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. (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 $1 \le n \le 12$;
   (b) Dimostrare: se M_n è primo, allora n è primo;
   (c) Far vedere che il viceversa di (b) non vale;
   (d) Fattorizzare M_n per $1 \le n \le 40$.

   (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 $1 \le n \le 4$;
   (c) Fattorizzare F_5 e F_6.

   (si veda http://mathworld.wolfram.com/FermatNumber.html)
5. Si consideri la funzione φ di Eulero.
   (a) Calcolare $\varphi(n)$ per i seguenti numeri: 100, 10!, 101, 1001, 10001.
   (b) Determinare n tale che $\varphi(n) < \frac{1}{10}n$.
   (c) Dimostrare la formula di Gauss: $\sum_{d|n} \varphi(d) = n$. (nella sommatoria d varia fra i divisori positivi di n)
6. 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 $\overline{x} \in \mathbf{Z}_n^*$.
7. (Algoritmi fondamentali)
   (a) Dimostrare che per calcolare il mcd di $n, m \in \mathbf{Z}_{>0}$ usando l'algoritmo euclideo, ci vogliono al più $\log(\max(n,m))/\log(2)$ divisioni con resto.
   (b) Sia $n \in \mathbf{Z}_{>0}$. Dimostrare che per calcolare $a^M \pmod{n}$ ci vogliono al più $2\log(M)/\log(2)$ moltiplicazioni in $\mathbf{Z}_n$.
8. 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 $n \ge 1$.
   (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 $n \ge 1$.
   (b) Calcolare le ultime 10 cifre di $\Phi_{1000000}$. (in altre parole, calcolare $\Phi_{1000000}$ modulo 10^{10}).
9. Sia $n = 7538415671$. Decidere se le classi di congruenza modulo n dei seguenti numeri stanno in $\mathbf{Z}_n^*$ o meno: 56893415, 3674509, 92367458.
10. (Esperimento fattorizzare usando il metodo "$p-1$") Sia $M = 10!$
    (a) Sia $n = 95431706263$. Scegliere $\overline{a} \in \mathbf{Z}_n^*$ a caso. Calcolare $\overline{b} = \overline{a}^M \pmod{n}$. Calcolare $\mathrm{mcd}(b-1, n)$.
    (b) Sia $n = 57841557763361$. Scegliere $\overline{a} \in \mathbf{Z}_n^*$ a caso. Calcolare $\overline{b} = \overline{a}^M \pmod{n}$. Calcolare $\mathrm{mcd}(b-1, n)$.
    (c) Come mai si riescono a fattorizzare questi due numeri n in questo modo?