TEN 2012-2013. Esercizi sugli argomenti delle prime 3 settimane di corso.

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. Sia $n = 7538415671$. Decidere se le classi di congruenza modulo n dei seguenti numeri stanno in $\mathbb{Z}_n^*$ o meno: $56893415,\ 3674509,\ 92367458$.

2. A partire dalla relazione $62 \cdot 61728 - 97 \cdot 39455 = 1$, calcolare:

$$\gcd(62, 97), \quad \gcd(62, 39455), \quad \gcd(61728, 97), \quad \gcd(61728, 39455), \quad \overline{62}^{-1} \in \mathbb{Z}_{97}.$$

   Quali altri inversi possiamo ottenere?

3. Verificare che $p = 347$ è primo. Calcolare $\varphi(347)$. Enunciare il Piccolo Teorema di Fermat per $p = 347$. Verificarlo per qualche classe a caso $\bar{x} \in \mathbb{Z}_p^*$.

4. Calcolare $\varphi(2012)$. Speriamo che sia un anno fortunato...

5. Fattorizzare $n = 1925$. Calcolare $\varphi(1925)$. Esibire qualche elemento di $\mathbb{Z}_{1925}^*$.

6. 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.

7. Stimare il numero di primi

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

8. 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?

9. 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 $A = 10^{50}$.

10. 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`.

11. 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

$$m = 10000000000000000000000000000000000000000000000000000000000000000000000000012345678907797$$

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

12. 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)).

13. 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`

14. Siano dati i numeri

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

    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.