

Notazione: Indichiamo con $\log n$ il logaritmo di n in base 2 e con $\ln n$ il logaritmo naturale di n , in base e . Alcuni esercizi richiedono PARI/GP.

1. 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^{350} (usare PARI-GP). Spedire all'utente il messaggio

$$m = 1000000$$

dopo averlo criptato. Provate poi a decriptarlo con la chiave segreta.

Qual è la complessità totale di tutta l'operazione? E scegliendo p, q dell'ordine di grandezza di 10^{500} ?

2. Sia n un intero. Supponiamo che per ogni divisore primo p di n valga $p - 1 \mid n - 1$. Allora per ogni a con $\gcd(a, n) = 1$, vale

$$a^{n-1} \equiv 1 \pmod{n}.$$

3. Verificare che i numeri di Carmichael

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

soddisfano le condizioni dell'esercizio precedente (fattorizzarli con PARI-GP e controllare). Verificare che superano il test di primalità basato sul Piccolo Teorema di Fermat, ma non il test di Miller-Rabin (possibilmente ripetuto per basi diverse). Per Test di Miller-Rabin potete usare <http://www.mat.uniroma2.it/~geo2/TEN/MRsteps.txt>.

4. Sia $n = pq$, con p e q primi. Sia $\bar{x}_0 \neq \pm \bar{1}$ un elemento di \mathbb{Z}_{pq}^* che soddisfa $\bar{x}_0^2 = \bar{1}$.
 - (a) Verificare che n non è \bar{x}_0 -pseudoprimo.
 - (b) Determinare x_0 come sopra per $n = 21$.
5. Sperimentare col comando `nextprime()` in Pari/GP.
 - (a) Sia $n = 10^{10} + 47865876$ un numero di 10 cifre. Di quante cifre differisce approssimativamente da n il numero primo successivo?
 - (b) Sia $n = 10^{100} + 47547645$ un numero di 100 cifre. Di quante cifre differisce approssimativamente da n il numero primo successivo?
 - (c) Sia $n = 10^{500} + 6546546457657$ un numero di 500 cifre. Di quante cifre differisce approssimativamente da n il numero primo successivo?

6. Stimare il numero di primi

$$10^{40} - 500 \leq p \leq 10^{40} + 500, \quad 10^{100} - 1000 \leq p \leq 10^{100} + 1000, \quad 10^{100} - 3000 \leq p \leq 10^{100} + 3000.$$

Vai su <http://www.mat.uniroma2.it/~geo2/TEN/Primes.txt> e confronta...

7. Stimare la probabilità che un numero intero a caso 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 $A = 1500$? Quante cifre in comune avranno approssimativamente tali primi? Confrontare il risultato costruendo la lista effettiva dei primi nell'intervallo dato e sperimentando col comando `nextprime` in PARI-GP. Ripetere con $N = 10^{350}$ ed $N = 10^{350} + 7657965$ ed $A = 1500$.