Block Notes Matematico

Sulle spalle dei giganti[1]

dedicato a Georg Friedrich Bernhard Riemann

ing. Rosario Turco[2], prof. Maria Colonnese, dott. Michele Nardelli, prof. Giovanni Di Maria, Francesco Di Noto, prof. Annarita Tulumello

Abstract

This work presents various mathematical basic ideas, for the understanding of issues relating to the Riemann hypothesis (RH), the RH's equivalent and the GRH. This "Block Notes of Math" shows also subproblems of the RH, the LH hypotheses, the factorization and the main links between all the equations involved, through a "grid connections".

The authors then show how the "RSA code" can be under attack, where the factorization of a semiprime N (N=a*b) is obtained through the Goldbach conjecture, with and a second-degree equation or through a second-degree equation of the type $x^2 = a^2 \bmod N$. Also they show how the problem of Basel has already solved in closed form for N odd with the constants zeta. Then they propose a new conjecture through the use of average cumulative Mertens function linked to the Mertens function and finally there is the presentation of a conjecture of how G(N), the number of solutions of Goldbach, and g(N), the number of twins primes, are linked with the logarithm integral of Gauss and the RH. This conjecture is candidate as additional and equivalent hypothesis of the RH .

Sommario

Nel lavoro vengono presentati i vari strumenti matematici e le idee di base, per la comprensione delle problematiche relative alla ipotesi di Riemann (RH), alle ipotesi equivalenti e alla ipotesi di Riemann generalizzata (GRH). Vengono mostrati sottoproblemi della GRH e della RH, come l'ipotesi LH, la fattorizzazione ed i principali legami tra tutte le equazioni in gioco, attraverso una griglia delle connessioni. Gli autori successivamente mostrano come il codice RSA sia attaccabile, sfruttando sia la congettura forte di Goldbach nella fattorizzazione di un semiprimo N con un'equazione di secondo grado (proponendone anche una generalizzazione a m fattori), sia attraverso una equazione di secondo grado del tipo $x^2 = a^2 \bmod N$. Inoltre mostrano come il problema di Basilea sia già risolto in forma chiusa per N dispari con le costanti zeta; poi propongono una nuova congettura introducendo la funzione media cumulativa di Mertens legata alla funzione di Mertens stessa e una funzione correttrice nell'ambito della RH4. Infine c'è la presentazione della congettura del legame del numero di soluzioni di Goldbach G(N) e del numero di soluzioni dei numeri gemelli g(N) con il Logaritmo integrale e la RH e la presentazione del relativo termine di errore, candidando l'espressione come ulteriore ipotesi equivalente della RH.

Ringraziamenti

Gli Autori ringraziano sin da adesso tutti i lettori pazienti che daranno un ritorno su quanto letto (vedi email) .

[1] E' una frase famosa di Isaac Newton , nonché titolo di uno dei capitoli del libro di Derbyshire [riferimento 1]. Vista però la "statura" dei matematici che ci hanno portato fino a Riemann, e che purtroppo non possiamo menzionare tutti, ci sembra un giusto titolo per l'articolo.

[2] Rosario Turco è un ingegnere presso Telecom Italia (Napoli) ed ideatore di "Block Notes Matematico" insieme alla prof. Maria Colonnese del Liceo Classico "De Bottis" di Torre del Greco, provincia di Napoli; tutti gli altri autori fanno parte del gruppo ERATOSTENE di Caltanissetta

Introduzione

L'ipotesi di Riemann è un argomento estremamente affascinante, non solo per chi ci lavora da professionista, ma anche per i tanti appassionati di matematica. Dietro a tale ipotesi si scoprono ogni giorno una vastità di argomenti, forse tra i più belli della matematica.

L'ipotesi coinvolge l'aritmetica, la Teoria dei numeri, l'algebra, la geometria, l'analisi, la statistica, la probabilità, i campi finiti e infiniti, gli operatori e ogni tipo di campo numerico: interi, razionali e irrazionali, reali, complessi, p-adici; si estende, inoltre, a problemi come la fattorizzazione, la crittografia e le curve ellittiche e poi si collega a problemi pratici nel campo della fisica e dei linguaggi formali (come la Teoria delle stringhe etc), fino ad arrivare a progetti di enorme importanza come quello Langlands.

Il lavoro di Riemann, e la matematica da lui ideata a supporto della sua stessa ipotesi, sono stati di notevole aiuto per risolvere molti altri problemi a partire dalla dimostrazione del TNP. La mole di pubblicazioni e di teorie nate successivamente accanto all'ipotesi di Riemann è di una vastità enorme.

In "Block Notes Matematico" mostreremo, là dove possibile, il sentiero intrapreso dalle principali idee e come sono nate, facendo riflettere sull'impalcatura su cui si è poggiata la teoria stessa; fino a far comprendere l'enigma del secolo. Mostreremo gli strumenti necessari alla comprensione del problema, a volte in modo rigoroso e a volte in modo semplicistico, sia per motivi di spazio oltre che per adeguata competenza su taluni argomenti molto complessi, sia per non appesantire troppo "*Block Notes Matematico*" e far perdere di vista il filo logico che porta a Riemann.

Sono ovviamente consigliati ulteriori approfondimenti che possono essere fatti sia su articoli accademici sia su validi testi, universitari e non, per ognuno degli argomenti qui mostrati.

Lo scopo di "Block Notes Matematico" è, quindi, divulgativo, suddiviso in capitoli, con la teoria strettamente necessaria; con considerazioni, calcoli e disquisizioni, a volte corretti e a volte come volo pindarico (non ce ne vogliate!), desideroso di trovare altre strade e fornire nuovi spunti, destinati sia all'appassionato sia al lettore attento, che sa un po' più di matematica. Se saremo riusciti a farvi appassionare alla matematica e a farvi dedicare ad un problema della Teoria dei Numeri avremmo raggiunto il nostro piccolo obiettivo.

INDICE

Capitolo 1. Numeri primi e loro distribuzione 6
Capitolo 2. L'andamento del logaritmo naturale e delle potenze 9
Capitolo 3. Le serie e il concetto di estensione del dominio 11
La serie armonica 11
La serie del problema di Basilea 15
La zeta di Riemann come funzione reale di variabile reale 16
Estensione del dominio di una funzione definita da una serie 17
L'estensione del dominio della funzione zeta di Riemann 20
Capitolo 4. La funzione O grande 21
Definizione della O grande 21
La funzione O(1) 21
La funzione O(g(x)) 22
Intervallo di validità della funzione O grande 22
Capitolo 5. I numeri complessi e le serie complesse 22
Capitolo 6. Le funzioni gamma e beta 25
Problemi di interpolazione 26
Il fattoriale positivo e razionale 27
Esiste il fattoriale negativo? 31
Numeri complessi, la funzione gamma ed il fattoriale 32
Formule varie 34
Capitolo 7. La funzione zeta di Riemann 35
Zeri banali e non banali 38
Riemann Hypotesis (RH) 40
Spaziatura media degli zeri nella striscia critica 42
$\pi(x)$ e gli zero di ς (s) 42
RH1 equivalente a RH (risultato di Lagarias) 48
RH2 equivalente a RH (funzione di Mertens) 49
L'interpretazione probabilistica di Denjoy 50
RH3 equivalente a RH (risultati di Von Kock) 51
RH4 equivalente a RH (funzione Θ) 52
RH5 equivalente a RH (sequenza di Farey) 52
RH6 equivalente a RH (teoria dei gruppi e funzione di Landau) 53
RH7 equivalente a RH (Derivata della zeta di Riemann) 53
Considerazioni sulle ipotesi equivalenti della RH 53
Conseguenze deboli della RH (LH: l'ipotesi Lindelhof) 54
Generalized Riemann Hypotesis (GRH) 57
Conseguenze della GRH 58
Capitolo 8. Teoria dei campi, degli operatori e legge di Montgomery-Odlyzko 59
Fisica nucleare, Meccanica Quantistica e zeri non banali della zeta di Riemann 63
La legge di Montgomery-Odlyzko 64
Il caos e i sistemi caotici classici 66
Campo p-adico e spazio adelico 66
Capitolo 9. Sottoproblemi della RH 67
Congettura di Cramer 67
Osservazioni su R(p) 69
Congettura di Cramer come sottoproblema della RH 70
Considerazioni sul termine d'errore 71

Tecniche informatiche per i gap massimali....72
Capitolo 10. Osservazioni, calcoli e disquisizioni....72
Accendiamo i motori....72
Calcolo dei numeri primi tra n e 2n....74
Goldbach e Riemann....75
Congettura per forme chiuse G(N) e g(N) – ipotesi equivalenti RH....76
Goldbach e la fattorizzazione dei semiprimi e del RSA....80
Metodo algoritmico per fattorizzare in base a Goldbach....80
E' generalizzabile il metodo ad un numero di fattori qualsiasi?....81
Fattorizzazione e quadrati perfetti....82
Fattorizzazione dei semiprimi e del RSA col modulo....83
L'RSA è attaccabile? In pratica sì e senza RH!....83
Il problema di Basilea e le costanti zeta....83
Costanti zeta....84
Formula generale delle costanti zeta $\zeta(2n+1)$....85
Formula generale delle costanti zeta $\zeta(2n)$....85
La dimostrazione di Eulero per N pari....86
Funzioni correttrici....87
Congettura sulla funzione media cumulativa di Mertens....88
Capitolo 11. Grafici e tabelle funzioni coinvolte con la RH....90
Legami tra formule e griglia delle connessioni....98
Capitolo 12. Scarabocchi e calcoli finali sulla RH4....101
Appendice - Costanti Matematiche....104
Riferimenti....105
Ripassi veloci e approfondimenti....105
Email per suggerimenti e segnalazioni....106

FIGURE

Figura 1 – Andamento $\pi(N)$....6
Figura 2 – Teorema TNP....8
Figura 3 – logaritmo vs potenze....9
Figura 4 – funzione ξ....17
Figura 5 – la funzione S(x)....18
Figura 6 – Dominio della funzione 1/1-x....19
Figura 7 – x vs O(1)....22
Figura 8 – Il fattoriale....32
Figura 9 – La funzione gamma....33
Figura 10 – TNP in vari intervalli....36
Figura 11 – ξ e piano degli argomenti....39
Figura 12 - ξ in vari intervalli del piano dei valori....40
Figura 13 – zeri non banali e striscia critica....40
Figura 14 – J(x)....44
Figura 15 – Schiacciamento con J(x)....44
Figura 16 – Termini periodici di Riemann....47

Figura 17 - Andamento LH (a).....54
Figura 18 – Andamento LH (b).....54
Figura 19 – Funzione di Lindelhof.....55
Figura 20 – Ipotesi di Lindelhof.....56
Figura 21 – radx*logx vs logx*logx 71
Figura 22 – Coefficienti costanti zeta.....85
Figura 23 – costanti zeta per 2n.....86
Figura 24 – funzione di Moebius (a).....91
Figura 25 – funzione di Moebius (b).....92
Figura 26 – L(n) 92
Figura 27 - Goldbach.....93
Figura 28 – Funzione totiente di Eulero.....94

TABELLE

Tabella 1 – N/π(N).....7
Tabella 2 – Andamento della derivata.....10
Tabella 3 – Andamento dell'integrale.....10
Tabella 4 – Valori serie di Basilea 16
Tabella 5 – Pendenze di x vs O(1) 21
Tabella 6 – Valori del fattoriale 27
Tabella 7 – Storia degli zeri non banali.....41
Tabella 8 – Filtro di Chebyscev 46
Tabella 9 – Valori di Θ(x) 52
Tabella 10 - Anello Z/4Z.....61
Tabella 11 – Gap e Rp.....68
Tabella 12 – Andamenti di g(p) 70
Tabella 13 – G(N) : ipotesi equivalente RH.....77
Tabella 14 – g(N) ipotesi equivalente RH.....79
Tabella 15 - φ(n) ed n.....96
Tabella 16 - Tabella dei valori di φ(n) 97
Tabella 17 - Griglia delle connessioni.....99

Capitolo 1. Numeri primi e loro distribuzione

La prima prova del fatto che esistono infiniti numeri primi fu data da *Euclide* nel terzo secolo a.C. ; mentre una maggiore comprensione sulla distribuzione dei numeri primi venne data nel 1896, quando *Jacques Hadamard* e *Charles de la Valle Poussin* indipendentemente dimostrarono il Teorema dei Numeri primi (**TNP**). In verità la RH era già stata formulata da Riemann e molti suoi strumenti matematici furono utili alla dimostrazione del TNP che poteva far uso di una ipotesi meno forte della RH.

Definiamo adesso la seguente funzione a gradino, che conta i numeri primi:

$$\pi(x) = \sum_{p \le x} 1 = \quad \text{\# di primi minori o uguali a } x \quad (2)$$

Il grafico di $\pi(x)$, per vari intervalli, è mostrato in Fig. 1. Dalla (2), sapendo che esistono infiniti numeri primi è:

$$\pi(x) \mapsto \infty \, as \, x \mapsto \infty \qquad (3)$$

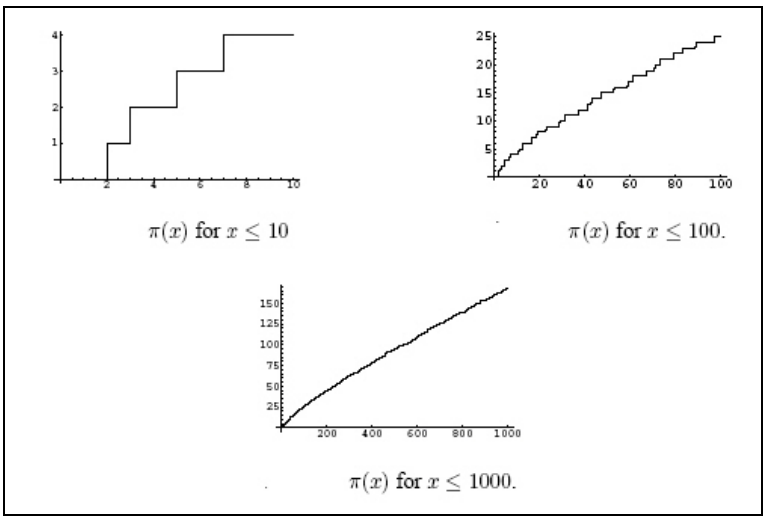


Figura 1 – Andamento π(N)

Il problema, postosi già all'epoca di *Eulero*, era di trovare una formula per ottenere il valore $\pi(x)$, in corrispondenza di x, senza contare i numeri primi e senza dover stilare tabelle infinite.

