COMPITO DI ARITMETICA
19 luglio 2018
Soluzioni

1. Sia n un intero positivo e sia $A = \{1, \dots, 100\}$.

(a) Quante sono le terne ordinate $(x, y, z) \in A^3$ tali che $x < y < z$?

(b) Quante sono le terne ordinate $(x, y, z) \in A^3$ tali che $x < y < z$ e $z = x + y$?

SOLUZIONE:

(a) Ogni sottoinsieme $\{a_1, a_2, a_3\}$ di A di cardinalità 3 determina un'unica terna ordinata semplicemente elencando i tre elementi in ordine crescente. Viceversa, una terna ordinata $(x, y, z) \in A^3$ con $x < y < z$ determina univocamente un sottoinsieme $\{x, y, z\}$ di A di cardinalità 3. Quindi le terne cercate sono tante quante i sottoinsiemi di A di 3 elementi, ovvero $\binom{100}{3}$.

(b) Fissato $x \in A$, i possibili valori di y sono quelli compresi fra $x + 1$ (infatti y deve essere maggiore di x) e $100 - x$ (infatti $z = x + y$ deve essere al massimo 100). Inoltre, se si avesse $x \geq 50$ si avrebbe anche $y \geq 51$ e $z = x + y \geq 101$, assurdo, dunque il massimo valore possibile per x è 49. Per quanto osservato sopra, fissato x fra 1 e 49, y può assumere $(100 - x) - (x + 1) + 1 = 2(50 - x)$ valori diversi, e z è determinato dalla coppia (x, y). La risposta è quindi

$$\sum_{x=1}^{49} 2(50 - x) = 2 \sum_{w=1}^{49} w = 2 \cdot \frac{49 \cdot 50}{2} = 50 \cdot 49 = 2450,$$

dove la prima uguaglianza è ottenuta grazie al cambio di variabili $w = 50 - x$.

2. Sia a un parametro intero che soddisfa la condizione $(a, 9) = 3$. Determinare, al variare del parametro a, il numero di soluzioni dell'equazione $x^a \equiv -1 \pmod{19}$.

SOLUZIONE:

Certamente l'equazione non ha mai la soluzione $x \equiv 0 \pmod{19}$. Per il piccolo teorema di Fermat, le potenze di $x \not\equiv 0 \pmod{19}$ hanno un periodo che divide 18, ed in particolare si possono descrivere con classi di congruenza modulo 18. Visto che la condizione $(a, 9) = 3$ è descritta da congruenze modulo 9, ed in particolare $a \equiv 3 \pmod 9$ oppure $a \equiv 6 \pmod 9$, basta considerare i valori del parametro a modulo il minimo comune multiplo fra 18 e 9, cioè 18.

Si verifica immediatamente che i valori accettabili di a sono $a \equiv 3, 6, 12, 15 \pmod{18}$.

Consideriamo dapprima il caso $a \equiv 3 \pmod{18}$. Una soluzione si trova facilmente, cioè $x \equiv -1 \pmod{19}$. La funzione $x \mapsto x^3$ è un omomorfismo del gruppo ciclico $(\mathbb{Z}/19\mathbb{Z})^*$ in se stesso e, visto che $3 \mid 18$, il suo nucleo è il sottogruppo di ordine 3 (si può calcolare che questo sottogruppo è $H = \{\overline{1}, \overline{7}, \overline{11}\}$, ma questo non è richiesto dal testo del problema). Ne segue che le soluzioni di $x^3 \equiv -1 \pmod{19}$ sono la classe laterale $(-1)H$, e quindi sono 3.

Un discorso completamente analogo si può fare per il caso $a \equiv 15 \equiv -3 \pmod{18}$, poiché $x^{-3} = (x^{-1})^3$ e quindi basta sostituire $y = x^{-1}$ per ottenere le tre soluzioni.

