$ MATRICOLA: .... **SI** | **NO**

NOME: .... COGNOME: ....

Algebra 1 – Prova Intermedia – 17.11.11

Rispondere alle domande su questo foglio usando gli appositi spazi e giustificando brevemente ma esaurientemente tutte le risposte.

1. Siano A un insieme non vuoto e $\mathcal{P}(A)$ l'insieme delle parti di A. Per $E \in \mathcal{P}(A)$ fissato, sia $f_E : \mathcal{P}(A) \to \mathcal{P}(A)$ l'applicazione $X \mapsto X \cap E$. Al variare di E si consideri l'applicazione $E \mapsto f_E$ che denotiamo $f : \mathcal{P}(A) \to \mathcal{P}(A)^{\mathcal{P}(A)}$

   (a) f_E è iniettiva ? [No] — 1

   Si scelga $E = \emptyset$. Si ha $f_\emptyset(A) = \emptyset = f_\emptyset(\emptyset)$, ma $A \neq \emptyset$.

   (b) f è iniettiva ? [Sì] — 2

   Siano E_1, E_2 elementi di $\mathcal{P}(A)$ tali che $f_{E_1} = f_{E_2}$. In particolare vale $f_{E_1}(A) = f_{E_2}(A)$, dunque $E_1 = E_1 \cap A = E_2 \cap A = E_2$.

   (c) f_E è surgettiva ? [No] — 2

   Come per il punto (a)*, prendiamo $E = \emptyset$. L'applicazione $f_\emptyset$ manda ogni elemento di $\mathcal{P}(A)$ in $\emptyset$ e dunque, ad esempio, la preimmagine di $A \in \mathcal{P}(A)$ sotto $f_\emptyset$ è vuota.*

   (d) f surgettiva ? [No] — 2

   Osserviamo che l'applicazione f_E manda E in E. Dunque qualunque applicazione di $\mathcal{P}(A)$ in sé che non fissi alcun elemento non potrà essere della forma f_E per alcun E (si consideri ad esempio l'applicazione che manda ogni sottoinsieme di A nel suo complementare).

2. Si consideri in $\mathbb{C}$ il sottoinsieme $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$ e sia ∇ la relazione in $\mathbb{Z}[i]$ definita ponendo $a + ib \,\nabla\, c + id$ se esistono $m, n \in \mathbb{N}$ tali che $c = ma$ e $d = nb$.

   (a) Mostrare che la relazione ∇ è una relazione d'ordine su $\mathbb{Z}[i]$. — 2

   Verifichiamo che valgono le proprietà riflessiva, antisimmetrica e transitiva. Per quanto riguarda la riflessività, fissato un qualunque $a + ib \in \mathbb{Z}[i]$, si ha $a = 1a$ e $b = 1b$, dunque $a + ib \nabla a + ib$.

   Supponiamo ora che valgano $a + ib \nabla c + id$ e $c + id \nabla a + ib$: la prima condizione significa $c = ma$ e $d = nb$ per opportuni $m, n \in \mathbb{N}$, la seconda significa $a = hc$ e $b = kd$ per opportuni $h, k \in \mathbb{Z}$. Segue che $c = mhc$ e $d = nkd$. Ora, se $c = 0$ evidentemente vale anche $a = 0$, mentre se $c \neq 0$ vale $mh = 1$, da cui $m = h = 1$; in ogni caso otteniamo $a = c$. Analogamente si ottiene $b = d$, e l'antisimmetricità è provata.

   Supponiamo infine $a + ib \nabla c + id$ e $c + id \nabla e + if$. Allora, esistono $m, n, h, k \in \mathbb{N}$ tali che $c = ma$, $d = nb$, $e = hc$, $f = kd$. Concludiamo che vale $e = (hm)a$ e $f = (kn)b$, da cui $a + ib \nabla e + if$, e la transitività è verificata.

   (b) ∇ è un ordine totale in $\mathbb{Z}[i]$? — 2

   No. Ad esempio, $1 + 2i$ e $2 + i$ sono elementi non confrontabili.