Il primo teorema dei numeri primi (**TNP**), fu proposto da *Gauss* nel 1792, che forniva una formula asintotica per $x \mapsto \infty$, e successivamente dimostrato rigorosamente da Hadamard e Poussin:

$$\pi(x) \approx \frac{x}{\ln(x)} \qquad (4)$$

In alternativa la (4) si esprime:

$$\lim_{x\to\infty}\frac{\pi(x)\ln(x)}{x}=1$$

La (4) (vedi [1]) è una conseguenza dell'osservazione di *Gauss* circa i dati della tabella 1 seguente.

N	Log N	N/π(N)	Errore %
1000	6,9077	5,9524	16,0490
1000000	13,8155	12,7392	8,4487
1000000000	20,7352	19,6665	5,3731
1000000000000	27,6310	26,5901	3,9146
1000000000000000	34,5387	33,5069	3,0794
1000000000000000000	41,4465	40,4204	2,5386

Tabella 1 – N/π(N)

La tabella 1 è la rappresentazione di una funzione tabellare, con valori di ingresso e di uscita. L'ingresso in questo caso è l'argomento N mentre l'uscita è il valore della funzione N/π(N). E' un classico della matematica scoprire da una tabella di dati che se un argomento varia per somma costante ed il corrispondente valore funzione per un prodotto costante allora il tutto è indice dell'esistenza di una dipendenza logaritmica (logaritmo naturale). Se, viceversa, N fosse aumentato come somma mentre N/π(N) come prodotto allora la dipendenza sarebbe stata esponenziale. Dalla tabella 1 si osserva proprio che al crescere dell'argomento N con il prodotto di uno stesso fattore (1000 nell'esempio), il "valore funzione" N/π(N) cresce, invece, per somma costante (in questo caso di circa 7 unità) mentre l'errore percentuale diminuisce sempre più.

Successivamente Gauss definì la funzione **Logaritmo integrale Li(x)**:

$$Li(x):=\int_2^x\frac{dt}{\ln(t)}$$

L'integrale parte dal valore 2 poiché il numero naturale 1 non viene considerato numero primo. In tal caso il TNP può essere anche riscritto nella versione evoluta:

$$\pi(x)\approx Li(x) \qquad (5)$$

In altri termini si approssima π(x) con l'area sottesa del logaritmo integrale.

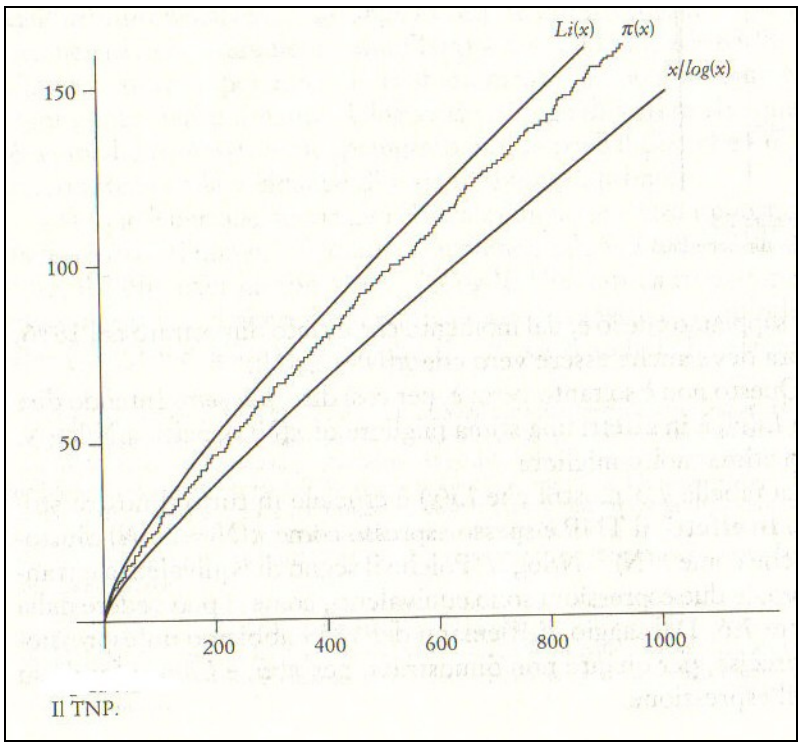


Figura 2 – Teorema TNP

Dalla figura 2 si vede che l'errore che si ottiene con la (5) è migliore di quello ottenibile con la (4). Apparentemente sembra che Li(x) sia leggermente superiore ai valori ottenibili con $\pi(x)$. Ma ci renderemo conto che non è sempre così.

Conseguenze del TNP

Il TNP comporta almeno due conseguenze:

- *La probabilità che N sia un numero primo è* $\sim$ *1/log N*
- *L'N-esimo numero primo è* $\sim$ *N log N*

La prima conseguenza è giustificata dal fatto che se esistono N/log N numeri primi tra 1 e N, la densità media dei numeri primi è 1/log N; inoltre poiché per N alti l'ordine di grandezza della maggior parte di essi è confrontabile con N, la densità dei numeri primi è proprio 1/log N.

Con un analogo ragionamento si può stimare anche la grandezza dell'N-esimo numero primo. Ad esempio ipotizzando un numero K grande e considerando un intervallo di numeri da 1 a K in cui ci sono P numeri primi, allora in media ci si può attendere che il primo numero primo si trovi a K/P, il secondo a 2K/P etc. e l'ultimo a PK/P = K. Per il TPN però P = K/log K e l'N-esimo numero primo è dalle parti di NK/P = NK/(K/log K) = N log K. Ora però K è dello stesso ordine di grandezza di N per cui l'N-esimo numero primo è intorno a N log N.

Capitolo 2. L'andamento del logaritmo naturale e delle potenze

Non abbiamo l'intenzione di mostravi che cos'è il logaritmo, decimale o quello naturale, né le regole delle potenze a cui esso è legato. Quello che ci interessa mostrare è, invece, il comportamento del logaritmo naturale ln, rispetto al comportamento delle potenze x^a. Questo tornerà utile, successivamente, quando parleremo della funzione O grande e delle ipotesi equivalenti di Riemann..

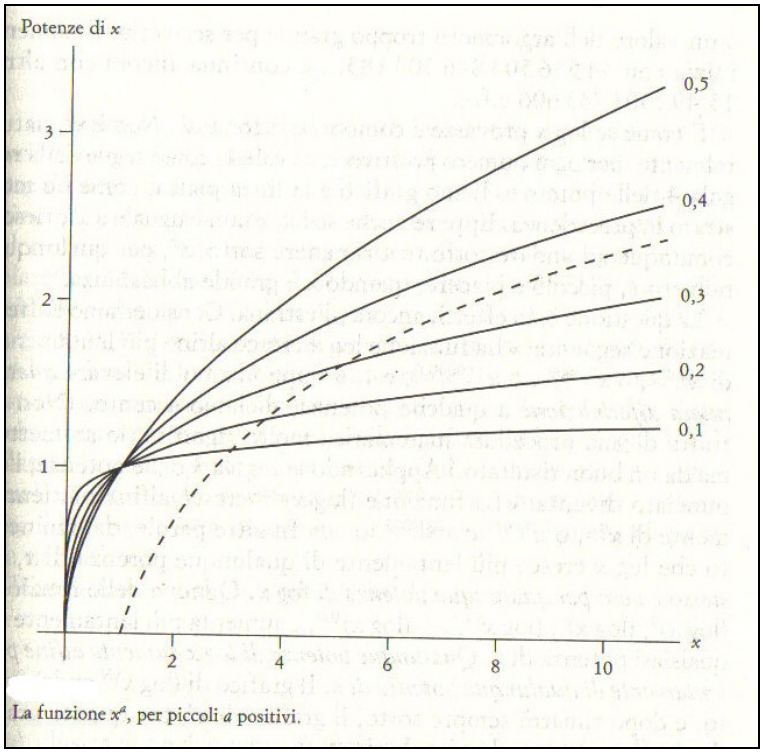


Figura 3 – logaritmo vs potenze

In Figura 3, in tratteggio c'è l'andamento del logaritmo naturale *ln x* ; mentre con tratto continuo c'è l'andamento delle *potenze* x^a con a=0,1 , 0,2 , 0,3 , 0,4 e 0,5 ovvero per piccoli valori di a .

Si osservano le seguenti cose:

- più piccolo è il valore di a, più piatto è l'andamento della potenza x^a; finché ad a=0 l'andamento diventa quello piatto massimo, cioè pari alla costante $1=x^0$
- per valori di a minori di un certo valore (in pratica 1/e) la curva del ln x incrocia presto la potenza x^a (mai oltre a e^e)
- indipendentemente da quanto sia piccolo a, alla fine ln x è più piatta della potenza. In realtà per a < 1/e ciò è sempre vero, mentre per a > 1/e , per valori di x grandi, il ln x interseca di nuovo la curva x^a e poi per sempre rimane più basso. Ad esempio se poniamo a=0,00000000001 la potenza è quasi piatta, corrispondente a 1 (cresce lentamente in realtà); il ln x la oltrepassa a destra di poco, a distanza e, diventando piatta sempre di più, incrociando la potenza e rimanendo per sempre sotto essa. In realtà è come se il ln x si volesse

comportare come x^0!

In altri termini ln x cresce molto più lentamente di una potenza x^{ε} , con ε piccolo a piacere, e lo stesso è vero per qualsiasi potenza del logaritmo e si potrebbe osservare con un grafico analogo a quello precedente.

Logaritmo naturale, derivata e integrale

Supponiamo di considerare le derivate delle potenze di x ed avremo una tabella come quella che segue.

Funzione	x^{-3}	x^{-2}	x^{-1}	x^0	x^1	x^2	x^3
Derivata	$-3x^{-4}$	$-2x^{-1}$	$-x^{-2}$	0	1	2x	$3x^2$

Tabella 2 – Andamento della derivata

Ricordiamo che la derivata indica una variazione rispetto una variabile. Ad esempio *dv/dt* in fisica è la variazione della velocità, quindi l'accelerazione. La derivata rappresenta comunque la pendenza o il gradiente (o tasso di variazione) di una curva in un determinato punto. Ad esempio la pendenza del ln x è sempre 1/x.

Ora supponiamo di considerare gli integrali delle potenze di x ed avremo una tabella come quella che segue.

Funzione	x^{-3}	x^{-2}	x^{-1}	x^0	x^1	x^2	x^3
Integrale	$-\frac{1}{2}x^{-2}$	-x-1	Ln x	x	$\frac{1}{2}x^2$	$1/3x^3$	$1/4x^4$

Tabella 3 – Andamento dell'integrale

Si nota di nuovo come il logaritmo si sforzi ancora a comportarsi come la potenza x^0.

Se la derivata ci indica il gradiente di una curva in un punto che ci indica l'integrale? Semplicemente l'area sottesa dalla curva.

Gli *integrali definiti*, cioè definiti in un intervallo preciso della variabile, possono avere un *intervallo limitato* oppure un *intervallo non limitato* con almeno uno degli estremi è $+\infty$ o $-\infty$.

Nel primo caso si ottiene certamente un'area finita, nel secondo caso dipende anche dalla funzione che si integra. Ad esempio l'integrale indefinito:

$$\int_2^{\infty} x^{-4}dx$$

secondo la regola di integrazione dà luogo a:

$$\left[-\frac{1}{3}x^{-3}\right]_2^{\infty} = 0-(-\frac{1}{3}2^{-3}) = \frac{1}{24}$$

In questo esempio otteniamo un valore reale finito.

Gli *integrali indefiniti*, invece, hanno alla base un concetto diverso: sono sostanzialmente l'operazione inversa della derivata.

Capitolo 3. Le serie e il concetto di estensione del dominio

Nel prosieguo incontreremo diversi tipi di serie: la serie armonica, la serie di Basilea, la serie della zeta di Riemann …

Ma cos'è esattamente una serie? Cercheremo di presentarvi solo i concetti, demandando i volenterosi ad approfondire il rigore matematico su qualche buon testo scolastico o universitario.

La serie armonica

La serie armonica è espressa dalla formula:

$$\sum_{n=1}^{\infty}\frac{1}{n}$$

Il simbolo $\sum_{n=1}^{\infty}$ significa "sommatoria" dei termini 1/n per i valori di n che variano da 1 all'infinito; in altri termini è equivalente alla somma degli inversi di tutti i numeri Naturali ($n \in N$):

$$1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{5}+\ldots=\infty$$

Infatti se sommiamo i termini all'infinito, la serie "*diverge*" cioè assume valore *NaN* o infinito. Approfittiamo anche per dire che $\propto$ è solo una convenzione, non esiste in matematica un tale valore (NaN = **N**ot is **a** **N**umber).

La prima dimostrazione della divergenza della serie armonica risale al '300 ad opera di *Nicola di Oresme*, che osservò che 1/3+1/4 è più grande di ½; lo stesso dicasi per 1/5+1/6+1/7+1/8. In altri termini se prendiamo due termini, poi 4, poi 8, poi 16 etc. si trova che il valore della serie cresce sempre. Per cui è inevitabile che la serie armonica diverga.

In generale, una serie somma degli inversi dei numeri naturali è detta *serie di Dirichlet* (furono introdotte sia da Dirichlet che da *Dedekind*); esse sono della forma:

$$\frac{a_1}{1^s}+\frac{a_2}{2^s}+\frac{a_3}{3^s}+...+\frac{a_n}{n^s}+...$$

Se delle serie armonica (di infiniti elementi) si considerano solo n elementi, allora si parla di *numero armonico* H_n.

Esistono solo serie divergenti? No. Esistono anche le *serie convergenti* e le *serie condizionalmente convergenti.*

Una serie è convergente se la somma di tutti i suoi infiniti termini dà un valore finito. In verità sarebbe bastato dire valore - senza finito - perché infinito non è un valore.

Inoltre esistono anche serie che sono *convergenti, solo se si rispetta l'ordine di somma degli addendi*! Ecco perché queste ultime sono dette *condizionalmente convergenti*; altrimenti sarebbe più giusto definirle *assolutamente convergenti*.

