Su alcuni possibili contributi utili alla dimostrazione dell'ipotesi di Riemann I (RH ed RHG)

F. Di Noto, A. Tulumello, G. Di Maria, M. Nardelli[1,2]

[1] Dipartimento di Scienze della Terra
Università degli Studi di Napoli Federico II, Largo S. Marcellino, 10
80138 Napoli, Italy

[2] Dipartimento di Matematica ed Applicazioni "R. Caccioppoli"
Università degli Studi di Napoli "Federico II" – Polo delle Scienze e delle Tecnologie
Monte S. Angelo, Via Cintia (Fuorigrotta), 80126 Napoli, Italy

CONGETTURE CORRELATE ALLE IPOTESI DI RIEMANN (RH e GRH)

(I nostri possibili contributi)

Com'è noto, all'ipotesi generalizzata di Riemann (GRH) sono connesse la congettura debole di Goldbach, la congettura dei numeri primi gemelli e il test di primalità di Miller - Rabin, mentre all'ipotesi di Riemann (RH) sono connessi il Teorema dei Numeri Primi (TNP) e, forse, (non c'è accordo su questo tra i matematici) anche la fattorizzazione polinomiale (caso particolare della congettura NP = P). In sintesi:

GRH → Congettura debole di Goldbach

GRH → Congettura dei numeri gemelli

GRH → Test di primalità di Miller Rabin

RH → TNP

RH → Fattorizzazione (Congettura NP = P)

Con i nostri lavori e contributi su tutte queste connessioni e relativi argomenti, per es. sul test di primalità, sul TNP, ecc., vorremmo contribuire ad una migliore comprensione dei numeri primi, ed infine ad una possibile dimostrazione diretta o indiretta dell'ipotesi di Riemann.

Per quanto riguarda Goldbach, riportiamo alla fine per intero il nostro lavoro "Note su una soluzione positiva per le due congetture di Goldbach", già pubblicato sul sito

http://xoomer.alice.it/stringtheory

anche sul sito del Centro Nazionale delle Ricerche (CNRSOLAR http://150.146.3.1.132.406/); per quanto riguarda il TNP, il lavoro ancora in corso è:

“Due formule per una stima più precisa dell’N° numero primo e di π(N) tramite due funzioni logaritmiche correttrici (relazioni con il TNP e abbattimento dell’errore percentuale)”; per quanto riguarda invece la congettura dei numeri gemelli riporteremo un nostro ragionamento per assurdo che dimostra la verità della congettura.

Per quanto riguarda il test di primalità, riporteremo solo il test di Rabin – Miller, l’unico che dipende dalla GRH; per quanto riguarda infine la fattorizzazione polinomiale, riporteremo soltanto le opinioni del Prof. Cerruti e del Prof. Zaccagnini, scettiche su una possibile relazione tra fattorizzazione e GRH oppure con la RH.

Il nostro principio di base in questo lavoro è che se l’ipotesi debole di Goldbach è vera (noi proponiamo la nostra soluzione positiva),e se la congettura degli infiniti

numeri gemelli è anch'essa vera (noi proponiamo il nostro ragionamento per assurdo), e se il teorema di Miller – Rabin sul loro test di primalità funziona, come pure il Teorema dei Numeri primi o TNP, migliorato con le nostre due funzioni logaritmiche capovolte c e c', che abbattono a meno dell'1 % l'errore percentuale (vedi capitolo 4) allora la GRH, che comporta la congettura debole di Goldbach, la congettura dei numeri primi gemelli e il test di Miller – Rabin, è vera anch'essa, e quindi di conseguenza anche la RH è vera (cosi come la congettura debole di Goldbach è vera solo se è vera la congettura forte, vedi la nostra dimostrazione nel capitolo 1) così come è vero anche il TNP, che com'è noto è stato già dimostrato da Hadamard e da de la Vallee – Poussin.

Questo nostro lavoro, pur non dimostrando direttamente la GRH o la RH, raccoglie tuttavia diversi indizi utili, nostri e altrui, per una possibile futura dimostrazione positiva: insomma le spiana un po' la strada, soprattutto per quanto riguarda Goldbach, i numeri primi gemelli e il TNP, questo rivisto alla luce delle due nostre funzioni correttrici, e con il calcolo ulteriormente perfezionabile con metodi proporzionali. (vedi Capitolo 4)

Così rivisto, il TNP può essere connesso ancora meglio alla RH, dalla quale peraltro deriva, e quindi potrebbe anch'esso essere utile ad una futura dimostrazione della RH, poiché esso migliora le conoscenze sulla distribuzione dei numeri primi e quindi pemette di stimare molto meglio di prima sia la grandezza N dell' N° numero primo, sia π (N), con precisione simile a quella ottenuta con il

logaritmo integrale Li(N).

