1. Sia $R$ un anello commutativo. La *derivata* $f'$ di un polinomio $f = a_nX^n + \ldots + a_2X^2 + a_1X + a_0 \in R[X]$ è definita da

$$f' = na_nX^{n-1} + \ldots + 2a_2X + a_1.$$

Dimostrare

$$\begin{aligned} (f+g)' &= f' + g', && \text{per ogni } f, g \in R[X]; \\ (fg)' &= fg' + f'g, && \text{per ogni } f, g \in R[X]; \\ f' &= 0, && \text{per ogni } f \text{ costante.} \end{aligned}$$

2. Determinare i polinomi ciclotomici $\Phi_5(X)$, $\Phi_{10}(X)$, $\Phi_{15}(X)$ e $\Phi_{20}(X)$.

3. (a) Sia $m > 1$ un intero dispari. Dimostrare che $\Phi_{2m}(X) = \Phi_m(-X)$.
   (b) Sia $m > 1$ un intero pari. Dimostrare che $\Phi_{2m}(X) = \Phi_m(X^2)$.
   (c) Determinare $\Phi_{80}(X)$.

4. Sia $n \geq 2$ e sia $\Phi_n(X)$ l'$n$-esimo polinomio ciclotomico.
   (a) Dimostrare che $\Phi_n(0) = 1$.
   (b) Dimostrare che $\Phi_n(X)$ è un polinomio *palindromo*. In altre parole, si ha che $\Phi_n(X) = X^{\phi(n)}\Phi_n(1/X)$.

5. Sia $n \geq 2$ e sia $\Phi_n(X)$ l'$n$-esimo polinomio ciclotomico.
   (a) Dimostrare che $\Phi_n(1) = p$ se $n$ è potenza di un primo $p$, altrimenti $\Phi_n(1) = 1$.
   (b) Supponiamo che $n \geq 3$. Dimostrare che $\Phi_n(-1) = p$ se $n$ è il doppio di una potenza di un primo $p$, altrimenti $\Phi_n(-1) = 1$.
   (c) Dimostrare che se $n \geq 3$ e $a \in \mathbf{Z}$ soddisfa $|a| \geq 2$, allora $\Phi_n(a) \neq 1$.

6. Sia $n \geq 1$ e sia $a \in \mathbf{Z}$.
   (a) Sia $p$ un divisore primo di $\Phi_n(a)$. Dimostrare che $p$ divide $n$ oppure $p$ è congruo a 1 (mod $n$).
   (b) Fattorizzare i numeri $\Phi_3(7)$, $7^3 - 1$, $3^5 - 1$, $2^9 - 1$.

7. Sia $p$ un primo e sia $K$ un campo di caratteristica $p$. Per ogni $n \geq 1$ sia $k_n$ il sottoinsieme $\{a \in K : a^{p^n} = a\}$.
   (a) Dimostrare che per ogni $n \geq 1$ l'insieme $k_n$ è un sottocampo di $K$.
   (b) Dimostrare che $k_n \subset k_m$ quando $n$ divide $m$.

8. (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 $\mathbf{F}_5(\sqrt{2})^*$.

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