1. Sia ϕ la funzione di Euler. Calcolare $\phi(n)$ per $n = 89$, 90, 91 e 92.

2. Sia $n \in \mathbf{Z}_{\geq 1}$. Determinare l'ordine di $-\overline{1}$ nel gruppo $\mathbf{Z}_n^*$. Dimostrare che $\phi(n)$ è pari per $n \geq 3$.

3. Per ogni $n < 10$ calcolare $a \in \{0, 1, \ldots, n-1\}$ tale che $(n-1)! \equiv a \pmod{n}$.

4. Lo scopo di questo esercizio è di dimostrare la classica formula di Wilson che dice che per ogni numero primo p si ha che $(p-1)! \equiv -1 \pmod{p}$.
   (a) Osservare che la classe di $(p-1)!$ in $\mathbf{Z}_p^*$ è uguale al prodotto P di tutti gli elementi di $\mathbf{Z}_p^*$.
   (b) Dimostrare che gli unici elementi di $\mathbf{Z}_p^*$ che sono uguali al loro inverso, sono $\pm\overline{1}$.
   (c) Dimostrare la formula di Wilson (Sugg: nel prodotto P cancellare elementi $\overline{x}$ con $\overline{x}^{-1}$)

5. Sia ϕ la funzione di Euler.
   (a) Sia $n = 10$. Per ogni divisore d di n calcolare $\phi(d)$. Calcolare $\sum_{d|n} \phi(d)$.
   (b) Stessa domanda per $n = 11$.
   (c) Stessa domanda per $n = 12$.

6. Lo scopo di questo esercizio è di dimostrare la seguente formula di Gauss: per ogni numero naturale n si ha che $\sum_{d|n} \phi(d) = n$.
   (a) Sia S l'insieme delle frazioni $\{\frac{a}{n} : a \in \mathbf{Z} \text{ con } 0 \leq a < n\}$. Determinare $\#S$.
   (b) Ridurre le frazioni ai minimi termini. Dimostrare che per ogni divisore d di n, ci sono $\phi(d)$ frazioni in S con denominatore uguale a d.
   (c) Dimostrare la formula di Gauss.

7. Sia $n > 0$ un intero e sia m un divisore di n.
   (a) Dimostrare che la mappa $f : \mathbf{Z}_n \longrightarrow \mathbf{Z}_m$ data da $f(a \pmod{n}) = a \pmod{m}$, è ben definita, nel senso che se $a = a' \pmod{n}$, allora $f(a \pmod{n}) = f(a' \pmod{n})$. In altre parole, il valore di f non dipende dal rappresentante $a \in \mathbf{Z}$, ma solo dalla sua classe $\overline{a} = a \pmod{n}$.
   (b) Dimostrare che $f : \mathbf{Z}_n \longrightarrow \mathbf{Z}_m$ è suriettiva.
   (c) Dimostrare che se $a \pmod{n}$ è in $\mathbf{Z}_n^*$, allora $f(a \pmod{n})$ sta in $\mathbf{Z}_m^*$.
   (d) Dimostrare che $f : \mathbf{Z}_n^* \longrightarrow \mathbf{Z}_m^*$ è suriettiva (Sugg. Per induzione basta supporre che $n = mp$ per qualche primo p).

8. (a) Determinare tutti gli interi $n > 0$ per cui il gruppo $\mathbf{Z}_n^*$ ha cardinalità 1.
   (b) Determinare tutti gli interi $n > 0$ per cui il gruppo $\mathbf{Z}_n^*$ ha cardinalità 2.
   (c) Determinare tutti gli interi $n > 0$ per cui il gruppo $\mathbf{Z}_n^*$ ha la proprietà che $\overline{x} \cdot \overline{x} = \overline{1}$ per ogni $\overline{x} = \mathbf{Z}_n^*$. (Sugg: distinguere i casi $n \equiv 0 \pmod{5}$ e $n \not\equiv 0 \pmod{5}$).

9. Sia $n > 0$ un intero tale che $\mathrm{mcd}(n, 10) = 1$. Dimostrare che la lunghezza del periodo della frazione decimale di $1/n$ è uguale all'ordine dell'elemento $\overline{10}$ di $\mathbf{Z}_n^*$. In particolare, la lunghezza è un divisore di $\phi(n)$.