Un esempio di serie assolutamente convergente potrebbe essere:

$$1+\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\frac{1}{16}+\frac{1}{32}+\frac{1}{64}+...=2$$

E' una serie che a denominatore ha il doppio del termine precedente per cui è la metà del termine immediatamente precedente. Non è difficile comprendere che converge al valore 2 perché, man mano, il contributo incrementale di ogni termine si dimezza sempre più.

Difatti se si rappresentano due segmenti, uno di file all'altro, per rappresentare il valore 2 e ci si mette dal lato del primo segmento che rappresenta 1, allora ½ significa aggiungere mezzo segmento del secondo e otteniamo 1 1/2 (*da leggere come 1 e mezzo*). Poi aggiungere ¼ significa aggiungere a 1 ½ un mezzo segmento rimasto del secondo; aggiungere 1/8 significa etc.

Vediamo, invece, l'*effetto gambero* della seguente serie a segni alterni e con i denominatori che raddoppiano (simile alla precedente tranne per i segni alterni):

$$1-\frac{1}{2}+\frac{1}{4}-\frac{1}{8}+\frac{1}{16}-\frac{1}{32}+\frac{1}{64}+...=\frac{2}{3}$$

Se vi rappresentate il tutto con due segmenti, come fatto prima, si scopre presto che mettendosi alla fine del primo segmento (valore 1) si deve poi tornare indietro a

causa del segno negativo di ½ (ritorniamo alla metà del segmento); poi a questo mezzo segmento devo andare avanti di ¼ etc. Non riuscirò mai a superare i 2/3 del primo segmento!

La serie a segni alterni simile a quella armonica è detta sia *serie armonica a segni alterni* che funzione η *(leggi "eta") di Dirichlet con s=1*. La funzione η di Dirichlet nella forma più generale è:

$$\eta(s) := 1 - \frac{1}{2^s} + \frac{1}{3^s} - \ldots + \frac{(-1)^{n+1}}{n^s} + \ldots$$

Se s=1 allora converge a log2.

Mengoli è noto anche per una sua serie (*serie di Mengoli*) che ha la seguente forma:

$$\frac{1}{1*2} + \frac{1}{2*3} + \frac{1}{3*4} + \ldots \frac{1}{n(n+1)} + \ldots = 1$$

La serie che, invece, faceva inorridire *Abel* è la serie di *Grandi*:

G. Grandi, 1671-1742

N. Abel, 1802-1829

$$1 - 1 + 1 - 1 + 1 - 1 + \ldots + (-1)^n + \ldots$$

Secondo Grandi ed Eulero tale serie vale ½. La giustificazione sta nel fatto che se poniamo s = 1 - s questo implica che s=1/2 e l'equazione è soddisfatta. Secondo la matematica di oggi, tale serie è definita comunque divergente, perché è 0 o 1 a seconda se alternativamente si considera un numero pari o dispari di termini.

Un altro concetto che vogliamo sottolineare è che le serie convergono ad un valore *in forma chiusa,* che in matematica significa che tende ad un valore preciso, un calcolo esatto e non approssimato come una misura. Tipicamente un valore approssimato è una rappresentazione in forma decimale periodica o irrazionale (con infinite cifre). Un valore intero o un valore frazionario (numero razionale) sono un valore esatto.

Provate a dimostrare, col metodo sopra descritto, se le due serie che vi proponiamo sono convergenti o divergenti e se è vero che convergono al valore di seguito proposto:

$$1 + \frac{1}{3} + \frac{1}{9} + \frac{1}{27} + \frac{1}{81} + \ldots = 1\frac{1}{2}$$

$$1-\frac{1}{3}+\frac{1}{9}-\frac{1}{27}+\frac{1}{81}+...=\frac{3}{4}$$

Vi diamo la risposta, non temete: sono entrambe convergenti ai valori proposti; però fate qualche prova anche voi!

Le serie sono studiate nell'ambito dell'analisi matematica e l'analisi matematica è il regno dello studio dei limiti, dell'infinitamente grande (infinito) e dell'infinitamente piccolo (infinitesimo), ma anche dell'integrale.

I limiti sono il cuore dell'analisi; molti altri concetti analitici nascono da essi come:

- la derivata come limite di un rapporto incrementale $\lim_{\Delta x\to 0}\frac{\Delta y}{\Delta x}$
- le approssimazioni di un termine rispetto ad un altro
- l'integrale come limite di una sommatoria
- la convergenza di una serie o di una successione

Alle serie sono legate anche le *successioni* di numeri, rappresentate da un insieme di numeri separati da virgole e tali che ognuno di essi è ricavato da una regola. Ad esempio supponiamo la seguente regola: "ogni numero è una frazione dove il nuovo denominatore è ottenuto dalla somma del numeratore e denominatore precedente e il nuovo numeratore è ottenuto dalla somma del numeratore e del doppio del denominatore". Ci rendiamo subito conto che a causa della regola anche la successione trova infiniti numeri. La successione è allora:

$$\frac{1}{1},\frac{3}{2},\frac{7}{5},\frac{17}{12},...$$

Dove converge la successione di sopra? In realtà stiamo parlando quindi della serie:

$$\frac{1}{1}+\frac{3}{2}+\frac{7}{5}+\frac{17}{12}+...=\sqrt{2}$$

Il limite della successione è $\sqrt{2}$.

Un modo per rendersene conto è considerare un numero piuttosto grande della serie, ricavabile con le regole di cui prima. Per evitare le radici quadrate, possiamo considerare il quadrato di esso, che tende a 2.

Ad esempio il quadrato di 3363/2378 è 11309769/5654884 che fa circa 2,00000017683827… Se andiamo avanti con altri numeri sempre più grandi aumenteranno il numero di 0 dopo la virgola.

I tre puntini dopo il numero indicano che in realtà siamo dinnanzi ad un numero

irrazionale, ovvero con infinite cifre; quindi non ha senso rappresentarlo tutto e ci si deve accontentare di una precisione che dipende dal numero cifre rappresentato. In pratica approssimiamo il numero o è in forma aperta. Per i matematici questo fa storcere il naso: è la differenza tra calcolo e misura. Un calcolo deve essere preciso, possibilmente una espressione va calcolata in forma chiusa. Una misura, invece, può essere approssimata, visti i limiti pratici e, quindi, in forma aperta.

Consideriamo un'altra successione:

$$\frac{4}{1},\frac{8}{3},\frac{32}{9},\frac{128}{45},...$$

La regola che segue è:"L'N-esimo termine si ricava nel seguente modo: se N è pari allora si moltiplica per N/(N+1) il termine precedente; se N è dispari si multipla il termine precedente per (N+1)/N". Questa successione converge lentamente a π.

Una successione famosa che rappresenta la *e di Nepero* è la seguente:

$$1,(1+\frac{1}{2})^2,(1+\frac{1}{3})^3,(1+\frac{1}{4})^4,...$$

Il limite di questa successione vale il *numero di Nepero* e=2,718281828459, o in alternativa si dice che la serie converge ad *e*.

La serie del problema di Basilea

La serie di Basilea è stata la porta di ingresso per la zeta di Riemann. Inizialmente il quesito a che valore convergesse la serie fu posto da *Mengoli* nel 1650. Essa, nella sua forma più semplice, si presenta nel seguente modo:


P. Mengoli. 1626-1686

$$1+\frac{1}{2^2}+\frac{1}{3^2}+\frac{1}{4^2}+\frac{1}{5^2}+...$$

Una semplice osservazione (*criterio del confronto*) ci porta a dire che ogni termine essendo più grande (sono quadrati) di ogni termine della serie armonica, allora ci sono ottime speranze che la serie di Basilea converga. Difatti ad esempio il quadrato di ½ che fa ¼ è più piccolo di ½ e così via.

Se proviamo a sommare, con un excel o col programma PARI, i primi 10 termini la somma dà 1,5497677…; con 100 termini la somma dà 1,6349839…, con 1000 dà 1,6439345…, con 10000 dà 1,6448340… etc. Quindi assume un numero tra 1,644 e 1,645.

Il problema fu affrontato da Wallis, Leibniz e i fratelli Bernoulli senza successo. Si

dovrà aspettare un secolo dopo ad Eulero, per ottenerne la soluzione.

Il problema di Basilea fu quello di trovare una forma chiusa a tale serie con esponente N; cioè esaminiamo la serie generale:

$$\sum_{n=1}^{\infty} \frac{1}{n^N}$$

ovvero:

$$1+\frac{1}{2^N}+\frac{1}{3^N}+\frac{1}{4^N}+\frac{1}{5^N}+...$$

Essa è anche denominata *serie armonica generalizzata*. Converge se N>1, mentre diverge per N≤1. La divergenza è evidente per il criterio del confronto con la serie armonica difatti se N<1, per n≥1, $n^N<n$ e quindi $1/n < 1/n^N$.

A cosa converge? Eulero dimostrò, per N pari fino a N=26, i valori riportati nella seguente tabella 4.

N	Valore di convergenza
2	$\pi^2/6$
4	$\pi^4/90$
6	$\pi^6/945$
…	…

Tabella 4 – Valori serie di Basilea

Eulero arrivò fino a N=26; mentre nessuno era riuscito a trovare una forma chiusa per N dispari (almeno fino a che non è stata studiata la zeta di Riemann, Vedi approfondimento Capitolo 11).

La zeta di Riemann come funzione reale di variabile reale

La zeta di Riemann, anch'essa studiata da Eulero per numeri reali, è analoga alla serie di Basilea sopra. Solo che al posto di N Riemann pose s, intendendo s come numero complesso e quindi la studiò come funzione complessa di variabile complessa; ma se s ha solo parte reale allora coincidono. Nel seguito per iniziare a fissare le idee ipotizziamo s come variabile reale e la zeta di Riemann come funzione reale di variabile reale, cioè coincidente con la serie di Basilea. Un modo per sintetizzare la zeta di Riemann come serie è il seguente:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

Se s=1 la serie diverge (serie armonica). Se, invece, s>1 la serie converge (serie di Basilea). In realtà è solo a s=1 che diverge; se consideriamo s=1,0001 converge a

10000,577222… Ovvero ha un polo in s=1; si comporta come se fosse la funzione 1/(s-1) che ad s=1 diverge.

Se nella serie di Basilea (o zeta di Riemann di variabile reale) poniamo s=0, la serie diverge ancora (perché $n^0 = 1$). Per valori negativi come s = -1 diverge ancora, perché ad esempio il termine $1/2^{-1}=2$ e così otterrei la somma di tutti i numeri naturali 1+2+3+4+… . Se s = ½, a denominatore abbiamo le radici quadrate. Ad esempio il termine $1/2^{1/2}$ confrontiamolo con il termine ½ della serie armonica: la radice di 2 è maggiore di 1, mentre il termine della serie armonica è 2 e più grande della radice di 2; ora se la serie armonica diverge, a maggior ragione diverge anche la serie con s=1/2. Nel campo delle variabili reali, quindi, l'andamento della zeta di Riemann è come in Figura 4.

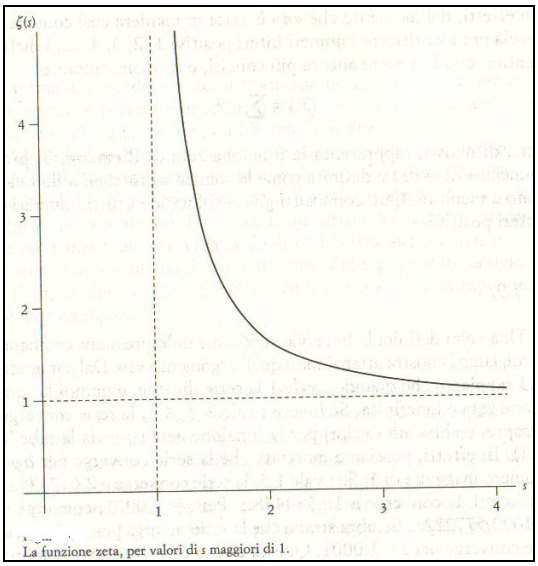


Figura 4 – funzione ξ

Secondo quanto appreso si dovrebbe dire che il dominio della funzione zeta è formato da valori maggiori di 1. In realtà, come vedremo in seguito, non è proprio così…

Estensione del dominio di una funzione definita da una serie

Consideriamo la funzione S(x), ottenuta da una serie così definita:

$$S(x) = \sum_{n=0}^{\infty} x^n$$

Essa è la *serie geometrica* e corrisponde a scrivere:

$$S(x) = 1 + x + x^2 + x^3 + \ldots$$

Se x=1/2 la serie di sopra coincide con quella vista prima:

$$1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \frac{1}{32} + \frac{1}{64} + \ldots = 2$$

Per cui è:
S(1/2)=2, S(-1/2)=2/3, perché ritorniamo alla serie con segni alterni di prima;
S(1/3)=1 ½, S(-1/3)=3/4, S(0)=1, S(1) diverge, S(-1) diverge.

Con S(-1) siamo costretti a dire che diverge perché a causa dell'alternanza dei segni, se consideriamo un numero pari di termini si ottiene zero, se consideriamo un numero dispari di termini si ottiene 1: non va all'infinito ma neanche converge assolutamente per cui l'*indecisione tra due valori* in matematica è comunque una forma di divergenza. S(-2)=diverge. Qui l'alternanza dei segni ci porta ad una situazione ancora peggiore: 1-2+4-8+… e la funzione sembra andare all'infinito in entrambe le direzioni. Tutto questo per dire che la funzione S(x) ha valori nel dominio tra -1 e 1, estremi 1 e -1 esclusi, cioè [-1,1]. Per cui si può immaginare di aver completato lo studio della funzione S(x) e che il suo grafico sia quello in Figura 5.

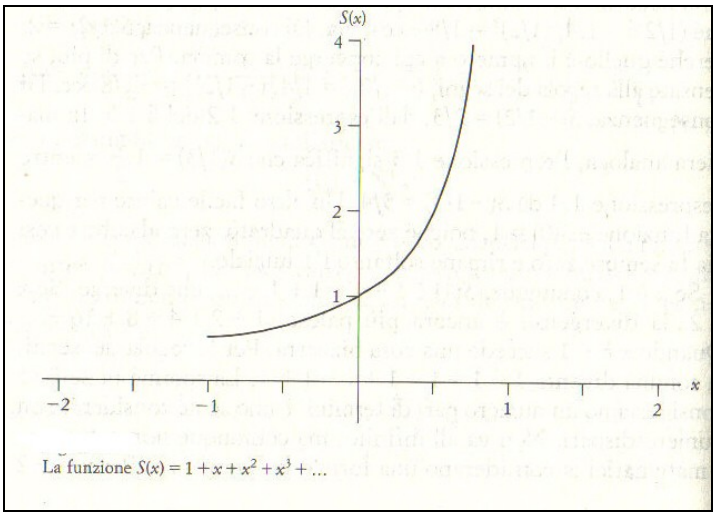


Figura 5 – la funzione S(x)

Adesso facciamo qualche riflessione su S(x). Finora per poter calcolare i valori di S(x) abbiamo dovuto un pò "faticare", usando le serie o le successioni ed il limite.

