I tre problemi del millennio sui numeri primi

(RH, P =N P e congettura di Birch e Swinnerton – Dyer: possibili connessioni e una nostra previsione)

Dedicato a Bernhard Riemann

Giovanni Di Maria, Francesco Di Noto, Michele Nardelli, Annarita Tulumello

Sommario

Tra i sei problemi del millennio rimasti ancora insoluti dopo la dimostrazione della congettura di Poincarè da parte del matematico russo G. Perelman, ce ne sono tre nei quali sono coinvolti i numeri primi; i quali indirettamente riguarderebbero anche il problema del gap di massa, nel caso questo fosse risolto tramite qualche gruppo di Lie (il cui numero di elementi è un multiplo di un numero primo n' ottenuto con la formula n^2 + n + 1 in cui anche n è un numero primo o una sua potenza).

In questo lavoro riepilogativo - divulgativo vedremo brevemente in che modo i tre problemi del millennio accennati nel titolo sono basati sui i numeri primi, come poi possano essere connessi tra di loro, e come tale connessione possa facilitare la soluzione di qualcuno di loro, che potrebbe facilitare in seguito la soluzione dei due problemi rimanenti ai matematici impegnati in tale impresa (gli sforzi maggiori sembrano dedicati alla RH, l'ipotesi di Riemann)

Per esempio, il problema P = NP è connesso alla RH tramite la fattorizzazione, sottoproblema di P, e che con la RH ha in comune i numeri primi (o meglio, la loro distribuzione. Un prodotto infinito simile alla funzione zeta lega invece la RH alla congettura di Birch e Swinnerton – Dyer. Infine, sia sul problema della fattorizzazione (in P se la RH è vera) , sia sulla congettura di Birch e Swinnerton – Dyer, sono basati due famosi sistemi crittografici (RSA nel primo caso, ECC nel secondo, tramite le curve ellittiche).

Di entrambi ne parla l'Ing. Rosario Turco in "Le basi della crittografia" (Rif. 1)

Abstract

In this paper on Millennium's Problems as RH, P = NP , Birch and Swinnerton - Dyer's conjecture, connected with prime numbers, we anticipate that it will result: or all them true or all them untrue, because them have some relations with factoring and cryptographics systems (RSA, ECC). More probable is positive solution (all them are true) The other problems (Theory of Yang – Mils, Hodge's conjecture and Navier - Stokes equations), they here are only shortly mentioned).

Introduzione

I sei problemi del millennio rimasti ancora aperti dopo la recente dimostrazione della congettura di Poincarè da parte del matematico russo Grigory Perelmann, sono, com'è noto, i seguenti:
P versus NP
- La congettura di Hodge
- L'ipotesi di Riemann (che chiameremo d'ora in poi brevemente RH)
- La teoria di Yang – Mills e il problema del gap di massa
- Le equazioni di Navier – Stokes
- La congettura di Birch e Swinnerton – Dyer (che chiameremo brevemente Birch)

Di tutti questi , tutti ben esposti nel libro di Keith Devlin "I problemi del millennio" (Longanesi & C), quelli che si basano direttamente sui numeri primi sono chiaramente:
- la RH, tramite la sua famosa funzione zeta ("tutti gli zeri non banali sono sulla retta critica reale ½")
- P = NP con il problema esponenziale, o per lo meno sub – esponenziale, della fattorizzazione veramente veloce di grandi numeri composti (per esempio i cosiddetti numeri RSA usati in crittografia) nei loro fattori primi, lunghi qualche centinaio di cifre, nonostante la creazione di algoritmi sempre più potenti (Rif. 1). P =NP non è sempre possibile e, in generale, P è diverso da NP;
- infine, la Birch (forse vera ma ancora da dimostrare, proprio come la RH)e che concerne le curve ellittiche (il relativo problema è se ci sono o no infiniti numeri razionali su tali curve). Essa ha dato luogo ad un sistema crittografico basato sulle curve ellittiche (Rif.1), concorrente del sistema RSA basato invece sul prodotto di due grandi numeri primi, e si pensa che la dimostrazione della RH possa poi permettere di violare il codice RSA, ma non è ancora detto (c'è chi ritiene indipendenti i due problemi, e forse potrebbe anche avere ragione: il codice RSA potrebbe essere violato anche da futuri algoritmi di fattorizzazione veramente veloci ma anche indipendenti dalla RH, viceversa, con la dimostrazione della RH, si potrebbero trovare alcuni di questi algoritmi, magari perfezionando quelli attuali, già esistenti, che presuppongono la verità della RH).