I casi $a \equiv 6, 12 \pmod{18}$ non danno invece luogo a soluzioni. Per vederlo, si può argomentare in vari modi diversi: (1) le potenze seste sono il sottogruppo di ordine 3 di $(\mathbb{Z}/19\mathbb{Z})^*$, che non può contenere la classe di -1, poiché essa genera un sottogruppo di ordine 2; (2) poiché l'esponente è pari, se ci fosse una soluzione allora -1 dovrebbe essere un quadrato modulo 19, ma questo non è vero in quanto $19 \equiv 3 \pmod{4}$; (3) esistono delle verifiche dirette, che si possono fare a mano anche senza l'ausilio di strumenti teorici; per esempio, si può escludere che -1 sia una sesta potenza semplicemente calcolando quali sono le potenze di 2 modulo 19 (si constata che $\bar{2}$ genera $(\mathbb{Z}/19\mathbb{Z})^*$).

3. Sia G un gruppo finito di ordine n, non necessariamente abeliano.

Per ogni intero positivo d definiamo $H^{(d)}$ come il sottogruppo di G generato dall'insieme $S^{(d)} = \{x^d \mid x \in G\}$.

(a) Dimostrare che $H^{(d)}$ è un sottogruppo normale di G per ogni $d \geq 1$.

(b) Determinare tutti i possibili indici $[G : H^{(2)}]$ al variare di G fra tutti i gruppi di ordine n con n pari.

(c) Supponiamo che $6 \mid n$. Dimostrare che $S^{(2)} \cap S^{(3)} = \{e\}$ se e solo se per tutti gli elementi di $x \in G$ si ha $\mathrm{ord}(x) \mid 6$.

Soluzione:

(a) Basta verificare che per ogni $g \in G$ e per ogni $s \in S^{(d)}$ si ha $gxg^{-1} \in H^{(d)}$: infatti, da $\langle S^{(d)} \rangle = H^{(d)}$ si ha che $\langle gS^{(d)}g^{-1} \rangle = g\langle S^{(d)} \rangle g^{-1} = gH^{(d)}g^{-1}$, e quindi, se tutti i generatori di $gH^{(d)}g^{-1}$ appartengono ad $H^{(d)}$, allora anche $gH^{(d)}g^{-1} \subseteq H^{(d)}$.

Ora, se x è una d-esima potenza, ossia se esiste $y \in G$ tale che $x = y^d$, allora $gxg^{-1} = gy^dg^{-1} = (gyg^{-1})^d$, che è ancora una d-esima potenza e dunque appartiene ad $H^{(d)}$.

(b) Per ogni $x \in G$ si ha che $x^2 \in H^{(2)}$, perciò tutti gli elementi di $G/H^{(2)}$ eccetto l'identità hanno ordine 2. Un tale gruppo è necessariamente abeliano, in quanto da $\alpha^2 = \beta^2 = (\alpha\beta)^2 = e$ si ricava immediatamente che $\alpha^2\beta^2 = \alpha\beta\alpha\beta$ e dunque $\alpha\beta = \beta\alpha$. Per il teorema di Cauchy sui gruppi abeliani, l'ordine di G non può essere

divisibile per nessun primo diverso da 2, ossia l'ordine di $G/H^{(2)}$ è del tipo 2^k con $k \geq 0$. Tutti i valori di k sono possibili: per ottenere i valori positivi basta prendere $G = (\mathbb{Z}/2\mathbb{Z})^k$, per i quale di verifica immediatamente che $H^{(2)} = \{e\}$, e dunque $G/H^{(2)} \cong G$. Per ottenere il valore $k = 0$, si osservi che qualsiasi gruppo diedrale è generato dalle simmetrie, che hanno ordine 2, e quindi in questo caso $H^{(2)} = G$ e $|G/H^{(2)}| = 1$.

(c) Dimostriamo dapprima che se $S^{(2)} \cap S^{(3)} = \{e\}$ allora per ogni $x \in G$ si ha $\mathrm{ord}(x) \mid 6$, ragionando per assurdo. Supponiamo che esista un elemento $x \in G$ il cui ordine non divide 6, e quindi tale che $x^6 \neq e$. Allora $x^6 = (x^3)^2 = (x^2)^3$ è un elemento di $S^{(2)} \cap S^{(3)}$ diverso dall'identità.

