Notazione: Indichiamo con $\log n$ il logaritmo di n in base 2 e con $\ln n$ il logaritmo naturale di n, in base e.

1. Stimare il numero di primi

$$1 \leq p \leq 10^{10}, \qquad 10^{20} - 10^5 \leq p \leq 10^{20} + 10^5.$$

2. Sperimentare col comando `nextprime( )` in Pari/GP.
   (a) Sia $n = 10^{10}$ un numero di 10 cifre. Di quante cifre differisce approssimativamente da n il numero primo successivo?
   (b) Sia $n = 10^{20}$ un numero di 20 cifre. Di quante cifre differisce approssimativamente da n il numero primo successivo?
   (c) Sia $n = 10^{50}$ un numero di 50 cifre. Di quante cifre differisce approssimativamente da n il numero primo successivo?

3. Stimare la probabilità che un numero intero dell'ordine di grandezza di 10^{200} sia primo. Quanti numeri primi possiamo aspettarci all'incirca nell'intervallo $[N - A, N + A]$, con $N = 10^{200}$ ed $A = 10^{20}$? Quante cifre in comune avranno verosimilmente tali primi? Confrontare il risultato costruendo la lista effettiva dei primi nell'intervallo dato e sperimentando col comando *nextprime* in PARI-GP.
   Ripetere con $N = 10^{250}$ ed $A = 10^{50}$.

4. Verificare che i numeri di Carmichael

$$561,\ 1729,\ 2465,\ 2821,\ 6601,\ 41041,\ 825265,\ 321197185,\ 9746347772161$$

   superano il test di primalità basato sul Piccolo Teorema di Fermat, ma non il test di Miller-Rabin.
   Verificare che ognuno soddisfa il criterio di Korselt (fattorizzarlo con PARI-GP e controllare).
   Per Test di Miller-Rabin provare con
   `http://www.mat.uniroma2.it/~geo2/MRsteps.txt`.

5. Costruire un KIT di chiavi $\{N = p \cdot q,\ E, D\}$ per un utente del sistema crittografico RSA, con p, q primi dell'ordine di grandezza di 10^{250} (usare PARI-GP). Spedire all'utente il messaggio

$$m = 10000000000000000000000000000000000000000000000000000000000000000000000012345678907797$$

   dopo averlo criptato.
   Qual è la complessità totale di tutta l'operazione? E scegliendo p, q dell'ordine di grandezza di 10^{300}?

ATTENZIONE: i links ai file vanno ribattuti completamente (col copia-incolla non funzionano).