Sistemi crittografici tramite numeri primi, quindi, connessi sia alla RH sia alla Birch. Dei rimanenti problemi del millennio, solo la Teoria di Yang - Mills e il relativo problema del gap di massa potrebbe, stando alle attuali conoscenze, coinvolgere i numeri primi, direttamente o indirettamente.

Tale Teoria è basata, matematicamente, sulla teoria dei gruppi: tra i gruppi più accreditati ci sono i gruppi di gauge di Lie ed in particolare un gruppo di gauge di Lie, non abeliano, semplice e compatto. Tali gruppi sono connessi ai numeri primi in modi diversi:

a) i gruppi semplici sono i costituenti fondamentali della teoria dei gruppi, così come i numeri primi sono i costituenti fondamentali di tutti i numeri interi;
b9 i fattori dei numeri di dimensione dei gruppi di Lie sono tutti numeri primi di Chen;
c) il numero n della formula delle geometrie proiettive per es. il piano di Fano,
n^2 + n + 1 deve essere primo, o una sua potenza, e anche il risultato della formula:
per n = 2, 3, 5 e 11 abbiamo i seguenti, connessi ai numeri di Lie:

2^2 + 2 + 1 = 7, e 7 x 2 = 14 = G2, il più piccolo dei gruppi di Lie
3^2 + 3 + 1 = 13, e 13 x 4 = 56 = F4
13 x 6 = 78 = E6
5^5 + 5 + 1 = 31, e 31 x 8 = 248 = E8
11^2 + 11 + 1 = 133, e 131 x 1 = 133 = E7

con 7, 13, 31 e 133 anch'essi numeri primi e fattori dei numeri di dimensione dei primi cinque sporadici gruppi di Lie, con G2 e E8 molto importanti nel Modello Standard e nelle Teorie di stringa (Rif.3.)

Per le equazioni di Navier – Stokes (che però contengono il simbolo Φ, la sezione aurea, connessa alla serie armonica, dalla quale nasce poi la funzione zeta) e la congettura di Hodge, non sembrano esserci evidenti connessioni dirette o indirette con i numeri primi.

Vediamo ora in breve, nell'ordine, i nostri tre problemi del millennio connessi con i numeri primi.

Capitolo I

Cominceremo con P versus NP, altrimenti detto anche P=NP

Un suo sottoproblema,com'è noto, è quello della fattorizzazione veloce, cioè eseguibile in tempo polinomiale. Noi abbiamo ricondotto,tramite un'equazione di secondo grado con congettura di Goldbach (Rif.1) tale problema P, ma non NP-completo, ad un problema polinomiale P risolvibile (ma non esiste nessun problema NP – completo riducibile a P (Rif.4).

Tale nostra equazione è identificabile con il già noto algoritmo di Fermat, ma da noi riscoperto in modo indipendente tramite la nostra soluzione della congettura di Goldbach, basata sulla semisomma s = (p+q)/2 e sulla semidifferenza d = (q-p)/2 e tramite la formula N = s^2 – d^2, per cui poi abbiamo N + d^2=s^2, e p = s - d e q = s + d; l'algoritmo di Fermat si basa sul calcolo di s con la formula

$$s = \sqrt{N + d^2}$$

e quindi con d tentativi.

