

1. Calcolare la tabella dei numeri primi $p < 200$.
 2. Fattorizzare come prodotto di numeri primi i seguenti numeri: 100, 10!, 101, 1001, 10001 e il coefficiente binomiale $\binom{50}{25}$.
 3. (Numeri di Mersenne). Per ogni numero naturale n , si definisce l'ennesimo numero di Mersenne come $M_n = 2^n - 1$.
 - (a) Fattorizzare M_n per $1 \leq n \leq 12$;
 - (b) Dimostrare: se M_n è primo, allora n è primo;
 - (c) Far vedere che il viceversa di (b) non vale;
 (si veda <http://mathworld.wolfram.com/MersenneNumber.html>)
 4. (Numeri di Fermat) Per ogni numero naturale n , si definisce l'ennesimo numero di Fermat come $F_n = 2^{2^n} + 1$;
 - (a) Dimostrare: se $2^m + 1$ è primo, allora m è potenza di 2;
 - (b) Far vedere che F_n è primo per $1 \leq n \leq 4$;
 (si veda <http://mathworld.wolfram.com/FermatNumber.html>)
 5. Per ogni $n \in \mathbf{Z}_{>0}$, calcolare $(n - 1)!$ modulo n .
 6. (Pollard ρ) Sia p un numero primo e $f : \mathbf{Z}_p \rightarrow \mathbf{Z}_p$ la funzione data da $\bar{x} \mapsto \overline{x^2 + 1}$. Per $p = 41$ e 61 disegnare il seguente grafo diretto: i vertici sono le classi $\bar{x} \in \mathbf{Z}_p$. Esiste una freccia da \bar{x} verso \bar{y} se e soltanto se $f(\bar{x}) = \bar{y}$.
 7. 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 .
 8. 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 $\text{mcd}(x, n) = 1$.
 - (a) Dimostrare che 1105 e 1729 sono numeri di Carmichael.
 - (b) Supponiamo che $n \in \mathbf{Z}_{>1}$ abbia la proprietà che per ogni divisore primo p di n si ha che p^2 non divide n , ma $p - 1$ divide $n - 1$. Far vedere che n è primo oppure n è un numero di Carmichael.
 9. Si consideri la funzione φ di Eulero. Calcolare $\varphi(n)$ per i numeri: 100, 10!, 101, 1001, 10001.
 10. Sia n un numero naturale. Dimostrare che $4^n + n^4$ può solo essere primo quando $n = 1$.
 11. 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.*
12. Sia $n = 7538415671$. Decidere se le classi di congruenza modulo n dei seguenti numeri stanno in \mathbf{Z}_n^* o meno: 56893415, 3674509, 92367458.
 13. 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 $1 \leq n \leq 8$.
 14. Calcolare le ultime 10 cifre decimali della 123456789-esima potenza di 123456789. (in altre parole, calcolare $123456789^{123456789}$ modulo 10^{10}).
 15. 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

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, \dots$$
 - (a) Sia $w = \frac{1+\sqrt{5}}{2}$ e sia $\bar{w} = \frac{1-\sqrt{5}}{2}$. Dimostrare che $\sqrt{5}\Phi_n = w^n - \bar{w}^n$ per ogni $n \geq 1$.
 - (b) Calcolare le ultime 10 cifre decimali di $\Phi_{1000000}$. (in altre parole, calcolare $\Phi_{1000000}$ modulo 10^{10}).