COMPITO DI ARITMETICA
11 giugno 2018
Soluzioni

1. (a) Determinare il numero di soluzioni (terne ordinate) in $\mathbb{Z}/37\mathbb{Z}$ dell'equazione $x + y + z = \bar{0}$.

(b) Determinare il numero di sottoinsiemi di 3 elementi $\{x, y, z\}$ di $\mathbb{Z}/37\mathbb{Z}$ tali che $x + y + z = \bar{0}$.

SOLUZIONE: (a) Comunque si scelga una coppia ordinata (x, y) in $(\mathbb{Z}/37\mathbb{Z})^2$ esiste uno e un solo z che risolve l'equazione. Dunque il numero di soluzioni corrisponde al numero di scelte delle coppie ordinate, ossia, $37^2 = 1369$.

(b) Dalle soluzioni precedenti si devono intanto scartare quelle che hanno almeno due coordinate uguali. Si possono avere i seguenti casi:

(a) $x = y$, $z = -2x$;

(b) $x = z$, $y = -2x$;

(c) $y = z$, $x = -2y$.

I tre casi sono mutualmente esclusivi, eccetto quando $x = y = z = \bar{0}$. Quindi si hanno $3 \times 36 + 1 = 109$ possibilità di almeno due coordinate uguali. Restano $1369 - 109 = 1260$ casi di 3 coordinate distinte. Siccome un insieme non dipende dall'ordine in cui si scrivono i suoi elementi, e un insieme di 3 elementi si può scrivere ordinando i suoi elementi in $3! = 6$ modi distinti, i sottoinsiemi cercati sono $1260/6 = 210$.

2. Determinare per quali numeri primi $p > 2$ il seguente sistema ammette soluzione:

$$\begin{cases} 17^a \equiv 2^a \pmod{p} \\ 5a \equiv 1 \pmod{p-1} \end{cases}$$

SOLUZIONE: Supponiamo che esista una soluzione a del sistema proposto. Siccome $p \neq 2$ possiamo riscrivere la prima congruenza come $(17 \cdot 2^{-1})^a \equiv 1 \pmod{p}$, il che implica che, detto k l'ordine di $17 \cdot 2^{-1}$ modulo p, si ha $k \mid a$. D'altro canto, la seconda congruenza è risolubile solo se $(a, p-1) = 1$: in effetti, se $d > 1$ è un divisore comune fra a e $p - 1$, riducendo la congruenza modulo d si trova $0 \equiv 1 \pmod{d}$, il che è chiaramente assurdo. Ricordando che k è sempre un divisore di $\varphi(p) = p-1$, otteniamo che k divide sia a che $p-1$, e siccome $(a, p-1) = 1$ deduciamo che $k = 1$. Ne segue $17 \cdot 2^{-1} \equiv 1 \pmod{p}$, da cui $17 \equiv 2 \pmod{p} \Rightarrow 15 \equiv 0$

(mod p) $\Rightarrow p \in \{3, 5\}$. Per $p = 3$ e $p = 5$ è immediato verificare che $a = 1$ è una soluzione, dunque il sistema proposto ha soluzione se e solo se $p = 3$ o $p = 5$.

SECONDA SOLUZIONE: La seconda congruenza implica che a e $p - 1$ sono primi fra loro. Come noto, questo implica a sua volta che la funzione $f(x) : x \mapsto x^a$ sia iniettiva modulo p: la prima congruenza, che è $f(17) \equiv f(2) \pmod{p}$, fornisce allora $17 \equiv 2 \pmod{p}$, da cui $p = 3$ o 5. Come sopra è facile vedere che per questi valori di p il sistema ammette soluzione.

3. Sia G un gruppo finito e α un automorfismo di G con la proprietà che $\alpha(x) = x$ se e soltanto se x è l'elemento neutro e di G.

(a) Mostrare che per ogni $g \in G$ esiste $x \in G$ tale che $g = x^{-1}\alpha(x)$.

(b) Dimostrare che se inoltre vale anche $\alpha(\alpha(x)) = x$ per ogni $x \in G$, allora si ha $\alpha(g) = g^{-1}$ per ogni g in G.

