COMPITO DI ARITMETICA
12 febbraio 2018
Soluzioni

1. Siano n un intero positivo maggiore di 1 e $X = \{1, \dots, n\}$.

(a) Determinare il numero delle funzioni $f\colon X \to X$ tali che l'immagine di f abbia esattamente 2 elementi.

(b) Determinare il numero delle funzioni $f\colon X \to X$ tali che l'immagine di $f \circ f$ contenga esattamente $n-1$ elementi.

SOLUZIONE : (a) Le possibili scelte dei due elementi che possono costituire l'immagine di X sono tutti i sottoinsiemi di 2 elementi di X, e quindi il loro numero è uguale a $\binom{n}{2}$. Per ciascuno di questi sottoinsiemi, diciamo $Y = \{a, b\}$, ci devono essere $1 \leq k \leq n$ elementi di X la cui immagine è a e i restanti $n-k$ elementi la cui immagine è b. Pertanto il numero di funzioni possibili è uguale a

$$\binom{n}{2} \cdot \sum_{k=1}^{n-1} \binom{n}{k} = \binom{n}{2} \cdot (2^n - 2).$$

(b) I possibili sottoinsiemi Y di X che possono costituire l'immagine di f sono tutti i sottoinsiemi di $n-1$ elementi di un insieme di n elementi, e quindi il loro numero è uguale a $\binom{n}{n-1} = n$. Poiché f non può essere surgettiva (altrimenti lo sarebbe anche $f \circ f$), ed in generale $\mathrm{Im}(f) \supseteq \mathrm{Im}(f \circ f)$, necessariamente $\mathrm{Im}(f) = \mathrm{Im}(f \circ f) = Y$. Sia x l'elemento di X che non appartiene a Y; allora per $f(x)$ ci sono $n-1$ possibilità. Poiché però $f(f(X)) = f(Y) = Y$, f deve permutare fra loro gli elementi di Y: ci sono quindi $(n-1)!$ possibilità. In totale, il numero delle funzioni cercate è quindi

$$n \cdot (n-1) \cdot (n-1)! = (n-1) \cdot n!.$$

2. Determinare per quali valori del parametro $a \in \mathbb{N}$ il seguente sistema ammette soluzione:

$$(S) : \begin{cases} x^2 \equiv 2^a \pmod{13^5} \\ x^a + a^3 + a \equiv 5 \pmod 8 \end{cases}$$

SOLUZIONE: Dimostriamo che la prima equazione del sistema ha soluzione se e solo se a è pari. In effetti, se $a = 2b$ è pari allora è sufficiente prendere $x \equiv 2^b \pmod{13^5}$; reciprocamente, se l'equazione $x^2 \equiv 2^a \pmod{13^5}$ ha soluzione, dimostreremo che a deve necessariamente essere pari. Se esiste un x intero che verifica $x^2 \equiv 2^a$

(mod 13^5), allora anche l'equazione $x^2 \equiv 2^a \pmod{13}$ ha soluzione; siccome 2 è un generatore modulo 13, possiamo scrivere $x \equiv 2^k \pmod{13}$ per un certo k intero. La congruenza diventa allora $2^{2k} \equiv 2^a \pmod{13}$, ovvero $2^{2k-a} \equiv 1 \pmod{13}$. Dal momento che l'ordine di 2 modulo 13 è 12, questo implica $12 \mid (2k-a)$, e quindi in particolare $2 \mid (2k-a) \Rightarrow a$ pari. Studiamo ora la seconda equazione del sistema sapendo che a è pari. Riducendo modulo 2 troviamo $x^a \equiv 1 \pmod{2}$, il che implica che x è dispari. Siccome a è pari, x è dispari, e i quadrati dei numeri dispari sono congrui ad 1 (mod 8), la seconda equazione del sistema diventa semplicemente $1 + a \equiv 5 \pmod{8}$, ovvero $a \equiv 4 \pmod{8}$. Sotto questa condizione necessaria, il sistema ammette sicuramente soluzione: in effetti, scrivendo $a = 8m + 4$, è immediato vedere che ogni soluzione del sistema $(S') : \begin{cases} x \equiv 2^{4m+2} \pmod{13^5} \\ x \equiv 1 \pmod{8} \end{cases}$ è anche soluzione del sistema (S); d'altro canto, la risolubilità di (S') è una conseguenza immediata del teorema cinese del resto. Gli a cercati sono dunque tutti e soli gli interi positivi congrui a 4 modulo 8.

