TAVOLE ARITMETICHE PER ALCUNE CONGETTURE E TEOREMI SUI NUMERI PRIMI (Goldbach, Goldbach debole, Polignac, Teorema fondamentale della fattorizzazione. Possibili connessioni con la crittografia RSA)

Francesco Di Noto, Michele Nardelli

Abstract

In this paper we show some arithmetic Tables on some conjecture or theorem about prime numbers: strong Goldbach, weak Goldbach, Polignac, and so on)

Riassunto

In questo lavoro esporremo delle tavole aritmetiche (di addizione, differenza, moltiplicazione (come la vecchia

Tavola pitagorica) , rapporto, a sostegno della verità delle congetture e teoremi di cui al titolo

°°°°°°°°°°°°°°°

Per comprendere meglio le suddette congetture e teoremi e la loro verità, e a sostegno delle recenti dimostrazioni ufficiali , useremo delle tabelle aritmetiche riguardanti i numeri primi,

Con accenno alle conseguenze per la crittografia RSA

Tabelle

Congettura forte di Goldbach **(Rif.1)**

TABELLA 1

		p	p	p	c	p	p	c	p	p	c	
	d, d,,	3	5	7	9	11	13	15	17	19	21	
p	3	6	8	10	12	14	16	18	20	22	24	…
p	5	8	10	12	14	16	18	20	22	24	26	…
p	7	10	12	14	16	18	20	22	24	26	28	…
c	9	12	14	16	18	20	22	24	26	28	30	…
p	11	14	16	18	20	22	24	26	28	30	32	…
p	13	16	18	20	22	24	26	28	30	32	34	…
c	15	18	20	22	24	26	28	30	32	34	36	…
p	17	20	22	24	26	28	30	32	34	36	38	…
p	19	22	24	26	28	30	32	34	36	38	40	…
c	21	24	26	28	30	32	34	36	38	40	42	…
	…	…	…	…	…	…	…	…	…	…	…	

TABELLA 2

	2	3	5	7	11	13	17	19	23	29	...
2	4										
3		6	8	10	14	16	20	22	26	32	...
5		8	10	12	16	18	22	24	28	34	...
7		10	12	14	18	20	24	26	30	36	...
11		14	16	18	22	24	28	30	34	40	...
13		16	18	20	24	26	30	32	36	42	...
17		20	22	24	28	30	34	36	40	46	...
19		22	24	26	30	32	36	38	42	48	...
23		26	28	30	34	36	40	42	46	52	...
29		32	34	36	40	42	46	48	52	58	...
...		...	...	...	...	...	...	...	...	...	...

Da Rif. 2; possibilmente riprese da Rif. 1, oppure sono scoperte indipendenti:

TABELLA 3

	3	5	7	11	13	17	19	23	29
3	6	8	10	14	16	20	22	26	32
5		10	12	16	18	22	24	28	34
7			14	18	20	24	26	30	36
11				22	24	28	30	34	40
13					26	30	32	36	42
17						34	36	40	46
19							38	42	48
23								46	52
29									58

TABELLA 4

	3	5	7	11	13	17	19	23	29	31	37	41	43	47	53
3	6	8	10	14	16	20	22	26	32	34	40	44	46	50	56
5		10	12	16	18	22	24	28	34	36	42	46	48	52	58
7			14	18	20	24	26	30	36	38	44	48	50	54	60
11				22	24	28	30	34	40	42	48	52	54	58	64
13					26	30	32	36	42	44	50	54	56	60	66
17						34	36	40	46	48	54	58	60	64	70
19							38	42	48	50	56	60	62	66	72
23								46	52	54	60	64	66	70	76
29									58	60	66	70	72	76	82
31										62	68	72	74	78	84
37											74	78	80	84	90
41												82	84	88	94
43													86	90	96
47														94	100
53															106

Per la crittografia RSA, vedi congetture e Tabelle successive

Congettura debole **(Rif. 3)**

(TAVOLA DI ADDIZIONE DEI NUMERI PARI E DEI NUMERI PRIMI PER CONGETTURA DEBOLE DI GOLDBACH (NUMERI DISPARI COME SOMMA DI TRE PRIMI)