Con numeri primi tra loro paragonabili, e quindi con valori di d piccoli, l'algoritmo è relativamente veloce ed efficace. Per esempio, con N = 127 x 229 = 29083, s = 178 =171 +7, dove 171 è la radice intera + 1 di N (poiché √29083= 170,53), con d = 7 tentativi prima di arrivare ad s = 178 e d = 51,tali che p = s - d = 178 – 51 = 127 e q = s + d = 178 + 51 = 229. Notiamo che in questo caso, e anche per casi simili, 7 ≈ √d = √51 = 7,14; ma attualmente non c'è modo di conoscere l'entità, neanche approssimativa, di d, quindi dobbiamo affidarci a successivi tentativi aggiungendo unità a √N fino a trovare il valore esatto di s^2 dal quale, togliendo N, abbiamo d^2: nel nostro esempio, s^2 = (170 + 7)^2 = 178^2 = 31684, e 31684 – 29083 = 2601 = 51^2 = d^2, sono bastati, quindi, solo 7 tentativi per giungere ad s e a d e quindi alla fattorizzazione di N = 29083 = 128 x 229.

Ci sarebbe anche una interessante relazione con la RH: se questa fosse vera,allora il problema della fattorizzazione veloce starebbe in P, cosa in genere ritenuta possibile, salvo qualche parere diverso(prof. Umberto Cerruti), per quanto anch'esso possibile .

Secondo il prof. Bottazzini, invece,"il problema della scomposizione di un numero in fattori sta in Np, ma non si a se stia anche in P (la risposta è positiva se l'ipotesi di Riemann è vera" (Rif.5)

Infine, noi abbiamo connesso la nostra soluzione della congettura di Goldbach (dalla quale poi deriva indirettamente l'algoritmo di Fermat, basato sulla semisomma anziché sulla somma di due numeri primi) anche alla congettura dei numeri primi gemelli (D = 2 e d = 1) e ai numeri primi di Polignac (D= 2n e d = n), dove D è la differenza sempre pari e quindi D =2n, tranne che p =2, vedi lavoro "Goldbach, Twin numbers and Polignac" sui nostri siti. Qui ricordiamo brevemente che la somma di due numeri primi gemelli p e p +2 (tranne i due soli gemelli 3 e 7, per i quali 3 + 7=8), è sempre di forma N = 12n, mentre per i numeri di Polignac , p e p+2n, (tranne che per il 2) , la loro somma è sempre di forma N pari = 6n $\pm$ 2, valida anche per i numeri gemelli quando n = 0, e quindi 6n $\pm$ 2 = 6 x 0 $\pm$ 2 = $\pm$ 2.

Questo perché, per la forma generale dei numeri primi (tranne il 2 e il 3)

$$P = 6n \pm 1 \qquad (1)$$

p si può scrivere come p = 6m$\pm$1 e q = 6n $\pm$1 , per cui la loro somma si può scrivere come p + q = 6m$\pm$1 + 6n $\pm$ 1 = 6(m+n) $\pm$ 2 (se i segni della (1) sono uguali per p e q, si avrà $\pm$ 2, se invece sono diversi, +1 e -1 si elidono a vicenda e si ha come somma solo 6(m+n). per il caso particolare dei numeri primi gemelli . di forma p = 6n -1 e p + 2 = q = 6m +1, abbiamo la differenza q - p = (6n+1) – (6n – 1) = 6n+1 - 6n +1 = +1 +1 = + 2, e la somma p + q = 6n -1 + 6n +1 = 6n + 6n = 12n. Le forme 6n$\pm$1 (che fanno parte delle forme 6 possibili forme ***6n-1***, 6n, ***6n+1***, 6n+2, 6n+3, 6n+4 e che contengono ***tutti*** i numeri) e danno luogo a diversi risultati sui

numeri primi, vedi nostri vari articoli; e una di esse, la forma N = 6n (i multipli di 6) è molto importante anche per la RH1, ipotesi equivalente alla RH) , s su tale forma abbiamo di recente scritto l'articolo "Dai multipli di 6 alla Riemann Hypothesis" (vedi sezione "Lavori Ing. Rosario Turco") che ci dà la certezza della verità della RH, essendo RH1 = RH.

