TEN 2013-2014. Esercizi sugli argomenti della quarta settimana: il metodo ρ di Pollard.

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. Siano dati i numeri

$$n1 = nextprime(10^5 + 7687) * nextprime(10^{10} + 5587987), \quad n2 = nextprime(10^6) * nextprime(10^{10}),$$

$$n3 = nextprime(10^7 + 687633) * nextprime(10^{10}), \quad n3 = nextprime(10^8) * nextprime(10^{10}),$$

$$n5 = nextprime(10^{10}+5876876)*nextprime(10^{50}+856987608760897), \quad n6 = nextprime(10^{10})*nextprime(10^{100}),$$

$$n7 = nextprime(10^{10}) * nextprime(10^{200}), \quad n8 = nextprime(10^{10} + 760670987) * nextprime(10^{400}).$$

   (a) Fattorizzarli col metodo ρ di Pollard.
   (b) Quante iterate dobbiamo aspettarci di fare nei singoli casi per avere buona probabilita' di successo?
   (c) Qual è la complesssita' (probabilistica) del calcolo per la fattorizzazione di $n5$, $n6$, $n7$, $n8$?

2. Implementare l'algoritmo ρ di Pollard e usarlo per
   (a) fattorizzare i numeri di Mersenne M_n per $1 \leq n \leq 60$;
   (b) fattorizzare i numeri di Fermat F_n, per $1 \leq n \leq 8$.

3. Sia n un numero intero composto di 200 cifre. Dopo 10000 iterazioni l'algoritmo ρ di Pollard non ha trovato nessun fattore. Cosa possiamo concludere?

4. Sia n un numero intero composto di 200 cifre, e sia $B = 10000$. Dopo quante iterazioni dell'algoritmo di Pollard ρ possiamo verosimilmente che escludere che n sia B-smooth (cioè che si decomponga in fattori primi minori o uguali a B, elevati ad opportuni esponenti)?

5. Sia n un intero da fattorizzare. Stimare il numero di operazioni (probabilmente) necessarie a fattorizzare un intero n col metodo 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 quoziente $\frac{n}{p}$ ha una cifra decimale in più (mentre p resta fisso).

   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?

6. 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 $1 \leq m \leq n$.

7. Sia $n = p * q * r$ un intero da fattorizzare, dove $p,\ q,\ r$ sono primi con $p << q << r$. Verificare che l'algoritmo ρ di Pollard individua il fattore piu' piccolo per primo.