3. Dimostrare che per $n \geq 1$ si ha : $1 \cdot 3 \cdot 5 \cdot \dots \cdot (2n-1) = \dfrac{(2n)!}{2^n \cdot n!}$ 3

Procediamo per induzione su n (il numero di fattori nel primo membro dell'uguaglianza). Per $n = 1$ otteniamo 1 ad entrambi i membri, e la base dell'induzione è verificata. Supponiamo dunque che l'uguaglianza sia valida per un certo $n \geq 1$ e proviamola vera per $n+1$: si ha

$$1 \cdot 3 \cdot 5 \cdots (2n-1) \cdot (2(n+1)-1) = \frac{(2n)!}{2^n \cdot n!} \cdot (2n+1) = \frac{(2n)! \cdot (2n+1) \cdot (2n+2)}{2^n \cdot 2 \cdot n! \cdot (n+1)} = \frac{(2(n+1))!}{2^{n+1} \cdot (n+1)!}$$

ed il passo induttivo è completato.

4. Sia data l'equazione diofantea $k^2 x + (k^2+1)y = 7$ con $k, x, y \in \mathbb{Z}$.

   (a) Per quali valori di $k \in \mathbb{Z}$ l'equazione ha soluzioni? [Tutti] 2

   Infatti, la condizione affinché una equazione diofantea del tipo considerato abbia soluzione è che l'MCD tra i coefficienti delle due variabili sia un divisore del coefficiente di grado 0, e nel nostro caso $MCD(k^2, k^2+1) = 1$.

   (b) Per $k = 2$ le soluzioni sono [$\{(-7+5t, 7-4t) \ : \ t \in \mathbb{Z}\}$] 2

   Per $k = 2$ l'equazione è $4x + 5y = 7$. Esprimiamo $1 = MCD(4,5)$ come "combinazione lineare" di 4 e 5: $1 = 4 \cdot (-1) + 5 \cdot 1$. Dunque, moltiplicando per 7 i due membri, si ottiene che $(-7, 7)$ è una soluzione dell'equazione diofantea. La soluzione generale si esprime poi come indicato nella risposta.

5. Nell'insieme $\mathbb{G} = \mathbb{Q}^* \times \mathbb{Q}$ dove $\mathbb{Q}^* = \mathbb{Q} - \{0\}$ si consideri l'operazione $\star$ così definita:

$$(r, n) \star (s, m) = (rs, ns + m)$$

   (a) È vero che $\star$ è commutativa ? [No] 2

   Ad esempio, $(1,1) \star (2,0) = (2,2)$, mentre $(2,0) \star (1,1) = (2,1)$.

   (b) È vero che $\star$ è associativa ? [Sì] 2

   Si ha $((r_1, n_1) \star (r_2, n_2)) \star (r_3, s_3) = ((r_1 r_2) r_3, (n_1 r_2 + n_2) r_3 + n_3)$, mentre $(r_1, n_1) \star ((r_2, n_2) \star (r_3, n_3)) = (r_1 (r_2 r_3), n_1 (r_2 r_3) + n_2 r_3 + n_3)$. Poiché i risultati coincidono, deduciamo che l'operazione è associativa.

   (c) È vero che $\star$ ammette elemento neutro ? [Sì] 2

   È immediato verificare che $(1,0)$ funziona da elemento neutro.

   (d) $\mathbb{G}$ è un gruppo rispetto a $\star$? [Sì] 2

   L'inverso di (r, n) è $(1/r, -n/r)$.

6. Sia $x \in \mathbb{Z}$ tale che $\begin{cases} x \equiv_2 10 \\ x \equiv_5 9 \\ x \equiv_{11} 13 \end{cases}$

(a) Trovare un tale x minimo positivo. | 2 | |

Utilizziamo la prima congruenza: questa significa $(*)$ $x = 2k_1$ *per qualche* $k_1 \in \mathbb{Z}$. *Sostituendo nella seconda congruenza:* $2k_1 \equiv_5 4$, *ovvero* $k_1 \equiv_5 2$, *ovvero esiste* $k_2 \in \mathbb{Z}$ *tale che* $k_1 = 5k_2+2$. *Tornando a* $(*)$, *otteniamo* $(**)$ $x = 2(5k_2+2) = (2\cdot5)k_2+4$. *Sostituiamo ora nella terza congruenza:* $(2 \cdot 5)k_2 + 4 \equiv_{11} 2$, *ovvero* $k_2 \equiv_{11} 2$, *da cui* $k_2 = 11k_3 + 2$ *per qualche* $k_3 \in \mathbb{Z}$. *Tornando infine a* $(**)$: $x = (2 \cdot 5)(11k_3 + 2) + 4 = (2 \cdot 5 \cdot 11)k_3 + 24$. *La minima soluzione positiva è dunque* 24.

(b) Rappresentare tale x in base 7. | 2 | |

Si ha $24 = 7 \cdot 3 + 3$, *dunque* 24 *in base* 7 *si scrive* 33.