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.

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

1. Stimare il numero di primi

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

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 $A = 10^{10}$? 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 $A = 10^{20}$.

3. Il metodo di fattorizzazione per tentativi (*trial division*) consiste nel dividere un numero intero $n \geq 0$ per tutti i primi $p \leq \sqrt{n}$, in ordine crescente fino a che non si trova un fattore.

- (a) Sia n un intero. Quanti sono approssimativamente i primi $p \leq \sqrt{n}$?
- (b) Qual è la complessità di una divisione di n per un primo $p \leq \sqrt{n}$?
- (c) Verificare che la complessità del metodo di fattorizzazione per tentativi si può stimare come

$$\mathcal{O}(p \log n),$$

dove n è l'intero da fattorizzare e p è il più piccolo fattore di n (usare (a) e (b)).

4. Sia n un intero da fattorizzare. Stimare il numero di operazioni necessarie a fattorizzare un intero n col metodo di fattorizzazione per tentativi ogni volta che n diventa dieci volte più grande (ossia ha una cifra decimale in più): osservare la differenza fra il caso in cui il fattore più piccolo p ha una cifra decimale in più e il caso in cui il quoziente $\frac{n}{p}$ ha una cifra decimale in più (mentre p resta fisso).

Esempio1: <http://www.mat.uniroma2.it/~geo2/naif-exper1.txt>

Esempio2: <http://www.mat.uniroma2.it/~geo2/naif-exper2.txt>

5. Siano dati i numeri

$$n1 = \text{nextprime}(10^5) * \text{nextprime}(10^{10}), \quad n2 = \text{nextprime}(10^6) * \text{nextprime}(10^{10}).$$

Fattorizzare $n1$ ed $n2$ con "trial division". Sulla base del tempo impiegato, esibire degli interi la cui fattorizzazione con tale algoritmo richiede un minuto, un'ora, un giorno, un mese, un anno,....., un secolo.

6. Calcolare $\varphi(2014)$.

7. Per $m = 66, 67, 68$ esibire un numero naturale n tale $\varphi(n) = m$, oppure spiegare che non esiste.

8. Sia n un numero naturale e sia p un primo che divide n .

- (1) Verificare che $\varphi(p)$ divide $\varphi(n)$.
- (2) Verificare che se p^2 non divide n , allora $\varphi(n) = \varphi(p)\varphi(\frac{n}{p})$.
- (3) Verificare che se $p \mid \frac{n}{p}$, allora $\varphi(\frac{n}{p}) = \frac{n}{p} \prod_d (1 - \frac{1}{d})$, dove d varia fra i divisori primi distinti di n .