Spesso è stato anche difficoltoso comprendere bene la cosa. L'idea ora è quella di ottenere *l'espressione analitica* di una funzione più facile (una formula) che assuma gli stessi valori nel dominio [-1,1], anche se la nuova funzione avrà un dominio più esteso o diverso.

Come la otteniamo la nuova funzione? Abbiamo visto che:

$$S(x) = 1+x+x^2+x^3+\ldots$$

Se al secondo termine mettiamo in evidenza x si ottiene:

$$S(x) = 1+x(1+x+x^2+x^3+\ldots)$$

Da qui è evidente che il termine in parentesi è ancora S(x), per cui è:

$$S(x) = 1+xS(x)$$

Da cui discende che:

$$S(x) = 1/(1-x) = 1+x+x^2+x^3+\ldots \quad (6)$$

Questa nuova funzione S(x) ha gli stessi valori della precedente nell'intervallo [-1,1]; difatti è: S(0)=1; S(1/2)=2; S(-1/2)=2/3; S(1/3)=1 ½; S(-1/3)=3/4

Però le due funzioni hanno domini differenti ed è apparsa nella Figura 6 una parte di dominio dei valori prima "non visto". Infatti posso trovare anche S(10)=-1/9 etc.

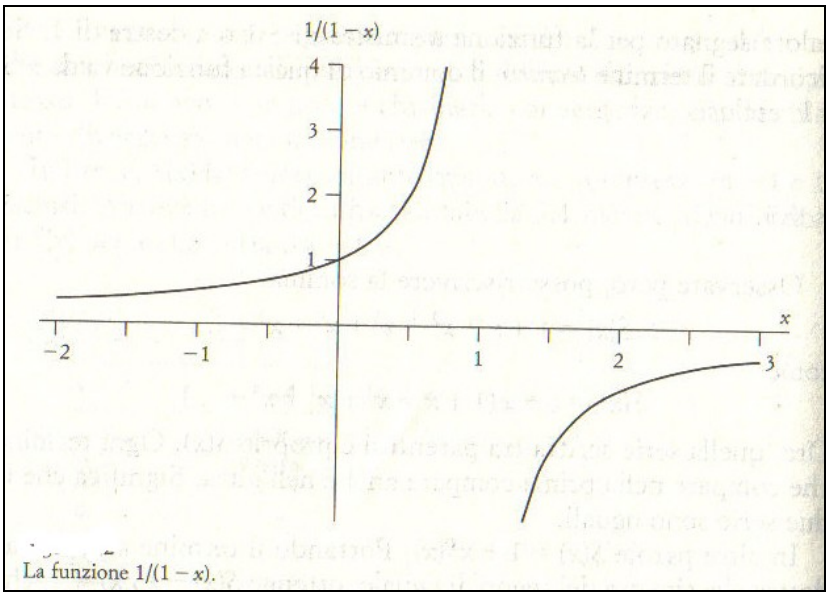


Figura 6 – Dominio della funzione 1/1-x

Da questo esempio quale insegnamento si trae? *Una serie infinita può definire solo una parte di una funzione*.

Il resto della funzione potrebbe essere nascosto da qualche altra parte. Occorre molto tempo e pazienza per lo studio di una funzione complessa come la zeta di Riemann.

L'estensione del dominio serve a comprendere meglio la funzione e generalmente per fare l'estensione occorre operare qualche manipolazione della funzione come abbiamo visto sopra.

Prima di passare all'estensione del dominio della zeta di Riemann, vogliamo concludere con la serie geometrica vista qualche riga sopra.

Newton la utilizzò calcolandone l'integrale, ottenendo che:

$$-\ln(1-x) = x + \tfrac{1}{2}x^2 + \tfrac{1}{3}x^3 + \ldots \quad (7)$$

L'estensione del dominio della funzione zeta di Riemann

Se nella zeta di Riemann di variabile reale vista prima volessimo ricavarci i valori la cosa non è semplice. Quanto vale ad esempio $\zeta(-7,5)$?

In realtà una estensione di dominio che ci consenta di valutare rapidamente la $\zeta(s)$ torna estremamente utile.

Un trucco è quello di usare la funzione $\eta(s)$ di Dirichlet. Difatti avendo compreso che la forma della $\zeta(s)$ è del tipo A+B+C+D+E+F+… allora introduciamo una forma $\eta(s)$ del tipo:

$$A-B+C-D+E-F+\ldots = (A+B+C+D+E+F+\ldots) - 2\,(B+D+F+\ldots)$$

Da cui:

$$\eta(s) = \zeta(s) - 2\,(1/2^s+1/4^s+1/6^s+1/8^s+\ldots)$$

In altri termini è:

$$\zeta(s) = \frac{\eta(s)}{(1-\frac{1}{2^{s-1}})} \quad (8)$$

La formula dice che se sappiamo calcolare $\eta(s)$, che rappresenta una serie a segni alternanti che converge, allora sappiamo anche calcolare i valori di $\zeta(s)$.

$\eta(s)$ posso addirittura calcolarla tra 0 e 1, nonostante che la serie reale di $\zeta(s)$ non converge in quell'intervallo.

E' lecito, però, manipolare due serie infinite quando una converge e l'altra no? In termini di rigore matematico no, ma in termini pratici se il calcolo sui valori aiuta, lo si fa (è un "*consentitemi di …*").

Ora tranne per s=1 siamo in grado di trovare valori di $\zeta(s)$. Ma possiamo trovare anche i valori s<=0?

Questo enigma è stato risolto da Eulero con la funzione gamma (vedi capitolo dedicato):

$$\zeta(s) = \zeta(1-s)\Gamma(1-s)2^s\pi^{s-1}\sin\frac{1}{2}\pi s \qquad (9)$$

Oppure equivalentemente, per trovare i valori negativi:

$$\zeta(1-s) = \zeta(s)(s-1)!2^{1-s}\pi^{-s}\sin\frac{1-s}{2}\pi \qquad (10)$$

Da quest'ultima formula può uscir fuori l'esigenza di calcolare il fattoriale di ½ o di un numero negativo. Come? Dite che non è definito il fattoriale? Vedremo nei prossimi capitoli con quale trucchetto Eulero ha sbrogliato la matassa del problema dell'interpolazione. Per il momento abbiate fede. Come S. Tommaso vedrete con i vostri occhi! .

Capitolo 4. La funzione O grande

In questo capitolo ci prendiamo una pausa teorica, affrontando un argomento meno difficile concettualmente, ma nello stesso tempo importante da comprendere. La O grande è una notazione che permette di arrivare alla comprensione delle ipotesi equivalenti alla RH.

Definizione della O grande

Una funzione f(x) è O grande di una funzione g(x) se, per valori abbastanza grandi (al tendere all'infinito in generale), la dimensione di f(x), intesa come valore indipendentemente dal segno, non supera mai un qualche multiplo fisso di g(x). In tal caso andrebbe scritto che:

$$|f(x)| = O(g(x))$$

In altri termini esiste un $k \in N$: $|f(x)| < k\,|g(x)|$

In base a questo significa che la O grande fornisce un limite superiore positivo e uno inferiore negativo (la dimensione di f(x), intesa come valore indipendentemente dal segno) all'interno del quale si mantiene g(x).

La funzione O(1)

La funzione O grande è indipendente anche dal valore del multiplo k. Ad esempio se g(x)=1 dire che è f(x)=O(1) stiamo dicendo che se riportiamo su un grafico f(x) sulle ordinate e x sulle ascisse, la f(x) è contenuta tra -1 e 1 (rette costanti parallele all'asse x e che rappresentano la |g(x)|).

Ora se la f(x) fosse una retta che passa per l'origine e con una pendenza k, il valore di k può essere qualsiasi, come indicato in tabella 5.

k	f(x)
10	10*x
1	1*x
0,1	0,1*x
0,01	0,01*x

Tabella 5 – Pendenze di x vs O(1)

Il k varia solo la pendenza della retta che passa per l'origine e alla fine, rispetto alla O(1), cioè al limite superiore, comunque la f(x) attraverserà prima o poi il limite superiore al crescere di x e in dipendenza del valore k (vedi Figura 7). Per cui nella discussione precedente con $k \geq 1$ è ininfluente il reale valore del k.

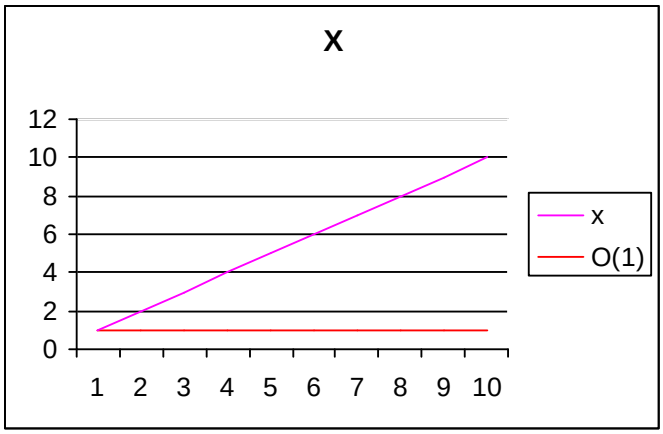


Figura 7 – x vs O(1)

La funzione O(g(x))

Ovviamente g(x) può essere qualsiasi non necessariamente uguale a 1 e altrettanto f(x). Ad esempio $g(x)=x^{1/2}\log x$ oppure $g(x)=(\log x)^2$. Naturalmente dipende dal problema e dalla teoria che stiamo considerando.

Intervallo di validità della funzione O grande

La f(x)=O(g(x)) non necessariamente deve essere sempre al di sotto dei limiti posti dalla O grande. Anche se la f(x) considerata fosse al di fuori dei limiti della O grande, in un certo intervallo x, si può considerare vera f(x) = O(g(x)) nell'intervallo rimanente. In realtà dipende da quello che si vuole evidenziare nella teoria.

Quanto detto in questa parte e quello detto sui logaritmi e le potenze è sufficiente per comprendere determinate problematiche che vedremo in seguito.

Capitolo 5. I numeri complessi e le serie complesse

La vita è già difficile, perché introdurre nella zeta di Riemann i numeri complessi?

I numeri naturali $\mathbb{N}$, sono nati per contare: 1,2,3,4,5,6,… Successivamente furono introdotti i numeri interi $\mathbb{Z}$ che comprendevano anche i numeri negativi e la loro utilità tra gli egiziani era per calcolare i flussi di denaro: attivo e passivo o guadagno e perdita.

In seguito, molti secoli dopo, ci si rese conto che tali insiemi erano incompleti o come si dice ora *non chiusi rispetto alle operazioni aritmetiche*. Un insieme si dice chiuso rispetto ad un'operazione se il risultato di essa restituisce un numero appartenente

ancora all'insieme.

Se in $\mathbb{N}$ facciamo l'operazione 7 - 12 otteniamo un risultato che non è appartenente a $\mathbb{N}$ ma a $\mathbb{Z}$ (dove esistono i numeri negativi). Per cui $\mathbb{N}$ non è chiuso rispetto alla differenza, e di conseguenza nemmeno rispetto ad una divisione (ricordare che algoritmicamente è possibile fare una divisione con n differenze), ad esempio 1/2 non appartiene a $\mathbb{N}$ ma all'insieme $\mathbb{Q}$.

Chi è $\mathbb{Q}$? E' l'insieme dei ***numeri razionali*** ottenibili da frazioni e contenente, quindi, anche i numeri periodici. $\mathbb{Q}$ è chiuso rispetto a tutte le operazioni? No, la divisione è un problema anche per $\mathbb{Q}$: alcune divisioni danno luogo a numeri che non sono esprimibili come frazioni o numeri periodici e per questo motivo sono detti *irrazionali* e contenuti in $\mathbb{R}$. In verità per $\mathbb{N}$, $\mathbb{Z}$ e $\mathbb{Q}$ è un problema anche la radice quadrata[3]. Ad esempio $\sqrt{5}$ non è un numero razionale, ma sicuramente esiste al di fuori di $\mathbb{Q}$ perchè dal Teorema di *Pitagora* è $1^2+2^2=5$. Esso è difatti è un numero irrazionale in $\mathbb{R}$, non rappresentabile come frazione o rapporto di due interi. Non tutti i risultati delle radici sono fuori $\mathbb{Q}$; ad esempio $\sqrt{36} = 6/1$. Un numero irrazionale famoso è $\sqrt{2}$ (*costante di Pitagora*): da Pitagora si è avuta la prima dimostrazione dell'irrazionalità[4]. Ulteriori problemi sono posti, come vedremo, dalle radici di numeri negativi.

$\mathbb{R}$ è l'insieme dei ***numeri reali*** che comprende sia i razionali che gli irrazionali e, quindi, R è chiuso rispetto a tutte e quattro le operazioni aritmetiche.

$\mathbb{R}$ sembra che possa fare tutto, allora a che pro i numeri complessi $\mathbb{C}$? In realtà il problema dei numeri complessi è nato con le soluzioni delle equazioni (ad esempio $x^2 = -1$). Alcune radici erano "illogiche", ma pur sempre radici. Per superare la difficoltà di radici che coinvolgessero termini come $\sqrt{-1}$ o altri numeri negativi sotto radice *Raffaele Bombelli* (1526-1572) introdusse il concetto di numero immaginario (la "i" è dovuta, invece, ad Eulero):

$$i = \sqrt{-1}$$
$$i^2 = -1$$

[3] In realtà è sufficiente solo la differenza; con essa si possono ricavare le altre tre operazioni: la somma è una differenza tra un termine positivo ed uno negativo; la moltiplicazione è una iterazione di somme; la divisione è fattibile per differenze successive. Analogamente le radici.