Ecco perché tali forme sono importanti ma ancora molto trascurate: a noi ha permesso di aggirare la funzione zeta (moltiplicativa) e di dimostrare l'ipotesi equivalente RH1 (additiva) basata invece sulla funzione σ(n), somma divisori, a sua volta collegata alla nostra soluzione della congettura di Goldbach, che prevede più coppie di Goldbach per N = 6n, numeriche hanno più divisori rispetto ai numeri di altre forme, e quindi le somme di tali divisori sono più alte; funzione di Goldbach = G(N) e funzione σ(n) hanno quindi entrambe valori più elevati rispetto ai numeri di altre forme, e sono entrambe connesse tra di loro (i loro grafici di tipo comet, cometa, sono simili e non permettono contro esempi G(N) = 0 e L(n) = 0) per la congettura di Goldbach e per la RH1, per cui sono entrambe vere; e quindi anche la RH = RH1, essendo equivalenti . Ecco come nei numeri primi tutto è connesso,ed è compito di noi matematici studiare tali numerose connessioni, che arrivano a far luce anche sui problemi del millennio (per esempio le connessioni 6n → Goldbach → RH1, 6n$\pm$1 → primi gemelli → primi di Polignac → RH, 6n$\pm$1 → fattorizzazione con quadrati perfetti, con fattorizzazione connessa a P problema polinomiale se la RH è vera, ecc.)

Capitolo II

In questo secondo capitolo vedremo l'ipotesi di Riemann. RH, connessa sulla distribuzione non casuale dei numeri primi. Essa si basa sulla famosa funzione zeta

$$\zeta(s) = \Pi \frac{1}{1 - 1 / p\text{^}s}$$

tuttora studiatissima, per dimostrare come tutti i suoi zeri non banali debbano giacere sulla retta critica reale ½ affinché l'ipotesi sia vera.

Tra tutti e tre i problemi oggetto di questo lavoro, la RH è forse il più importante e difficile, sia in matematica sia in fisica per le possibili connessioni con la fisica quantistica e le teorie di stringa, ma anche il più studiato di tutti e quindi la sua soluzione potrebbe essere la prima ad essere trovata.

" Per Riemann tutte le sue previsioni e il suo lavoro sono un magnifico esempio di metodo da cui si apprende ancora oggi: Molte sue congetture sono state dimostrate, la teoria delle superfici ha preso piede. E' messo in dubbio solo il fatto che tutti gli zeri non banali, che sono infiniti, sono lì sulla retta critica" (Ing. Rosario Turco).

Tutti i nostri contributi sulla RH ("Sulle spalle dei giganti" versione in italiano e in inglese, ecc. sono già sui nostri siti (vedi sezione Link, e Riferimenti vari in calce al presente lavoro.) Circa una possibile relazione tra la fattorizzazione veloce e la RH, così scrive Keith Devlin nel suo libro (op.cit.) pag. 166:

> **"Il problema dell'apertura del codice per la crittografia RSA non è noto come NP completo (e probabilmente non lo è) quindi forse se ne potrebbe sviluppare una soluzione senza dimostrare che P = NP. Viceversa, la dimostrazione di quell'entità implicherebbe immediatamente che il problema dell'apertura del codice potrebbe essere risolto in tempo polinomiale mettendo pertanto in discussione l'intero sistema di sicurezza su Internet. Poiché attualmente non conosciamo alcun modo che garantisca la sicurezza di comunicazioni aperte in internet senza dipendere dall'effettiva impossibilità di risolvere un problema NP, l'attuale dipendenza delle economie occidentali da comunicazioni elettroniche sicure in Internet non fa che confermare quanto sia alta la posta legata alla verifica di P = NP"**

(Circa i sistemi crittografici, vogliamo ricordare qui che non ci sono solo RSA ed ECC, ma se ne stà sviluppando un altro, attualmente ritenuto inattaccabile, detto "crittografia quantistica" (vedi omonima voce di Wikipedia; anche con possibili sviluppi del computer quantistico e relativi algoritmi, per es. quello di Shor) e che potrebbe alla fine sostituire i primi due, specie se saranno resi violabili da futuri algoritmi di fattorizzazione veloce, nuovi di zecca o possibilmente derivati da algoritmi già noti, per esempio quello di Constant o di Fermat, ecc. (Rif. 1).

