1. (a) Dimostare 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 $\mathbf{F}_2[X]/(f) \cong \mathbf{F}_{32}$?

2. Sia p un primo, sia $n \geq 1$ e sia $q = p^n$. Per un elemento $a \in \mathbf{F}_q$ definiamo la sua *traccia* $Tr(a) = a + a^p + a^{p^2} + \ldots + a^{p^{n-1}}$ e la sua *norma* $N(a) = a \cdot a^p \cdot a^{p^2} \cdot \ldots \cdot a^{p^{n-1}}$.
   (a) Provare che la traccia $\mathbf{F}_q \to \mathbf{F}_p$ è un omomorfismo suriettivo di gruppi additivi (Sugg: il nucleo della traccia consiste negli zeri di un polinomio di grado p^{n-1}).
   (b) Provare che la norma $\mathbf{F}_q^* \to \mathbf{F}_p^*$ è un omomorfismo suriettivo di gruppi moltiplicativi.

3. Sia k il campo $\mathbf{F}_{16}$.
   (a) Dimostrare che k ammette un unico sottocampo k' di 4 elementi.
   (b) Sia N il nucleo della traccia $Tr : \mathbf{F}_{16} \to \mathbf{F}_2$. Dimostrare che $k' \subset N$.
   (c) Esibire un elemento in $N - k'$ (dare il suo polinomio minimo su $\mathbf{F}_2$).
   (d) Esibire un elememto in k^* di ordine 5 (dare il suo polinomio minimo su $\mathbf{F}_2$).

4. Sia E il campo $\mathbf{F}_{27}$. Sia $S = \{a \in E : \text{si ha che } E = \mathbf{F}_3(a)\}$.
   (a) Dimostrare che $\#S = 24$.
   (b) Dimostrare che ci sono otto polinomi irriducibili di grado 3 in $\mathbf{F}_3[X]$.
   (c) Dimostrare che $S \subset E^*$ e che gli elementi di S hanno ordine 13 oppure 26.
   (d) Dimostrare che quattro dei polinomi della parte (b) hanno termine noto uguale a $+1$ e quattro hanno termine noto uguale a -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. Sia p, sia $n \geq 1$ e sia $q = p^n$. Diamo il campo finito $\mathbf{F}_q$ la struttura di $\mathbf{F}_p[X]$-modulo come segue. Definiamo che

$$X \cdot a = a^p, \qquad \text{per } a \in \mathbf{F}_q.$$

   Quindi, per $f = \sum_{k=0}^m b_k X^k \in \mathbf{F}_p[X]$ e $a \in \mathbf{F}_q$ definiamo che $f \cdot a = \sum_{k=0}^m b_k a^{p^k}$.
   (a) Dimostrare che $(X^n - 1) \cdot a = 0$ per ogni $a \in \mathbf{F}_q$.
   (b) Sia $a \in \mathbf{F}_q$. Dimostrare che $(X - 1) \cdot a = 0$ se e solo se $a \in \mathbf{F}_p$.
   (c) Sia $a \in \mathbf{F}_q$. Dimostrare che $\{g \in \mathbf{F}_p[X] : g \cdot a = 0\}$ è un ideale di $\mathbf{F}_p[X]$.
   Per $a \in \mathbf{F}_q$ scriviamo $r(a)$ per il generatore monico dell'ideale della parte (d).
   (d) Dimostrare che per ogni $a \in \mathbf{F}_q$ il polinomio $r(a)$ divide $X^n - 1$.
   (e) Per $p = 3$ e $n = 2$ esibire elementi $a \in \mathbf{F}_9$ con $r(a) = 1$, $X - 1$, $X + 1$ e $X^2 - 1$ rispettivamente (dare i loro polinomi minimi su $\mathbf{F}_3$).
   (f) In generale, quanti elementi $a \in \mathbf{F}_{p^2}$ con $r(a) = 1$, $X - 1$, $X + 1$ e $X^2 - 1$ ci sono?