COMPITO DI ARITMETICA
15 gennaio 2018
Soluzioni

1. Sia $a_0, a_1, \ldots, a_n \ldots$ la successione definita da

$$\begin{cases} a_0 = 0 \\ a_1 = 1 \\ a_{n+1} = 3a_n - a_{n-1} \text{ per } n \geq 1\,. \end{cases}$$

(a) Determinare una formula esplicita per la successione $a_0, a_2, a_4, \ldots, a_{2n}, \ldots$ e determinare dei coefficienti r, s per i quali $a_{2n+2} = ra_{2n} + sa_{2n-2}$.

(b) Dimostrare che per ogni numero primo p esistono un intero $k > 0$ ed un intero n_0 tali che per cui $a_{n+k} \equiv a_n \pmod{p}$ per ogni $n \geq n_0$.

Soluzione : (a) Siano α, β le due radici del polinomio $X^2 - 3X + 1$, ossia

$$\alpha, \beta = \frac{3 \pm \sqrt{5}}{2}\,.$$

Allora si dimostra facilmente per induzione che $a_n = A\alpha^n + B\beta^n$ per opportuni coefficienti A, B. Infatti, se (A, B) è la soluzione del sistema

$$\begin{cases} A + B = 0 \\ A\alpha + B\beta = 1 \end{cases}$$

e cioè $A = \frac{1}{\sqrt{5}}$, $B = -\frac{1}{\sqrt{5}}$, si ottiene la validità della formula per i casi iniziali a_0 e a_1.

Per quanto riguarda il passo induttivo, osserviamo che da, $a^2 = 3\alpha - 1$ e $\beta^2 = 3\beta - 1$ segue che $\alpha^{n+1} = 3\alpha^n - \alpha^{n-1}$ e $\beta^{n+1} = 3\beta^n - \beta^{n-1}$ per ogni $n \geq 1$, e quindi

$$a_{n+1} = 3a_n - a_{n-1} = \frac{1}{\sqrt{5}}(3\alpha^n - 3\beta^n - \alpha^{n-1} + \beta^{n-1}) = \frac{1}{\sqrt{5}}(\alpha^{n+1} - \beta^{n+1})\,.$$

Una formula esplicita per a_{2n} è dunque

$$a_{2n} = \frac{1}{\sqrt{5}}(\alpha^{2n} - \beta^{2n}) = \frac{1}{\sqrt{5}}[(\alpha^2)^n - (\beta^2)^n].$$

Infine osserviamo che $\alpha^2, \beta^2 = \frac{7 \pm 3\sqrt{5}}{2}$ sono le radici del polinomio $X^2 - 7X + 1$ e quindi, ragionando come nel caso precedente,

$$a_{2n+2} = 7a_{2n} - a_{2n-2} \quad \text{per } n \geq 1\,.$$

(b) Dato un primo p, consideriamo la coppia di classi di resto $(\overline{a_n}, \overline{a_{n+1}})$ modulo p per ogni $n = 0, 1, 2, \ldots$. Poiché le classi di resto sono in numero finito, esisteranno due indici distinti, n_0 ed m_0, tali che $(\overline{a_{n_0}}, \overline{a_{n_0+1}}) = (\overline{a_{m_0}}, \overline{a_{m_0+1}})$. Senza perdita di generalità, possimo supporre $m_0 > n_0$, $m_0 = n_0 + k$ con $k > 0$.

Dimostriamo ora per induzione su j che per ogni indice $i = n_0 + j$, con $j \geq 0$, vale $a_{i+k} = a_i \pmod{p}$. Per ipotesi, la tesi è vera per $j = 0, 1$. Per quanto riguarda il passo induttivo, supponiamo la tesi vera per $j \leq h$, e dimostriamola per $j = h + 1$.

Abbiamo $a_{n_0+k+j+1} = 3a_{n_0+k+j} + a_{n_0+k+j-1} \equiv 3a_{n_0+j} + a_{n_0+j-1} \equiv a_{n_0+j+1} \pmod{p}$, e quindi la tesi è dimostrata.

2. (a) Per ogni numero primo $p > 2$ sia $S(p)$ l'insieme degli interi n che soddisfano la congruenza $n \cdot 2^n \equiv 1 \pmod{p}$. Dimostrare che se a è un elemento di $S(p)$ e $b \equiv a \pmod{p(p-1)}$, allora $b \in S(p)$.

(b) Determinare il numero di soluzioni del sistema $S : \begin{cases} n \cdot 2^n \equiv 1 \pmod{31} \\ 1 \leq n \leq 930 \end{cases}$

SOLUZIONE: (a) Siano a, b due interi tali che $a \equiv b \pmod{p(p-1)}$. Questa congruenza implica $a \equiv b \pmod{p-1}$ che, in virtù del piccolo teorema di Fermat, implica a sua volta $2^a \equiv 2^b \pmod{p}$; inoltre, si ha certamente $a \equiv b \pmod{p}$. Moltiplicando fra loro le due congruenze appena trovate otteniamo allora $a \cdot 2^a \equiv b \cdot 2^b \pmod{p}$; in particolare, se a appartiene ad $S(p)$ allora anche b appartiene ad $S(p)$ (e, simmetricamente, è vero anche il viceversa).