E a pag. 72, capitolo "La musica dei numeri primi", sulla possibile relazione tra RH e fattorizzazione:

> **"… Poiché l'ipotesi di Riemann ci dice moltissimo sui numeri primi, la sua dimostrazione potrebbe benissimo portarci ad un fondamentale progresso nelle tecniche di fattorizzazione. E questo non perchè in tal caso finalmente sapremo che l'ipotesi è vera; infatti, sospettando che lo fosse, sono anni che i matematici ne studiano le conseguenze. In effetti alcuni metodi di fattorizzazione funzionano *presupponendo* che essa sia vera. Piuttosto, chi si serve dei codici cifrati, teme che i metodi impiegati per dimostrare l'ipotesi comportino la comprensione di nuovi elementi attinenti al modello di distribuzione dei numeri primi – una comprensione che potrebbe portare a metodi di fattorizzazione più efficienti…"**

Quindi, tra P =NP e la RH c'è una profonda connessione, anche se riguarda soltanto la fattorizzazione veloce Fv, sottoproblema di P = NP; sottoproblema che starebbe in P se la RH fosse vera;: in poche parole, Fv $\rightarrow$ P se RH vera . E poiché la RH è vera per il primo miliardo e mezzo di numeri primi, non si vede ancora il perché non dovrebbe essere vera per gli infiniti numeri primi successivi…

Capitolo III

Rimane ora da vedere un po' meglio la congettura di Birch e Swinnerton - Dyer (Rif. 1), basata sulle curve ellittiche, a loro volta connesse ad un altro sistema

crittografico (ECC) concorrente del più famoso sistema RSA, ma con chiavi più corte e quindi più adatte a sistemi elettronici portatili,come palmari o telefonini

> "**La RH e Birch – Swinnerton-Dyer sono legati per molte cose: numeri primi, crittografia, infinità, densità (densità degli zeri vedi Montgomery e densità dei punti razionali). Si può adottare anche per la RH per aggirare l'infinità degli zeri usando una tecnica modulo sulla retta anziché sulla curva ellittica? Se ci si deve ricondurre alla funzione L di Dirichlet è già noto con la GRH e non serve usare l'alto metodo che sarebbe difficile.**
>
> **L'altra differenza è che sulle curve ellittiche si cercano gli infiniti punti razionali (interi o frazioni) e sulla retta critica i valori hanno un solo valore razionale /frazione ovvero ½) mentre l'altro è irrazionale: la parte immaginaria dello zero. Con Riemann anche qui gruppi di punti ma irrazionali…"**

(Da corrispondenza privata – 17.7. 2009 – con l'Ing. Rosario Turco)

Anche qui, come tra RH e P = NP tramite la Fv, una nuova possibile connessione numeri razionali sulle curve ellittiche della Birch…, numeri irrazionali sulla retta critica della RH… connessione che si potrebbe approfondire in seguito.

Alcune formule della Birch si basano sui numeri primi (Rif 1, pag 247) sulle "funzioni di densità":

$$\prod_{p \leq M,\ p \text{ primo}} \frac{p}{N_p}$$

con il più semplice prodotto infinito:

$$\prod_{P} \frac{p}{N_p}$$

dal quale si arriva alla formula

$$L(E,1) = \prod_{p} \frac{p}{N_p}$$

che è alla base della congettura:

> "la curva ellittica, avrà un numero infinito di punti razionale, se, e solo se
> $L(E,1) = 0$ "

Per i dettagli su questo problema rimandiamo al libro di Devlin (Rif.2)
Un'altra sintetica definizione di questa congettura è su Wikipedia, voce "Problemi del millennio:

