TEN 2009. Esercizi 1. Argomenti settimane 1,2,3.

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

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. Il metodo di fattorizzazione per tentativi consiste nel dividere un numero intero $n \ge 0$ per tutti i primi $p \le \sqrt{n}$, fino a che non si trova un fattore.
   (a) Sia n un intero. Quanti sono approssimativamente i primi $p \le \sqrt{n}$?
   (b) Qual è la complessità di una divisione di n per un primo $p \le \sqrt{n}$?
   (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 fattore più piccolo (usare (a) e (b)).

4. Sia n un intero da fattorizzare. Stimare la complessità (probabilistica) del metodo di fattorizzazione che consiste nel calcolare il massimo comun divisore fra n e un numero a caso $1 \le m \le n$.

5. Sia n un intero da fattorizzare. Stimare come varia 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 piu' e il caso in cui il p resta fisso e il quoziente $\frac{n}{p}$ ha una cifra decimale in più.
   Esempio1: `http://www.mat.uniroma2.it/~geo2/naif-exper1.txt`
   Esempio2: `http://www.mat.uniroma2.it/~geo2/naif-exper2.txt`

6. Sia n un intero da fattorizzare. Stimare come varia il numero di operazioni necessarie a fattorizzare un intero n col metodo di fattorizzazione ρ di Pollard ogni volta che n diventa dieci volte più grande: osservare la differenza fra il caso in cui il fattore più piccolo p ha una cifra decimale in piu' e il caso in cui il p resta fisso e il quoziente $\frac{n}{p}$ ha una cifra decimale in più.
   Esempio1: `http://www.mat.uniroma2.it/~geo2/pollard-exper1.txt`
   N.B.: Nel caso del metodo ρ di Pollard la stima è probabilistica: se ripetiamo il calcolo con gli stessi dati, impieghiamo sempre lo stesso tempo?

7. Siano dati i numeri
$$n1 = nextprime(10^5) * nextprime(10^{10}), \quad n2 = nextprime(10^6) * nextprime(10^{10}),$$
$$n3 = nextprime(10^7) * nextprime(10^{10}), \quad n3 = nextprime(10^8) * nextprime(10^{10}),$$
$$n5 = nextprime(10^{10}) * nextprime(10^{50}), \quad n6 = nextprime(10^{10}) * nextprime(10^{100}),$$
$$n7 = nextprime(10^{10}) * nextprime(10^{200}), \quad n8 = nextprime(10^{10}) * nextprime(10^{400}).$$
   (a) Fattorizzarli col metodo ρ di Pollard.
   (b) Quante iterate dobbiamo aspettarci di fare nei singoli casi?
   (c) Come varia il numero di operazioni necessarie a fattorizzare $n5$, $n6$, $n7$, $n8$?

8. A proposito del metodo ρ di Pollard, vedi anche Esercizi n.4,6,7,8 del foglio Esercizi4.

9. Calcolare $\varphi(2010)$. Speriamo che sia un anno fortunato...

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

11. Fattorizzare $n = 1925$. Calcolare $\varphi(1925)$. Enunciare il Teorema di Lagrange per $\mathbb{Z}_{1925}^*$. Possiamo applicarlo a $\bar{x} = 5$, $\bar{x} = 12$, $\bar{x} = 101$?

12. Dimostreremo che se p è un numero primo ed $f \in \mathbb{Z}_p[X]$ è un polinomio di grado n a coefficienti in $\mathbb{Z}_p$ (ossia $f(X) = a_n X^n + a_{n-1}X^{n-1} + \ldots + a_1 X + a_0$, con $a_i \in \mathbb{Z}_p$ e $a_n \neq 0$), allora f ha al più n zeri in $\mathbb{Z}_p$.
    (a) Sia $p > 2$ un primo. Determinare tutti gli zeri di $f(\bar{x}) = \bar{x}^2 - \bar{1} \in \mathbb{Z}_p[X]$.
    (b) Sia $p = 11$. Determinare tutti gli zeri di $f(\bar{x}) = \bar{x}^2 - \bar{1} \in \mathbb{Z}_p[X]$. Determinare tutti gli zeri di $f(\bar{x}) = \bar{x}^2 - \bar{2} \in \mathbb{Z}_p[X]$.
    (c) 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. Prova con
    `http://www.mat.uniroma2.it/~geo2/MRsteps.txt`.
    Perché?

13. Enunciare e verificare il Lemma di Gauss (il Lemma 1 della nota sulla radice primitiva) per $n = 60$.

14. Verificare che $p = 61$ è primo. Quali sono gli ordini possibili per gli elementi $\bar{x} \in \mathbb{Z}_p^*$? Quanti ce ne sono per ogni ordine? (vedi: Osservazione sulla formula di Gauss, nella nota sulla radice primitiva). Che ordine deve avere un generatore di $\mathbb{Z}_{61}^*$?

15. Sia $p = 13$. Quali sono gli ordini possibili per gli elementi $\bar{x} \in \mathbb{Z}_p^*$? Quanti ce ne sono per ogni ordine?(vedi: Osservazione sulla formula di Gauss, nella nota sulla radice primitiva). Determinarli (vedi Lemma 2 della nota sulla radice primitiva).

16. Sulla teoria di gruppi, anelli, campi, vedi anche Esercizi n. 1, 2, 3, 5, 6, 7, 8 ,9 ,10, 12, 13, 14, 15, 20, 21, 22, 23. Le soluzioni di quasi tutti questi esercizi si trovano su
    `http://www.mat.uniroma2.it/~gealbis/SolEAL08esercizi4.pdf`

17. Sia n un numero naturale e sia p un primo che divide n.
    (1) Verificare che $\varphi(p)$ divide $\varphi(n)$, cioè $\varphi(n) = \varphi(p)\varphi(\frac{n}{p})$.
    (2) 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.

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