Viceversa, supponiamo che per ogni $x \in G$ si abbia $\mathrm{ord}(x) \mid 6$ e sia $a = b^2 = c^3$ un elemento di $S^{(2)} \cap S^{(3)}$. Allora, dall'equazione $a^3 = b^6 = e$ si ha che $\mathrm{ord}(a) \mid 3$ e dall'equazione $a^2 = c^6 = e$ si ha che $\mathrm{ord}(a) \mid 2$. In definitiva, $\mathrm{ord}(a)|(3, 2) = 1$, quindi $a = e$.

4. Sia $g(x) = x^5 - 1 \in \mathbb{Q}[x]$ e sia $\zeta_5 \in \mathbb{C}$ una radice di $g(x)$ diversa da 1. Sia inoltre L il campo di spezzamento su $\mathbb{Q}$ del polinomio $f(x) = x^5 - 3$.

(a) Determinare il grado di L su $\mathbb{Q}$.

(b) Determinare il polinomio minimo di $\zeta_5 + \zeta_5^{-1}$ su $\mathbb{Q}$.

(c) Determinare un intero n tale che $\sqrt{n}$ appartenga ad $L \setminus \mathbb{Q}$.

Soluzione:

(a) Le radici di $f(x)$ in $\mathbb{C}$ sono i numeri algebrici $\sqrt[5]{3} \cdot \zeta_5^i$, dove $i = 0, \ldots, 4$. Ne segue immediatamente che L è il composto dei campi $K_1 = \mathbb{Q}(\zeta_5)$ e $K_2 = \mathbb{Q}(\sqrt[5]{3})$: in effetti è chiaro che $\sqrt[5]{3} \in L$, dunque $K_2 \subseteq L$, e d'altro canto L contiene anche il rapporto $\frac{\sqrt[5]{3}\zeta_5}{\sqrt[5]{3}} = \zeta_5$, dunque contiene K_1: ne segue $K_1K_2 \subseteq L$. Viceversa, se un campo contiene sia $\sqrt[5]{3}$ che ζ_5, allora contiene tutte le radici di $f(x)$, e dunque $L \subseteq K_1K_2$. Inoltre, si ha $[K_1 : \mathbb{Q}] = 4$ (come visto a lezione) e $[K_2 : \mathbb{Q}] = 5$ (perché il polinomio $f(x)$ è irriducibile su $\mathbb{Q}$ per il criterio di Eisenstein): siccome $([K_1 : \mathbb{Q}], [K_2 : \mathbb{Q}]) = (4, 5) = 1$, il campo composto K_1K_2, ovvero L, ha grado 20 su $\mathbb{Q}$.

(b) Osserviamo innanzitutto che $g(x) = (x - 1)(x^4 + x^3 + x^2 + x + 1)$, dunque ζ_5 soddisfa $\zeta_5^4 + \zeta_5^3 + \zeta_5^2 + \zeta_5 + 1 = 0$, o equivalentemente $\zeta_5^4 = -\zeta_5^3 - \zeta_5^2 - \zeta_5 - 1$. Sia per semplicità $\tau = \zeta_5 + \zeta_5^{-1} = \zeta_5 + \zeta_5^4 = -\zeta_5^3 - \zeta_5^2 - 1$. Si ha $\tau^2 = \zeta_5^2 + 2 + \zeta_5^{-2} = \zeta_5^2 + 2 + \zeta_5^3$, ed è quindi immediato osservare che $\tau^2 + \tau = 1$. Ne segue che τ è una radice del polinomio $x^2 + x - 1$, il quale è monico ed irriducibile su $\mathbb{Q}$ (perché il suo discriminante è $1^2 - 4(-1) = 5$, che non è un quadrato in $\mathbb{Q}$), quindi è il polinomio minimo di τ.

(c) È chiaro che τ è un elemento di $\mathbb{Q}(\zeta_5)$, ed abbiamo già osservato che $\mathbb{Q}(\zeta_5) \subseteq L$. D'altro canto, dalla formula esplicita per la risoluzione delle equazioni di secondo grado otteniamo che τ è uno dei due numeri

$$\frac{-1 \pm \sqrt{5}}{2};$$

in particolare, ogni campo contenente τ contiene $\sqrt{5}$. Possiamo quindi scegliere $n = 5$.