

Appunti sulla futura fattorizzazione del numero RSA-190 e di altri numeri RSA (previsioni sulla probabile grandezza di p in base alla congettura sui numeri RSA)

oooooooooooooooo

Gruppo Eratostene

Abstract

The **number RSA -190** is not factorized. In this paper an our prevision on probable approximated values of p and q.

Il **numero RSA-190** è il più piccolo numero non ancora fattorizzato . Con la nostra congettura sui numeri RSA (Rif.1), secondo la quale p si trova, per i numeri RSA, sempre tra $n/2$ ed n con $n = \sqrt{N}$, e molto spesso anche prossimo alla loro media :

$$p \sim (n/2 + n)/2$$

possiamo stabilire, sia pure in modo approssimativo ma attendibile, la probabile grandezza del fattore p , risparmiando notevolmente sul tempo di calcolo. Ecco come:

Il numero RSA -190 è il seguente (Rif.2):

RSA-190 [\[modifica\]](#)

RSA-190 è il più piccolo dei numeri RSA a non essere stato fattorizzato.

RSA-190 =

1907556405060696491061450432646028861081179759533184460647975622318915025587
1841757540549761551215932934922604641526300932385092466032074171247261215808
58185985938946945490481721756401423481

Poiché 190 è un numero pari di cifre, per una nota regola delle radici quadrate (chi la sa calcolare ancora manualmente sicuramente la ricorderà), togliendo un numero pari di cifre a partire dalla fine, rimarranno sole le prime quattro cifre iniziali, che formeranno il numero 1907, la cui radice quadrata avrà le stesse cifre iniziali di RSA -190:

$$N^p = 1907 \quad n = \sqrt{1907} = 43,66 \quad n/2 = 43,66/2 = 21,83\dots$$

$$n/2 > p < n, \quad 21,83 > p < 43,66$$

$$p \sim (n/2 + n)/2 = (43,66 + 21,83)/2 = 65,49 / 2 = 32,74$$

quindi per RSA -190 p sarà un numero compreso tra 21... e 32... e seguito da $(190 - 1) / 2 - 2 = 92,5$ cifre (valore stimato, valore reale 92 oppure 93 cifre (questo perché la radice quadrata di un numero è lunga circa la metà delle sue cifre, meno le prime due cifre già considerate (tra 21 e 32); facendo un'ulteriore media

avremo

$$p' \sim (21,83 + 32,74)/2 = 27,28$$

il che significa che p potrebbe cominciare con **27...** (o un numero molto vicino, 26... o 28...), seguito da 92 o 93 cifre.

Per fattorizzare RSA -190, quindi, si suggerisce di testare solo tutti i numeri primi di 92 cifre che cominciano per 21... (trascurando tutti i numeri precedenti, con notevole risparmio di tempo di calcolo), fino a quando, intorno a **27...**, (oppure anche **28...** o meglio ancora **29...** (vedi *Nota* finale) si troverà il valore reale di p tale che:

$$N / p = q, \quad \text{con } N = \text{RSA-190}$$

Di conseguenza, q sarà approssimativamente

$$q \sim N / 27... \sim 70... \quad (\text{o anche da } 68... \text{ a } 65...$$

se dividiamo 1907... per **28...** e per **29...**)

Quando tale numero sarà fattorizzato con altri metodi e relativi algoritmi, avremo un'ulteriore conferma della nostra congettura sui numeri RSA, che nel frattempo cercheremo di dimostrare

con ulteriori lavori.

Circa qualche numero RSA già fattorizzato, possiamo verificarla rapidamente ; per esempio con:

RSA-576 [\[modifica\]](#)

RSA-576 è stato fattorizzato il 3 dicembre **2003** da J. Franke e T. Kleinjung all'[Università di Bonn](#), usando il Crivello dei campi di numeri.^{[18][19][20]}

La fattorizzazione di RSA-576 è la seguente:

```
RSA-576 =  
18819881292060796383869723946165043980716356337941738270076335642298885971523466  
5485319  
  
06060650474304531738801130339671619969232120573403187955065699622130516875930765  
0257059  
RSA-576 =  
39807508642406493739712550055038649119906436234252670840638518957594638895726176  
8583317  
×  
47277214610743530253622307197304822463291469530209711645985217113052071125636359  
0397527
```

(l'evidenziazione in **rosso** delle prime **due** cifre di p e q è nostra)

Con la nostra congettura, abbiamo

$$N = 1881; n = 43,37; n/2 = 21,68; p \sim (43,37 + 21,68) / 2 = \mathbf{32,52}$$