[4] Si dimostra per assurdo che $\sqrt{2}$ è irrazionale. Se fosse razionale allora $\sqrt{2} = \frac{m}{n}$ da qui $2 = \frac{m^2}{n^2} \rightarrow 2n^2 = m^2$. Ora $2n^2$ è pari per forza, per il 2, allora di conseguenza lo è anche m^2 e in cascata anche m (il quadrato di un pari è pari, il quadrato di un dispari è dispari). Allora se m è pari lo possiamo scrivere come $m^2=(2k)^2$ per cui $2n^2=4k^2$ da cui $n^2=2k^2$ ora anche $2k^2$ è pari per il 2 e di conseguenza lo è anche n. Ma se n e m sono pari e sono semplificabili nella frazione siamo arrivati ad un assurdo perché l'ipotesi di partenza è che m e n non sono irriducibili per definizione di razionale!

Un numero complesso appartenente a $\mathbb{C}$ ha di conseguenza una parte reale $\Re$e ed una parte immaginaria $\Im$m (anch'essa reale come numero). Ad esempio s $=1+i\sqrt{2}$ è un numero complesso; dove 1 è $\Re$e(s), mentre $\sqrt{2}$ è la parte $\Im$m(s).

La rappresentazione di un numero reale è solitamente su una retta, con gli irrazionali infinitamente addensati tra i razionali (un mistero anche questo non del tutto svelato), ma che coinvolge una sola dimensione.

La rappresentazione di un numero complesso viene fatta sul piano di Gauss, bidimensionale, dove l'asse delle ascisse indica la parte reale del numero complesso e l'asse delle ordinate rappresenta la parte immaginaria.

Nel seguito non intendiamo riportare come si opera con i numeri complessi, cosa che potrete vedere da soli su un buon testo scolastico: le operazioni di somma, moltiplicazione, divisione, sottrazione, radice, potenza, esponenziale e logaritmo, la rappresentazione polare e quella trigonometrica. Comunque vi raccomandiamo di prendere pratica in tal senso, se vi interessa la Teoria dei Numeri e la congettura di Riemann.

Evidenzieremo, invece, come una serie S(x), vista precedentemente, si comporta nel campo complesso C, cioè quando in S(x) sostituiamo a x, la variabile s complessa.

Riprendiamo la (6) e sostituiamo x con s:

$$1/(1-s) = 1+s+s^2+s^3+\ldots \quad (11)$$

La serie espressa dalla (11) vale anche per i numeri complessi? Sotto certe condizioni sì, ad esempio supponiamo s = 1/2 i, allora la serie converge.

La (11) si trasforma in:

$$\frac{1}{1-\frac{1}{2}i} = 1+\frac{1}{2}i+\frac{1}{4}i^2+\frac{1}{8}i^3+\frac{1}{16}i^4+\ldots$$

Se moltiplichiamo numeratore e denominatore della parte di sinistra per 1+1/2 i si ottiene a sinistra il termine 4/5 + 2/5 i, e tenendo conto che:

$$i^2 = -1$$
$$i^3 = i^2 i = -i$$
$$i^4 = i^3 i = -i^2 = 1$$

da qui:

$$0,8+0,4i=1+\frac{1}{2}i-\frac{1}{4}-\frac{1}{8}i+\frac{1}{16}+...$$

Se vi mettete sul piano complesso di Gauss e fate un passo nella direzione di ogni termine che si trova a destra dell'uguaglianza, vi accorgerete che vi state muovendo a spirale avvicinandovi sempre più al valore complesso 0,8+0,4i.

In altri termini abbiamo perso in semplicità ma *abbiamo guadagnato in espressività*: nel piano complesso si vede direttamente come una serie infinita si chiude sul suo limite.

Capitolo 6. Le funzioni gamma e beta

Nel seguito presentiamo la funzione gamma e la via attraverso cui essa è cresciuta, dai tempi d'Eulero al più recente trattato matematico di Bourbaki e come, in questa crescita, essa assunse una importanza notevole in vari settori della matematica, compresa l'ipotesi di Riemann.

La nascita della funzione Gamma risale al 1729 e coinvolge nel secolo figure come Leonhard Eulero (1707-1783) e Christian Goldbach (1690-1764).

La teoria di tale funzione nasce in un momento in cui si consolidavano due teorie di grosso interesse:

- La teoria dell'interpolazione, una materia molto pratica, campo di analisi soprattutto dei matematici inglesi del 1600;
- La teoria del calcolo integrale e degli integrali indefiniti.

Un semplice problema di interpolazione vide gli insuccessi di Goldbach, Daniel Bernoulli (1700-1784) e precedentemente di James Stirling (1692-1770).

Eulero

Successivamente il problema venne posto ad Eulero, il quale prima enunciò la soluzione a Goldbach in due lettere; e poi pubblicò tutti i dettagli in un articolo "*De progressionibus trascendentibus seuy quorum termini generales algebraice dari nequeunt"* Volume primo dell'opera omnia di Eulero.

Problemi di interpolazione

La più semplice sequenza di numeri interi (una successione) che porta ad un interessante teoria è la seguente:

$$1, \quad 1 + 2, \quad 1+ 2 + 3, \quad 1 + 2 + 3 + 4, \quad \ldots$$

Questi sono i *numeri triangolari*. Sono così chiamati perché rappresentano il numero di oggetti che si possono mettere in un array triangolare. L'ennesimo elemento viene chiamato T_n ed è:

$$T_n = ½ \, n \, (n + 1)$$

La formula presentata ha diversi vantaggi:

- semplifica la computazione, riducendo larghe addizioni di numeri a tre operazioni fisse: una di addizione, una di moltiplicazione e una di divisione . Ad esempio: $T_{100} = ½ \, 100 \, (100 + 1) = 5050$.

- se occorre, nei casi per cui abbia senso, può fornire anche risultati per N non intero; ad esempio la somma dei primi 5 1/2 interi. In tal caso è: $T_{5\ 1/2} = ½ \, (5\ 1/2) \, (5\ 1/2 + 1) = 17\ 7/8$.

In altri termini la formula estende lo scopo del problema originario e risolve il problema dell'interpolazione tra i valori elementari conosciuti.

Un analogo problema si pensò a traslarlo all'algebra delle potenze: vediamo come. La quantità a^m è definita come il prodotto di m volte a o si diceva "di m successivo a".

Questa definizione ha significato quando m è un intero positivo, ma cosa succede se m=5 ½; cioè quanto vale $a^{(5\ ½)}$? Il prodotto di 5 ½ successione di a ha senso?

Le misteriose definizioni:
$a^0 = 1$
$a^{(m/n)} = \sqrt[n]{a^m}$
$a^{(-m)} = 1/a^m$
$a^m \ a^n = a^{(m+n)}$

furono risolte esplicitamente da *Isaac Newton* solo nel 1776. Oggi, ad esempio, sappiamo facilmente dimostrare che $a^m / a^m = 1 = a^{m-m} = a^0$.

Esistono però molti altri problemi di questo tipo che comportano difficoltà. Ad esempio Leibnitz introdusse la nozione d^n per la derivata ennesima e identificò d^-1 come l'integrale e la definizione d^{-n} come l'ennesimo integrale.

Ma che significa d^n se n = 5 ½? E' la 5 ½-esima derivata? Ha senso? E' un problema risolto solo di recente, in verità.

Il fattoriale positivo e razionale

Fattoriale									
N	1	2	3	4	5	6	7	8	**…**
N!	1	2	6	24	120	720	5040	40320	**…**

Tabella 6 – Valori del fattoriale

Riprendiamo la sequenza triangolare di numeri e sostituiamo il segno di addizione con quello di moltiplicazione e otteniamo una nuova sequenza o successione di numeri:

$$1, \quad 1 * 2, \quad 1 * 2 * 3, \quad 1 * 2 * 3 * 4, \ldots$$

questa è la successione di un fattoriale. Il fattoriale di n è indicato n!

Essi crescono anche molto rapidamente. Ad esempio 100! ha 158 cifre mentre T_{100} = 5050 ha solo 4 cifre.

Ma quanto fa il seguente fattoriale: 1½! ? E' ancora un problema di interpolazione; quello di Stirling, di Bernoulli e di Goldbach .

I due problemi T_n e n! sono correlati, solo che per il primo esiste una semplice formula mentre per il secondo no. Ciò è implicito anche nel titolo dell'articolo di Eulero, che tradotto dice all'incirca "*Sulle progressioni trascendentali, il cui termine generale non può essere espresso algebricamente*".

La soluzione dell'interpolazione fattoriale è nascosta nell'algebra. Eulero formulò il problema in modo moderno, cioè di trovare una funzione che porti dai valori di n (*il dominio*) ai valori di n! (*il codominio*). In altri termini è importante *la relazione* tra i due domini e non la natura delle regole.

Se ci si basasse solo sulla natura delle regole, allora dato un insieme di punti del piano "il problema di interpolazione" diventerebbe banalmente quello di trovare una curva che passi per tutti i punti o che si avvicina abbastanza alla maggior parte di essi. In tal caso si risolverebbe il problema del caso in gioco in modo banale, ma nulla si è fatto per trovare una legge generale per ogni casistica.

Il metodo di Eulero era differente, caratteristico del 1700, tipico anche della scuola francese del secolo 1600-1700 (Descartes = Cartesio è ricordato come filosofo; mentre in realtà era un grande matematico: basta solo pensare al piano cartesiano!). Una funzione era sinonimo di formula ed una formula era una espressione che si potesse ricavare con manipolazioni di operazioni elementari come addizione,

sottrazione, moltiplicazione, divisione, esponenziale, radicale, potenza, logaritmo, differenziale, integrazione, serie con termini infiniti.

Per questo motivo una formula veniva chiamata *espressione analitica*.

L'interpolazione del fattoriale, quindi, consisteva nella ricerca di una espressione analitica, tale che inserendo nella formula un numero positivo dovesse fornire in uscita il valore del fattoriale, il quale avrebbe dovuto avere senso anche nel caso di un n non intero ma frazionario (razionale).

Eulero, sperimentando con infiniti prodotti di numeri, notò che se n è un intero positivo vale la seguente formula:

$$\left[\left(\frac{2}{1}\right)^n \frac{1}{n+1}\right]\left[\left(\frac{3}{2}\right)^n \frac{2}{n+2}\right]\left[\left(\frac{4}{3}\right)^n \frac{3}{n+3}\right]\ldots = n! \quad (12)$$

Trascurando problematiche delicate, come la convergenza di un prodotto infinito, si può verificare quest'equazione cancellando via tutti i fattori comuni che appaiono sopra e sotto la parte di sinistra. Esso comunque è definito per tutti i tipi di n, anche per interi negativi.

Eulero notò, inoltre, che quando viene inserito il valore n = ½ si ottiene sulla parte destra il famoso "prodotto infinito" di *John Wallis* (1616-1703):


J. Wallis, 1616-1703

$$\left(\frac{2*2}{1*3}\right)\left(\frac{4*4}{3*5}\right)\left(\frac{6*6}{5*7}\right)\left(\frac{8*8}{7*9}\right)\ldots = \frac{\pi}{2} \quad (13)$$

In realtà già così Eulero aveva raggiunto l'obiettivo, poiché il suo problema era già risolto *in forma chiusa*; infatti la teoria completa della funzione gamma poteva già essere basata sul prodotto infinito (1) che oggi viene scritto più convenzionalmente come:

$$\lim_{m\to\infty} \frac{m!(m+1)^n}{(n+1)(n+2)\ldots(n+m)} \quad (14)$$

Ma Eulero sviluppò ulteriormente l'idea che era dietro al comportamento strano del prodotto: per valori di n interi si ottenevano degli interi, mentre per valori razionali, come n = ½, si otteneva una espressione contenente π.

Il π richiama subito l'*idea del cerchio* mentre *la sua quadratura* richiama l'utilizzo dell'*integrale*. Eulero cercò, quindi, una trasformazione che gli permettesse di esprimere il suo risultato attraverso un integrale. Considerò:

$$\int_0^1 x^e (1-x)^n dx$$

Vediamo il ragionamento. Assumendo che n sia un intero, mentre *e* sia un valore arbitrario qualsiasi, si espande $(1 – x)^n$ con il *Teorema binomiale* e si trova che:

$$\int_0^1 x^e (1-x)^n dx = \frac{1*2*...*n}{(e+1)(e+2)...(e+n+1)} \quad (15)$$

L'obiettivo ora è di isolare il numeratore della parte di destra, perché esso rappresenta proprio il fattoriale n!.

Per cui sostituendo *f/g* al posto di *e*:

$$\int_0^1 x^e (1-x)^n dx = \frac{g^{n+1}}{f+(n+1)g} \frac{1*2*...*n}{(f+g)(f+2g)...(f+ng)} \quad (16)$$

da cui:

$$\frac{1*2*...*n}{(f+g)(f+2g)...(f+ng)} = \frac{f+(n+1)g}{g^{n+1}} \int_0^1 x^{f/g} (1-x)^n dx \quad (17)$$

Per isolare adesso 1 * 2 …n, si pone f = 1, g = 0 nel termine di sinistra, ma si otterrà nel termine di destra una *forma indeterminata*, che si può scrivere qualitativamente come:

$$\int_0^1 x^{\frac{1}{0}} dx \frac{(1-x)^n}{0^{n+1}} \quad (18)$$

Sostituendo $x^{(g/(f+g))}$ al posto di x si ottiene:

$$\frac{g}{f+g} x^{-\frac{f}{g+f}} dx \quad (19)$$

al posto di dx ed il membro di destra della (17) diviene:

$$\frac{f+(n+1)g}{g^{n+1}} \int_0^1 \frac{g}{f+g} (1-x^{\frac{g}{f+g}})^n dx \quad (20)$$

Se ancora una volta si pone f = 1, g = 0, riducendo prima questo integrale a:

$$\frac{f+(n+1)g}{(f+g)^{n+1}} \int_0^1 \left(\frac{1-x^{\frac{g}{f+g}}}{\frac{g}{f+g}}\right)^n dx \quad (21)$$

Il tutto porta ad un integrale indeterminato:

$$\int_0^1 dx \frac{(1-x^0)^n}{0^n} \qquad (22)$$

Considerando l'espressione relativa $(1 - x^z)/z$ per far scomparire z; poi differenziando il numeratore dal denominatore, con la nota regola dell'Hospital si ottiene:

$$\frac{-x^z dz lx}{dz} \quad (lx = \log x) \qquad (23)$$

che per z = 0 produce – ln.

