Brevi considerazioni sulla congettura di Goldbach e possibili relazioni con la fattorizzazione polinomiale e con l'ipotesi di Riemann

°°°°°°°°°°°°°°°°°°°°°°°°°

Gruppo Eratostene

Abstract

In this paper we show some relations between Goldbach's conjecture (and our proof), fast factoring and Rieman Hypothesis (RH).

Alla base di ogni dimostrazione della congettura di Goldbach (p + q = N pari) c'è la condizione necessaria N – p = q, e solo se p e q sono primi siamo in presenza di una coppia di Goldbach che soddisfa la congettura. Poiché p e q sono simmetrici rispetto alla semisomma s = N/2, p è sempre minore di s, e q sempre maggiore, entrambi con eguale

distanza (o differenza) da s (vedi la nostra proposta di dimostrazione, Rif. 1). Quindi ogni coppia di Goldbach è sempre formata da un numero primo p compreso tra 1 ed N/2 (con la sola eccezione di 2 + 2 = 4), ed un numero q compreso tra N/2 ed N. Ora, affinché un qualsiasi numero pari non è la somma di due numeri primi, significa che in una delle due metà di N non ci sia alcun numero primo p oppure q oppure entrambi) , in modo che sia impossibile la formazione di una coppia p + q = N. Il contro esempio della congettura, ricordiamo, è G(N) = 0, cioè per un ipotetico N non esiste nessuna coppia di Goldbach tale che p + q = N (quindi 0 coppie). Questa condizione estrema però in realtà non si verifica mai, poiché nelle due metà di N ci sono circa la meta di numeri primi che ci sono fino ad N, e quindi

$$\sim \pi (N)/2 \text{ fino ad } N/2, \text{ e } \sim \pi(N)/2 \text{ da } N/2 \text{ ad } N$$

per esempio, fino ad N = 100 ci sono 25 numeri primi, dei quali 15 fino a 100/2 = 50 e 10 da 50 a 100, e le loro combinazioni p + q = N = p + q = 100 sono 6 (infatti G(100)= 6, vedi Rif.1

La quantità approssimativa di coppie di Goldbach è data dalla noto formula logaritmica, poiché si ha mediamente una coppia di Goldbach ogni log(N)^2:

$$G(N) \sim N/(\log N)^2, \quad (1)$$

infatti per N = 100 abbiamo:

$G(100) \sim N/(\log(100)^2 = 4{,}60^2 = 100/21{,}16 = 4{,}72 \sim 6$

con 4,72 valore stimato e 6 valore reale di G(100)

Tale formula vale per tutti i numeri pari di forma $6k \pm 2$, come N = 100: ma se N = 6k, il valore di G(N) è circa il doppio, per l'effetto dell' “”abbondanza di Goldbach” (vedi Rif. 2 e Rif. 3) dovuta al ruolo dei multipli dispari dei numeri primi fattori di N. Il massimo delle coppie di Goldbach lo hanno i numeri primoriali p#, un po' meno i fattoriali n!

Nessun numero di forma $6k \pm 2$ ha un numero di coppie di Goldbach inferiore a circa quello dato dalla (1)

Quindi, ipotizzare, com'è stato già fatto, numeri pari N molto

grandi come possibili contro esempi non sarebbe molto prudente, visto anche che G(N) cresce con N, in base alla formula logaritmica (1), alla quale bisogna aggiungere il valore dell'abbondanza relativa ad eventuali primordiali come fattori (per esempio 2*3 = 6 ha abbondanza di circa 2) o primordiali essi stessi , il chè spiega benissimo le oscillazioni di G(N) tra N di forma 6k e i numeri pari contigui di forma $6k \pm 2$ Quanto sopra esclude qualsiasi contro esempio del genere, poiché più grande è N, più grande è anche $\pi(N)$, diviso in due parti quasi uguali tra loro, da 3 ad N/2 e da N/2 ad N, in modo da formare almeno G(N) coppie di Goldbach in base alla (1), e ancora di più se N è di forma 6k (forma che comprende tutti i multipli di primoriali e di fattoriali, con la loro relativa "abbondanza")

Premesso quanto sopra (verità di Goldbach, basata sia su buone evidenze numeriche sia soprattutto su buoni argomenti teorici), vediamo ora brevemente le relazioni con la

fattorizzazione e con la RH

a) Fattorizzazione

Nell'algoritmo di fattorizzazione alla Fermat, compare il simbolo s della semisomma s = S/2 (p + q)/2, e quindi c'entra la congettura di Goldbach, basata su S = N = p + q.

N = s + d^2, con d = semidifferenza d = (q - p)/2 , da cui

p = s - d e q = s + d

Questa relazione ha particolare importanza per i numeri p e q con relativamente piccole differenze, e quindi con bassi rapporti (da 1 a 2 circa, talvolta anche più grande), come per esempio i numeri RSA (Rif. 4) del noto sistema crittografico, per cui tale algoritmo è spesso efficace per questo tipo di numeri.

