

L'algoritmo di Fermat e il nostro algoritmo

$N + d^2 = s^2$, da cui esso deriva: $s = (\sqrt{N + i})^2$,
con $i \approx \sqrt{d}$.

Circa il nostro algoritmo

$$N + d^2 = s^2 \quad (1)$$

da cui $p = s - d$ e $q = s + d$

esposto nel nostro ultimo lavoro “Fattorizzazione veloce e problema P = NP) recentemente pubblicato sul nostro sito, abbiamo saputo solo ora, dalle “Osservazioni sull’articolo Fattorizzazione veloce e problema P =NP) dell’ing. Cristiano Teodoro. Carolla (vedi Lavori dell’Ing. Teodoro”), dell’algoritmo di Fermat, al quale anche noi eravamo recentemente arrivati e indipendentemente dallo stesso Fermat, pur non conoscendolo. Esso è descritto nella voce di Wikipedia “Metodo della fattorizzazione di Fermat” alla quale rimandiamo. La nostra versione, pur non essendo stata accennata nel nostro lavoro (per essere oggetto di eventuali lavori successivi), consiste nella

formula accennata nel titolo:

$$s = \sqrt{(N + i)^2} \quad (2)$$

dove i non è però la nota unità immaginaria dei numeri quanto più piccola è la differenza $q - p$. Se $q-p = 0$, anche $i = 0$. Tale algoritmo è comunque molto più veloce della (1), come ha mostrato l'ing. Teodoro nelle sue "Osservazioni..." sopra accennate.

Abbiamo scoperto che se il rapporto q/p è circa 2, $i \approx \sqrt{p/2}$, e proporzionalmente minore se il rapporto q/p è inferiore a 2. Il che significa che la difficoltà computazionale, per numeri p e q di questo tipo, passa dal numero di cifre di p al numero di cifre di $i \approx \sqrt{p/2}$, con quindi circa metà delle cifre che compongono p . Facciamo un solo esempio :

$N = p \times q = 127 \times 229 = 29083$, con $q/p = 229/127 = 1,80 \approx 2$, e con semidifferenza:

$(q-p)/2 = (229-127)/2 = 102/2 = 51$ (due sole cifre invece delle tre di $p = 127$).

Con la (1) occorrono 51 tentativi per trovare s ,
 poiché $N + 51^2 = 29083 + 2601 = 31684 = 178^2$
 da cui poi $p = 178 - 51 = 127$ e $q = 178 + 51 = 229$,
 ora, con la (2) ne occorrono $i = 8 \approx \sqrt{51}$ tentativi,
 poiché, essendo $\sqrt{29083} = 170,53$ e 170 intero
 otteniamo, dopo soli 8 tentativi, il quadrato perfetto

$$178^2 = 31684, \text{ infatti}$$

$$s = \sqrt{(170 + 8)^2} = \sqrt{178^2} = \sqrt{31684}, \text{ con } 8 \approx \sqrt{51} = 7,14$$

Nell'esempio dell'ing. Teodoro, invece:

$$p = 97, q = 127 \text{ con differenza } 127 - 97 = 30$$

(e rapporto = $q/p = 127/97 = 1,30$, inferiore a 2 e a 1,80 dell'esempio precedente) e $d = 30/2 = 15$, con $\sqrt{15} = 3,8$. Applicando ora la (1), abbiamo

$$N = 97 \times 127 = 12319, \sqrt{12319} = 110,99,$$

$$\text{intero } 110; s = \sqrt{(110+2)^2} = \sqrt{12544} = 112,$$

$$\text{da cui } d = \sqrt{(12544 - 12319)} = \sqrt{225} = 15$$

$$\text{con } p = 112-15 = 97 \text{ e } q = 112 + 15 = 127$$

in questo esempio $i = 2$, con $2 < 3,8 = \sqrt{d} = \sqrt{15}$.

“2 soli tentativi invece che con i 15 tentativi che con la (1), molto efficiente solo se d è molto piccola, per esempio con i numeri gemelli ($d = 1$) o molto vicini ($d = 2, 3, 4$, ecc.) . Per differenze un po' più grandi è molto meglio la (2), cioè l'algoritmo di Fermat, come nei due esempi sopra riportati. Poiché i numeri RSA hanno un rapporto generalmente minore di 2, la (2) potrebbe essere molto efficace, e tanto più quanto tale rapporto tende a 1, e quindi d tende a 0.

Ma per questo tipo di numeri è ancora meglio il “Crivello quadratico” (vedi Wikipedia) con il quale nel 1994 è stato fattorizzato il numero RSA -129, composto da 129 cifre in base dieci.

Rispetto all’algoritmo di Fermat, la nostra sola novità ora è che $i \approx \sqrt{d}$, per numeri primi p e q con basso rapporto. Se si potesse calcolare in qualche modo, anche approssimativamente, la differenza D tra q e p partendo solo da $N = p \times q$, e quindi anche la semidifferenza $d = D/2$, si potrebbe avere facilmente $i \approx \sqrt{d}$, diminuendo ancora il numero dei tentativi permessi dall’algoritmo di Fermat, e ottenere così una fattorizzazione ancora più efficace e veloce, magari al livello ottenibile con il crivello quadratico di Carl Pomerance.

Gruppo ERATOSTENE

Riferimenti

1. “Fattorizzazione veloce e problema $P = NP$ ”
(Gruppo Eratostene)
2. “Osservazioni sull’articolo Fattorizzazione veloce e problema $N = NP$ ” (Ing. Cristiano Teodoro)
3. Wikipedia, “Metodo di fattorizzazione di Fermat”
4. Wikipedia, “Crivello quadratico”