Una possibile dimostrazione positiva della RH potrebbe però dirci poco o nulla sull'altro grande problema ancora irrisolto riguardante i numeri primi, e cioè la fattorizzazione polinomiale , più veloce di quella tradizionale più o meno facilitata da metodi di fattorizzazione, ancora però lontani da un sistema veramente efficiente e soprattutto veloce; sarebbe bene non farsi molte illusioni su questo argomento, perché la RH non sarebbe pericolosa per il sistema crittografico RSA, come invece dicono alcuni matematici. Per esempio K.Devlin dice che alcuni metodi di fattorizzazione derivano dalla RH ma non dice quali sono.

Però non si sa mai, in questo campo tutto è ancora possibile, per cui a priori non escludiamo del tutto una pur sempre possibile e più o meno lontana e più o meno

efficiente connessione tra RH e fattorizzazione polinomiale, o che questa potrebbe anche giungere per altre vie.

C A P I T O L O 1.

G O L D B A C H

(le sue due congetture, forte e debole)

Sulla congettura debole di Goldbach è già noto ai matematici il lavoro di Deshowillers, Effinger,Te Riele e Zinoviev:

" A complete Vinogradov 3 – primes theorem under the Riemann Hypothesis" in Electronic Research Announcement of the American Mathematical Society, Vol. 3, pp 99-104 (1997) , disponibile sul sito

http://www.ams.org/1997-03-15/S1079-6762-97-0031-0/S1079-6762-0031-0.pdf

Gli Autori hanno dimostrato con questo lavoro che se è vera la Congettura di Riemann generalizzata (GRH) allora tutti gli interi $n \geq 7$ si possono scrivere come somma di tre primi.

Questo comporterebbe anche che una prova della congettura debole di Goldbach, che sia la nostra (vedi lavoro " Note su una soluzione positiva per le due congetture di Goldbach" già accennato nell'introduzione), oppure di altri matematici, comporterebbe viceversa la validità della GRH, e indirettamente, anche della RH.

Per quanto riguarda la congettura forte di Goldbach, qui accenneremo soltanto a Montgomery e Vaugan secondo i quali, in un loro lavoro degli anni '70, concludevano, forse frettolosamente, che

"quasi tutti i pari sono somma di due numeri primi,; più precisamente, per x sufficientemente grandi ma almeno $x > 10^{18}$, visto che fino a tale numero tutti i numeri pari sono stati testati positivamente

(da Oliveira e Silva, N.d.A.A.), il numero dei numeri pari fino a x che non sono somma di due numeri primi è minore di x^{1-a} , dove a > 0 è una costante piuttosto piccola (l'attuale record è circa 1/50). Certamente ci sarà stato qualche errore nel loro lavoro, poiché dalle nostre tabelle e dal nostro grafico non risultano possibilità di contro esempi G(N) = 0, cioè di numeri N che non abbiamo nessuna coppia di Goldbach, cioè che non sono almeno una volta la somma di due numeri primi; tali eventuali contro esempi si troverebbero sull'ascissa orizzontale, nella zona inferiore libera da valori (e quindi compreso lo zero di G(N) = 0), essendo tutti i valori reali compresi nell'angolo descritto dal nostro grafico finale). Il che comporta la verità della congettura forte di Goldbach, e di conseguenza anche di quella debole; e infine, indirettamente, anche della GRH, che comporta la congettura debole; anche se le

nostre dimostrazioni sono state trovate senza assumere nè la GRH nè la RH, e nemmeno il teorema di Vinogradov et al. (che connette la GRH e la Congettura debole di Goldbach). Anche la nostra dimostrazione prevede il numero minimo 7 = 2 + 2 + 3, ma noi estendiamo la nostra dimostrazione anche ad N dispari come somma di k dispari numeri primi, con numero minimo 2k +1, ed anche a N pari come somma di k pari numeri primi, con numero minimo = 2k, generalizzazione della congettura forte dove k = 2 e quindi il numero minimo è 2k = 2 x 2 = 4 = 2 + 2; per k = 3, avremo 2k +1 = 2 x 3 +1 = 7 = 2 + 2 + 3, per k = 5 avremo:

2k +1 = 2 x 5 +1 = 11 = 2 + 2 + 2 + 2 + 3, e così via, come analoga generalizzazione della congettura debole a k primi con k dispari, anche grandissimo, purchè il numero minimo sia 2k + 1. Crescendo N, le ripetizioni

del 2 diminuiscono fino a scomparire del tutto, e al 3 finale si sostituiscono numeri primi sempre più grandi di 3, per esempio 21 = 2 + 2 + 17 = 3 + 5 + 13 ecc. ecc.