“ La congettura di Birch e Swinnrton –Dyer è basata su un particolare tipo di curve, le curve ellittiche dei numeri razionali. Questa congettura si basa sul fatto che le equazioni abbiano finite o infinite soluzioni razionali. Il decimo problema di Hilbert era simile ma trattava delle funzioni diofantee e si è dimostrato che non si è in grado neanche di decidere se esiste o no una soluzione” - Se la congettura di Birch e Swinnerton -Dyer fosse vera, sarebbe possibile rompere la cifratura basata sulle funzioni ellittiche in tempo polinomiale e non esponenziale”

Scrive ancora l’ing. Turco:

“ E’ difficile ai più decrittare una funzione ellittica che trovare la scomposizione in fattori…il problema è poco noto. Esiste un polinomio? Occorre Goldbach? Il metodo di ricerca della radici di Newton o di Sturm sono più veloci? Quali equazioni sono le migliori? Quali sono i metodi più veloci e migliori? Esistono altre curve di grado superiore a 3 e più difficoltose di quelle ellittiche? Esiste un nuovo algoritmo?”

A queste domande cercheremo di rispondere in seguito, con ulteriori lavori sull’argomento. Continua Devlin:

“ Il problema è riuscire a dimostrare o a confutare il fatto che non esistono problemi NP o detto con diversi termini che tutti i problemi NP possano essere resi di tipo P. Questa è una domanda molto importante per l’informatica teorica. Vedi teoria della complessità algoritmica per una discussione più completa.

Per l’ipotesi di Riemann, invece, da Wikipedia”I problemi del millennio”, pag. 1 di 3:

“ Inoltre, se l’ipotesi di Riemann fosse vera, sarebbe possibile trovare un algoritmo per rompere anche le cifrature basate sui numeri primi in tempo polinomiale….L’ipotesi di Riemann riguardala distribuzione dei numeri primi: Riemann ipotizzò che la distribuzione dei numeri primi seguisse una particolare funzione chiamata funzione zeta di Riemann. Questa ipotesi è stata verificata per un miliardo e mezzo di numeri primi, ma la sua verifica definitiva attraverso un teorema avrebbe profonde ripercussioni sulla matematica pura come nelle applicazioni di crittologia. Una controversa proposta di soluzione non per la soluzione in se, ma per l’Autore) è stata presentata da Louis Branges de Bourcia nel 2004 “

In pratica, le cifrature basate sul sistema RSA e sulle curve ellittiche sarebbero messe in pericolo dalla soluzione dei rispettivi problemi del millennio (RH e Birch), visto che entrambi hanno in comune numeri primi, sistemi crittografici, fattorizzazioni e prodotti infiniti, oltre alle altre cose accennate prima (nfinità, densità di zeri e di punti razionali, ecc.) riportate prima dall’Ing. Turco.

Sintesi grafica delle connessioni:

P =PN (**fattorizzazione** e sistema crittografico ***RSA***) ← ***RH***

↓ (**fattorizzazione** e sistema crittografico ***ECC***) prodotto infinito per $\zeta(s)$ e per l'equazione: $L(E,1) = 0$ ↑

↓ Congettura di ***BIRCH e SWINNERTON-DYER*** ↑

Così il cerchio delle connessioni si chiude, "accerchiando" i tre problemi, ed è già pronto per nostri o altrui ulteriori possibili approfondimenti, fino alla dimostrazione finale, possibilmente positiva, di uno o più di essi.

Conclusioni

PN = NP, RH e Birch sono quindi, come abbiamo visto, i tre problemi del millennio connessi ai numeri primi, e la dimostrazione di uno di essi , che al momento riteniamo tutti e tre veri (cioè con soluzione positiva) potrebbe benissimo influire, prima o poi, sulla dimostrazione degli altri due. E quindi possiamo concludere che, date le notevoli interconnessioni viste in questo lavoro, essi si dimostreranno o tutti e tre veri, o tutti e tre falsi, e con maggiori probabilità si verificherà il primo caso.

Sulla RH ogni tanto qualcuno propone una dimostrazione positiva, che poi però sembra non reggere alle verifiche (per esempio quella di Louis Branges de Bourcia).

