1. (a) Per ogni $\overline{x} \in \mathbf{Z}_{13}^*$ calcolare l'ordine di $\overline{x}$ nel gruppo moltiplicativo $\mathbf{Z}_{13}^*$.
   (b) Per ogni $\overline{x} \in \mathbf{Z}_{13}$ calcolare l'ordine di $\overline{x}$ nel gruppo additivo $\mathbf{Z}_{13}$.

2. Determinare $n \in \mathbf{Z}_{>1}$ con $\mathrm{mcd}(n, 10)$ e che hanno la proprietà che il periodo dell'espansione decimale di n ha lunghezza ≤ 6.

3. Sia n un numero naturale e sia $x \in \mathbf{Z}$ con $\mathrm{mcd}(x, n) = 1$. Sia $a = \mathrm{ord}_n(x)$ e sia $k \in \mathbf{Z}$. Dimostrare che $\mathrm{ord}_n(x^k) = a/\mathrm{mcd}(a, k)$.

4. Sia n un numero naturale dispari.
   (a) Dimostrare che $H = \{\overline{x} \in \mathbf{Z}_n^* : \overline{x}^2 = \overline{1}\}$ è sottogruppo di $\mathbf{Z}_n^*$.
   (b) Dimostrare che $\#H = 2^d$ dove d è il numero di divisori primi di n.
   (c) Determinare H per $n = 91$.

5. Un numero naturale $n \in \mathbf{Z}_{>1}$ si dice *numero di Carmichael* se *non* è primo, ma soddisfa $x^{n-1} \equiv 1 \pmod{n}$ per ogni $x \in \mathbf{Z}$ con $\mathrm{mcd}(x, n) = 1$.
   (a) Dimostrare che 1105 e 1729 sono numeri di Carmichael.
   (b) Dimostrare che $n \in \mathbf{Z}_{>1}$ è numero di Carmichael se e solo se n non è primo e ha la proprietà che per ogni divisore primo p di n si ha che p^2 non divide n, ma $p - 1$ divide $n - 1$.

6. Dimostrare che non esiste nessun $n \in \mathbf{Z}_{>0}$ tale che $\mathbf{Z}_n^* \cong \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2 \times \mathbf{Z}_2$.

7. (a) Dimostrare che $\mathbf{Z}_{60}^* \cong \mathbf{Z}_4 \times \mathbf{Z}_2 \times \mathbf{Z}_2$.
   (b) Esibire elementi $x_1, x_2, x_3 \in \mathbf{Z}_{60}^*$ di ordine 4, 2, 2 rispettivamente, che hanno le proprietà che $\mathbf{Z}_{60}^*$ è generato da x_1, x_2, x_3.

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

9. 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: $e(2) = 24$, $e(4) = 240$, $e(6) = 504$, ...)
   (b) per $n = e(m)$, scrivere $\mathbf{Z}_n^*$ come prodotto di gruppi ciclici.

PER I SEGUENTI ESERCIZI È UTILE UN COMPUTER.

10. Siano $n = 56492375429317645$ e $m = 986764526573$.
    (a) Far vedere che $\mathrm{mcd}(n, m) = 1$;
    (b) Calcolare $\lambda, \mu \in \mathbf{Z}$ tali che $\lambda n + \mu m = 1$.
    (c) Calcolare $\lambda, \mu \in \mathbf{Z}$ tali che $\lambda n + \mu m = 2$.

11. Sia $n = 10001 = 73 \cdot 137$.
    (a) Fattorizzare $\varphi(n)$.
    (b) Esibire, se esiste, un $\overline{x} \in \mathbf{Z}_n^*$ di ordine 17.
    (c) Esibire, se esiste, un $\overline{x} \in \mathbf{Z}_n^*$ di ordine 8.

12. (Esperimento fattorizzare usando il metodo "$p - 1$") Sia $M = 10!$
    (a) Sia $n = 95431706263$. Scegliere $\overline{a} \in \mathbf{Z}_n^*$ a caso. Calcolare $\overline{b} = \overline{a}^M \pmod{n}$. Calcolare il divisore $d = \mathrm{mcd}(b - 1, n)$ di n ed il cofattore n/d.
    (b) Sia $n = 57841557763361$. Scegliere $\overline{a} \in \mathbf{Z}_n^*$ a caso. Calcolare $\overline{b} = \overline{a}^M \pmod{n}$. Calcolare il divisor $d = \mathrm{mcd}(b - 1, n)$ di n ed il cofattore n/d.
    (c) Come mai si riescono a fattorizzare questi due numeri n in questo modo?