
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. Esperimenti con l'algoritmo ρ di Pollard: l'algoritmo generalmente spezza n nel prodotto del fattore più piccolo e il cofattore. La seconda versione fa lo stesso, e mostra il numero di iterate che hanno portato alla fattorizzazione. Notare che per individuare un fattore p , sono generalmente necessarie circa $\sqrt{p}$ iterate.

<http://www.mat.uniroma2.it/geo2/TEN/PollardRo.txt>

<http://www.mat.uniroma2.it/geo2/TEN/StartingPtSteps.txt>

- (a) Fattorizzare completamente il numero $n = 2107971466920603317676768413248655563326842644339$.
 - (b) Far girare l'algoritmo diverse volte: osservare che cambierà il punto iniziale, ma il numero delle iterate che producono un dato fattore avrà ogni volta all'incirca lo stesso numero di cifre.
2. Esperimenti con l'algoritmo $p - 1$ di Pollard <http://www.mat.uniroma2.it/geo2/TEN/pminus.txt>

- (a) L'intero

$$n = 10921275661953631228863996056455028253656397801562459096859$$

non ha probabilmente fattori primi p con $p - 1$ B -smooth, per $B = 100$. Aumentare B fino a dove è possibile, per determinare qualche fattore di n ...

- (b) Mostrare che $n = 2738529615166975764002789390120116356442544395246780752385913842699248259497469$ è il prodotto di quattro fattori primi p , con $p - 1$ di diversi ordini di smoothness. Aumentare B a partire da $B = 30$, fino a fattorizzare completamente n .
 - (c) Verificare che $n = 2047$ ha tutti i fattori primi p con $p - 1$ 11-smooth. Verificare che questi fattori non si possono separare con l'algoritmo $p - 1$, cambiando B .