

1. Fattorizzare il polinomio $X^9 - X \in \mathbf{F}_3[X]$ in fattori irriducibili.
2. Sia $k = \mathbf{F}_{16}$.
 - (a) Per quanti elementi $\alpha \in k$ si ha che $k = \mathbf{F}_2(\alpha)$?
 - (b) Quanti elementi $\alpha \in k^*$ hanno ordine 15?
3.
 - (a) Dimostrare che $X^2 - 2$ è un polinomio irriducibile in $\mathbf{F}_5[X]$.
 - (b) Dimostrare che $\mathbf{F}_5(\sqrt{2}) = \mathbf{F}_5[X]/(X^2 - 2)$ è un campo di 25 elementi.
 - (c) Calcolare gli ordini degli elementi $1 - \sqrt{2}$ e $2 - \sqrt{2}$ di $\mathbf{F}_5(\sqrt{2})^*$.
4.
 - (a) Dimostrare che $X^2 - 3$ è un polinomio irriducibile in $\mathbf{F}_5[X]$.
 - (b) Esibire un isomorfismo fra i campi $\mathbf{F}_5(\sqrt{2})$ e $\mathbf{F}_5(\sqrt{3})$.
5. Il polinomio $X^3 + 2$ è irriducibile in $\mathbf{F}_7[X]$? Stessa domanda per $X^3 + 2$ in $\mathbf{F}_{49}[X]$.
6.
 - (a) Dimostrare che per ogni $x \in \mathbf{F}_{32} - \mathbf{F}_2$ si ha che $\mathbf{F}_{32}^* = \langle x \rangle$.
 - (b) Per quanti polinomi $f \in \mathbf{F}_2[X]$ si ha che $\mathbf{F}_2[X]/(f) \cong \mathbf{F}_{32}$?
7. Sia $p > 2$ un primo.
 - (a) Dimostrare che il campo \mathbf{F}_{p^2} contiene una radice ottava dell'unità.
 - (b) Dimostrare che 2 è un quadrato in \mathbf{Z}_p se e solo se $p \equiv \pm 1 \pmod{8}$.

8. La funzione di Möbius $\mu : \mathbf{Z}_{\geq 1} \rightarrow \{-1, 0, +1\}$ è data da

$$\mu(n) = \begin{cases} 0; & \text{se esiste un primo } p \text{ tale che } p^2 \text{ divide } n, \\ (-1)^t; & \text{se } n \text{ è prodotto di } t \text{ primi distinti.} \end{cases}$$

- (a) Dimostrare che $\mu(nm) = \mu(n)\mu(m)$ se $\text{mcd}(n, m) = 1$.
- (b) Dimostrare che per ogni $n \geq 1$ si ha che

$$\sum_{d|n} \mu(d) = \begin{cases} 1; & \text{se } n = 1, \\ 0; & \text{se } n > 1. \end{cases}$$

- (c) (Inversione di Möbius) Siano f, g due funzioni $\mathbf{Z}_{\geq 1} \rightarrow \mathbf{C}$ con la proprietà che $\sum_{d|n} f(d) = g(n)$ per ogni $n \in \mathbf{Z}_{\geq 1}$. Dimostrare che

$$f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right)g(d).$$

9. Sia p un primo. Per ogni intero $n \geq 1$ sia b_n il numero di polinomi irriducibili monici nell'anello $\mathbf{Z}_p[X]$ di grado n .
 - (a) Dimostrare che $\sum_{d|n} db_d = p^n$ per ogni $n \geq 1$.
 - (b) Dimostrare che $b_n = \sum_{d|n} \mu\left(\frac{n}{d}\right)p^d$.
 - (c) Dimostrare l'identità

$$\prod_{n=1}^{\infty} \left(\frac{1}{1 - T^n} \right)^{b_n} = \frac{1}{1 - pT}$$

nell'anello $\mathbf{F}_p[[T]]$ (Sugg. valutare la sommatoria $\sum_{f \in \mathbf{F}_p[X], \text{monico}} T^{\deg f}$ in due modi diversi.)