Per cui è:

$$\frac{(1-x^0)}{0^n} = -lx \qquad (24)$$

e

$$\frac{(1-x^0)^n}{0^n} = (-lx)^n \qquad (25)$$

Si conclude perciò:

$$n! = \int_0^1 (-\log x)^n dx \qquad (26)$$

Questa formula, attraverso un integrale, è un modo per calcolare n! con interi positivi e n frazionari.

L'*integrale di Eulero* ottenuto si incontra oggi nella forma della **funzione gamma**:

$$\Gamma(x) = \int_0^\infty e^{-t} t^{x-1} dt \qquad e = 2,718284... \quad (27)$$

E' soprattutto ad opera di *Adrien Marie Legendre* (1752-1833) che lo conosciamo con il simbolo della Γ greca.

Legendre denominava *primo integrale euleriano* l'integrale della (15) e *secondo integrale euleriano* quello della (26) .

Il primo integrale euleriano oggi è conosciuto come *funzione Beta*:

$$B(m,n) = \int_0^1 x^{m-1}(1-x)^{n-1} dx \qquad (28)$$

L'integrale possiede significato per x > 0 e per n intero positivo è:

$$\Gamma(n+1) = n! \qquad (29)$$

Inoltre si è stabilito che per ogni x > 0 valgono anche:

$$x\Gamma(x) = \Gamma(x+1) \qquad (30)$$

$$B(m,n) = \frac{\Gamma(m)\Gamma(n)}{\Gamma(m+n)} \qquad (31)$$

e la formula di *Stirling*

$$\Gamma(x) \sim e^{-x} x^{x-\frac{1}{2}} \sqrt{2\pi} \qquad (32)$$

che ci dà un valore approssimato e semplice per Γ(x), quando x assume valori piuttosto grandi.

Esiste il fattoriale negativo?

La successiva domanda è: se il fattoriale esiste per valori interi e frazionari (razionali), che succede se introduciamo i numeri negativi? Ad esempio quanto vale e cosa rappresenta (-5 1/2)! ?

A questo punto, però, disponiamo di tre strumenti importanti:

- l'integrale di Eulero,
- il prodotto di Eulero,
- la relazione x Γ(x) = Γ(x + 1), x > 0 .

Quest'ultima relazione è la generalizzazione che per gli interi positivi vale:

$$(n + 1)\, n! = (n + 1)!\,, \quad n>0$$

Questa è una relazione apparentemente inutile ed ovvia che permette di eliminare il problema di calcolare un fattoriale di un reale arbitrario e il fattoriale di un numero appropriato tra 0 e 1. In questo modo se poniamo n = 4 1/2 nella formula precedente otterremmo (4 1/2 + 1)! = 5 1/2(4 1/2)! Se potessimo trovare solamente il valore di (4 1/2)! allora sapremmo quanto vale (5 1/2)! . Questo processo di riduzione ci da:

$$\left(5\frac{1}{2}\right)! = \left(\frac{3}{2}\right)\left(\frac{5}{2}\right)\left(\frac{7}{2}\right)\left(\frac{9}{2}\right)\left(\frac{11}{2}\right)\left(\frac{1}{2}\right)! \qquad (33)$$

e finché abbiamo (1/2)! = $1/2\sqrt{\pi}$ dalla (12) e la (13) noi possiamo risolvere il nostro problema. La formula precedente (n + 1) n! = (n + 1)! é equivalente a:

$$(n + 1) * 1 * 2 * \ldots * n = 1 * 2 * \ldots * n * (n + 1)$$

Essa ha senso solo per n = 1, 2, …, ed impedisce l'inserzione di altri valori; ma produce un risultato interessante. Infatti se consideriamo n = 0 otteniamo: 0! = 1 . Se consideriamo n = -5 1/2, n = -4 1/2, …, scopriamo la formula:

$$\left(-5\frac{1}{2}\right)! = \left(\frac{2}{1}\right)\left(-\frac{2}{1}\right)\left(-\frac{2}{3}\right)\left(-\frac{2}{5}\right)\left(-\frac{2}{7}\right)\left(-\frac{2}{9}\right)\left(\frac{1}{2}\right)! \quad (34)$$

dato che sappiamo già quanto vale (1/2)! allora sappiamo allora risolvere (-5 1/2)! . In questo modo la ricorrente relazione ci permette di risolvere valori di numeri fattoriali negativi .

Numeri complessi, la funzione gamma ed il fattoriale

La domanda successiva è: che succede se introduciamo ora anche i numeri complessi, tanto cari a Gauss? Quanto vale $\sqrt{-5}!$? Se nell'integrale di Eulero si sostituisce, per la variabile x, un numero complesso a + i b, con a > 0, otteniamo una funzione complessa che è definita per ogni numero complesso giacente sulla parte destra del piano gaussiano e che coincide con la Γ ordinaria per valori reali, eccetto i valori 0, -1, -2, … Il metodo della estensione della definizione del dominio della funzione gamma come anche il metodo per la continuità analitica fu indicato nel lavoro di *Bernhard Riemann* (1826-1866) e di *Karl Weierstrass* (1815-1897). La funzione con valori complessi, che risulta dalla sostituzione di numeri complessi nell'integrale di Eulero, è una funzione analitica. La funzione che emerge dal prodotto di Eulero è anche una funzione analitica. Se la ricorrente relazione per la funzione gamma è soddisfatta in alcune regioni allora deve essere soddisfatta anche in tutte le altre regioni in cui la funzione può essere analiticamente continua. Tutte le porzioni del piano complesso con l'eccezione dei valori 0, -1, -2, … sono accessibili per la funzione gamma complessa che è diventata l'unica estensione analitica per i valori complessi dell'integrale di Eulero (figura 8) .

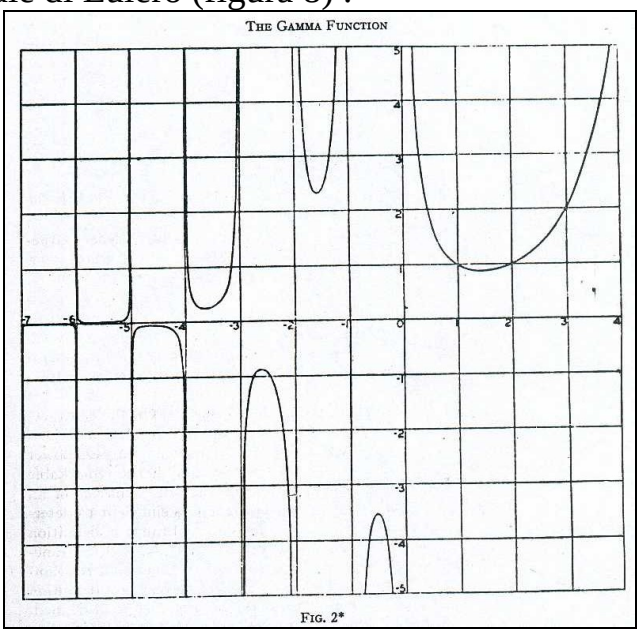


Figura 8 – Il fattoriale

La figura 8 è la stessa che, in [1], Derbyshire mostra come estensione del dominio del fattoriale, solo che è ottenibile con i ragionamenti sulla funzione gamma. Per comprendere perché devono essere esclusi alcuni punti come detto precedentemente si osservi che dalla (30) è:

$$\Gamma(x)= \Gamma(x + 1) / x$$

Se x tende a 0 otteniamo $\Gamma(0) = 1/0$; ovvero è una forma indeterminata che vale $+ \infty$ o $- \infty$ in dipendenza dal verso da cui si tende allo zero, se da sinistra o da destra .

La funzione gamma è compresa tra un numero infinito di punti di discontinuità (i punti di singolarità o poli), nei quali essa esibisce uno comportamento strano.

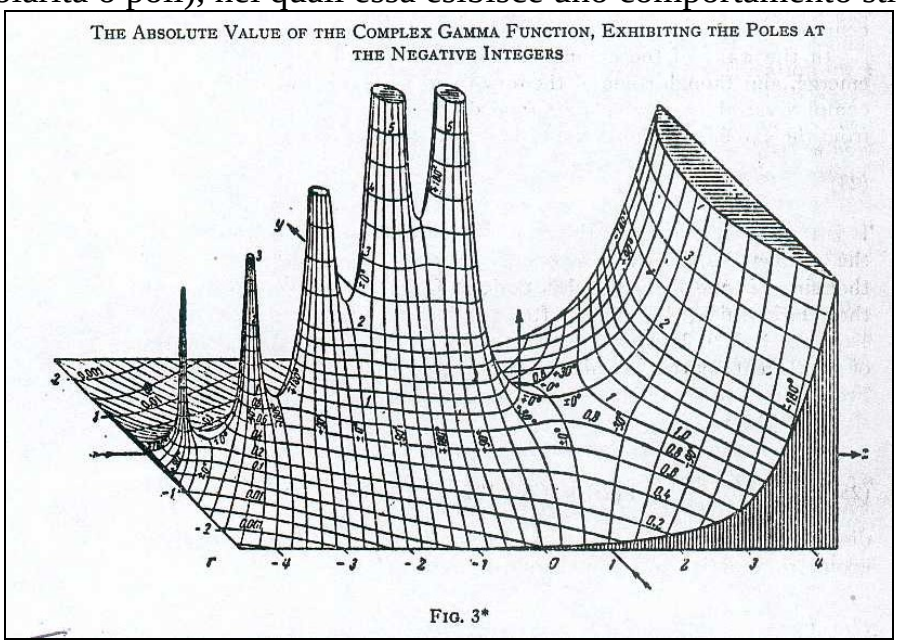


Figura 9 – La funzione gamma

I poli sono punti dove la funzione ha un comportamento infinito. Un comportamento del genere è quello dell'iperbole $y = 1/x$ intorno ad $x = 0$ oppure $y = tg\ x$ intorno ad $x = \pi/2$.

Le funzioni analitiche possiedono molti tipi di singolarità; quelle *con poli unici* sono conosciute come *funzioni analitiche meromorfiche*.

Vi sono anche funzioni che non possiedono singolarità per argomenti infiniti e sono note come *funzioni intere*, cioè definite per tutto il dominio dei valori, ovvero non ci sono punti esclusi.

Esempio di funzioni intere sono i polinomi mentre le funzioni meromorfiche appartengono ai polinomi razionali, cioè con numeratore e denominatore.

La funzione gamma è una funzione analitica meromorfica. Il suo reciproco 1/Γ(x), non ha punti di esclusione.

Formule varie

La formula di riflessione di Eulero è:

$$\Gamma(z)\Gamma(1-z)=\frac{\pi}{\sin \pi z} \qquad (35)$$

Esiste una formula di duplicazione dovuta a Legendre:

$$\Gamma(2z)=(2\pi)^{-\frac{1}{2}}2^{2z-\frac{1}{2}}\Gamma(z)\Gamma(z+\frac{1}{2}) \quad (36)$$

Ed una di Gauss:

$$\Gamma(nz)=(2\pi)^{\frac{1}{2}(1-n)}n^{nz-\frac{1}{2}}\Gamma(z)\Gamma(z+\frac{1}{n})\Gamma(z+\frac{2}{n})...\Gamma(\frac{z+n-1}{n}) \qquad (37)$$

Vi sono molte formule per derivare la funzione gamma come

$$d^2\log\Gamma(z)/dz^2=\frac{1}{z^2}+\frac{1}{(z+1)^2}+\frac{1}{(z+2)^2}+... \qquad (38)$$

Vi è poi una stretta relazione tra la funzione gamma e la funzione zeta, che vedremo in seguito:

$$\zeta(z)=\zeta(1-z)\Gamma(1-z)2^z\pi^{z-1}\sin\frac{1}{2}\pi z \qquad (39)$$

dove

$$\zeta(z)=1+\frac{1}{2^z}+\frac{1}{3^z}+... \qquad (40)$$

Questa formula e' stata usata per la prima volta da Riemann nel 1859 e viene convenzionalmente attribuita a lui. Nel 1894, però, venne scoperta una versione modificata dell'identità in alcuni lavori di Eulero del 1749 .

Per i numeri complessi, esiste anche una formula aggiunta nel 1848 da F.W. Newman:

$$\frac{1}{\Gamma(z)}=ze^{\gamma z}\left\{(1+z)e^{-z}\right\}\left\{\left(1+\frac{z}{2}\right)e^{-\frac{z}{2}}\right\}... \qquad \gamma=.5772156649... \qquad (41)$$

Perché l'integrale di Eulero dovrebbe essere considerato come soluzione per eccellenza? La sua frequenza d'uso è dovuta alla sua semplicità: è parzialmente un problema di estetica matematica. L'integrale di Eulero soddisfa l'equazione fondamentale ricorrente, xΓ(x) = Γ(x + 1), e che quest'equazione ci permette di avere tutti i valori reali della funzione gamma nell'intervallo da 0 ad 1.

Finché la soluzione del problema di interpolazione non è determinata unicamente, ha senso aggiungere al problema più condizioni e indagare se il problema possiede un'unica soluzione. Se è così speriamo che la soluzione coincida con quella di Eulero.

La ricorrente relazione è naturalmente una condizione da aggiungere. Se procediamo in tale direzione troviamo che la funzione gamma non è l'unica funzione che soddisfa questa relazione di ricorrenza e prodotti fattoriali. Si può, difatti, costruire una pseudo funzione gamma $\Gamma s(x)$ definendola, ad esempio tra 1 e il 2 ($\Gamma s(1) = 1 \quad \Gamma s(2) = 1$) e permettendo alla relazione ricorrente di estendere i propri valori in tutto lo spazio.