3. Siano G un gruppo abeliano di cardinalità $2^a \cdot 3^b$, denotato additivamente, dove a e b sono numeri naturali positivi. Siano inoltre G_2, G_3 i sottogruppi di G definiti da

$$G_2 = \{x \in G \mid 2^a x = 0\}, \qquad G_3 = \{x \in G \mid 3^b x = 0\}.$$

(a) Dimostrare che $G \cong G_2 \times G_3$.

(b) Dimostrare che, se G_2 può essere generato da h elementi e G_3 può essere generato da k elementi, allora G può essere generato da $M = \max\{h, k\}$ elementi.

SOLUZIONE: (a) Definiamo una funzione $\varphi : G_2 \times G_3 \to G$ nel modo seguente:

$$\varphi(x, y) = x + y.$$

Si verifica immediatamente che φ è un omomorfismo: infatti $\varphi((x,y) + (x',y')) = \varphi(x+x', y+y') = x+x'+y+y' = x+x'+y+y' = (x+y)+(x'+y') = \varphi(x,y)+\varphi(x',y')$ per ogni $x, x' \in G_2$ e per ogni $y, y' \in G_3$.

Inoltre φ è iniettivo: se $x+y \in \ker\varphi$, allora $x+y = 0$, $x = -y$ e, siccome i gruppi G_2 e G_3 hanno cardinalità relativamente prime, e quindi la loro intersezione è uguale a $\{0\}$, si ha $x = y = 0$.

Per quanto riguarda la surgettività, osserviamo che, per il teorema di Cauchy, $|G_2| = 2^{a'}$, $|G_3| = 3^{b'}$, dove necessariamente $a' \leq a$ e $b' \leq b$ (teorema di Lagrange). D'altra parte, G/G_2 non ha elementi di ordine 2. Infatti, se x fosse un rappresentante in G di una classe $\bar{x} \in G/G_2$ di ordine 2, allora avremmo $2x \in G_2$, da cui $2^{a+1}x = 0$, ed in definitiva, siccome l'ordine di un elemento deve dividere l'ordine del gruppo,

$2^a x = 0$, cioè $x \in G_2$, contraddizione. Quindi, sempre per il teorema di Cauchy e per il teorema di Lagrange, $|G/G_2| = 3^{b''}$, con $b'' \leq b$. Ricordando che

$$2^a \cdot 3^b = |G| = |G_2| \cdot |G/G_2| = 2^{a'} \cdot 3^{b''}$$

si ottiene in particolare che $a' = a$ e, ragionando in maniera simmetrica, che $b' = b$. Dunque $G_2 \times G_3$ ha la stessa cardinalità di G. Poiché una funzione iniettiva tra due insiemi della stessa cardinalità è necessariamente surgettiva, ne segue che φ è surgettivo, e quindi è un isomorfismo.

Alternativamente, per dimostrare la surgettività di φ si potrebbe ragionare come segue. Poiché 2^a e 3^b sono primi fra loro, esistono degli interi s, t tali che $s3^b + t2^a = 1$. Dato comunque $g \in G$, si può quindi scrivere $g = s3^b g + t2^a g$. Ora, chiaramente, $s3^b g \in G_2$ e $t2^a g \in G_3$, in quanto ogni elemento moltiplicato per l'ordine del gruppo fa 0. Quindi $g = \varphi(s3^b g, t2^a g)$.

