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

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

2. 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 $\mathrm{ord}_2(x^2 - n) = 2$.

3. (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 $x^2 \equiv 33 \pmod{64}$.

4. 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.

5. 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 $\varphi(p^k) = (p-1)p^{k-1}$.

6. Scrivere i seguenti gruppi come prodotto di gruppi ciclici: $\mathbf{Z}_{24}^*$, $\mathbf{Z}_{30}^*$, $\mathbf{Z}_{25}^*$.

7. Per $m = 2, 4, 6, 8, 10, 12, \ldots, 20$.
   (a) determinare
   $$e(m) = \max\{n \in \mathbf{Z}_{>0} : \overline{x}^m = \overline{1} \text{ per ogni } \overline{x} \in \mathbf{Z}_n^*\};$$
   (Per esempio: $e(2) = 24$, $e(4) = 240$, $e(6) = 504$, $\ldots$)
   (b) per $n = e(m)$, scrivere $\mathbf{Z}_n^*$ come prodotto di gruppi ciclici.

8. Sia p un numero primo e sia E una curva ellittica su $\mathbf{Z}_p$ di equazione $Y^2 = X^3 + AX + B$.
   (a) Dimostrare che un punto $P = (x, y) \in E(\mathbf{Z}_p)$ ha ordine 3 se e solo se
   $$3x^4 + 6Ax^2 + 12Bx - A^2 = 0.$$
   (b) Dimostrare che ci sono al più 8 punti di ordine 3.
   (c) Dimostrare che il gruppo $\{P \in E(\mathbf{Z}_p) : 3P = \infty\}$ è isomorfo a $\mathbf{Z}_3$, $\mathbf{Z}_3 \times \mathbf{Z}_3$ o al gruppo banale.

9. Sia $x \in \mathbf{R}_{>1}$ e sia y la funzione implicita di x data da $y\log(y) = x$. Dimostrare che
$$\lim_{x \to \infty} \left(\frac{x}{\log x} \right) / y \ = \ 1.$$

10. 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 $p \equiv \pm 1 \pmod 8$.
    (Sugg. http://en.wikipedia.org/wiki/Gauss's_lemma_(number_theory))