

OSSERVAZIONI su l'articolo FATTORIZZAZIONE VELOCE E IL PROBLEMA P =NP...

Leggendo l'articolo FATTORIZZAZIONE VELOCE E IL PROBLEMA P =NP..., nei riguardi dell'algoritmo della Fattorizzazione Veloce (chiamato FV nel seguito per comodità di esposizione), proposto ed illustrato nell'articolo per la scomposizione di numeri composti da due soli fattori primi, c'è da sottolineare, come del resto messo in evidenza nell'articolo, che la sua maggiore efficienza si limita solo per i numeri composti formati da due soli fattori primi, abbastanza vicini fra di loro.

Si deve subito osservare tuttavia che, se si volesse scomporre in generale un numero qualsiasi, non si sa a priori se esso rientra nella categoria dei numeri sopraddetti, per cui risulta sempre più opportuno utilizzare almeno per numeri non grandi il tradizionale algoritmo delle Divisioni Successive (Trial Division algorithm).

In effetti nella maggior parte dei casi i numeri da scomporre non rientrano nella suddetta categoria e per essi la loro fattorizzazione con l'algoritmo FV verrebbe effettuata con tempi più lunghi rispetto ai tempi che si hanno utilizzando l'algoritmo delle Divisioni Successive.

Se si volesse poi cercare di scomporre con l'algoritmo FV un numero effettivamente primo i tentativi risulterebbero illimitati e vani.

Si vuole fare presente che nella letteratura tecnica si ha a disposizione un altro algoritmo classico simile all'algoritmo FV, preposto anch'esso sostanzialmente alla scomposizione di numeri composti da due fattori primi con valori abbastanza vicini fra di loro, ed è quello noto con il nome di algoritmo di Fermat (FERMAT).

Utilizzando questo algoritmo si è potuto constatare che esso risulta ancora più efficiente dell'algoritmo FV almeno per i numeri che sono stati posti a verifica e che vengono riportati più avanti.

Per quel che riguarda l'argomento della Crittografia e dell'algoritmo RSA, a cui si fa riferimento nell'articolo, anche per un rapporto fra i due numeri primi scelti q e p compreso tra 1 e 2 il valore della differenza $(q - p)$, ammesso che tale differenza non sia veramente minima, per numeri $n = p \cdot q$ di 300 cifre (e quindi q e p ciascuno di 150 cifre) risulta essere così grande da scongiurare l'utilizzo di algoritmi del tipo FV o di FERMAT.

Ma supposto pure che la differenza $(q - p)$ sia effettivamente molto piccola, allora si avrebbe $p \approx \sqrt{n}$ per cui il numero n potrebbe essere fattorizzato in modo efficiente semplicemente provando per mezzo dell'algoritmo delle Divisioni Successive solo gli interi dispari vicini a \sqrt{n} . L'utilizzo di questo algoritmo in questo caso sembrerebbe pertanto preferibile all'algoritmo FV od a quello di FERMAT.

Alcuni ESEMPI relativi alla fattorizzazione con l'algoritmo FV e l'algoritmo di FERMAT

N = 12319: con l'algoritmo FV si devono effettuare 15 tentativi per riuscire a scomporre il numero $N = 12319$ nei suoi due fattori 97, 127; utilizzando invece l'algoritmo FERMAT sono sufficienti solo 2 tentativi per scomporlo (si veda la seconda pagina di questa nota)

N = 30053021: per trovare i suoi fattori 5003, 6007 con FV occorrono 565 tentativi;
con FERMAT sono sufficienti 23 tentativi.

N = 4053962251: per scomporlo nei suoi due fattori 63029 e 64319 con FV sono necessari 645 tentativi
con FERMAT sono sufficienti 4 tentativi

N = 37241: per trovare i suoi fattori 167, 223 con FV occorrono 28 tentativi
Con FERMAT sono sufficienti 3 tentativi

N = 34241: per trovare i suoi fattori 97, 1153 con FV occorrono 128 tentativi
con FERMAT sono sufficienti 40 tentativi

N = 2652511009: per trovare i suoi fattori 51001, 52009 con FV occorrono 504 tentativi
con FERMAT sono sufficienti 3 tentativi

N = 4488139001 per trovare i suoi fattori 51001, 88001, con FV ci sono voluti 18500 tentativi
con FERMAT ci sono voluti 2508 tentativi

Per il numero N= 12319 si mostrano i risultati completi utilizzando l' ESEGUIBILE relativo all' algoritmo FV , e all' algoritmo di FERMAT,
(per avere disponibile L'ESEGUIBILE si sono realizzati due opportuni programmi in linguaggio Qbasic, uno per l' algoritmo o FV , l' altro per l' algoritmo di FERMAT, costituiti ciascuno da un massimo di 15 righe di istruzioni).

FATTORIZZAZIONE DI $N = p * q$

ATTENZIONE : accertarsi che il numero N non sia primo e che non sia composto da più di due fattori

===== algoritmo FV =====

N? 12319

k	k ²	N+k ²	s = sqrt(N+k ²)
1	1	12320	110.9954954040929
2	4	12323	111.009008643443
3	9	12328	111.0315270542561
4	16	12335	111.0630451590447
5	25	12344	111.1035552986492
6	36	12355	111.1530476415289
7	49	12368	111.2115101956628
8	64	12383	111.2789288230256
9	81	12400	111.3552872566004
10	100	12419	111.4405671198779
11	121	12440	111.5347479487895
12	144	12463	111.6378072160144
13	169	12488	111.7497203575919
14	196	12515	111.8704608017684
15	225	12544	112

 $p = s \bullet k = 112 \bullet 15 = 97$ $q = s + k = 112 + 15 = 127$

$N = 97 * 127 = 12319$

numero di tentativi:= 15 tempo di calcolo: 0 sec

===== algoritmo di FERMAT =====

N ? 12319

$r = \text{int}(\text{sqr}(N)) = 110$

h	x = r+h	(r+h) ² - N	z = sqrt ((r+h) ² - N)
1	111	2	1.414213562373095
2	112	225	15

 $p = x \bullet z = 112 \bullet 15 = 97$ $q = x + z = 112 + 15 = 127$

$N = 97 * 127 = 12319$

numero di tentativi:= 2 tempo di calcolo: 0 sec