COMPITO DI ARITMETICA
13 settembre 2018
Soluzioni

1. Sia $n = 2^2 3^3 5^5$.

(a) Determinare il numero dei divisori di n che hanno al più due fattori primi distinti.

(b) Determinare il numero di coppie ordinate (a, b) di divisori di n tali che ab ha al più due fattori primi distinti.

SOLUZIONE: (a) Il numero totale dei divisori di n è uguale a $(2+1)(3+1)(5+1) = 72$. Tra di essi, quelli che hanno tutti e 3 i fattori primi 2, 3 e 5 sono quelli della forma $2^a 3^b 5^c$ con $1 \le a \le 2$, $1 \le b \le 3$, $1 \le c \le 5$; essi sono perciò $2 \cdot 3 \cdot 5 = 30$. I divisori cercati sono il complementare di questo insieme rispetto a tutti i divisori, e dunque sono $72 - 30 = 42$.

(b) L'insieme X delle coppie ordinate da cercare si può scrivere come

$$X = X_2 \cup X_3 \cup X_5 \,,$$

dove X_2 è l'insieme delle coppie (a, b) per cui ab non è divisibile per 2, e similmente X_3 e X_5 sono, rispettivamente, le coppie (a, b) per cui ab non è divisibile per 3 e per 5. Per contare la cardinalità di X usiamo il principio di inclusione-esclusione. Abbiamo

$$|X_2| = |\{(a, b) \colon a, b \mid 3^3 \cdot 5^5\}| = \{(3 + 1)(5 + 1)\}^2 = 576 \,.$$

Similmente,

$$|X_3| = \{(2 + 1)(5 + 1)\}^2 = 324 \quad \text{e} \quad |X_5| = \{(2 + 1)(3 + 1)\}^2 = 144 \,.$$

Considerando le intersezioni a due a due, abbiamo che gli elementi di $X_2 \cap X_3$ sono le coppie (a, b) che non hanno né il fattore 2 né il fattore 3, quindi sono costituite da divisori di 5^5. Esse sono dunque $6^2 = 36$. Similmente, $|X_2 \cap X_5| = 16$ e $|X_3 \cap X_5| = 9$. Infine $X_2 \cap X_3 \cap X_5$ contiene solo la coppia $(1, 1)$, dato che 1 è l'unico divisore di ab non divisibile per alcuno dei primi 2, 3 e 5.

Concludendo,

$$|X| = 576 + 324 + 144 - 36 - 16 - 9 + 1 = 984 \,.$$

2. (a) Sia p un numero primo. Supponiamo che la congruenza $(x^5-1)(x^3-1) \equiv 0 \pmod{p}$ abbia 7 soluzioni distinte modulo p: dimostrare che allora $p \equiv 1 \pmod{15}$.

(b) È vera la stessa conclusione se si cambia il modulo p con un numero n non primo?

SOLUZIONE:

Osserviamo innanzitutto che se una classe di resto x mod p soddisfa $x^3 \equiv 1 \pmod{p}$ si ha che $\mathrm{ord}_p(x)$ divide 3, dunque è 1 o 3. La prima possibilità implica $x \equiv 1 \pmod{p}$; la seconda implica che $3 = \mathrm{ord}_p(x) \mid p-1$, ovvero che $p \equiv 1 \pmod{3}$. Similmente, la congruenza $x^5 \equiv 1 \pmod{p}$ implica $x \equiv 1 \pmod{p}$ o $p \equiv 1 \pmod{5}$.

Se $p \not\equiv 1 \pmod{3}$, la congruenza $x^3 \equiv 1 \pmod{p}$ ha esattamente una soluzione ($x \equiv 1 \pmod{p}$), quindi ci sono al più 6 soluzioni della congruenza del testo. Similmente, se $p \not\equiv 1 \pmod{5}$, la congruenza $x^5 \equiv 1 \pmod{p}$ ha esattamente una soluzione, quindi ci sono al più 4 soluzioni della congruenza del testo. L'ipotesi che le soluzioni siano almeno 7 implica quindi $p \equiv 1 \pmod{3}$ e $p \equiv 1 \pmod{5}$, da cui segue $p \equiv 1 \pmod{15}$ per il teorema cinese del resto.