Un altro nostro lavoro riguarda la "Connessione Goldbach – gemelli – Polignac", consultabile sul sito: http://xoomer.alice.it/stringtheory e basato sul fatto che tutte le coppie di gemelli (q - p = 2) e di Polignac (q – p = 2n) sono sempre le ultime coppie di Goldbach, oltre che numeri primi consecutivi (mentre le altre coppie di Goldbach sono fatte da numeri primi non consecutivi, pur essendo sempre p + q = N pari).

C A P I T O L O 2.

I NUMERI PRIMI GEMELLI

Per quanto invece riguarda la congettura dei numeri numeri primi gemelli, anch'essa correlata alla GRH, è recente la notizia che una sua dimostrazione è stata trovata da due matematici cinesi: dall' articolo di Patrizio Perrella su Internet " Esistono infinite coppie di numeri primi gemelli, l'Autore scrive che:

"…Un sottoproblema della congettura di Riemann, anch'esso irrisolto, riguarda la distribuzione delle coppie di "numeri primi gemelli (coppie di numeri primi la cui differenza è 2; ad esempio 3 e 5, 5 e 7, 11 e 13, 17 e 19, etc.). A tale proposito i matematici concordano nell'affermare che "esistono infinite coppie di numeri primi gemelli" ma anche in questo caso non è stato fino

ad ora possibile trovare una dimostrazione di questa proposizione né della sua negazione. La proposizione appena enunciata, che dà anche il titolo al presente testo, è nota appunto come congettura dei primi gemelli.

Il lavoro di Goldston e Yldirim… era connesso in particolare con quest'ultima congettura. Il loro risultato non provava la congettura dei primi gemelli ma sicuramente ne forniva una fortissima argomentazione a favore.

La comunità scientifica la accolse, infatti, come il più significativo risultato che si fosse mai ottenuto in favore della validità di questa congettura.

Oggi la soglia raggiunta circa due anni fa da Goldston e Yldirim potrebbe essere stata superata. Lo scorso 9 ottobre è apparso in pre-print su "arXiv" (Open Archive di Fisica, Matematica e Informatica e Scienze non lineari gestito dalla Cornell University) un articolo dal titolo: "There are Infinitely Many Pairs of Twin Prime" scritto

dai matematici cinesi Zhanle Du e Shouyu Du della Chinese Academy of Sciences

(http://arxiv.org./abs/math.GM/0510171).

L'abstract è lapidario: "We proved that there are infinitely many pair of twin prime". L'articolo è breve: 17 pagine e appena 4 citazioni bibliografiche. A pag. 1, già nell'introduzione, viene enunciata la congettura dei primi gemelli proponendola come un teorema (proposizione 1.1) e nelle successive pagine, dopo aver introdotto alcune proprietà ed alcuni lemmi, per l'esattezza a pag. 15, se ne fornisce una dimostrazione per assurdo…"

Rimandiamo a tale articolo, ma anche noi abbiamo una nostra breve dimostrazione per assurdo: premesso che abbiamo trovato una formula più precisa sia per il calcolo delle (GN) coppie di Golbach per N di forma N = 6n ± 2,

N = 6n ± 4 :

$$G(N) \approx \frac{N}{(\log N)^2} \cdot 1{,}08366$$

e

$$G(N') \approx 2 \frac{N'}{(\log N')^2} \cdot 1{,}08366$$

(log = logaritmo naturale)

per N' di forma N' = 6n oppure N' = 12n,

dove c = 1,08366 è il numero correttore di Legendre,

ed log N il logaritmo naturale di N e di N';

sia per il calcolo del g(N) numero di coppie di gemelli fino a N (ora indipendentemente dalla sua forma aritmetica):

$$g(N) \approx \frac{N^{3,5}}{(\log N)^2} \cdot c \approx \frac{N}{(\log N)^2} \cdot 1{,}3247$$

Altre formule citano la costante 1,32032…, e il rapporto

$\frac{g(N)}{G(N)} \approx 1, 3247$ **si avvicina a tale costante.**

Le nostre suddette formule sono molto più precise della formula unica generale ma meno precisa trovata dai matematici per entrambe le congetture:

$$G(N) \approx g(N) \approx \frac{N}{(\log N)^2}$$

La nostra dimostrazione per assurdo si basa sul fatto che, per la forma generale dei numeri primi :

$$P = 6n \pm 1$$

(che esclude i due soli numeri primi 2 e 3 ma che include anche i prodotti $N = p \cdot q$ e tutte le potenze dei primi p^n con $p \geq 5$), le due colonne $6n - 1$ e $6n + 1$ contengono in parti pressocchè uguali sia i numeri primi sia i loro prodotti e le loro potenze, e in modo solo apparentemente disordinato (in realtà un ordine di fondo c'è, come vedremo in seguito ($s=(N\pm1)/6 = qm \pm n = pn \pm m$)

