1. Quanti polinomi irriducibili monici di grado 5 ci sono in $\mathbf{F}_3[X]$? E quanti di grado 6?

2. (a) Dimostare che ogni elemento $x \in \mathbf{F}_{32} - \mathbf{F}_2$ genera il gruppo $\mathbf{F}_{32}^*$.
   (b) Per quanti polinomi $f \in \mathbf{F}_2[X]$ si ha che $\mathbf{F}_2[X]/(f) \cong \mathbf{F}_{32}$?

3. Sia $\mathrm{Tr} : \mathbf{F}_{16} \to \mathbf{F}_2$ la mappa *traccia*.
   (a) Per quanti elementi $x \in \mathbf{F}_{16}$ si ha che $\mathrm{Tr}(x) = 0$?
   (b) Sia $k \subset \mathbf{F}_{16}$ l'unico sottocampo di cardinalità 4. Dimostrare che ogni $x \in k$ ha traccia zero.
   (c) Esibire un elemento in $H - k$ (dare il suo polinomio minimo su $\mathbf{F}_2$).

4. Sia E il campo $\mathbf{F}_{27}$. Sia $S = \{a \in E \text{ per cui } E = \mathbf{F}_3(a)\}$.
   (a) Dimostrare che $\#S = 24$.
   (b) Dimostrare che ci sono otto polinomi irriducibili monici di grado 3 in $\mathbf{F}_3[X]$.
   (c) Dimostrare che quattro dei polinomi della parte (b) hanno termine noto $+1$ e quattro hanno termine noto -1.

5. Sia $p > 2$ un primo.
   (a) Dimostrare che il campo $\mathbf{F}_{p^2}$ contiene una radice primitiva ottava dell'unità ζ.
   (b) Dimostrare che il quadrato di $\alpha = \zeta + \zeta^{-1}$ è uguale a 2.
   (c) Dimostrare che α sta nel sottocampo $\mathbf{F}_p$ se e solo se $p \equiv \pm 1 \pmod 8$.
   (d) Dimostrare che 2 è un quadrato in $\mathbf{F}_p$ se e solo se $p \equiv \pm 1 \pmod 8$.

6. (a) Dimostrare che $X^2 - 2$ è un polinomio irriducibile in $\mathbf{F}_5[X]$.
   (b) Dimostrare che $k = \mathbf{F}_5(\sqrt{2}) = \mathbf{F}_5[X]/(X^2 - 2)$ è un campo di 25 elementi.
   (c) Calcolare gli ordini degli elementi $1 - \sqrt{2}$ e $2 - \sqrt{2}$ di k^*.

7. (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 $\mathbf{F}_5(\sqrt{3})$.

8. Sia p un primo. Per $n \geq 1$, sia a_n il numero di polinomi irriducibili monici di grado n nell'anello $\mathbf{F}_p[X]$. Dimostrare l'identità

$$\prod_{n=1}^{\infty} (1 - T^n)^{a_n} \;=\; 1 - pT$$

   nell'anello delle serie di potenze $\mathbf{Z}[[T]]$.
   (Sugg. considerare il logaritmo: $-\log(1 - X) = X + \frac{1}{2}X^2 + \frac{1}{3}X^3 + \ldots$)

9. Sia p un primo. Per $n \geq 1$, sia $\Phi_n(X)$ l'ennesimo poliniomio ciclotomico.
   (a) Dimostrare che se p non divide n, allora $\Phi_n(X)$ si fattorizza nell'anello $\mathbf{F}_p[X]$ in $\phi(n)/d$ fattori irriducibili di grado d, dove d è l'ordine di $\overline{p} \in \mathbf{Z}_n^*$.
   (Sugg. usare l'esercizio 2 del foglio 10).
   (b) Cosa succede se p divide n?