Questa volta il valore reale di $p = \mathbf{3980}...$ è maggiore della media

$32,52 = \mathbf{3252}.....$, ma sempre compreso tra $\mathbf{2168} = N/2$ e

$$\mathbf{4337} = \sqrt{N}.$$

Un altro esempio:

“ **RSA-200** [\[modifica\]](#) ”

RSA-200 è stato fattorizzato il 9 maggio [2005](#) da F. Bahr, M. Boehm, J. Franke, e T. Kleinjung della Bundesamt für Sicherheit in der Informationstechnik (BSI). La potenza di calcolo utilizzata è paragonabile a quella di 75 anni di lavoro su un PC basato su processore Opteron a 2,2 Ghz. [\[25\]\[26\]](#)

La fattorizzazione di RSA-200 è la seguente:

```

RSA-200 = 2799783391122132787082946763872260162107044678695
          5428537560009929326128400107609345671052955360856
          0618223519109513657886371059544820065767750985805
          57613579098734950144178863178946295187237869221823983
RSA-200 =
3532461934402770121272604978198464368671197400197625023649303468776121253679
          423200058547956528088349
          ×
7925869954478333033347085841480059687737975857364219960734330341455767872818
          152135381409304740185467
  
```

Abbiamo :

$$N = 2799... \quad n = 52,90 \quad n/2 = 26,45 \quad p \sim (52,90 + 26,45)/2 = 39,67$$

Quindi p sarà compreso tra 2645... e 5290..., e molto probabilmente vicino a 3967... infatti in questo caso abbiamo p reale = 35324619.... (vedi sopra i fattori reali di RSA -200), e naturalmente compreso, secondo la nostra congettura , tra 2645 e 5290...., ma anche prossimo alla seconda media p' (come per RSA – 190):

$$p' = (26,45 + 39,67)/2 = 33,06 \sim 35,32 = 3532... \text{ valore reale}$$

Conclusion

La nostra congettura sui numeri RSA potrebbe quindi aiutare non poco nella fattorizzazione dei numeri RSA ancora non fattorizzati.

Attendiamo conferme dalla futura fattorizzazione di tali numeri con altri metodi ma anche con l'eventuale aiuto della nostra congettura, per poi fare dei confronti tra i fattori p e q reali e le nostre suddette previsioni sulla probabile grandezza di p per ognuno dei numeri RSA sopra elencati.

Caltanissetta 15.11.2010

Riferimenti

- 1) Congettura sui numeri RSA, in sezione “Articoli sulla fattorizzazione”
- 2) “Numeri RSA” da omonima voce di Wikipedia
- 3) “News” SET. 2010, in rubrica NEWS, che qui riportiamo integralmente:

“SET 2010

Fattorizzato di recente (notizia del 7.1.2010) il numero RSA -768. Ne parla il Dott. Armando Leotta in “Il taccuino di Armando Leotta” (sul web).

RSA a 768 bit fattorizzato. Avanti il prossimo - gen 17th, 2010 by ArMyZ.

RSA-768: è di questi giorni la notizia della fattorizzazione del numero di 768 bit, 232 cifre decimali su cui si basa il modulo 768-bit dell'RSA. Un successo, visto che era nella Challenge list dell'RSA. L'approccio utilizzato è il Morrison-Brillhart. Alcune considerazioni. Il modulo a 768-bit, ovviamente, non è più raccomandato specie per le implementazioni prossime. Dando uno sguardo alle velocità con cui siamo passati dalla fattorizzazione del modulo a 512-bit (1999) a quello a 768-bit si ritiene che in una decade si possa arrivare a fattorizzare anche il numero (chiave) a 512-bit (number field sieve factoring method). Per gli addetti ai lavori, è possibile approfondire scaricando il paper. La sola attività di identificazione degli interi (number field sieve) appropriati ha comportato uno sforzo computazionale equivalente a 1500 anni di elaborazione con un core di un opteron a 2.2 GHz ed ha prodotto oltre 5 TB di dati. Nessuno sconvolgimento quindi, ma solo un gran bel risultato che aiuta il phasing out del modulo con chiave a 1024-bit previsto proprio nel 2010.