T A B E LL A 1

n	1° colonna 6n - 1	2° colonna 6n + 1
1	5	7
2	11	13
3	17	19
4	23	25 = 5 x 5
5	29	31
6	35 = 5 x 7	37
7	41	43
8	47	49 = 7 x 7
9	53	55 = 5 x 11
10	59	61
…	…	…

In tal modo, per lo stesso n, si formano sia coppie di numeri di gemelli, sia coppie formate da un numero primo e da un numero composto, per es. 55 = 5 x 11, in entrambi i casi con differenza 2 = 6n+1 – (6n -1) = 1 + 1 = 2. Si noti che i numeri della prima colonna sono di forma -1 + 6n e quelli della seconda colonna di forma 1 + 6n Per quanto riguarda le coppie di gemelli, fa eccezione la prima coppia di gemelli 3 e 5, poiché 3 non è di forma

generale $6n \pm 1$, ma di forma $6n + 3 = 6 \cdot 0 + 3 = 0 + 3 = 3$.

Ma veniamo al nostro ragionamento per assurdo per cui le coppie di gemelli sono infinite: ammettiamo che esse siano finite, il che significa che esiste un'ipotetica ultima coppia di gemelli, dopo la quale non ce ne saranno più.

Ora, affinché ciò sia possibile, occorre che

a) dopo tale presunta ultima coppia di numeri primi gemelli, la prima colonna della Tabella 1 sia formata soltanto da numeri primi p, tutti di forma $6n - 1$, e la seconda colonna invece soltanto da composti c, tutti di forma $6n + 1$, o viceversa, :

1° colonna	2° colonna	
…	…	
p	p'	(ultima coppia di gemelli)
p	c	
p	c	
p	c	
p	c	

e così via (o viceversa, c in prima colonna e p in 2° colonna) all'infinito, solo così non si formerebbero più altre coppie di gemelli oltre l'ultima presunta coppia p e p'.

b) oppure numeri primi e numeri composti perfettamente alternati, anche in questo caso ovviamente non si possono più formare nuove coppie di numeri primi gemelli:

1° colonna	2° colonna
…	…
p	p' (ultima coppia di gemelli)
p	c
c	p
p	c
c	p
…	…

E così via all'infinito, anche in questo secondo caso, equivalente del primo, non si formeranno più coppie di numeri primi gemelli dopo la presunta ultima coppia p e p'.

In altre parole, i numeri di forma 6n-1 e 6n+1 dopo tale e presunta ultima coppia di gemelli dovrebbero essere come i numeri pari e dispari: perfettamente uguali fino a N pari e perfettamente divisi in due colonne, o perfettamente alternati, affinché non si formi mai nella stessa riga una coppia di numeri o entrambi dispari d o entrambi pari p, ed è proprio questo che non succede in entrambi i casi:

1° colonna d	2° colonna p
1	2
3	4
5	6
7	8
9	10
…	…

e così via all'infinito, non si avrà mai nella stessa riga una

coppia di numeri entrambi pari o entrambi dispari,

e nemmeno con l'alternanza:

1° colonna	2° colonna (in entrambe i numeri sono alternati)
1	2
4	3
5	6
8	7
9	10
…	…

e anche così non si formano mai coppie di numeri entrambi pari o entrambi dispari nella stessa riga.

Allo stesso modo, non si formano coppie di gemelli se essi fossero fino a un dato N, perfettamente uguali quantitativamente e perfettamente alternati tra primi e composti; il che non è vero per i numeri primi di forma 6n -1 e 6n +1 per lo stesso n (affinché la loro differenza sia sempre 2), poiché :

nel caso a) la cosa è impossibile, perché i prodotti tra due

numeri primi > 5 si distribuiscono in entrambe le colonne, e più precisamente i prodotti di due numeri primi di uguale forma, per es. 6n - 1 oppure 6n + 1, tutti sulla 2° colonna della Tabella 1, mentre i prodotti di due numeri di forma diversa (6n-1 e 6n+1 o viceversa), finiscono nella prima colonna, per esempio 5 x 11 (entrambi di forma 6n-1) = 55 = 6x9+1: 11 x 19 (di forma diversa) = 209 = 6 x 35 - 1 = 210 -1 = 6 x 35 -1 = 209; questo significa che tutti i prodotti di due primi (o anche di un primo e un composto, o di due composti, purchè tutti di forma 6n ± 1) finiscono sempre in tutte e due le colonne, e mai nella stessa colonna, nemmeno dopo la presunta ultima coppia di numeri primi gemelli, e quindi il caso

a) è impossibile, e pertanto non può impedire la formazione di nuove e successive coppie di numeri primi gemelli;