Lasciamo che $\Gamma s(x)$ sia uno ovunque tra 1 e 2, la ricorrente relazione ci porterà alla funzione:

$$\begin{aligned} \Gamma s(x) &= \frac{1}{x} && 0 < x \le 1 \\ \Gamma s(x) &= 1 && 1 \le x \le 2 \\ \Gamma s(x) &= x - 1 && 2 \le x \le 3 \\ \Gamma s(x) &= (x-1)(x-2) && 3 \le x \le 4 \end{aligned} \qquad (42)$$

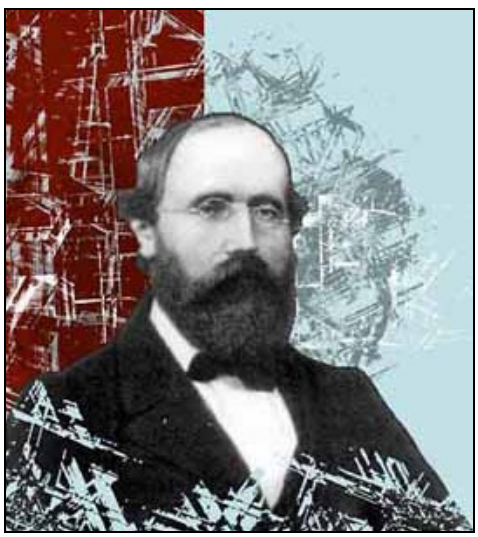
Consideriamo ora la costante $\gamma = 0,57721$ che appare nella formula (41); essa è la *costante di Eulero – Mascheroni*. Ci sono per essa molte espressioni:

$$\gamma = -d\Gamma(x)/dx\,|_{x=1}$$
$$\gamma = \lim_{n\to\infty}\left(1+\frac{1}{2}+\frac{1}{3}+\ldots+\frac{1}{n}\right)-\log n \qquad (43)$$

Ci fermiamo qui, si potrebbe in realtà scrivere ancora molto su essa e per ambiti molto diversi come la fisica oltre che la matematica. Certamente la funzione gamma non finirà mai di stupirci, nemmeno con le generazioni future.

Capitolo 7. La funzione zeta di Riemann

La funzione zeta fu studiata inizialmente da Eulero per valori reali di s e successivamente da Riemann.



Riemann

La funzione zeta è espressa secondo la formula vista da Eulero e in generale nel seguente modo :

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s} = \Pi_p \frac{1}{1-\mathrm{p}^{-s}} \qquad (44)$$

Dove s=a+jb con $s \in C$ ovvero numero complesso, mentre il produttorio è sviluppato all'infinito rispetto a tutti i numeri primi. La seconda parte a destra dell'uguale è ricordata come "prodotto di Eulero"-

La parte destra della (44) esprime che la funzione zeta di Riemann è una serie costituita dalla "potenza complessa" di tutti i numeri naturali; mentre la parte sinistra della (44), ricavata già da Eulero in campo reale R, mostra il legame esistente tra la serie ed il prodotto dei numeri primi; questo in sostanza perché anche i numeri primi fanno parte dell'insieme dei numeri naturali.

La dimostrazione di come si giunge alla parte sinistra è mostrata di seguito con i passaggi (a)(b)(c)(d). Ed è anche un elegante crivello di Eratostene in versione analitica che tiene però conto anche del numero naturale 1 (senza escluderlo).

Difatti è:

$$\zeta(s) = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \ldots \quad \text{(a)}$$

Se nella (a) si moltiplica per $1/2^s$ si ottiene:

$$\frac{1}{2^s}\zeta(s) = \frac{1}{2^s} + \frac{1}{4^s} + \frac{1}{6^s} + \frac{1}{8^s} + \ldots \quad \text{(b)}$$

Se alla (a) si sottrae la (b) si ottiene:

$$(1 - \frac{1}{2^s})\zeta(s) = 1 + \frac{1}{3^s} + \frac{1}{5^s} + \frac{1}{7^s} \quad \text{(c)}$$

L'analogia col crivello di Eratostene, per setacciare numeri primi, è evidente; ad esempio nella (c) si sono eliminati i termini potenza di 2 o multipli di 2. Se si ripete il procedimento all'infinito anche per $1/3^s$, $1/5^s$, $1/7^s$ etc, si ottiene:

$$(1 - \frac{1}{2^s})(1 - \frac{1}{3^s}).....\zeta(s) = 1 \quad \text{(d)}$$

Dalla (d) discende rapidamente la (44) osservando di avere a che fare con numeri primi.

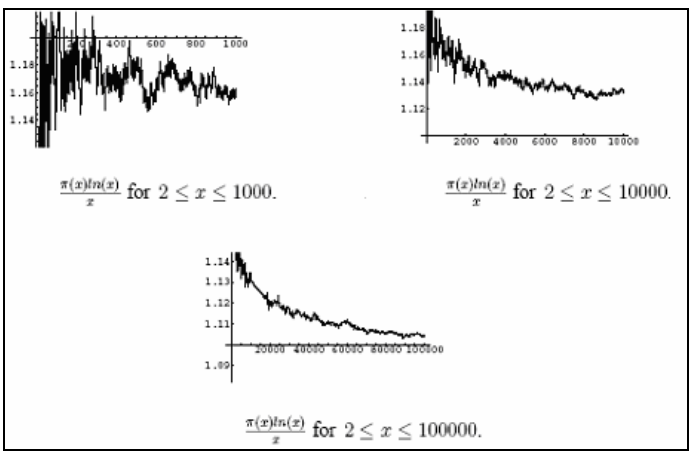


Figura 10 – TNP in vari intervalli

Riemann riscoprì l'utilizzo della funzione zeta proprio mentre si interessava della

distribuzione dei numeri primi ma la traslò logicamente dal campo reale a quello complesso. In tal modo studiò una funzione complessa di variabile complessa e definì una continuazione analitica all'intero piano complesso.

Dal prodotto di Eulero nella (44) è chiaro che non vi sono zeri per la funzione zeta per $Re(s) > 1$.

Continuazione analitica ed equazione funzionale

La funzione zeta di Riemann (è derivante da una serie) converge solo per $Re(s) > 1$. Essa può essere analiticamente continuata (vedi [1]), così da convergere anche per $Re(s) > 0$ (eccetto $s = 1$) usando le seguenti formule:

$$\varsigma(s) = \frac{\eta(s)}{2^{1-s} - 1} \qquad \text{dove } \eta(s) = \sum_{n=1}^{\infty} (-1)^n n^{-s} \qquad (45)$$

La funzione $\eta(s)$, anch'essa derivante da una serie, è convergente per $Re(s) > 0$. La continuazione analitica è espressa nel piano complesso nel seguente modo:

$$\varsigma(s) = \frac{\Gamma(1-s)}{2\pi i} \oint_C \frac{u^{s-1}}{e^{-u} - 1} du \qquad (46)$$

Dove C è un percorso che inizia da $-\infty$ e parallelo sopra l'asse reale, circondante l'origine e che ritorna a $-\infty$ parallelo sopra l'asse reale.

La **funzione Gamma**, $\Gamma(s)$ è definita come:

$$\Gamma(s) = \int_0^{\infty} e^{-t} t^{s-1} dt \qquad (47)$$

La (47) dà una definizione della zeta di Riemann per tutti i valori $s \neq 1$. $\varsigma(s)$ ha un polo a $s = 1$ con residuo 1. Essa può essere espansa in serie di Laurent attorno a $s = 1$:

$$\varsigma(s) = \frac{1}{s-1} + \gamma_0 + \gamma_1 (s-1) + \gamma_2 (s-1)^2 + ... \qquad (48)$$

Dove:

$$\gamma_k = \frac{(-1)^k}{k!} lim_{N \to \infty} \left(\sum_{m \leq N} \frac{\ln^k(m)}{m} - \frac{\log^{k+1} N}{k+1} \right) \qquad (49)$$

γ_0 è la *costante di Eulero-Mascheroni* uguale a $0.5772157...$

La zeta di Riemann soddisfa anche la **equazione funzionale**, data da

$$\pi^{-\frac{1-s}{2}}\Gamma(\frac{1-s}{2})\varsigma(1-s)=\pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})\varsigma(s) \qquad (50)$$

L'equazione funzionale può essere provata usando le proprietà modulari della funzione $\theta(t)=\sum_{n=-\infty}^{+\infty} e^{i\pi n^2 T}$:

$$\theta(T)=\frac{1}{\sqrt{-iT}}\theta(-\frac{1}{T}) \qquad (51)$$

E ne segue la formula per $Re(s) > 1$,

$$\varsigma(s)=\frac{\pi^{\frac{s}{2}}}{\Gamma(\frac{s}{2})}\int_0^{\infty}(\frac{\theta(it)-1}{2})t^{\frac{s}{2}-1}dt \qquad (52)$$

Zeri banali e non banali

Dall'equazione funzionale contenente la funzione Gamma segue che $\varsigma(s)$ si annulla a $s=-2n$, n =1, 2, 3…

Per verificare questo basta inserire $s=-2n$ nella (50) e si ottiene:

$$\varsigma(-2n)=\pi^{-2n-\frac{1}{2}}\frac{\Gamma(n+\frac{1}{2})\varsigma(2n+1)}{\Gamma(-n)} \qquad (53)$$

Poiché $\Gamma(n+\frac{1}{2})$ e $\varsigma(2n+1)$ sono finite e $\Gamma(s)$ ha un polo a $s=-n$ di conseguenza $\varsigma(-2n)=0$ per n=1, 2, 3 ...

I punti in cui una qualsiasi funzione si annulla, e quindi anche la zeta, sono detti "zeri della funzione"; in particolare gli zeri della funzione zeta sull'asse reale negativo sono detti zeri banali.

Gli zeri non banali della funzione zeta sono quelli maggiormente interessanti e sono legati direttamente a. $\pi(x)$.

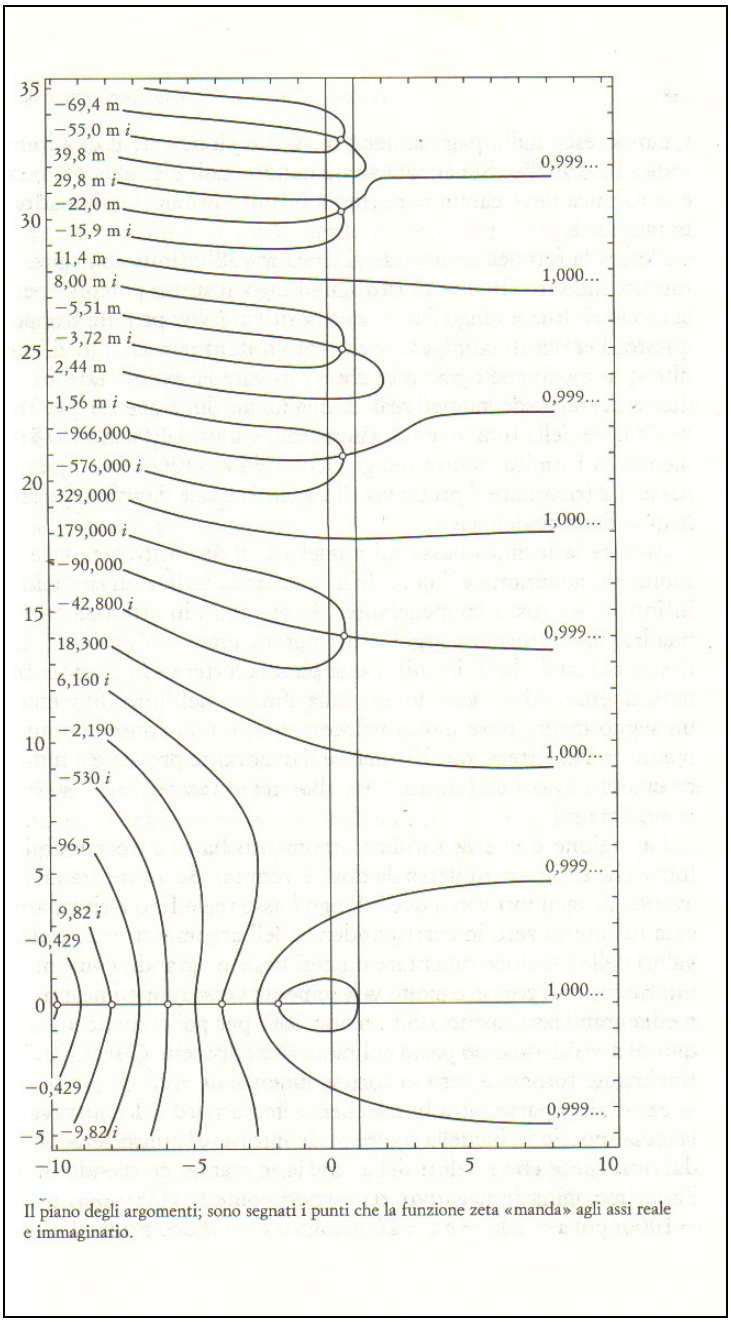
Se poniamo nell'equazione funzionale $s=s_0$ come zero complesso di $\varsigma(s)$ allora anche $1-s_0$ è un suo zero.

Inoltre poiché $\overline{\varsigma(s)}=\varsigma(\bar{s})$ allora anche $s=\overline{s_0}$ è uno zero complesso se s_0 è uno zero complesso.

In figura 11, che abbiamo ingrandito abbastanza per permettervi di analizzarla

visivamente in modo adeguato, viene riportata la rappresentazione della funzione zeta nel **piano dei valori**, con le due rette della striscia critica e gli zeri della funzione.

Nella figura 12 sono segnati i punti che la funzione zeta di Riemann manda, al variare dei valori s da cui dipende, sull'asse reale e sull'asse immaginario, cioè dove ci sono gli zeri non banali. Per cui è la rappresentazione del piano degli argomenti s della funzione ζ. Mentre nella figura 12 successiva si ha la rappresentazione della stessa ζ nel piano dei valori.



Il piano degli argomenti; sono segnati i punti che la funzione zeta «manda» agli assi reale e immaginario.

Figura 11 – ξ e piano degli argomenti

Riemann Hypotesis (RH)

La congettura di Riemann, denominata RH, afferma che "gli zeri complessi della funzione zeta sono su una retta, detta linea critica, ed hanno $\mathrm{Re}(s) = 1/2$."

