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 $\binom{40}{20}$.
3. Sia n un numero naturale. Dimostrare che $4^n + n^4$ può solo essere primo quando $n = 1$.
4. Dimostrare: se p è primo e $p^2 + 8$ è primo, allora $p^3 + 4$ è primo.
5. Per ogni $n \in \mathbf{Z}_{>0}$, calcolare $(n-1)!$ modulo n.
6. (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)
7. (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)
8. Si consideri la funzione φ di Eulero. Dimostrare la formula di Gauss: $\sum_{d|n} \varphi(d) = n$. (nella sommatoria d varia fra i divisori positivi di n)
9. Si consideri la funzione φ di Eulero. Calcolare $\varphi(n)$ per i seguenti numeri: 100, 10!, 101, 1001, 10001.
10. Sia $\mathbf{Z}_n$ l'anello degli interi modulo n e sia $\mathbf{Z}_n^*$ il gruppo degli elementi invertibili di $\mathbf{Z}_n$.
    (a) Scrivere la tavola pitagorica di $\mathbf{Z}_n^*$ per $n = 5$, 8, e 12.
    (b) Dimostrare che si ha $\overline{x}^2 = \overline{1}$ per ogni $\overline{x} \in \mathbf{Z}_{24}^*$.
    (c) Determinare gli interi positivi n che hanno la proprietà che $\overline{x}^2 = \overline{1}$ per ogni $\overline{x} \in \mathbf{Z}_n^*$.
11. (Pollard ρ) Sia p un numero primo e $f : \mathbf{Z}_p \longrightarrow \mathbf{Z}_p$ la funzione data da $\overline{x} \mapsto \overline{x^2 + 1}$. Scegliere p fra 30 e 60 e disegnare il seguente grafo diretto: i vertici sono le classi $\overline{x} \in \mathbf{Z}_p$. Esiste una freccia da $\overline{x}$ verso $\overline{y}$ se e soltanto se $f(\overline{x}) = \overline{y}$.

    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
    (a) fattorizzare i numeri di Mersenne M_n per $1 \leq n \leq 60$;
    (b) fattorizzare i numeri di Fermat F_5, F_6 e F_7.
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

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

    (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}).