Una delle nostre proposte di soluzione è ""dai multipli di 6 alla Riemann Hypothesis" tramite l'equivalenza RH1 = RH, che non ammette contro esempi L(n) = 0 per la RH1 (poiché L(n) cresce in proporzione al crescere di n), e quindi non dovrebbero essercene nemmeno per la RH (uno zero fuori dalla retta critica reale ½), essendo le due ipotesi equivalenti.

Un'altra, di Rosario Turco e Maria Colonnese, è "Proposta di dimostrazione alle Ipotesi di Riemann e Congettura molteplicità degli zeri", vedi riferimenti vari.

Altri nostri contributi sulla RH sono nel lavoro "Sulle spalle dei giganti", e in altri lavori. Se la RH è vera, deve esistere un polinomio per la fattorizzazione veloce in tempo polinomiale, e quindi la fattorizzazione veloce sta in P, ed ecco la connessione tra P=NP ed RH; mentre la congettura di Birch potrebbe avere una connessione con

la RH tramite il comune prodotto infinito, e/o anche un altro tipo di connessione ancora da scoprire, e quindi sarebbe vera anch'essa (vedi Rif.1).

L'opinione generale è che siano entrambe vere (in verità sono ben poche le voci anti – RH).

Il "filo rosso" dei numeri primi attraversa entrambe le congetture, ma anche il problema della fattorizzazione veloce; e seguendo bene il percorso di tale filo rosso attraverso i tre problemi del millennio qui considerati, potremmo arrivare (noi o altri) alla loro soluzione positiva: questa previsione è la nostra piccola "profezia" matematica, quale che sia il tempo in cui si avvererà, noi pensiamo già entro pochissimi anni.

Per quanto riguarda invece altre congetture non riguardanti i numeri primi,, per esempio la congettura di Hodge, L'ing. Turco pensa che:

"**Il problema di Hodge è molto più slegato dagli altri anche se riguarda sempre il campo delle funzioni complesse di variabile complessa, le superfici di Riemann, le geometrie proiettive etc. Una sua soluzione non avrebbe una immediata ricaduta sugli altri problemi"**

Però…ci sarebbe un però. l'Ing. Turco ha parlato qui genericamente di geometrie proiettive, le quali si basano su una formula per il calcolo del numero dei loro elementi

$$n^2 + n + 1$$

con n numero primo o una sua potenza, e anche il risultato sarà primo, come per esempio nel piano di Fano (la più semplice geometria proiettiva) , dove n = 2, e il numero degli elementi è quindi 4+2+1 = 7, anch'esso numero primo, e legato a G2 = 2 x 7 = 14, come gruppo di simmetria di Lie degli ottonioni, e molto importante nel Modello Standard (vedi nostro lavoro "Il piano di Fano") sul nostro sito sezione "Lavori Di Noto", Rif.7).

Conseguenza interessante: i numeri primi potrebbero rientrare in gioco anche nella congettura di Hodge, tramite l'eventuale contributo che le geometrie proiettive potrebbero dare ad una futura dimostrazione della congettura di Hodge, un problema del millennio apparentemente molto lontano dai numeri primi, il cui "filo rosso" prima accennato, potrebbe intrufolarsi in qualche modo anche in quest'altro problema del millennio. Ma per ora limitiamoci ai soli tre problemi trattati in questo lavoro, per gli altri due (YangMills, equazione di Navier –Stokes), se ne parlerà eventualmente in seguito.

Riferimenti

1.) “Le basi della crittografia”, sul nostro sito www.gruppoeratostene.com sezione “Lavori Ing. Rosario Turco) e “Congettura di Birch e Swinnertyon – Dyer - Curve ellittiche –Fattorizzazione discreta –Crittografia”
2.) Keith Devlin “I problemi del millennio” Longanesi e Cpag.127.
3.) Mario Livio, L’equazione impossibile” BUR
4.) Articoli vari sulla congettura di Goldbach sui siti sottoelencati
5.) Umberto Bottazzini “articolo “Goldbach e altre ipotesi tutte da dimostrare” su “Il Sole - 24 Ore” del 20 maggio 2000
6.) Voce “I problemi del millennio” di Wikipedia
7.) “Il piano di Fano”, Gruppo Eratostene, vedi nostro sito
8.) Libro “L’ossessione dei numeri primi” , Bollati Boringhieri
9.) Altri nostri articoli vari sull’ipotesi di Riemann, pubblicati sui seguenti siti

