COMPITO DI ARITMETICA

11 giugno 2018

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 $x + y + z = \bar{0}$.

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

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

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.

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 $[\mathbb{F}_p(\sqrt{m} + \sqrt{3}) : \mathbb{F}_p]$.