Similmente, nel caso b), tali prodotti non possono essere perfettamente alternati con i numeri primi, come invece lo sono i pari e i dispari (vedi precedente confronto con tali numeri), nè tanto meno quantitativamente uguali fino ad un dato N (come lo sono i pari e i dispari); e quindi la suddetta reale disposizione dei numeri primi e dei numeri composti su entrambe le colonne 6n -1 e 6n+1, non può mai impedire, dopo una qualsiasi presunta ultima coppia di numeri gemelli, la formazione di nuove e successive ulteriori coppie di gemelli ancora più grandi, per quanto sempre più rare, il che dipende dal quadrato della frequenza dei numeri primi fino ad un dato N quantunque grande, per esempio fino a $N = 10^9$ **la frequenza dei numeri primi è** $1/(\log 10^9)^2 = 1/20{,}72^2 = 1/429{,}45$, **cioè mediamente una coppia ogni 429,45 unità,**

in realtà è leggermente superiore (la formula più precisa per il calcolo approssimativo del numero delle coppie di primi gemelli la vedremo tra poco).

La disposizione reale tra primi e composti è ovviamente quella risultante, per i motivi di cui sopra (impossibilità di uguaglianza numerica tra primi p e composti c, e anche dell'impossibilità della loro uguaglianza numerica)

dalla Tabella 1, che rivediamo in tal senso:

n	1° colonna 6n -1	2° colonna 6n +1
1	5 = p	7 = p gemelli
2	11 = p	13 = p ‘’
3	17 = p	19 = p ‘’
4	23 = p	25 = c = 5 x 5
5	29 = p	31 = p gemelli
6	35 = c= 5 x 7	37 = p
7	41 = p	43 = p gemelli
8	47 = p	49 = c = 7 x 7
9	53 = p	55 = c = 5 x 11
10	59 = p	61 = p gemelli
…	…	… …

17 101= p 103 = p gemelli

… … … …

come si vede, p e c si alternano in modo solo apparentemente irregolare e non numericamente uguali in entrambe le colonne (un solo composto nella prima colonna e tre composti nella seconda), condizioni che si ripetono all'infinito per l'impossibilità dei casi a) e b) e quindi permetteranno all'infinito e senza alcun limite la formazione di nuove coppie di gemelli, che in tal modo sono infinite, così come sono infiniti i numeri primi, cosa dimostrata da Euclide con un ragionamento per alcuni versi analogo al nostro (dato un qualsiasi numero primo, si dimostra che ce n'è sempre uno ancora più grande), e quindi infiniti altri (ma ci sono anche altre più recenti dimostrazioni per l'infinità dei numeri primi). Per le infinite coppie di numeri

primi gemelli, con altra dimostrazione per assurdo, rimando al recente lavoro dei due matematici cinesi; se anche la loro dimostrazione risultasse esatta, la connessione tra GRH e congettura dei numeri gemelli sarebbe confermata, ed entrambe potrebbero essere vere, cosa confermata anche dalla connessione GRH e congettura debole di Goldbach, da noi dimostrata.

Tornando brevemente sulla frequenza delle coppie di primi gemelli sulla retta numerica, descriviamo la nostra formula più precisa prima accennata, ora però con esempio per N = 10 000. Il numero reale delle coppie di gemelli fino a N = 10 000 è 170, mentre il numero reale delle coppie di Goldbach è 128; con la formula nota e unica per entrambe le congetture,

$$G(N) \approx g(N) \approx \frac{N}{(\log N)^2} = \frac{10000}{84,83} = 117,88$$

il numero stimato è 117,88 in errore per difetto,

per il numero delle coppie di Goldbach, di circa

l'8 % rispetto a quello reale (infatti 128 / 117 = 1,085)

e in errore per difetto, per il numero delle coppie di

gemelli, di circa il 40%, infatti 170 / 117,88 = 1,44,

valore che si avvicina alla costante 1,32

Per N ancora più grandi, per esempio per

N = 1 000 000 000 abbiamo:

stima logaritmica comune 2 331 002

$$G(N) \approx 2\,331\,002 \times 1{,}08 = 2\,517\,482$$

$$g(N) \approx 2\,331\,002 \times 1{,}32 = 3\,076\,922$$

entrambi valori molto più vicini ai valori reali,

dei quali si conosce solo g(N) = 3 424 506

con rapporto $g(N) / G(N) = g(10^9) / G(10^9)$

$= 3\,424\,506 / 2\,517\,482 = 1{,}360 \approx 1{,}32032\ldots$

con rapporto $g(N) / (\log N) = g(10^9) / (\log 10^9)^2 =$

= 3 424 506 / 2 331 002 = 1,4691 .