(b) Per ogni intero $t \in T = \{0, 1, \ldots, 29\}$, consideriamo il sistema

$$S_t : \begin{cases} n \cdot 2^n \equiv 1 \pmod{31} \\ n \equiv t \pmod{30} \\ 1 \leq n \leq 930 = 31 \cdot 30 \end{cases} .$$

Per il piccolo teorema di Fermat abbiamo $2^n \equiv 2^t \pmod{31}$; inoltre, 2^t è invertibile modulo 31, con inverso 2^{-t}. Ne segue che S_t è equivalente al sistema

$$\begin{cases} n \equiv 2^{-t} \pmod{31} \\ n \equiv t \pmod{30} \\ 1 \leq n \leq 31 \cdot 30 \end{cases} .$$

Per ogni $t \in T$, per il teorema cinese del resto, il sottosistema formato dalle due congruenze ammette una e una sola soluzione modulo $31 \cdot 30$, dunque (dal momento che ci interessiamo solo agli interi nell'intervallo $[1, 31 \cdot 30]$, che realizzano una ed una sola volta ogni resto modulo $31 \cdot 30$) il sistema S_t ha un'unica soluzione. Notando poi che l'insieme delle soluzioni del sistema S del testo è dato dall'unione degli

insiemi delle soluzioni dei sistemi S_t per $t \in T$, otteniamo che il sistema proposto ha esattamente 30 soluzioni.

3. (a) Siano G un gruppo e H, K due sottogruppi normali di G. Supponiamo che $H \cap K = \{e\}$: dimostrare che per ogni $h \in H$ e ogni $k \in K$ si ha $hkh^{-1}k^{-1} = e$.

(b) Sia p un numero primo. Determinare tutti i gruppi finiti G con la seguente proprietà: ogni elemento di G (tranne l'identità) ha ordine p, e per ogni $g \in G \setminus \{e\}$ si ha che $\langle g \rangle$ è normale in G, con $G/\langle g \rangle \cong \mathbb{Z}/p\mathbb{Z}$.

SOLUZIONE: (a) Data la normalità di H e K in G, esistono $k_1 \in K$ e $h_1 \in H$ tali che $hkh^{-1} = k_1$ e $kh^{-1}k^{-1} = h_1$. Ne segue che $hkh^{-1}k^{-1}$ è uguale sia a k_1k^{-1} (che è un elemento di K, in quanto prodotto di elementi di K), sia a hh_1 (che è un elemento di H, in quanto prodotto di elementi di H). Ne segue che $hkh^{-1}k^{-1} \in H \cap K = \{e\}$, dunque che $hkh^{-1}k^{-1} = e$ come voluto.

(b) Sia $g_1 \neq e$ un elemento di G; poniamo $H_1 = \langle g_1 \rangle$. Le ipotesi ci dicono che $|H_1| = p$ e $G/H_1 \cong \mathbb{Z}/p\mathbb{Z}$, da cui $|G| = |H_1| \cdot |\mathbb{Z}/p\mathbb{Z}| = p^2$. In particolare, $H_1 \neq G$; siano g_2 un elemento di $G \setminus H_1$ e $H_2 = \langle g_2 \rangle$. L'intersezione $H_1 \cap H_2$ è un sottogruppo di H_1, dunque ha cardinalità 1 o p; se avesse cardinalità p, si avrebbe $H_1 \cap H_2 = H_1 = H_2$, da cui $g_2 \in H_1$, il che contraddice la nostra scelta di g_2. Ne segue che $H_1 \cap H_2 = \{e\}$. Osserviamo infine che l'omomorfismo

$$\begin{array}{ccc} G & \to & G/H_1 \times G/H_2 \\ x & \mapsto & (xH_1, xH_2) \end{array}$$

dato dal prodotto delle proiezioni canoniche ha come nucleo $\{x \in G : xH_1 = H_1, xH_2 = H_2\} = \{x \in G : x \in H_1, x \in H_2\} = H_1 \cap H_2 = \{e\}$, ed è dunque iniettivo. Esso è inoltre surgettivo visto che $|G| = p^2 = |G/H_1| \cdot |G/H_2|$. Esso è quindi un isomorfismo, perciò $G \cong G/H_1 \times G/H_2 \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

4. (a) Sia n un numero naturale. Determinare, al variare di k fra i numeri interi positivi, il grado $[\mathbb{Q}(\sqrt[n]{2^k}) : \mathbb{Q}]$.

(b) Dimostrare che, per ogni numero primo p, il grado d del campo di spezzamento di spezzamento di $f(X) = X^4 - 2$ sul campo $\mathbb{F}_p$ è un divisore di 4.

