

Informazioni sull'Eseguibile relativo a due algoritmi per la fattorizzazione di un numero

L'eseguibile presenta due semplici algoritmi per la scomposizione di un numero N in due fattori. Qui di seguito vengono illustrate sinteticamente le loro prestazioni e limitazioni.

Il primo algoritmo utilizzato è quello proposto recentemente (febbraio 2009) dal Prof. Di Noto in un suo articolo.

Il secondo algoritmo è quello classico di Fermat, illustrato insieme al primo algoritmo in un altro articolo (11 marzo 2009) sempre del Prof. Di Noto.

Per entrambi gli algoritmi è preferibile per una corretta utilizzazione dell'eseguibile che il numero N sia un numero dispari.

Risultano poi le seguenti ulteriori limitazioni:

- i due fattori trovati non sempre sono primi, per cui in tale caso per effettuare la scomposizione completa del numero in fattori primi bisogna procedere ulteriormente;
- poiché i calcoli vengono effettuati con una aritmetica limitata alla doppia precisione, se risultati ottenuti eccedono il valore di 10^{15} si possono avere su di essi degli arrotondamenti che portano ad avere valori errati; ciò può succedere se il numero N è sufficientemente grande (maggiore di 10^9), ma soprattutto se il numero di tentativi effettuati risulta molto alto (decine di milioni).
- i tempi di calcolo possono risultare lunghi se il numero N è grande e per di più primo.