Lo stesso succede con qualsiasi N; il numero delle coppie di gemelli cresce con N e con la frequenza delle coppie di gemelli, data dall'inverso del quadrato del logaritmo di N moltiplicato per la costante 1,32032…

Per cui una formula più precisa, riportata da articoli su Internet, è la seguente

$$g(N) \approx \frac{N \cdot 1{,}032032}{(\log N)^2}$$

con log N = logaritmo naturale di N.

Quindi, quando mai finiranno, e quindi saranno finite? Ovviamente, mai, e quindi sono infinite, anche per il nostro precedente ragionamento per assurdo. Ricordiamo che la più grande coppia nota di numeri primi gemelli è:

$$2\,003\,663\,613 \times 2^{195000} \pm 1,$$

un numero con 58 711 cifre decimali, come dire dell'ordine di 10^{58711} (per fare un paragone con il numero noto 10^{80}, il numero delle particelle elementari del nostro universo; numero già enorme ma che è ben 58 711 / 80 = 733 volte minore del primo numero solo come esponente, cioè solo come numero di cifre.

Se, come scrivono i due matematici cinesi nella loro dimostrazione, la congettura dei numeri primi gemelli fosse vera, allora sarebbe vera anche la GRH alla quale è connessa, vedi articolo "Piccole differenze tra due numeri primi consecutivi" sul sito

http://wwwBrainmindlife.org/primigemelli.htm ,

e di conseguenza anche la RH) così come già detto per

la congettura debole di Goldbach da noi dimostrata (vedi Capitolo 1).

C A P I T O L O 3.

TEST DI MILLER – RABIN

Il test di primalità di Rabin – Miller, dalla voce "Generalized Riemann Hypothesis", dice che

" Se GRH è vera, allora il test di primalità di Miller - Rabin funziona in tempo polinomiale"

(Il test in tempo polinomiale che non richiede la GRH, il test di primalità AKS, è stato pubblicato di recente)

Un'altra versione equivalente ma più tecnica (dal sito web della Prof. Marta Morigi) :

" Se vale l'ipotesi di Riemann generalizzata ed n è un intero composto dispari, allora n non passa il test di Miller per almeno una base b tale che $b < 2 \log^2 n$ ".

Su questa relazione tra la GRH e il test di Miller – Rabin non abbiamo ancora pronto alcun

nostro contributo utile, per cui passiamo al prossimo capitolo sul TNP, sul quale abbiamo delle novità interessanti (due funzioni logaritmiche correttrici c e c', che abbattono l'errore percentuale a meno dell' 1 % nella stima sia del N° numero primo, sia di π (N), come vedremo.

Un nostro test di primalità (basato sul test cinese)

$\frac{2^n - 2}{n}$ **= k intero se n è primo, decimale se composto, si imbatte nei numeri di Carmichael, che passano il test pur non essendo numeri primi (per esempio 341 = 11 x 31 dovrebbe essere primo e invece non lo è), e quindi si potrebbe completare in questo modo:**

se n passa il test, cioè k è intero di cui sopra e non è numero di Carmichael, allora è primo.

Il problema di questo test è che 2^n è esponenziale, cioè cresce rapidamente al crescere di n, il che allunga notevolmente i tempi di calcolo, e solo

futuri computer superveloci, quantistici o no, potranno essere in grado di verificare il suddetto test per n molto grandi. Il test deriva dal fatto che nel Triangolo di Tartaglia, se n è primo, tutti i termini della n-esima riga (tranne le due unità iniziale e finale), e quindi anche la loro somma, sono divisibili per n.

Poichè la somma dei termini di ogni riga è 2^n , togliendo le due unità finali, avremo $2^n - 2$ che è divisibile per n solo se n è primo o è un numero di Carmichael (su Internet esistono lunghi elenchi di questi numeri, che passano il test pur non essendo numeri primi).

C A P I T O L O 4.

TNP e funzioni correttrici.

Il lavoro sulle due funzioni correttrici dell'errore percentuale è ancora in corso di pubblicazione, e non appena pronto sarà pubblicato, come gli altri prima accennati, sul sito

http://xoomer.alice.it/stringtheory

e probabilmente anche sul sito dell'archivio CNR Solar già nel corso del 2007 o nel 2008.