(b) Siano $\{x_i, \ldots, x_h\}$ e $\{y_1, \ldots, y_k\}$, rispettivamente, insiemi di generatori di G_2 e G_3. Supponiamo, senza perdita di generalità, che $h \geq k$, cioè $M = h$, e poniamo $y_{k+1} = \cdots = y_h = 0$, $z_1 = x_1 + y_1, \ldots, z_M = x_M + y_M$. Allora, per ogni $i = 1, \ldots, M$, $3^b(x_i + y_i) = 3^b x_i$ è un multiplo di x_i con coefficiente primo con 2, e quindi genera lo stesso sottogruppo di x_i. Analogamente, $2^a x_i y_i = 2^a y_i$ è un multiplo di y_i con coeffciente primo con 3, e quindi genera lo stesso sottogruppo di y_i. Ne segue che il sottogruppo generato da $x_1 + y_1, \ldots, x_M + y_M$ contiene $x_1, \ldots x_M, y_1, \ldots, y_M$, e quindi è uguale a G.

4. Consideriamo il polinomio $f(x) = x^6 - x^3 - 1 \in \mathbb{F}_3[x]$.

(a) Determinare il grado del campo di spezzamento L di $f(x)$ su $\mathbb{F}_3$.

(b) Detta $\alpha \in L$ una radice di $f(x)$, determinare, al variare di k fra gli interi positivi, il grado dell'estensione $[\mathbb{F}_3(\alpha^k) : \mathbb{F}_3]$.

Soluzione:

(a) Osservando che tutti gli esponenti dei monomi che appaiono in $f(x)$ sono multipli di 3 otteniamo facilmente che $f(x) = (x^2 - x - 1)^3$. Il campo di spezzamento di $f(x)$ su $\mathbb{F}_3$ coincide allora con il campo di spezzamento di $g(x) = x^2 - x - 1$, che è irriducibile dal momento che non ha radici in $\mathbb{F}_3$. Ne segue che il campo di spezzamento di $f(x)$ su $\mathbb{F}_3$ è $\mathbb{F}_{3^2}$.

(b) Dato che $\alpha \neq 0$ è un elemento di $L \cong \mathbb{F}_9$ sappiamo che $\alpha^8 = 1$. Studiamo le potenze di α: dal momento che $\alpha^2 - \alpha - 1 = 0$ (visto che α è radice di $g(x)$) si ha $\alpha^2 = \alpha + 1$, $\alpha^3 = \alpha(\alpha + 1) = \alpha^2 + \alpha = 2\alpha + 1$, $\alpha^4 = \alpha(2\alpha + 1) = 2(\alpha + 1) + \alpha = 2$. Segue immediatamente che $\alpha^5 = 2\alpha$, $\alpha^6 = 2\alpha + 2$ e $\alpha^7 = \alpha + 2$. Ora osserviamo che ognuno degli elementi $\alpha + 1$, $\alpha + 2$, 2α, $2\alpha + 1$ e $2\alpha + 2$ genera $\mathbb{F}_9$ su $\mathbb{F}_3$, perché

per ogni scelta di $r \in \mathbb{F}_3^\times, s \in \mathbb{F}_3$ si ha $\mathbb{F}_3(r\alpha + s) = \mathbb{F}_3(r\alpha) = \mathbb{F}_3(\alpha) = \mathbb{F}_9$. Combinando quanto appena dimostrato con il fatto che $\alpha^4 = 2 \in \mathbb{F}_3$ e con l'osservazione che le potenze di α sono periodiche di periodo 8 si deduce che

$$\mathbb{F}_3(\alpha^k) = \begin{cases} \mathbb{F}_9, \text{ se } k \not\equiv 0 \pmod 4 \\ \mathbb{F}_3, \text{ se } k \equiv 0 \pmod 4 \end{cases}$$