Nostro commento: un altro passo avanti per la crittografia, e interessante per gli appassionati

dell'argomento. Prima o poi tutti i numeri RSA della Challenge list saranno fattorizzati, e i numeri di grandezza simili (poco oltre 200 cifre decimali) saranno fattorizzabili con lo stesso sistema; inoltre, nuovi eventuali e possibili progressi teorici sulla fattorizzazione veloce potrebbero mettere in crisi il sistema RSA, che dura indisturbato da circa quarant'anni, e con esso anche la sicurezza informatica (banche, Internet, servizi segreti, ecc.) Sarebbe ora che la Società che gestisce la crittografia RSA pensasse a sistemi alternativi e ovviamente ancora più sicuri, usando ancora i numeri primi, oppure altri tipi di numeri eventualmente più adatti allo scopo.

Nota

Il numero RSA - 190 è uno di quegli speciali numeri con rapporto

$q/p \sim 2,25$, per i quali vale la relazione

$$p \sim 2n/3 \quad e \quad q \sim 3n/2$$

Essendo la radice quadrata di RSA - 190 $n \sim 4366\dots$

e 43,66 la radice quadrata del numero 1907 (le prime quattro cifre di RSA - 190) e $1943 = 29*67$ con $n = 44,07 \sim 4366\dots$ un

semiprimo vicino alle prime quattro cifre 1907...(con rapporto

$67/29 = 2,31 \sim 2,25$ abbiamo che

$$p = 2n/3 \sim 44,07*2/3 = 88,14/3 = 29,38 \sim 29, \quad e$$

$$q = 3n/2 = 44,07*3/2 = 132,21/2 = 66,05 \sim 67$$

Allo stesso modo, essendo simile il rapporto $q/p \sim 2,31$ il numero

RSA -190, per $n = 4366\dots = \sqrt{1907}\dots$ abbiamo ora

$$p \sim 2n/3 = 4366\dots*2/3 = 8732\dots/3 = 2910\dots \quad e$$

$$q \sim 3n/2 = 4366... * 3/2 = 13098.../3 = 6549...$$

Ecco perché il fattore p di RSA -190 potrebbe benissimo cominciare con le cifre **29**10.... e il fattore q con **65**49... o giù di lì, analogamente a come $1943 = 29 * 67$, essendo simili i due rapporti q/p. Per $1943 = 29 * 67$ è stato facile calcolarlo in modo esatto con

$$67/29 = 2,31$$

mentre per RSA 190 no, non conoscendo ancora i valori reali di p e q, ma abbiamo approssimativamente

$$65.../29... \sim 2,24)$$

stima approssimativa con un semiprimo (1943) prossimo alle prime quattro cifre di RSA -190, e con questa stima poi calcolare la probabile grandezza di p e q, riducendo a circa il 2% il tempo di calcolo con gli algoritmi tradizionali. Non è molto, ma nemmeno poco. Per fattorizzare il numero RSA – 190 sarebbe bene quindi provare prima, con gli algoritmi attualmente disponibili (in attesa dei computer quantistici, che riducono di 10 000 volte il tempo di

calcolo), tutti i numeri primi che cominciano con **29**... (il loro numero è di 5 seguito da 81 cifre...più delle particelle dell'universo, stimate in 10^{80}) : con un po' di fortuna, tra di essi si potrebbe trovare p , senza quindi dover provare con **28**...o con **30**... seguiti da altre 93 cifre ($190/2$ meno le due cifre 2 e 9 di **29**...)

Per quanto riguarda la congettura di Goldbach per questi casi particolari, la loro somma sarebbe di circa **2,16** volte la radice quadrata, e quindi:

$$4366... * 2,16 = 9430... \quad (\text{con } 2/3 = 0,66 \text{ e } 3/2 = 1,5)$$

$$\text{essendo } p \sim 2n/3 = n * 0,66... \sim 4366 * 0,66 \sim 2881... \sim 29... \text{ e}$$

$$q \sim 3n/2 = n * 1,5 \quad \sim 4366 * 1,5 = 6549...$$

$$\text{e } p + q = 2881... + 6549... = 9430..., \text{ e } 0,6 + 1,5 = 2,16$$

Per esempio , nel caso del semiprimo $1943 = 29 * 67$ simile per rapporto $q/p = 2,31$ al numero RSA -190, abbiamo $29 + 67 = 96$ simile a **9430** come cifra iniziale (abbiamo **96** un po' più grande di **9430** poiché anche **1943** è un po' più grande di **1907**...)

$$e p = \mathbf{29} \sim 44,07 * 0,66... = 29,08 \sim \mathbf{29}$$

$$q = \mathbf{67} \sim 44,07 * 1,5 = 66,10 \sim \mathbf{67}$$

Per ora è però ancora difficile usare la somma $S = p + q$ come un valido aiuto alla fattorizzazione di un prodotto $N = p * q$.