E' un lavoro che conferma il TNP e dà una forma logaritmica capovolta (decrescente) all'errore percentuale sia nella stima dell' N° -esimo numero primo, sia nella stima di π(N), abbattendo l'errore percentuale a meno dell'1 %, per qualsiasi N° o N.

C A P I T O L O 5.

RH e Fattorizzazione polinomiale

Alcuni matematici, per es. D.K. Devlin, nel suo recente libro "I problemi del millennio", Longanesi ed. ritengono possibile una relazione tra fattorizzazione polinomiale e la RH:

"…Alcuni metodi di fattorizzazione presuppongono che la RH sia vera"

ma non dice quali sono; il Prof. Umberto Bottazzini, in un suo articolo su il Sole – 24 Ore del 14.5.2000, scrive invece che:

"… Nel 1972 è stata introdotta una classe Np di problemi, apparentemente più ampia della classe P dei problemi

risolubili in tempo polinomiale da una macchina deterministica. Ad esempio, il problema della scomposizione di un numero in fattori sta in Np, ma non si sa se sta anche in P (la risposta è positiva se l'ipotesi di Riemann è vera)"

Altri matematici invece sono più scettici, per es. il Prof. Alessandro Zaccagnini, in risposta ad una nostra lettera:

"… Negli algoritmi di fattorizzazione si usa la congettura di Riemann per dimostrare che valgono certe limitazioni per il numero delle istruzioni che il programma dovrà eseguire in alcuni suoi cicli, ma di per sé non da algoritmi particolarmente veloci".

Il Prof. Umberto Cerruti, nel suo blog matematico alla fine del capitolo"Congettura di Riemann e sicurezza mondiale", scrive che:

" … Il problema della fattorizzazione è diverso. Essa avviene o non avviene,semplicemente. Che io

sappia nessuno ha ricavato metodi di fattorizzazione dall'ipotesi che la RH sia vera. Non esiste un teorema del tipo:

" Se vale RH, dato un intero N, faccio questo e quello e lo fattorizzo velocemente: se esistesse lo si potrebbe usare : se N si fattorizza siamo felici e rompiamo il codice RSA, anche senza aver dimostrato la RH"

Anche il Prof. Cerruti potrebbe avere ragione, alla fin fine.

La fattorizzazione, più o meno veloce che sia, pur riguardante i numeri primi (ma anche tutti gli altri numeri) tuttavia non sembra direttamente collegata alla loro distribuzione lungo la retta numerica e quindi alla RH, basata proprio su tale distribuzione.

Una relazione da noi trovata tra numeri primi e fattorizzazione è il teorema e la formula del sesto

$$s = \frac{N \pm 1}{6} = pn \pm m = qm \pm n \qquad (1)$$

accennata nel capitolo 2) derivato dalla forma generale dei numeri primi

$$P = 6n \pm 1$$

per la quale possiamo scrivere $p = 6m \pm 1$ **e** $q = 6n \pm 1$**, e quindi il loro prodotto come**

$$N = p \cdot q = (6m \pm 1) \cdot (6n \pm 1) \qquad (2)$$

da cui $s = \frac{(N \pm 1)}{6} = pn \pm n = qn \pm m$

Formule (1) e (2), che pur essendo matematicamente corrette, non ci sono di nessun aiuto, salvo qualche eccezione (p e q gemelli), nella ricerca di p e q e quindi nella fattorizzazione più veloce di quella tradizionale (dividere N per tutti i primi fino a trovare $p \leq r = \sqrt{N}$**. Questo perché ora, invece di p e q, bisognerebbe trovare la coppia m ed n, e si ricade nella ricerca per tentativi, stavolta sui numeri naturali**

m ed n anzichè sui numeri primi p e q fino ad r = $\sqrt{N}$.

E con l'unica novità che per i numeri primi esiste la sola coppia banale m = 0 ed n = s, che danno i fattori banali 6 x 0 $\pm$ 1 = -1 e + 1, ed N = 6 x s $\pm$ 1 = N; mentre per tutti i numeri composti (ma senza i fattori 2 e 3) esiste almeno una coppia di m'>0 ed n'>0 tali che 6m' $\pm$ 1 = p, e 6n $\pm$ 1 = q, più in generale, tante coppie di m' ed n' diversi quante sono le coppie di fattori, primi o composti purchè tutti di forma 6n$\pm$1, e tali che il loro prodotto sia N.