Piccolo esempio per N = 29083 = 127*229, con rapporto 229/127 = 1,80, ed n=√N = 170,53 = √29083;

s = (127+229) = 356 /2 = 178 , d = (229 -127)/2 = 102/2 = 51

p = 178 - 51 = 127, q = 178 + 51 = 229

vale anche la relazione approssimativa

$s \sim n + \sqrt{d} = 170{,}53 + \sqrt{51} = 170{,}53 + 7{,}14 = 177{,}67 \sim 178$,

dovuta alla relazione

$s^2 = N + d^2$, da cui $s = \sqrt{N + d^2}$, e quindi $s = n + \sqrt{d}$;

il problema è che non si conosce con esattezza d, ne ci sono attualmente metodi per stimarla (come pure per il rapporto q/p) ; per cui si deve procedere per tentativi , $s = n + \sqrt{d}$ con d progressivo da 1 a d reale, fino a quando si trova $s = S/2$, con $S = p + q$, e quindi torniamo a Goldbach

Per i numeri RSA (Rif.4) , la somma massima $S = p + q$, per un rapporto massimo $q/p = 4$ (di solito tale rapporto è inferiore, tra 1 e 2 o più raramente tra 1 e 3) , è $S = 2{,}5 * n$;

per esempio (la regola vale anche per i numeri composti)

$N = p*q = 10*40 = 400$, $n = \sqrt{400} = 20$, $r = q/p = 4$,

$S = p + q = 10 + 40 = 50 = 20*2{,}5$

Non si escludono altre possibili relazioni tra S ed N, e quindi tra N prodotto di due primi e insieme numero RSA, ed S

somma di Goldbach per i numeri RSA:

$S = 2n$ per p e q numeri gemelli con rapporto r q/p ~ 1

$S > 2n < 2{,}5*n$ con rapporto r = q/p tra 1 e 4.

E neanche altre possibili relazioni tra congettura di Goldbach e l'ipotesi di Riemann, oltre quelle accennate in questo lavoro (vedi successivo punto b)

b) Ipotesi di Riemann (RH1) paragone tra abbondanza σ(N) e abbondanza di Goldbach, similitudine nei grafici e nei contro esempi , fuori dai grafici di tipo comet (quando i contro esempi si trovano fuori dal grafico di tipo comet, le congetture sono vere, in questo caso RH1 e Goldbach)

Rimandiamo al lavoro "Dai multipli di 6 alla Riemann's Hypothesis" (Rif. 9)

Circa infine una possibile relazione tra fattorizzazione e ipotesi di Riemann, possiamo dire che come sottoproblema di P = NP, la fattorizzazione in tempo polinomiale è possibile se

la RH è vera, quindi , almeno in questo caso, P=NP (rimandiamo all'articolo "La fattorizzazione veloce e il problema P=NP)

Conclusione

Concludendo, la congettura di Goldbach (ma che ora possiamo già definire ex congettura, a causa della nostra proposta di soluzione, Rif. 1), lungi da essere una semplice curiosità matematica come talvolta si pensa con leggerezza, è invece un argomento matematico molto importante, viste le suddette relazioni sia con la fattorizzazione veloce o polinomiale (sottoproblema di P = NP problema del millennio) e con l'ipotesi di Riemann (altro importante problema del millennio legato ai numeri primi), e infine tra tale problema e la RH, come nel seguente schema riepilogativo finale, che mostra le suddette relazioni/connessioni teoriche con due dei più noti e importanti problemi del millennio basati sui numeri primi :

<u>G O   L D B A C H</u>

↕ ↕

P = NP ↔ R H

Riferimenti finali **(tutti reperibili sul nostro sito www.gruppoeratostene.com)**

1) Gruppo Eratostene "Proposta di dimostrazione del teorema di Goldbach", in sezione "Articoli su Goldbach"

2) Gruppo Eratostene,"Nuova relazione di Goldbac – Abbondanza di Goldbach" idem

3) Rosario Turco, Maria Colonnese, Gruppo Eratostene "Abbondanza di Goldbach" idem

4) "Congettura sui numeri RSA", Gruppo Eratostene, in sezione "Articoli sulla Fattorizzazione"

5) Il Metodo del cerchio - Problemi additivi – congettura di Goldbach " ing. Rosario Turco, in "Articoli su Goldbach"

6)" The Circle's Method to investigate the Goldbach's Conjecture and the Germain primes: Mathematical connections with the p-adic strings and the zeta strings". Michele Nardelli 1,2 e Rosario Turco, in sezione "Articoli di Fisica - Matematica"

7) "Articoli sulla Fattorizzazione"

8) "Articoli su Riemann"

9) "Dai numeri multipli di 6 alla Riemann Hypothesis (i criteri di Robin e Lagarias)"Rosario Turco, gruppo Eratostene, in sezione "Articoli su Riemann

10) "La fattorizzazione veloce e il problema NP (con accenno alla RSA e al logaritmo discreto)" , in sezione "Articoli sulla Fattorizzazione"

Caltanissetta 15. 10.2010