1. Calcolare le ultime 10 cifre decimali della 123456789-esima potenza di 123456789. (in altre parole, calcolare $123456789^{123456789}$ modulo 10^{10}).
2. I numeri di Fibonacci Φ_n sono definiti ricorsivamente come segue: $\Phi_1 = 1$, $\Phi_2 = 1$ e $\Phi_{n+1} = \Phi_n + \Phi_{n-1}$ per $n \geq 1$. I primi numeri di Fibonacci sono

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, \ldots$$

   (a) Sia $w = \frac{1+\sqrt{5}}{2}$ e sia $\overline{w} = \frac{1-\sqrt{5}}{2}$. Dimostrare che $\sqrt{5}\Phi_n = w^n - \overline{w}^n$ per ogni $n \geq 1$.
   (b) Calcolare le ultime 10 cifre decimali di $\Phi_{1000000}$. (in altre parole, calcolare $\Phi_{1000000}$ modulo 10^{10}).
3. Sia $n = 7538415671$. Decidere se le classi di congruenza modulo n dei seguenti numeri stanno in $\mathbb{Z}_n^*$ o meno: 56893415, 3674509, 92367458.
4. A partire dalla relazione $62 \cdot 61728 - 97 \cdot 39455 = 1$, calcolare:

$$\gcd(62, 97), \quad \gcd(62, 39455), \quad \gcd(61728, 97), \quad \gcd(61728, 39455), \quad \overline{62}^{-1} \in \mathbb{Z}_{97}.$$

   Quali altri inversi possiamo ottenere?
5. Verificare che $p = 347$ è primo. Calcolare $\varphi(347)$. Enunciare il Piccolo Teorema di Fermat per $p = 347$. Verificarlo per qualche classe a caso $\bar{x} \in \mathbb{Z}_p^*$.
6. Calcolare $\varphi(2011)$. Speriamo che sia un anno fortunato...
7. Fattorizzare $n = 1925$. Calcolare $\varphi(1925)$. Enunciare il Teorema di Lagrange per $\mathbb{Z}_{1925}^*$. Possiamo applicarlo a $\bar{x} = 5$, $\bar{x} = 12$, $\bar{x} = 101$?
8. Sia n un numero naturale e sia p un primo che divide n.
   (1) Verificare che $\varphi(p)$ divide $\varphi(n)$.
   (2) Verificare che se p^2 non divide n, allora $\varphi(n) = \varphi(p)\varphi(\frac{n}{p})$.
   (3) Verificare che se $p \mid \frac{n}{p}$, allora $\varphi(\frac{n}{p}) = \frac{n}{p}\prod_d(1 - \frac{1}{d})$, dove d varia fra i divisori primi distinti di n.
9. Dimostreremo che se p è un numero primo ed $f \in \mathbb{Z}_p[X]$ è un polinomio di grado n a coefficienti in $\mathbb{Z}_p$ (ossia $f(X) = a_nX^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0$, con $a_i \in \mathbb{Z}_p$ e $a_n \neq 0$), allora f ha al più n zeri in $\mathbb{Z}_p$.
   (a) Sia $p > 2$ un primo. Determinare tutti gli zeri di $f(\bar{x}) = \bar{x}^2 - \bar{1} \in \mathbb{Z}_p[X]$.
   (b) Sia $p = 11$. Determinare tutti gli zeri di $f(\bar{x}) = \bar{x}^2 - \bar{1} \in \mathbb{Z}_p[X]$. Determinare tutti gli zeri di $f(\bar{x}) = \bar{x}^2 - \bar{2} \in \mathbb{Z}_p[X]$.
   (c) Verificare che i numeri di Carmichael

$$561, \ 1729, \ 2465, \ 2821, \ 6601, \ 41041, \ 825265, \ 321197185, \ 9746347772161$$

   superano il test di primalità basato sul Piccolo Teorema di Fermat, ma non il test di Miller-Rabin. Prova con
   `http://www.mat.uniroma2.it/~geo2/MRsteps.txt`.
   Perché?
10. Enunciare e verificare il Lemma di Gauss (il Lemma 1 della nota sulla radice primitiva) per $n = 60$.
11. Verificare che $p = 61$ è primo. Quali sono gli ordini possibili per gli elementi $\bar{x} \in \mathbb{Z}_p^*$? Quanti ce ne sono per ogni ordine? (vedi: Osservazione sulla formula di Gauss, nella nota sulla radice primitiva). Che ordine deve avere un generatore di $\mathbb{Z}_{61}^*$?
12. Sia $p = 13$. Quali sono gli ordini possibili per gli elementi $\bar{x} \in \mathbb{Z}_p^*$? Quanti ce ne sono per ogni ordine?(vedi: Osservazione sulla formula di Gauss, nella nota sulla radice primitiva). Determinarli (vedi Lemma 2 della nota sulla radice primitiva).