(c) Per ogni divisore d di 4, dare un esempio di un numero primo p per cui il grado del campo di spezzamento è uguale a d.

SOLUZIONE: (a) Siano $\alpha = \sqrt[n]{2}$ e $\beta_k = \sqrt[n]{2^k}$. Abbiamo $[\mathbb{Q}(\alpha) : \mathbb{Q}] = n$, poiché α è radice del polinomio $X^n - 2 \in \mathbb{Q}[X]$, irriducibile per il criterio di Eisenstein, e dunque $X^n - 2$ è il polinomio minimo di α su $\mathbb{Q}$.

Sia ora $d = (k, n)$. Allora $d|k$, $k = k_1 d$ per qualche intero k_1, e dunque $\beta_k^{\frac{n}{d}} = \sqrt[n]{2^{k_1 n}} = 2^{k_1} \in \mathbb{Q}$, quindi β_k è una radice del polinomio $X^{\frac{n}{d}} - 2^{k_1} \in \mathbb{Q}[X]$, da cui $[\mathbb{Q}(\beta_k) : \mathbb{Q}] \leq \frac{n}{d}$.

D'altra parte, osserviamo che $(k_1, \frac{n}{d}) = 1$, e quindi esistono interi r, s tali che $rk_1 + s\frac{n}{d} = 1$. Ora, $\alpha^d = \alpha^{d(rk_1+s\frac{n}{d})} = {\beta_k}^r \cdot 2^s$, quindi α è radice del polinomio $X^d - \beta_k^r \cdot 2^s \in \mathbb{Q}(\beta_k)[X]$, da cui $[\mathbb{Q}(\alpha) : \mathbb{Q}(\beta_k)] \leq d$.

Dalla formula delle torri, abbiamo l'uguaglianza

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\alpha) : \mathbb{Q}(\beta_k)] \cdot [\mathbb{Q}(\beta_k) : \mathbb{Q}] = n\,,$$

per cui necessariamente

$$[\mathbb{Q}(\beta_k) : \mathbb{Q}] = \frac{n}{d} \quad \text{e} \quad [\mathbb{Q}(\alpha) : \mathbb{Q}(\beta_k)] = d\,.$$

(b) Per $p = 2$, la fattorizzazione del polinomio $X^4 - 2$ è semplicemente X^4. Per $p \neq 2$, la fattorizzazione del polinomio $X^4 - 2$ in $\mathbb{F}_p[X]$ non può essere del tipo $X^4 - 2 = g_1(x)g_3(X)$ dove g_1 è un polinomio di primo grado e g_3 è un polinomio di terzo grado. Infatti, l'esistenza di un fattore di primo grado implica, per il teorema di Ruffini, l'esistenza di una radice α. Ma allora ci sarebbe anche la radice $-\alpha$, diversa dalla radice α, e quindi il polinomio sarebbe divisibile sia per $X - \alpha$ che per $X + \alpha$.

Ne segue che i gradi dei fattori irriducibili di $f(X)$ possono essere solo 1, 2 o 4, e quindi il loro comune multiplo, che è il grado del campo di spezzamento, può essere solo 1, 2 o 4.

(c)

(i) Per $p = 2$ abbiamo $f(X) = X^4$, quindi il grado del campo di spezzamento è uguale a 1.

(ii) Per $p = 7$ abbiamo $f(X) = (X^2 - 3)(X^2 + 3) = (X^2 - 3)(X + 2)(X - 2)$; siccome $X^2 - 3$ è irriducibile in $\mathbb{F}_7[X]$ (in questo caso basta controllare che non ci siano radici), il grado del campo di spezzamento è uguale a 2.

(iii) Per $p = 5$ il polinomio $X^4 - 2$ è irriducibile. Infatti sicuramente non ha radici, in quanto per ogni elemento $a \neq 0$ in $\mathbb{F}_5$ si ha $a^4 = 1$. La verifica che questo polinomio non si possa fattorizzare come prodotto di due polinomi di secondo grado è leggermente più tecnica, in quanto si dovrebbe analizzare la possibililtà di scrivere $X^4 - 2$ nella forma $(X^2 + AX + B)(X^2 + CX + D)$, dove $A, B, C, D \in \mathbb{F}_5$. I calcoli non sono difficili ma leggermente noiosi.

In alternativa, si può considerare il fatto che una radice α di questo polinomio deve soddisfare $\alpha^4 = 2$, quindi $\alpha^{16} = 1$, e quindi il suo ordine moltiplicativo deve essere uguale a 16 (non può essere un divisore proprio di 16, in quanto $\alpha^8 = -1$). Ma allora il campo di spezzamento di $f(X)$, che deve contenere α, deve avere un gruppo moltiplicativo di ordine multiplo di 16, ossia deve essere del tipo $\mathbb{F}_5^k$ con $5^k - 1 \equiv 0 \pmod{16}$. Questo significa che $k \equiv 0 \pmod 4$, quindi il minimo numero possibile è $k = 4$.