Un esempio per tutti:

N		p		q		p'		q'
1885	=	29	x	65	=	5	x	377
s = 314		m=5		n=11		m'=1		n'=63

$s = \frac{1885 - 1}{6} = 314 = pn - m = 29 \times 11 - 5 = 314$

$314 = qm - n = 65 \times 5 - 11 = 314$

$314 = p'n' \pm m' = 5 \times 63 - 1 = 314$

$314 = q'm' \pm n' = 377 \times 1 - 63 = 314$

Il segno – deriva dal fatto che tutti i fattori

5, 29, 65 e 377 sono di forma generale 6n -1.

Unico caso utile di fattorizzazione veloce, come prima accennato, è che il prodotto di due primi

$N = p \cdot q$ si può scrivere anche come:

$N = (6m \pm 1)(6n \pm 1) = 36mn \pm 6m \pm 6n + 1$,

che nel caso dei numeri primi $p = 6m-1$ e $q = 6m+1$

(essi condividono lo stesso m=n ma non il segno, affinché siano con differenza $q - p = 2$), diventa

$$N = p \cdot q = (6m-1)(6m+1) = 36m^2 + 6m - 6m - 1 = 36m^2 - 1,$$

da cui ora è facile trovare m con la sequenza di calcolo:

$$N = 36m^2 - 1$$

$$N + 1 = 36m^2$$

$$\frac{N+1}{36} = m^2$$

$$\sqrt{m^2} = m, \text{ da cui } p = 6m-1 \text{ e } q = 6m+1$$

Un esempio per tutti:

$N = 899$ **(899 = 29 x 31)**

(Se 899 + 1 è un quadrato perfetto, è un possibile prodotto di due numeri gemelli)

infatti $899 + 1 = 900$

$$\frac{900}{36} = 25 = 5^2, \quad m = 5,$$

$p = 6 \times 5 - 1 = 30 - 1 = 29$; $q = 6 \times 5 + 1 = 30 + 1 = 31$

o più direttamente:

$p = (\sqrt{N} + 1) - 1 = \sqrt{900} - 1 = 30 - 1 = 29$

$q = (\sqrt{N} + 1) + 1 = \sqrt{900} + 1 = 30 + 1 = 31$

Siamo così giunti ad un caso di fattorizzazione polinomiale veloce solo però quando N è di forma $N = 36m^2 - 1$, e quindi è il prodotto di due gemelli, o anche di un primo di forma $6n - 1$ e di un composto di forma $6m+1$, per esempio $N = 23 \times 25 = 575 = 576 - 1$,

con $\frac{576}{36} = 16 = m^2$ ed $m = \sqrt{16} = 4$,

da cui $p = 6 \times 4 - 1 = 24 - 1 = 23$,

e $q = 6 \times 4 + 1 = 24 + 1 = 25$.

Questo perché $36\,m^2 - 1 - N = 0$ è un polinomio di secondo grado ad una incognita (m), risolvibile facilmente anche senza fare ricorso all'ipotesi di Riemann, come scrive il Prof. Cerruti nel suo blog.

Il nostro futuro passo potrebbe essere l'estensione di tale metodo di fattorizzazione a tutti gli altri casi di $N = p \cdot q$ ma con p e q non gemelli.

E' un problema che cercheremo di risolvere con nostri futuri lavori, basati ovviamente su questo primo passo nella direzione giusta, utile al percorso generale: fattorizzazione – fattorizzazione veloce per $N = p \cdot q$ con p e q gemelli) – fattorizzazione veloce per tutti gli altri casi $N = p \cdot q$ con p e q non gemelli - soluzione del problema P versus NP (almeno nel caso particolare della fattorizzazione polinomiale) - eventuale connessione con la RH (come ipotizza il Prof. Bottazzini).

C O N C L U S I O N E

Viste le correlazioni tra la GRH, la RH e le Congetture (Goldbah deboli e primi gemelli) e teoremi (Rabin-Miller, TNP) connessi, e i nostri possibili utili contributi (Capitoli 1 e 2 e 4), e infine la questione della possibile fattorizzazione polinomiale (Capitolo 5), possiamo concludere che in base a tali correlazioni e ai nostri suddetti contributi (essendo ora da noi dimostrata la congettura debole di Goldbach, e rafforzata la congettura dei primi gemelli con il nostro ragionamento per assurdo, e confermato il TNP con le nostre due funzioni correttrici (c e c') dell'errore percentuale a meno dell'1%),

la GRH è vera, e di conseguenza anche la RH; come si dimostrerà definitivamente in seguito, sia con lavori altrui ma anche nostri (abbiamo in programma una dimostrazione della RH1, variante di Lagarias, ed equivalente alla RH, ma in forma matematica più facilmente trattabile di quest'ultima)