PER I SEGUENTI ESERCIZI È UTILE UN COMPUTER.

1. Sia $n = 7538415671$. Decidere se le classi di congruenza modulo n dei seguenti numeri stanno in $\mathbf{Z}_n^*$ o meno: 56893415, 3674509, 92367458.
2. Calcolare le ultime 10 cifre decimali della 123456789-esima potenza di 123456789. (in altre parole, calcolare $123456789^{123456789}$ modulo 10^{10}).
3. 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}).
4. Implementare l'algoritmo ρ di Pollard e usarlo per
   (a) fattorizzare i numeri di Mersenne M_n per $1 \leq n \leq 60$;
   (b) fattorizzare i numeri di Fermat F_n, per $1 \leq n \leq 8$.
5. (Esperimento fattorizzare usando il metodo "$p-1$") Sia $M = 2^3 \cdot 3^2 \cdot 5 \cdot 7$
   (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 divisore $d = \mathrm{mcd}(b-1, n)$ di n ed il cofattore n/d.
   (c) Come mai l'algoritmo trova queste due fattorizzazioni?

Siano dati i numeri

$$n1 = nextprime(10^5) * nextprime(10^{10}), \quad n2 = nextprime(10^6) * nextprime(10^{10}),$$

$$n3 = nextprime(10^7) * nextprime(10^{10}), \quad n3 = nextprime(10^8) * nextprime(10^{10}),$$

$$n5 = nextprime(10^{10}) * nextprime(10^{50}), \quad n6 = nextprime(10^{10}) * nextprime(10^{100}),$$

$$n7 = nextprime(10^{10}) * nextprime(10^{200}), \quad n8 = nextprime(10^{10}) * nextprime(10^{400}).$$

6. Fattorizzare $n1$ ed $n2$ con "trial division". Sulla base del tempo impiegato, esibire degli interi la cui fattorizzazione con tale algoritmo richiede un minuto, un'ora, un giorno, un mese, un anno.
7. Stimare quante iterazioni richiede verosimilmente l'algoritmo di Pollard ρ per fattorizzare i numeri $n1$, $n2, \ldots, n8$.
8. Sia n un numero intero composto di 200 cifre. Dopo 10000 iterazioni l'algoritmo di Pollard ρ non ha trovato nessun fattore. Cosa possiamo concludere?
9. Sia n un numero intero composto di 200 cifre, e sia $B = 10000$. Dopo quante iterazioni dell'algoritmo di Pollard ρ possiamo verosimilmente che escludere che n sia B-smooth ?