1. Sia n un numero naturale. Dimostrare che $4^n + n^4$ può solo essere primo quando $n = 1$.
2. Dimostrare: se p è primo e $p^2 + 8$ è primo, allora $p^3 + 4$ è primo.
3. Per ogni $n \in \mathbf{Z}_{>0}$, calcolare $(n-1)!$ modulo n.
4. Usare (induttivamente) il criterio di Pocklington per dimostrare che
$$10^{30} + 57 = 1000000000000000000000000000057$$
è primo.
5. Usare (induttivamente) il criterio di Pocklington per dimostrare che
$$10^{40} + 121 = 10000000000000000000000000000000000000121$$
è primo.
6. Sia p un numero primo dispari e sia p^k una potenza di p.
   (a) Dimostrare che $p + 1 \in \mathbf{Z}_{p^k}$ ha ordine p^{k-1}.
   (b) Dimostrare che esiste $g \in \mathbf{Z}_{p^k}^*$ di ordine $\varphi(p^k) = (p-1)p^{k-1}$.
7. (a) Dimostrare che ogni $\overline{x} \in \mathbf{Z}_2$ è quadrato.
   (b) Dimostrare che $\overline{x} \in \mathbf{Z}_4$ è quadrato se e solo $x \equiv 0 \pmod 4$ oppure $x \equiv 1 \pmod 4$.
   (c) Sia $k \geq 3$. Dimostrare che $\overline{x} \in \mathbf{Z}_{2^k}^*$ è quadrato se e solo se $x \equiv 1 \pmod 8$.
8. Sia $p > 3$ un numero primo. Dimostrare:
   (a) -1 è quadrato modulo p se e solo se $p \equiv 1 \pmod 4$.
   (b) -3 è quadrato modulo p se e solo se $p \equiv 1 \pmod 3$. (Sugg: T^2+3 ammette uno zero modulo p se e solo se $T^2 + T + 1$ ammette uno zero modulo p.)
   (c) Dedurre: 3 è quadrato modulo p se e solo se $p \equiv \pm 1 \pmod{12}$.
9. Sia $k \geq 1$ e sia $F_k = 2^{2^k} + 1$ il k-esima numero di Fermat.
   (a) Far vedere che $F_k \equiv 5 \pmod{12}$.
   (b) Dimostrare che F_k è primo se e solo se $3^{2^{2^k-1}} \equiv -1 \pmod{F_k}$.
10. Sia $n \in \mathbf{Z}_{>0}$ non divisibile per 3.
    (a) Dimostrare che $\overline{x} = \overline{1}$ è l'unico elemento di $\mathbf{Z}_n$ che soddisfa $x^3 \equiv 1 \pmod n$, se e solo se esiste un divisore primo di n congruo a 2 (mod 3).
    (b) Supponiamo che ogni divisore primo di n è congruo a 1 (mod 3). Far vedere che il numero di $\overline{x} \in \mathbf{Z}_n$ con $x^3 \equiv 1 \pmod n$, è uguale a 3^t dove t è il numero di divisori primi distinti di n.
11. (*Polinomi ciclotomici.*) Per $n \in \mathbf{Z}_{>0}$ definiamo l'ennisimo polinomio ciclotomico $\Phi_n(X)$ induttivamente per
$$\prod_{d|n} \Phi_d(X) = X^n - 1$$
(nel prodotto d varia fra i divisori positivi di n).
    (a) Calcolare $\Phi_n(X)$ per $n \leq 12$;
    (b) Calcolare $\Phi_n(X)$ quando n è primo;
    (c) Far vedere che il grado di $\Phi_n(X)$ è uguale a $\varphi(n)$.