(Additive table about weak Goldbach conjecture)

(in corso di pubblicazione)

TAVOLA DI ADDIZIONE PARI P E PRIMI p

TABELLA 5

P/p	*3*	*5*	*7*	*11*	*13*	*17*	*19*	*23*	*29*	*31*
4	7	9	11	15	17	21	23	27	33	35
6	9	11	13	17	19	23	25	29	35	37
8	11	13	15	19	21	25	27	31	37	39
10	13	15	17	21	23	27	29	33	39	41
12	15	17	19	23	25	29	31	35	41	43
14	*17*	*19*	*21*	*25*	*27*	*31*	*33*	*37*	*43*	*45*
16	19	21	23	27	29	33	35	39	45	47
18	21	23	25	29	31	35	37	41	47	49
20	23	25	27	31	33	37	39	43	49	51
22	25	27	29	33	35	39	41	45	51	53
...	....	...	...	...	...	...	...	...	...	...

Come possiamo notare, al crescere della tabella vengono fuori, anche più volte , tutti i numeri dispari maggiori di 7, come richiede la dimostrazione della congettura.

Per la crittografia RSA, vedi congetture e Tabelle successive

La congettura di Polignac **(Rif. 4): (in rosso le differenze tra due primi consecutivi, 2 ovviamente per i numeri primi gemelli; in blu i numeri cugini, per differenza 4, in marrone per i numeri sexy, con differenza 6.**

La tabella è simmetrica rispetto alla diagonale, per cui consideriamo solo la parte superiore:

TABELLA 6

Primi Consecutivi dispari ↓ Loro differnze→	*3*	*5*	*7*	*11*	*13*	*17*	*19*	*23*	*29*	*31*
3	0	2	4	8	10	14	16	20	26	28
5		0	2	6	8	12	14	18	24	26
7			0	4	6	10	12	16	22	24
11				0	2	6	8	12	18	20
13					0	4	6	10	16	18
17						0	2	6	12	14
19							0	4	10	12
23								0	6	8
29									0	2
31										0

Per la crittografia RSA, sconsigliamo l'uso di numeri primi con differenze piccole, facilmente fattorizzabili a ritroso (a partire dalla radice quadrata *n* di *N* = *p*q*, con il noto algoritmo di Fermat.

Teorema fondamentale TFF **(Rif.5)**

Per il Teorema Fondamentale della Fattorizzazione veloce, occorre una tavola di divisione, per calcolare il rapporto *q/p*, vedi (Rif. 4). Poiché il rapporti dei numeri primi che compongono i Numeri RSA sono al massimo 2,25, segneremo in blu i rapporti inferiori a tale rapporto massimo

TABELLA 7

Primi	3	5	7	11	13	17	19	23	29	31
3	1	1,66	2,33	3,66	4,33	5,66	6,33	7,66	9,66	10,33
5		1	1,4	2,2	2,6	3,40	3,8	4,60	5,80	6,20
7			1	1,57	1,85	2,42	2,71	3,28	4,14	4,42
11				1	1,18	1,54	1,72	2,09	2,63	2,81
13					1	1,30	1,46	1,76	2,23	2,38
17						1	1,11	1,35	1,70	1,82
19							1	1,21	1,52	1,63
23								1	1,26	1,34
29									1	1,06
31										1

La Tabella è simmetrica, per cui consideriamo solo la parte superiore

Crittografia RSA:i numeri RSA, con rapporto $q/p < 2{,}25$, si trovano appena sopra la diagonale, quelli ancora più in alto superano il rapporto 2,25.

Sconsigliamo l'uso di rapporti prossimi a 1 per lo stesso motivo di cui alla congettura di Polignac, poiché differenze piccole comportano rapporti piccoli, che comportano la posizione di p molto vicina alla radice quadrata n di N, molto vicina semisomma di p e q (in genere, per tutti i numeri RSA, p si trova sempre tra il $\approx 67\%$ e il 100% di n).

