Esercizi di Aritmetica, 3 novembre 2023

Sotto, trovate tre risultati con le relative dimostrazioni. Tali dimostrazioni sono *corrette*, ma non *complete*, perché sottintendono una gran quantità di passaggi. Riscrivete le dimostrazioni rendendole chiare e complete. [*Hint:* Se, rileggendo la vostra dimostrazione, alcune affermazioni che avete scritto vi fanno chiedere *perché?* e questa domanda non trova risposta in quanto avete scritto, probabilmente non avete finito.]

1. Sono equivalenti:

i) il principio di induzione forte, cioè un sottoinsieme $S \subset \mathbb{N}$ che verifica
- $0 \in S$,
- per ogni $k \in \mathbb{N}$, se $\{0, \dots, k\} \subset \mathbb{N}$ anche $k+1 \in S$,

è l'intero $\mathbb{N}$;

ii) il principio del minimo, cioè ogni $S \subset \mathbb{N}$ non vuoto ammette un elemento minimo.

Sketch. Supponiamo che valga il principio del minimo e sia $S \subset \mathbb{N}$ come in (i): se per assurdo $T = \mathbb{N} \setminus S$ non è vuoto, sia m il minimo di T. Allora, $m \neq 0$ e $\{0, \dots, m-1\} \in S$, e perciò anche $m \in S$, il che è assurdo.

Se invece vale il principio di induzione forte, sia $S \subset \mathbb{N}$ un sottoinsieme privo di minimo, e sia $T = \mathbb{N} \setminus S$. Allora, T è come in (i), per cui S è vuoto. □

2. Sia A un gruppo abeliano. Mostrare che, se A ha elementi di ordine m e elementi di ordine n, ha anche elementi di ordine $\operatorname{lcm}(m, n)$.

Sketch. Supponiamo prima $\gcd(m, n) = 1$. In tal caso, se $x, y \in A$ hanno ordini m, n rispettivamente, il loro prodotto xy ha ordine mn: certamente l'ordine di xy divide mn; viceversa, da $\langle x \rangle \cap \langle y \rangle = 1$ si deduce che l'ordine di xy divide entrambi m ed n, quindi anche mn.

In generale, se le fattorizzazioni di m ed n sono $m = \prod_i p_i^{e_i}$, $n = \prod_i p_i^{f_i}$ rispettivamente, vale $\operatorname{lcm}(m, n) = \prod_i p_i^{g_i}$, con g_i il massimo tra e_i, f_i. Allora, per ogni i, esiste un elemento z_i di ordine $p_i^{g_i}$ in $\langle x \rangle$ oppure in $\langle y \rangle$, e $z = \prod_i z_i$ ha ordine $\operatorname{lcm}(m, n)$. □

3. Sia k un numero naturale fissato. Esiste una funzione $f : \mathbb{N} \to \mathbb{N}$ tale che

$$f(f(n)) = n + k \tag{$\star$}$$

per ogni $n \in \mathbb{N}$ se e solo se k è pari.

Sketch. Se k è pari, è facile costruire una tale funzione.

Supponiamo allora k dispari e sia f una tale funzione: da $f(f(n)) = n + k$ si ottiene $f(n + k) = f(n) + k$, pertanto f è costante sulle classi di resto (mod k), e quindi induce una ben definita funzione $\overline{f} : \mathbb{Z}/k\mathbb{Z} \to \mathbb{Z}/k\mathbb{Z}$. Tale $\overline{f}$ verifica:

- $\overline{f}([i]_k) \neq [i]_k$ per ogni $[i]_k \in \mathbb{Z}/k\mathbb{Z}$ perché f è iniettiva;
- $\overline{f}([i]_k) = [j]_k$ se e solo se $\overline{f}([j]_k) = [i]_k$ per ogni $[i]_k, [j]_k \in \mathbb{Z}/k\mathbb{Z}$, usando ($\star$).

Poiché k è dispari, una tale $\overline{f}$ non può esistere, e ciò contraddice l'esistenza di f. □