SOLUZIONE: (a) La richiesta è quella di dimostrare che la funzione

$$\begin{array}{rccc} f: & G & \to & G \\ & x & \mapsto & x^{-1}\alpha(x) \end{array}$$

è surgettiva. Dal momento che G è un insieme finito, f è surgettiva se e solo se è iniettiva: ma d'altro canto $f(x) = f(y)$ è equivalente a $x^{-1}\alpha(x) = y^{-1}\alpha(y)$, il che accade se e solo se $yx^{-1} = \alpha(y)\alpha(x^{-1})$. Usando il fatto che α è un automorfismo, questa uguaglianza si riscrive come $yx^{-1} = \alpha(yx^{-1})$, il che per ipotesi significa $yx^{-1} = e \Rightarrow x = y$. Dunque f è iniettiva come voluto, e quindi surgettiva.

(b) Sia g un qualunque elemento di G. Dal punto precedente sappiamo che possiamo scrivere $g = x^{-1}\alpha(x)$ per qualche $x \in G$, e otteniamo quindi

$$\alpha(g) = \alpha\left(x^{-1}\right)\alpha(\alpha(x)) = \alpha(x)^{-1}x = \left(x^{-1}\alpha(x)\right)^{-1} = g^{-1}.$$

4. Sia m un numero intero.

(a) Determinare un polinomio a coefficienti interi che abbia le quattro radici $\pm\sqrt{m} \pm \sqrt{3}$.

(b) Sia $\alpha = \sqrt{m} + \sqrt{3}$. Determinare, in funzione di m, il grado $[\mathbb{Q}(\alpha) : \mathbb{Q}]$.

(c) Per ogni numero primo p, denotiamo ancora con $\sqrt{m}$ e $\sqrt{3}$, rispettivamente, delle radici dei polinomi $x^2 - m$ e $x^2 - 3$ in un'estensione di $\mathbb{F}_p$. Determinare tutti i possibili gradi $[\mathbb{F}_p(\sqrt{m} + \sqrt{3}) : \mathbb{F}_p]$.

SOLUZIONE (a) Il polinomio $f(x) = (x - \sqrt{m} - \sqrt{3})(x - \sqrt{m} + \sqrt{3})(x + \sqrt{m} - \sqrt{3})(x + \sqrt{m} + \sqrt{3}) = x^4 - (2m + 6)x^2 + (m - 3)^2$ soddisfa le condizioni richieste.

(b) Il campo $\mathbb{Q}(\sqrt{3})$ è uno spazio vettoriale su $\mathbb{Q}$ di dimensione 2, con base $\{1, \sqrt{3}\}$. Pertanto il polinomio $f(x)$ può avere radici razionali soltanto se $\sqrt{m} = \sqrt{3}$, ossia soltanto se $m = 3$. In questo caso $\alpha = 2\sqrt{3}$ ha grado 2 su $\mathbb{Q}$.

Se $m \neq 3$ possiamo vedere se il polinomio $f(x)$, che è multiplo del polinomio minimo di α, si fattorizza come prodotto di due polinomi di grado 2. Provando tutte le possibili combinazioni del fattore $x - \sqrt{m} - \sqrt{3}$ con un altro fattore, si ottiene:

(i) $(x - \sqrt{m} - \sqrt{3})(x - \sqrt{m} + \sqrt{3}) = x^2 - 2\sqrt{m}x + m - 3$;

(ii) $(x - \sqrt{m} - \sqrt{3})(x + \sqrt{m} - \sqrt{3}) = x^2 - 2\sqrt{3}x + 3 - m$;

(iii) $(x - \sqrt{m} - \sqrt{3})(x + \sqrt{m} + \sqrt{3}) = x^2 - (\sqrt{m} + \sqrt{3})^2 = x^2 - (m + 3) - 2\sqrt{3m}$.

Nel caso (i) si ottiene un polinomio a coefficienti razionali se e solo se m è il quadrato di un numero intero; nel caso (ii) il polinomio non è mai a coefficienti razionali; nel caso (iii) il polinomio è a coefficienti razionali se e solo se $3m$ è il quadrato di un numero intero. In conclusione, il grado cercato è uguale a 2 se m è della forma k^2 oppure $3k^2$, mentre negli altri casi è uguale a 4.

(c) In ogni caso sia $\sqrt{m}$ che $\sqrt{3}$ appartengono ad un'estensione di $\mathbb{F}_p$ di grado al più 2. Siccome esiste un'unica estensione di $\mathbb{F}_p$ di grado 2, allora anche la lora somma appartiene ad un'estensione di $\mathbb{F}_p$ di grado al più 2.

Facciamo vedere che sono possibili sia il caso di grado 1 che il caso di grado 2. Per il caso di grado 1, basta prendere $p = m = 3$. Per il caso di grado 2, basta prendere $p = 5$ e $m = 3$.