Quando il modulo n è un numero composto la conclusione non è più necessariamente vera. Prendiamo per esempio n della forma $n = p_1 p_2$, dove $p_1 \equiv p_2 \equiv 1 \pmod{3}$ sono primi distinti. In virtù del teorema cinese del resto, la congruenza $x^3 \equiv 1 \pmod{n}$ è equivalente al sistema

$$\begin{cases} x^3 \equiv 1 \pmod{p_1} \\ x^3 \equiv 1 \pmod{p_2}. \end{cases}$$

Siccome la prima e la seconda congruenza separatamente ammettono 3 soluzioni, il sistema ammette 9 soluzioni (distinte): si possono scegliere indipendentemente i valori di x modulo p_1 (fra le 3 soluzioni modulo p_1 dell'equazione $x^3 \equiv 1 \pmod{p_1}$) e di x modulo p_2 (fra le 3 soluzioni di $x^3 \equiv 1 \pmod{p_2}$). Ne segue che per ogni tale n la congruenza $x^3 - 1 \equiv 0 \pmod{n}$ ammette almeno 9 soluzioni distinte modulo n, e quindi anche $(x^3-1)(x^5-1) \equiv 0 \pmod{n}$ ne ammette almeno 9. Tuttavia è chiaro che un tale n può essere scelto in modo da non essere congruo ad 1 modulo 15, per esempio prendendo $p_1 = 7$ e $p_2 = 19$. Concretamente, per $n = 7 \cdot 19 = 133$, la congruenza $(x^3-1)(x^5-1) \equiv 0 \pmod{133}$ ammette le 9 soluzioni 1, 11, 30, 39, 58, 64, 102, 106, 121 modulo 133, ma $133 \not\equiv 1 \pmod{15}$.

Altri controesempi possono essere costruiti prendendo n con un fattore primo congruo ad 1 modulo 3 ed un fattore primo congruo ad 1 modulo 5, come ad esempio $n = 77 = 7 \cdot 11$.

3. Siano p, q due numeri primi, e sia G un gruppo di ordine $n = p^3q^4$. Sia poi $\varphi\colon G \to G$ un omomorfismo con la proprietà che $\varphi^2 = \varphi \circ \varphi$ sia l'omomorfismo banale, ossia l'omomorfismo che manda tutti gli elementi di G nell'identità.

(a) Dimostrare che la cardinalità di $K := \ker \varphi$ è divisibile per pq.

(b) Dterminare l'insieme dei divisori d di n per i quali esiste un gruppo G di ordine n ed un omomorfismo $\varphi\colon G \to G$ con la proprietà che φ^2 sia l'omomorfsimo banale e tale che $|\ker \varphi| = d$.

SOLUZIONE:

(a) Supponiamo, per assurdo, che $|K|$ non sia divisibile per pq. Senza perdita di generalità, possiamo supporre che p non divida $|K|$. Allora la cardinalità di $\varphi(G) \cong G/K$ è divisibile per p^3. Il nucleo K' dell'omomorfismo $\varphi|_{\varphi(G)}$ è evidentemente $K \cap \varphi(G)$, quindi la sua cardinalità non è divisibile per p. In particolare, $K' \neq \varphi(G)$, e dunque $\varphi|_{\varphi(G)}$ non è l'omomorfismo banale, ossia φ^2 non è l'omomorfismo banale.

(b) Abbiamo $|\varphi(G)| = |G|/|K|$ e $|\varphi^2(G)| = |\varphi(G)|/|\varphi(G) \cap K|$, pertanto

$$|\varphi^2(G)| = |G|/(|K| \cdot |\varphi(G) \cap K|)\,.$$

Poiché evidentemente $|\varphi(G) \cap K|$ è un divisore di $|K|$, il nucleo di φ^2 ha ordine divisore di $|K|^2$, Ma poiché φ^2 è l'omomorfismo banale, ne segue che necessariamente $p^3q^4 \mid |K|^2$, da cui $p^2q^2 \mid |K|$. D'altra parte, questa condizione è anche sufficiente per verificare la richiesta. Si prenda per esempio $G = \mathbb{Z}/p^3q^4\mathbb{Z}$ e, per ogni coppia (a, b) di esponenti tali che $a, b \geq 2$, l'omomorfismo definito da $x \mapsto p^aq^bx$. È ovvio che $|K| = p^aq^b$ e che $\varphi^2(x) = p^{2a}q^{2b}x$ è l'omomorfismo banale.

4. Siano $\alpha = \sqrt{2} + \sqrt[4]{2}$ e $\beta = -\sqrt{2} + i\sqrt[4]{2}$, dove $\sqrt[4]{2} \in \mathbb{R}$ indica l'usuale radice quarta positiva di 2 e $i \in \mathbb{C}$ soddisfa $i^2 = -1$.

(a) Determinare i polinomi minimi $f(x)$ e $g(x)$ di α e di β su $\mathbb{Q}$.

(b) Sia L il campo di spezzamento su $\mathbb{Q}$ di $f(x)$. Determinare il grado $[L : \mathbb{Q}]$.