***Tavola di moltiplicazione*,**

per trovare i numeri semiprimi iniziali; estendendo idealmente la tabella a numeri primi di centinaia di

cifre, troveremo numeri RSA , usati com'è noto, nella crittografia RSA

In tale tabella, i numeri RSA, sono prossimi alla diagonale centrale da sinistra a destra, composta ovviamente da quadrati *p^2 =q^2.*

TABELLA 8

Primi p→ Primi q↓	**2**	**3**	**5**	**7**	**11**	**13**
2	**4**	**6**	**10**	**14**	**22**	**26**
3	6	**9**	**15**	**21**	**33**	**39**
5	10	15	**25**	**35**	**55**	**65**
7	14	21	35	**49**	**77**	**91**
11	22	33	55	77	**121**	**143**
13	26	39	65	91	143	**169**
...	**...**	**...**	**...**	**...**	**...**	**...**

Come possiamo vedere, la parte superiore (in grassetto) è simmetrica ed equivalente rispetto alla parte inferiore e quindi possiamo considerare solo la parte superiore, sopra la diagonale centrale dei quadrati (in rosso)

I numeri RSA, in blu, si trovano nella stessa posizione dei rapporti *q/p* della Tabella di divisione precedente. Per es. 35= 5*7 corrisponde al rapporto 7/5 =1,4, e quindi sarà al posto di 1,4

Conclusioni

Come possiamo vedere, tutte le tabelle aritmetiche relative alle suddette congetture o ex congetture sui numeri primi (Goldbach forte e debole, Polignac, ecc.) hanno delle lontane e interessanti connessioni con i numeri RSA e la fattorizzazione, e potrebbero contribuire ad una fattorizzazione più veloce, ma non ancora tal da mettere in pericolo la crittografia RSA; che anzi potrebbe essere più sicura se si evitassero numeri *p* e *q* molto vicini e quindi con piccole differenze e piccoli rapporti, cosa che favorirebbe una fattorizzazione più veloce con l'algoritmo di Fermat, a

ritroso a partire da $n = \sqrt{N}$.

In ogni caso, per i numeri RSA, si troverebbe *p*, come prima accennato, tra il 67% e il 100% di n, il che eliminerebbe il 67% dei tempi di calcolo con il metodo tradizionale (provando per tutti i numeri primi da 3 al 67% di n). Per esempio, se per fattorizzare un particolare numero RSA occorressero 100 anni, con la nostra osservazione di anni ne basterebbero "soltanto" 33. Non è ancora molto, ma nemmeno poco.

Riferimenti

(Tutti sul nostro sito, salvo diversa indicazione)

1) "METODO", N. 20/2004

Francesco Di Noto – Annarita Tulumello

DIMOSTRAZIONE DELLA CONGETTURA DI GOLDBACH

Proof of Goldbach's Conjecture

, **sul link *: www.giovanniarmillotta.it/metodo/di_noto14.html***

2) "La congettura di Goldbach"

On April 18, 2013

La congettura di Goldbach, spiegata da Bruno Martin, docente presso il Laboratorio di ricerca in Matematica dell'Université du Littoral, Côte d'Opale, per Images des Mathématiques. Traduzione di Elena Toscano.

Link . ***maddmaths.simai.eu/divulgazione/la-congettura-di-goldbach/***

3) ""Congettura debole di Goldbach già dimostrata. Ne consegue la congettura forte (accenni alla fattorizzazione alla Fermat e alla RH1)

Gruppo "B. Riemann"*
Francesco Di Noto, Michele Nardelli

4) ""DIMOSTRAZIONE DELLA CONGETTURA DI POLIGNAC "

Ing. Pier Francesco Roggero, Dott. Michele Nardelli
Nardelli, Francesco Di Noto

5) "IL TEOREMA FONDAMENTALE DELLA FATTORIZZAZIONE"

Gruppo "B.Riemann"*
Francesco Di Noto, Michele Nardelli
*Gruppo amatoriale per la ricerca matematica sui numeri primi, sulle loro congetture e sulle loro connessioni con le teorie di stringa.