1. Sia $n \in \mathbf{Z}_{>0}$ con $n \not\equiv 2 \pmod 4$.
   (a) Scrivere n come differenza di due quadrati.
   (b) Supponiamo che n non sia primo. Esibire $x, y \in \mathbf{Z}$ tali che $n = x^2 - y^2$ e $\mathrm{mcd}(x \pm y, n) \neq 1$.

2. Risolvere il seguente sistema di equazioni lineari con coefficienti in $\mathbf{Z}_2$.

$$\begin{cases} x_1 + x_2 + x_4 = 1 \\ x_2 + x_3 + x_4 = 1 \\ x_1 + x_3 + x_4 = 0 \\ x_1 + x_2 + x_3 = 0 \end{cases}$$

3. Sia $n \in \mathbf{Z}_{>0}$ un intero dispari. Far vedere che:
   (a) il numero $x^2 - n$ è pari solo se $x \in \mathbf{Z}$ è dispari;
   (b) se $n \equiv 3 \pmod 4$ e x è dispari, allora $\mathrm{ord}_2(x^2 - n) = 1$;
   (c) se $n \equiv 5 \pmod 8$ e x è dispari, allora $\mathrm{ord}_2(x^2 - n) = 2$.

4. (a) Sia $k \geq 3$. Dimostrare che $\overline{x} \in \mathbf{Z}_{2^k}^*$ è quadrato se e solo se $x \equiv 1 \pmod 8$.
   (b) Determinare tutti gli elementi $\overline{x} \in \mathbf{Z}_{64}$ con $x^2 \equiv 33 \pmod{64}$.

5. *(Lemma di Hensel).* Sia $f(X) = x^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0$ un polinomio con coefficienti interi. Sia p un numero primo e supponiamo che $a \in \mathbf{Z}$ abbia la proprietà che $f'(a) \not\equiv 0 \pmod p$ e che $f(a) \equiv 0 \pmod{p^k}$ per un certo $k \in \mathbf{Z}_{>0}$. Controllare che l'elemento $b \in \mathbf{Z}_{p^{k+1}}$ dato da

$$b \;=\; a - \frac{f(a)}{f'(a)}$$

   ha la proprietà che $f(b) \equiv 0 \pmod{p^{k+1}}$.

6. Sia $p \equiv 3 \pmod 4$ un numero primo. Supponiamo che $a \in \mathbf{Z}$ sia un quadrato diverso da zero modulo p. Far vedere che:
   (a) vale $a^{(p-1)/2} \equiv 1 \pmod p$;
   (b) il numero $a^{(p+1)/4}$ è radice quadrata di a modulo p.

7. Sia $x \in \mathbf{R}_{>1}$ e sia y la funzione implicita di x data da $y\log(y) = x$. Dimostrare che

$$y \;=\; \frac{x}{\log(x)} \;+\; o(1), \quad (x \to \infty).$$

   dove $o(1)$ indica una funzione di x che tende verso zero quando $x \to \infty$.

8. *(Lemma di Gauss)* Per ogni primo dispari p, sia

$$S \quad = \quad \{\overline{1}, \overline{2}, \ldots, \overline{\tfrac{p-1}{2}}\} \quad \subset \quad \mathbf{Z}_p^*.$$

   Per $x \in \mathbf{Z}_p^*$ definiamo

$$\varepsilon_x : S \longrightarrow \{\pm 1\}$$

   nel modo seguente: $\varepsilon_x(a) = +1$ se $\overline{xa} \in S$ mentre $\varepsilon_x(a) = -1$ se $\overline{-xa} \in S$.
   (a) Dimostrare che per ogni $\overline{a} \in \mathbf{Z}_p^*$ abbiamo che $\overline{a} \in S$ oppure $\overline{-a} \in S$;
   (b) Calcolare la funzione ε_x per $p = 7$ ed per ogni $x \in \mathbf{Z}_7^*$;
   (c) Dimostrare che $x \in \mathbf{Z}_p^*$ è un quadrato se e solo se $\prod_{a \in S} \varepsilon_x(a) = +1$.

9. Sia p un numero primo dispari.
   (a) Far vedere che 2 è un quadrato modulo p per $p = 7, 17, 23, 31$, ma non è un quadrato modulo p per $p = 3, 5, 11, 19$.
   (b) Dimostrare che 2 è un quadrato modulo p se e solo se $p \equiv \pm 1 \pmod 8$.