TEN 2016. Esercizi 3. Algoritmo per divisioni successive & Pollard ρ.

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. Il metodo di fattorizzazione per divisioni successive (*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)).

2. Sia $n = p * q$ un intero prodotto di due primi, con $p << q$.
   (a) Stimare il numero di operazioni necessarie a fattorizzare n col metodo delle divisioni successive ogni volta che p diventa dieci volte più grande (ossia ha una cifra decimale in più) e q resta fisso.
   (b) Stimare il numero di operazioni necessarie a fattorizzare n col metodo delle divisioni successive ogni volta che q diventa dieci volte più grande (ossia ha una cifra decimale in più) e p resta fisso.
   (c) Verificare le previsioni con PARI/GP

   Caso (a): `http://www.mat.uniroma2.it/~geo2/TEN/TrialDivision1.txt`
   Caso (b): `http://www.mat.uniroma2.it/~geo2/TEN/TrialDivision2.txt`

3. Sulla base del tempo impiegato nel caso (a) dell'esercizio precedente, esibire degli interi la cui fattorizzazione con tale algoritmo richiede un mese, un anno,....., un secolo.

4. Alcuni programmi in PARI/GP che illustrano l'algoritmo ρ di Pollard.

`http://www.mat.uniroma2.it/~geo2/TEN/PollardRo.txt`
`http://www.mat.uniroma2.it/~geo2/TEN/FakePollard-steps.txt`
`http://www.mat.uniroma2.it/~geo2/TEN/PollardVsTrialDivision.txt`
`http://www.mat.uniroma2.it/~geo2/TEN/StartingPtSteps.txt`

5. Implementare l'algoritmo ρ di Pollard in PARI/GP.
   (a) fattorizzare i numeri di Mersenne $M_n = 2^n - 1$ per $1 \leq n \leq 20$;
   (b) fattorizzare i numeri di Fermat $F_n = 2^{2^n} + 1$, per $1 \leq n \leq 8$.

6. Sia $n = p * q$ un intero prodotto di due primi, con $p << q$.
   (a) Stimare il numero di operazioni necessarie a fattorizzare n col metodo ρ di Pollard ogni volta che p diventa dieci volte più grande (ossia ha una cifra decimale in più) e q resta fisso.
   (b) Stimare il numero di operazioni necessarie a fattorizzare n col metodo ρ di Pollard ogni volta che q diventa dieci volte più grande (ossia ha una cifra decimale in più) e p resta fisso.
   (c) Verificare le previsioni con PARI/GP.

Nota: Nel caso del metodo ρ di Pollard la stima è probabilistica: se ripetiamo il calcolo con gli stessi n, p, q, cosa succede?

7. 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 determinare il fattore primo più piccolo di n?

(c) Qual è la complessita' (probabilistica) del calcolo per la fattorizzazione di $n5$, $n6$, $n7$, $n8$?

8. 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?

9. Sia n un numero intero composto di 200 cifre, e sia $B = 10000$. Dopo quante iterazioni dell'algoritmo di Pollard ρ andate a vuoto possiamo concludere che n non ha neanche un fattore primo minore o uguale a B?

10. 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 $1 \leq m \leq n$.

11. 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.