1. Calcolare la tabella dei numeri primi $p < 100$.

2. Fattorizzare come prodotto di numeri primi i seguenti numeri: 100, 10!, 101, 1001, 10001 e il coefficiente binomiale $\binom{50}{25}$.

3. Per ogni $n \in \mathbf{Z}_{>0}$, determinare $(n-1)!$ modulo n.

4. Sia n un numero naturale di tre cifre in base 10. Supponiamo che $n \equiv 1 \pmod 7$, $n \equiv 2 \pmod{11}$ e $n \equiv 3 \pmod{13}$. Determinare n.

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) Sia $n \in \mathbf{Z}_{>1}$. Dimostrare che le seguenti affermazioni sono equivalenti:
   - n è primo oppure n è un numero di Carmichael.
   - Per ogni divisore primo p di n si ha che p^2 non divide n, ma $p-1$ divide $n-1$.

6. Si consideri la funzione φ di Eulero. Calcolare $\varphi(n)$ per $n = 100$, 10!, 101, 1001, 10001.

7. Sia $p > 2$ un numero primo e sia $k \geq 1$.
   (a) Dimostrare che $\mathbf{Z}_p^*$ è un gruppo ciclico.
   (b) Dimostrare che $H = \{x \in \mathbf{Z}_{p^k}^* : x \equiv 1 \pmod p\}$ è un sottogruppo di $\mathbf{Z}_{p^k}^*$ di p^{k-1} elementi.
   (c) Dimostrare che l'elemento $1 + p$ di H ha ordine p^{k-1}. Dedurne che H è ciclico.
   (d) Dimostrare che $\mathbf{Z}_{p^k}^*$ è un gruppo ciclico.

8. Sia $k \geq 2$.
   (a) Dimostrare che $\mathbf{Z}_2^*$ e $\mathbf{Z}_4^*$ sono gruppi ciclici, ma che $\mathbf{Z}_8^*$ non è un gruppo ciclico.
   (b) Dimostrare che $H = \{x \in \mathbf{Z}_{2^k}^* : x \equiv 1 \pmod 4\}$ è un sottogruppo di $\mathbf{Z}_{2^k}^*$ di 2^{k-2} elementi.
   (c) Dimostrare che l'elemento 5 di H ha ordine 2^{k-2}. Dedurne che H è ciclico.
   (d) Dimostrare che $\mathbf{Z}_{2^k}^*$ è isomorfo a $\mathbf{Z}_{2^{k-2}} \times \mathbf{Z}_2$.

9. Sia $n \in \mathbf{Z}_{>0}$. Dimostrare che $4^n + n^4$ può solo essere primo quando $n = 1$.

10. Dimostrare: se p è primo e $p^2 + 8$ è primo, allora $p^3 + 4$ è primo.

PER I SEGUENTI ESERCIZI È UTILE UN COMPUTER.

11. Sia $n = 7538415671$. Decidere se le classi resto modulo n dei seguenti numeri stanno in $\mathbf{Z}_n^*$ o meno: 56893415, 3674509, 92367458.

12. Calcolare le ultime 10 cifre decimali della 123456789-esima potenza di 123456789 (in altre parole, calcolare $123456789^{123456789}$ modulo 10^{10}).

13. 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}).