1.(a) Enunciare il teorema di Lagrange per il gruppo additivo $(\mathbf{Z}_7, +)$. Verificarlo per tutte le classi $\bar{x} \in \mathbf{Z}_7$.

(b) Enunciare il teorema di Lagrange per il gruppo moltiplicativo $(\mathbf{Z}_7^*, \cdot)$. Verificarlo per tutte le classi $\bar{x} \in \mathbf{Z}_7^*$.

2. Sia p un numero primo.
   (a) Dimostrare che la cardinalità di $\mathbf{Z}_p^*$ è uguale a $p-1$.
   (b) Sia $k > 1$ un intero. Dimostrare che la cardinalità di $\mathbf{Z}_{p^k}^*$ è uguale a $p^k - p^{k-1}$.
   (c) Verificare questo fatto per $p = 3$ e $k = 2$ e per $p = 3$ e $k = 3$.

3. Sia $n = 1001$.
   (a) Verificare che $\bar{x} = \overline{101}$ appartiene a Z_{1001}^* e determinare $\bar{x}^{-1}$.
   (b) Determinare la cardinalità di Z_{1001}^*.

4. Sia data la relazione $-173 \cdot 371 + 113 \cdot 568 = 1$.
   (a) Verificare che $\bar{x} = 113$ appartiene a $\mathbf{Z}_{371}^*$ e determinare il suo inverso $\bar{x}^{-1}$ (giustificare bene le risposte).
   (b) Verificare che $\bar{x} = 371$ appartiene a $\mathbf{Z}_{568}^*$ e determinare il suo inverso $\bar{x}^{-1}$ (giustificare bene le risposte).

5. Enunciare il Piccolo Teorema di Fermat per $p = 101$. Verificarlo per le classi $\bar{x} = \bar{2}, \bar{3}, \bar{5} \in \mathbf{Z}_{101}^*$.

6. Sia $n = 16$.
   (a) Fare la lista delle classi resto di $\mathbf{Z}_{16}^*$ e per ognuna di esse indicare l'inverso moltiplicativo.
   (b) Enunciare il teorema di Lagrange per il gruppo moltiplicativo $\mathbf{Z}_{16}^*$. Verificarlo per tutte le classi $\bar{x} \in \mathbf{Z}_{16}^*$.
   (c) Possiamo applicare il teorema di Lagrange per calcolare $\bar{x} = 6^{1000}$ in $\mathbf{Z}_{16}$? Spiegare.

7. Siano $n = 91$ ed $m = 117$.
   (a) Usare il Piccolo Teorema di Fermat per dimostrare che n non è primo (senza fattorizzarlo).
   (b) Usare il Piccolo Teorema di Fermat per determinare se m è primo (senza fattorizzarlo).

8. Siano $n = 3^3 \cdot 5^3 \cdot 101$ ed $m = 2^4 \cdot 17 \cdot 37$.
   (a) Determinare la cardinalità di $\mathbf{Z}_n^*$ e di $\mathbf{Z}_m^*$.
   (b) Enunciare il teorema di Lagrange per i gruppi moltiplicativi $\mathbf{Z}_n^*$ e $\mathbf{Z}_m^*$.
   (c) Esibire una classe $\bar{x} \in \mathbf{Z}_n$ a cui si applica il teorema di Lagrange ed una classe $\bar{y} \in \mathbf{Z}_n$ a cui il teorema di Lagrange *non* si applica.

9. *Non vale il viceversa del Piccolo Teorema di Fermat.* Sia $n = 2465 = 5 \cdot 17 \cdot 29$.
   (a) Verificare che $mcd(x, 2465) = 1$ se e solo se $mcd(x, 5) = mcd(x, 17) = mcd(x, 29) = 1$.
   (b) Verificare che $x^{2464} \equiv 1 \bmod 2465$, per ogni $x \in \mathbf{Z}$ che soddisfa $mcd(x, 2465) = 1$.

10. Sia p un numero primo.
    (a) Verificare che ci sono precisamente due classi resto in $\mathbf{Z}_p$ che soddisfano l'equazione $\bar{x}^2 = \bar{1}$, che sono $\bar{x} = \bar{1}$ e $\bar{x} = \overline{-1} = \overline{p-1}$.
    (b) Sia $p = 11$. Determinare le soluzioni dell'equazione $\bar{x}^2 = \bar{1}$ in $\mathbf{Z}_{11}$.
    (c) Esistono soluzioni dell'equazione $\bar{x}^2 = \bar{5}$ in $\mathbf{Z}_{11}$? Determinarle tutte.
    (d) Esistono soluzioni dell'equazione $\bar{x}^2 = \bar{6}$ in $\mathbf{Z}_{11}$? Spiegare.

11. Calcolare $\bar{5}^{1001133}$ modulo 7. Calcolare $\bar{5}^{10011}$ modulo 11.

12. Calcolare $\bar{2}^{100006548765987}$ modulo 101. Calcolare $\bar{3}^{1001133}$ modulo 70.

13. Il signor Rossi ha un kit RSA per i con chiavi pubbliche $N = 17 \cdot 19$ ed $E = 13$ e chiave segreta $D = 111$. Può funzionare?

14. Preparare un kit RSA per il signor Rossi, con chiavi pubbliche $N = 17 \cdot 19$ ed $E = 7$ e chiave segreta D.
    (a) Determinare D.
    (b) Spedire al Signor Rossi il messaggio $m = 11$, dopo averlo criptato. Cosa riceverà il Signor Rossi?

15. Il signor Rossi ha un kit RSA con chiavi pubbliche $N = 143$ ed $E = 7$ e chiave segreta $D = 103$.
    (a) Riceve il messaggio criptato $MC = 109$. Che messaggio gli hanno spedito?
    (b) Spedire al Signor Rossi il messaggio $m = 11$, dopo averlo criptato. Cosa riceverà il Signor Rossi?