Siti

CNR SOLAR
http://150146.3.132/

Prof. Mattew R Watkins
http://www.secamlocal.ex.ac.uk

Aladin’s lamp(ing. Rosario Turco)
www.geocities.com/SiliconValley/Port/3264
menu MiSC section MATEMATICA

ERATOSTENE group
http://wwwgruppoeratostene.com

Dr. Miche Nardelli
http://xoomer.alice.it/stringhtheory/

Blog
http://MATHBuildingBlok.blogspot.com

Bookshelf
http://rudimathematici.com/bookshelf.htm

Nota 1
Per la “Crittografia quantistica”, e gli argomenti connessi “Computer quantistico” e “Qnet” vedere le omonime voci di Wikipedia

Nota 2: Indizi attuali sulla verità della RH (da Derbyshire):

Circa i migliori attuali indizi sulla verità della RH, riporteremo qui le ”prove” elencate da Derbyshire nel suo libro (Rif. 8), pag. 340:

“…Questa linea di pensiero è stata ripresa in tempi dal matematico australiano James Franklin.. Il suo articolo del 1987, *Non- deductive Logic in Mathematics* (Logica non deduttiva in matematica), pubblicato sul << British Journal for the Philosophy of Sciences >> comprendeva un paragrafo intitolato << Evidence for the Riemann Hypothesis and Other Conjectures >> (Prova per l’ipotesi di Riemann ed altre congetture).

Franklin si avvicina alla RH come si farebbe in un processo, e presenta le prove per la verità della RH:

- Il risultato del 1914 di Hardy secondo cui infiniti zeri si trovano sulla retta critica;

- La RH implica il TNP, che si sa essere vero.

- << Interpretazione probabilistica di Denjoy >> , ovvero lo studio del lancio di una moneta esposto in questo capitolo.

- Un altro teorema del 1914 di Landau e Harald Bohr, secondo cui la maggior parte degli zeri, tranne una parte infinitesima, è molto vicina alla retta critica. Notate che dal momento che il numeri degli zeri è infinito, un trilione vale come una parte infinitesima.

- I risultati algebrici di Arti, Weil e Deligne, che ho citato nel paragrafo 17.3”

A tutte queste prove indiziarie per la verità della RH, vogliamo aggiungere anche un nostro solo risultato particolare , “Dai multipli di 6 alla Riemann Hypothesis” di Rosario Turco – Gruppo Eratostene, basato anche su precedenti nostri lavori sull’equivalenza di Lagarias RH1 = RH, vedi anche “Sulle spalle dei giganti”, e nei quali mostriamo l’inesistenza di contro esempi L(n) = 0 per la funzione L(n); e siccome RH1 = RH, non ci dovrebbero essere contro esempi nemmeno per la RH (zeri non banali fuori dalla retta critica). Noi riteniamo molto importante questo nostro risultato, poiché aggira la funzione moltiplicativa complessa $\zeta(s)$ tramite la più semplice funzione additiva reale $\sigma(n)$, o somma divisori, per giungere allo stesso risultato (verità della RH e equivalente alla verità dell’ipotesi equivalente RH1).

Mentre la RH si basa, tramite la funzione $\zeta(s)$, sui numeri primi, di forma generale $6k\pm1$, e con nessun fattore non banale, la RH1 si basa sui numeri di forma intermedia $6n$, che al contrario hanno più fattori rispetto ai numeri di forma diversa ($6k\pm2$, $6k\pm3$), e quindi con più alti valori di $\sigma(n)$, apparentemente più “pericolosi”per la RH1. Ma nei nostri suddetti lavori noi mostriamo chiaramente che nonostante ciò, essi non producono ugualmente contro esempi, comunque cresca n (anzi, più cresce n, più L(n) si allontana da 0, e quindi determinano la verità di RH1 = RH.