$\boxed{\cdot}$ Matricola: .... A ... B ... C ... D ... Voto$^{\geq 10}$: ......

Nome: .... Cognome: ....

Algebra 1 – Esame 19.07.12

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

A Siano A e B sono due sottoinsiemi di $\mathbb{N}$.

1. Se A e B sono finiti è vero che $|A \cap B| + |A \cup B| = |A| + |B|$? [Sì] | 2 | |

   Siano X e Y insiemi disgiunti, e supponiamo $|X| = n$ e $|Y| = m$ con $n, m \in \mathbb{N}$; dunque esiste una biezione di X in $\{1, ..., n\}$ ed una di Y in $\{1, ..., m\}$. È allora facile costruire una biezione di $X \cup Y$ in $\{1, ..., n+m\}$, dunque $|X \cup Y| = |X| + |Y|$. Ora, $A \cup B$ è unione disgiunta dei tre insiemi finiti $A \setminus B$, $B \setminus A$ e $A \cap B$, dunque la sua cardinalità è data da $|A \setminus B| + |B \setminus A| + |A \cap B|$. D'altra parte, A è unione disgiunta di $A \setminus B$ e $A \cap B$, mentre B lo è di $B \setminus A$ e $A \cap B$. Conculdiamo che $|A| + |B| = |A \setminus B| + |B \setminus A| + 2|A \cap B| = |A \cup B| + |A \cap B|$, ciò che si voleva.

2. Se A e B sono infiniti esiste sempre $f : A \to B$ bigettiva ? [Sì] | 2 | |

   Essendo A e B sottoinsiemi di $\mathbb{N}$, la loro cardinalità non può essere più che numerabile. D'altra parte si tratta di insiemi infiniti, e dunque la loro cardinalità è almeno numerabile. Concludiamo che A e B hanno entrambi la stessa cardinalità di $\mathbb{N}$, dunque esiste senz'altro una biezione di A in B.

B Sia $n \in \mathbb{N}$ un numero naturale $n \geq 1$.

1. Mostrare che 5 divide $3^{4n} - 1$ | 2 | |

   Essendo 3 coprimo con 5, per il Piccolo Teorema di Fermat si ha $3^4 \equiv_5 1$ (cosa che si può anche verificare direttamente), dunque $3^{4n} \equiv_5 (3^4)^n \equiv_5 1^n \equiv_5 1$, ovvero, 5 divide $3^{4n} - 1$.

2. Si ha che $3^{4n} \equiv_2 5$ se $n \equiv_3 0$? [Sì] | 2 | |

   Per ogni numero naturale n, 3^{4n} risulta un numero dispari, così come 5. Pertanto 3^{4n} e 5 sono congrui modulo 2 per ogni valore di n, in particolare per $n \equiv_3 0$.

C Sia $G = \left\{ \begin{bmatrix} d & 0 & 0 \\ 0 & a & b \\ 0 & b & a \end{bmatrix} \mid a, b, d \in \mathbb{R}, a^2 - b^2 = 1, \mid d \mid = 1 \right\}$ e sia $\star$ l'usuale prodotto righe per colonne:

1. È vero che G è chiuso rispetto a $\star$? [Sì] $\boxed{2}\boxed{}$

   Si ha
$$\begin{bmatrix} d & 0 & 0 \\ 0 & a & b \\ 0 & b & a \end{bmatrix} \star \begin{bmatrix} c & 0 & 0 \\ 0 & e & f \\ 0 & f & e \end{bmatrix} = \begin{bmatrix} cd & 0 & 0 \\ 0 & ae+bf & af+be \\ 0 & af+be & ae+bf \end{bmatrix}.$$
   Inoltre, $(ae+bf)^2-(af+be)^2 = (a^2-b^2)(e^2-f^2)$. *Ovviamente, se vale* $a^2-b^2 = e^2-f^2 = 1$ *e* $|c| = |d| = 1$, *si ha anche* $(ae+bf)^2 - (af+be)^2 = 1$ *e* $|cd| = 1$, *dunque* G *è chiuso rispetto all'operazione* $\star$.

2. È vero che $(G, \star)$ è un gruppo ? [Sì] $\boxed{2}\boxed{}$

   L'insieme delle matrici 3×3 *invertibili a coefficienti in* $\mathbb{R}$, *dotato dell'ordinario prodotto riga per colonna, è il gruppo* $\mathrm{GL}(3, \mathbb{R})$. *Poiché le matrici in* G *hanno determinante diverso da* 0, *si ha* $G \subseteq \mathrm{GL}(3, \mathbb{R})$; *si tratta dunque di provare che* G *è un sottogruppo di* $\mathrm{GL}(3, \mathbb{R})$. *Visto che (*$G$ *contiene la matrice identica e) la chiusura dell'operazione è già stata verificata, sarà sufficiente provare che l'inversa di una matrice in* G *è ancora in* G. *Ebbene, si ha*
$$\begin{bmatrix} d & 0 & 0 \\ 0 & a & b \\ 0 & b & a \end{bmatrix}^{-1} = \begin{bmatrix} d^{-1} & 0 & 0 \\ 0 & a & -b \\ 0 & -b & a \end{bmatrix},$$
   che evidentemente sta in G.

D Sia $A = \{a + ib \mid a, b \in \mathbb{Z}_5\}$ con somma e prodotto indotta da $\mathbb{Z}[i]$ l'anello degli interi di Gauss.

1. È vero che A è finito ? [Sì] $\boxed{2}\boxed{}$

   Ci sono 5 *possibili scelte per* a *ed altrettante per* b, *dunque* A *ha* 25 *elementi.*

2. È vero che A è un campo ? [No]

   In A *ci sono divisori dello zero. Ad esempio* $(2+i) \cdot (2-i) = 0$ *in* A. $\boxed{2}\boxed{}$