SOLUZIONE:

(a) Si ha $(\alpha - \sqrt{2})^2 = \sqrt{2}$, da cui ricaviamo $\alpha^2 - 2\sqrt{2}\alpha + 2 = \sqrt{2}$ e quindi $\alpha^2 + 2 = \sqrt{2}(1 + 2\alpha)$; elevando ancora una volta al quadrato otteniamo $\alpha^4 + 4\alpha^2 + 4 = 2(1 + 4\alpha + 4\alpha^2)$, ovvero $\alpha^4 - 4\alpha^2 - 8\alpha + 2 = 0$, per cui il polinomio $h(x) = x^4 - 4x^2 - 8x + 2$ si annulla per $x = \alpha$. D'altro canto $h(x)$ è irriducibile per il criterio di Eisenstein applicato con il primo 2, per cui il polinomio minimo di α è $h(x)$.

Procediamo similmente con β: si ha $(\beta+\sqrt{2})^2 = -\sqrt{2} \Rightarrow \beta^2+2 = -\sqrt{2}(1+2\beta)$. Questa relazione differisce soltanto per un segno dall'analoga relazione trovata per α, per cui elevando al quadrato otteniamo esattamente come prima $\beta^4 - 4\beta^2 - 8\beta + 2 = 0$, e $h(x)$ è il polinomio minimo anche di β.

(b) Dimostriamo che $[L : \mathbb{Q}] = 8$. Conosciamo già due radici di $f(x) = h(x)$, ovvero α e β. D'altro canto, sappiamo anche che le radici di un polinomio a coefficienti reali compaiono a coppie complesse coniugate, quindi anche $\overline{\beta} = -\sqrt{2} - i\sqrt[4]{2}$ è radice di $f(x)$. Il campo di spezzamento di un polinomio di grado 4 si ottiene aggiungendo al campo base tre qualsiasi delle sue radici, quindi

$$L = \mathbb{Q}(\alpha, \beta, \overline{\beta}) = \mathbb{Q}(\sqrt{2} + \sqrt[4]{2}, -\sqrt{2} + i\sqrt[4]{2}, -\sqrt{2} - i\sqrt[4]{2})$$

Osserviamo poi che un'estensione di $\mathbb{Q}$ contiene β e $\overline{\beta}$ se e solo se contiene $\beta + \overline{\beta} = -2\sqrt{2}$ e $\beta - \overline{\beta} = 2i\sqrt[4]{2}$ (infatti $2\beta = (\beta + \overline{\beta}) + (\beta - \overline{\beta})$, e una simile identità vale per $\overline{\beta}$), quindi

$$\begin{aligned}
L &= \mathbb{Q}\left(\sqrt{2} + \sqrt[4]{2}, -2\sqrt{2}, 2i\sqrt[4]{2}\right) \\
&= \mathbb{Q}\left(\sqrt{2}, \sqrt{2} + \sqrt[4]{2}, 2i\sqrt[4]{2}\right) && (1) \\
&= \mathbb{Q}\left(\sqrt{2}, \sqrt[4]{2}, i\sqrt[4]{2}\right) && (2) \\
&= \mathbb{Q}\left(\sqrt{2}, \sqrt[4]{2}, i\right) && (3) \\
&= \mathbb{Q}\left(\sqrt[4]{2}, i\right) && (4)
\end{aligned}$$

Qui l'uguaglianza (1) segue dal fatto che un'estensione di $\mathbb{Q}$ contiene $-2\sqrt{2}$ se e solo se contiene $\sqrt{2}$; l'uguaglianza (2) segue dal fatto che un'estensione di $\mathbb{Q}$ contiene $\sqrt{2} + \sqrt[4]{2}$ e $\sqrt{2}$ se e solo se contiene $\sqrt{2}$ e $(\sqrt{2} + \sqrt[4]{2}) - \sqrt{2} = \sqrt[4]{2}$, l'uguaglianza (3) segue similmente dal fatto che i è il rapporto fra $i\sqrt[4]{2}$ e $\sqrt[4]{2}$, e infine (4) segue dal fatto che un campo che contiene $\sqrt[4]{2}$ contiene anche $\sqrt{2} = (\sqrt[4]{2})^2$. Ne segue che L è il composto delle estensioni $\mathbb{Q}(\sqrt[4]{2})$ (di grado 4: il polinomio minimo di $\sqrt[4]{2}$ è $x^4 - 2$, irriducibile per il criterio di Eisenstein) e $\mathbb{Q}(i)$ (di grado 2): il grado $[L : \mathbb{Q}]$ è quindi 4 oppure 8. D'altro canto, se si avesse $[L : \mathbb{Q}] = 4$ si avrebbe $L = \mathbb{Q}(\sqrt[4]{2})$, ma questo è assurdo, perché $\mathbb{Q}(\sqrt[4]{2})$ è contenuto in $\mathbb{R}$ mentre $\mathbb{Q}(i) \subseteq L$ non lo è. Ne segue che $[L : \mathbb{Q}] = 8$.