In accordo con la RH se $\varsigma(s) = 0$ e $\mathrm{Im}(s) \neq 0$ allora $s = \frac{1}{2} + iw, w \in R.$

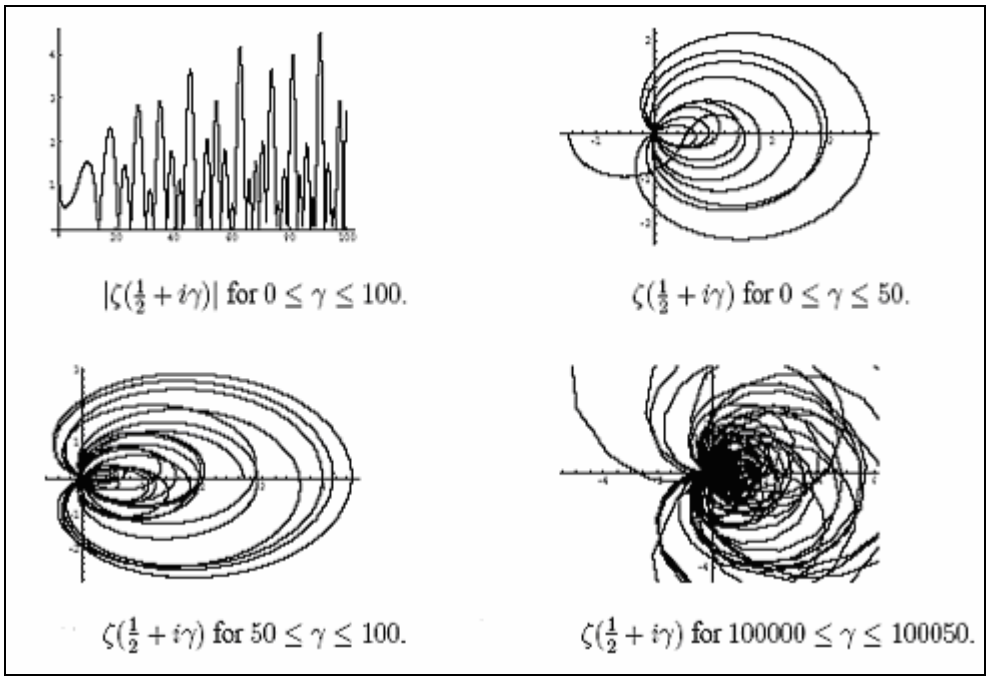


Figura 12 - ξ in vari intervalli del piano dei valori

La Figura 13 mostra i primi dieci zeri della funzione zeta.

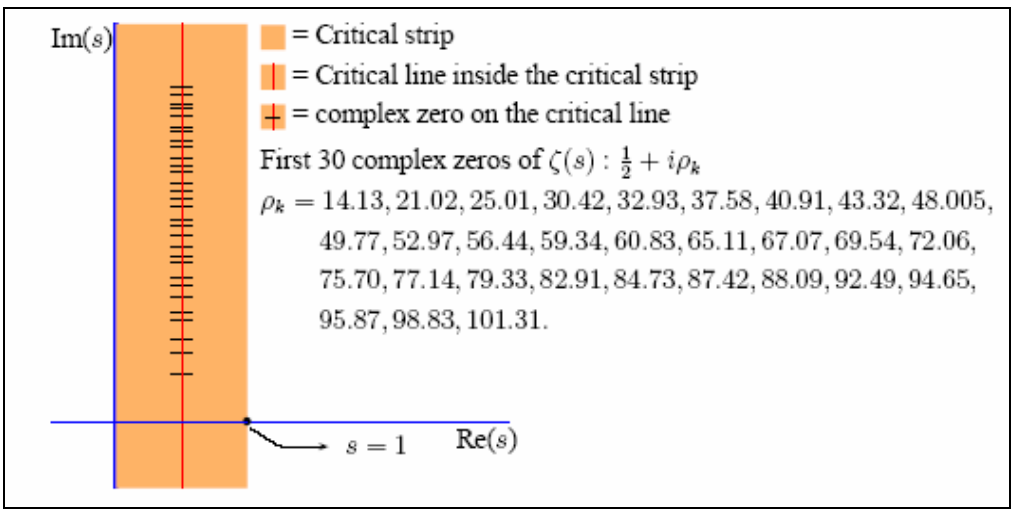


Figura 13 – zeri non banali e striscia critica

Nella Figura 13 per semplicità ci si è fermati alla seconda cifra decimale della parte immaginaria, ma in realtà i valori immaginari degli zeri sono valori irrazionali.

La storia della ricerca degli zeri è riassunta nella tabella 7 successiva.

Anno	Numero di zeri	Autore
1903	15	Gram
1914	79	Backlund
1925	138	Hutchinson
1935	1,041	Titchmarsh
1953	1,104	Turing
1956	25,000	Lehmer
1958	35,337	Meller
1966	250,000	Lehman
1968	3,502,500	Rosser, Yohe, Schoenfeld
1979	81,000,001	Brent
1982	200,000,001	Brent, Van de Lune, Te Riele, Winter
1983	300,000,001	Van de Lune, Te Riele
1986	1,500,000,001	Van de Lune, Te Riele, Winter
2001	10,000,000,000	Van de Lune
2004	900,000,000,000	Wedeniwski
2004	10,000,000,000,000	Gourdon en Demichel

Tabella 7 – Storia degli zeri non banali

Ricordando la funzione gamma di Eulero e che $s\Gamma(s) = \Gamma(s+1)$, l'equazione funzionale di Riemann è anche:

$$\xi(s)=\xi(1-s) \qquad (54)$$

$$\text{dove } \xi(s) = \pi^{s/2}\Gamma(\frac{s}{2})\zeta(s) \text{ per a>0}$$

Dalla (54) segue che se:

$$\theta(\mathrm{b}) = \arg(\pi^{-\frac{1}{2}ib}\Gamma(\frac{1}{4}+\frac{1}{2}\mathrm{ib}))=\Im[\log\Gamma(\frac{1}{4}+\frac{1}{2}\mathrm{ib})]-\frac{\mathrm{b}}{2}\log\pi$$

Allora:

$$Z(b) = e^{j\theta(b)}\zeta(\frac{1}{2}+ib) \text{ è reale (per b reale). In particolare è: } |Z(b)|=|\zeta(\frac{1}{2}+ib)|$$

Per cui, risultato fondamentale, è che gli zero di Z sono la parte immaginaria degli zeri di ζ sulla linea critica. La *Z è la funzione di Riemann-Siegel*. La Z fu introdotta da Siegel, anni dopo, consultando proprio il taccuino di appunti, il "*nachlass*" di Riemann. Nel nachlass, Riemann aveva introdotto un proprio metodo col quale era in grado di calcolare con sufficiente precisione almeno i primi 10 zeri.

In realtà per gli zeri non banali, avendo essi tutti parte reale pari a ½, ciò che varia è il valore della parte immaginaria che viene detto *altezza T*.

In particolare è possibile calcolare anche il numero di zeri (della parte positiva visto la simmetria) in gioco fino ad altezza T con la seguente *formula di Riemann - von Mangolt*:

$$N(T) = \frac{T}{2\pi}\log(\frac{T}{2\pi}) - \frac{T}{2\pi} + O(\log T) \qquad (55)$$

La formula è valida anche per valori bassi, se trascuriamo inizialmente il termine O(log T). Ad esempio per T=100, 1000 e 10000 N(T) vale 28,127 poi 647,741 e infine 10142,090; contro i valori reali che sono 29 poi 649 e 10142.

Esiste una parte di teoria che permette di trovare il numero di zeri nella *striscia critica* tra T1 e T2; mentre un'altra parte di teoria permette di trovare il numero di zeri che si trovano sulla *retta critica* tra T1 e T2. Ad esempio se chiamiamo con *m* il numero di zeri nella striscia critica tra 0 e 1 dell'asse reale e con *n* il numero di zeri sulla retta critica (in direzione parallela all'asse immaginario), allora se risultasse che *m = n* significherebbe che la RH sarebbe vera perché tutti gli zeri della striscia critica starebbero sulla retta critica; se invece fosse m>n allora la RH non sarebbe vera, perché esisterebbero anche zeri nella striscia critica.

Finora questo metodo non è stato efficace per dirci qualcosa di più. *Odlyzko,* come tanti altri, sostiene che la violazione della congettura, *forse*, potrebbe essere a valori di T2 molto alti che gli attuali computer non possono raggiungere. Il metodo di sopra comunque è sotto certi aspetti ingannevole: finora indagando localmente a zone si è trovato che m = n; tuttavia non potendo indagare oltre e sapendo che gli zeri sono infiniti dalla dimostrazione anche di Littlewood (e addirittura esiste l'ulteriore *congettura "gli zeri non banali sono di molteplicità 1"*) *potrebbe esistere* un qualche contro-esempio ancora non incontrato.

Questa incertezza dei matematici discende anche dal comportamento dei cosiddetti "termini periodici" di Riemann, dal risultato di Littlewood, circa il cambiamento infinito di segno della differenza $\pi(x) - \mathrm{Li}(x)$, tenendo conto anche dei filtri di Chebyscev. A valori molto alti difatti il segno dei termini periodici prende il sopravvento sul logaritmo integrale e il comportamento attualmente è imprevedibile.

Spaziatura media degli zeri nella striscia critica

La spaziatura media degli zeri nella striscia critica è di $\sim \frac{2\pi}{\log(\frac{T}{2\pi})}$. Questo vuol dire che in un intervallo unitario di retta ci sono un numero di zeri pari a:

$$\sim \frac{1}{2\pi}\log(\frac{T}{2\pi}) = \frac{1}{2\pi}\log T - \frac{1}{2\pi}\log 2\pi = \frac{1}{2\pi}\log T - 0,29250721...$$

Tale valore è denominato *densità degli zeri*. Al crescere di T il primo termine diventa molto maggiore della costante che di conseguenza diventa trascurabile.

$\pi(x)$ *e gli zero di* ς *(s)*

Per comprendere la relazione esistente tra $\pi(x)$ e gli zero della funzione zeta occorre introdurre la funzione a gradino J(x) (vedi [1] per il significato e l'uso) che conta, con

un certo peso, numeri primi e potenze di numeri primi minori o uguali a x:

$$J(x) = \sum_{r=1}^{\infty} \frac{1}{r} \pi(x^{1/r}) \qquad (56)$$

Da notare che la (56) non è una vera e propria serie, ma è costituita da un numero finito di termini: basta ad esempio calcolare J(100) per rendersene conto. Usando la funzione di Mobius (vedi [1] per il significato e l'uso) è possibile esprimere $\pi(x)$ in termini di $J(x)$,

$$\pi(x) = \sum_{r=1}^{\infty} \frac{\mu(r)}{r} J(x^{1/r}) \qquad (57)$$

Il legame tra la funzione $\varsigma(s)$ e J(x) si ricava nel seguente modo:

$$\varsigma(s) = \prod_{p=prime} (1 - p^{-s})^{-1} \qquad (58)$$

$$\ln \varsigma(s) = - \sum_{p=prime} \ln(1 - p^{-s}) = \sum_{p=primes} \sum_{k=1}^{\infty} \frac{p^{-ks}}{k} \qquad (59)$$

Come è ben spiegato in [1], nella (59) si è applicato l'integrazione di Newton legata all'espressione:

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + ...$$

Se la precedente espressione la si integra rispetto a x e si cambia di segno per portare il termine 1-x a numeratore si ottiene:

$$-\log(1-x) = x + \frac{1}{2}x^2 + \frac{1}{3}x^3 + \frac{1}{4}x^4 + ...$$

A questo punto la (59) è una somma infinita di somme infinite (la seconda delle quali dovuta allo sviluppo dei logaritmi). Ora a che cosa è uguale $1/p^{-k\,s}$? Consideriamo l'integrale di $x^{-s-1.}$ Si nota allora che è $\frac{1}{k} p^{-ks} = \frac{1}{k} s \int_{p^k}^{\infty} x^{-s-1} dx$. Quindi:

$$= s \sum_{p=primes} \sum_{k=1}^{\infty} \frac{1}{k} \int_{p^k}^{\infty} x^{-s-1} dx = s \sum_{k=1}^{\infty} \frac{1}{k} \sum_{prime} \int_{p^k}^{\infty} x^{-s-1} dx$$

$$= s \sum_{k=1}^{\infty} \frac{1}{k} \sum_{i=1}^{\infty} \int_{p_i^k}^{\infty} x^{-s-1} dx \qquad (60)$$

Cosa rappresenta un termine come $\frac{1}{k} p^{-ks} = \frac{1}{k} s \int_{p^k}^{\infty} x^{-s-1} dx$?

E' la striscia di area della J(x) che parte da p^k che è di altezza 1/k e che va all'infinito; nella figura successiva c'è l'esempio relativo al termine $1/2 * 1/3^s$.

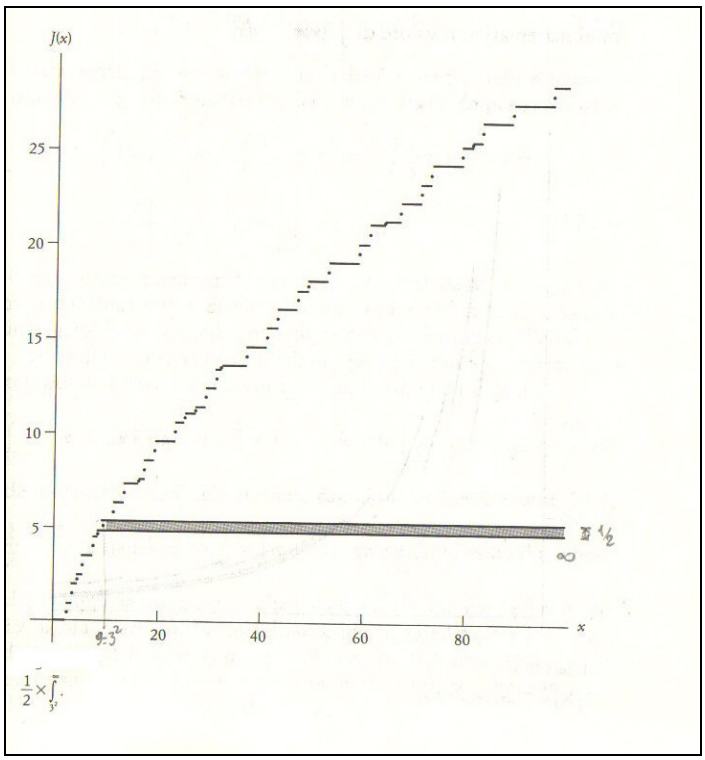


Figura 14 – J(x)

Dovendo sommare strisce di aree infinite il risultato darebbe infinito (un NaN, quindi non trattabile), per cui per poter comprimere tale area totale e ottenere un risultato finito si deve operare uno "*schiacciamento*" che è offerto dalla stessa J(x), ovvero si calcola il termine $\int_0^{\infty} J(x)x^{-s-1}dx$. Nella figura 15 successiva si vede che tale sistema permette lo "schiacciamento" del termine della figura precedente, per cui si può arrivare ad un'area finita.

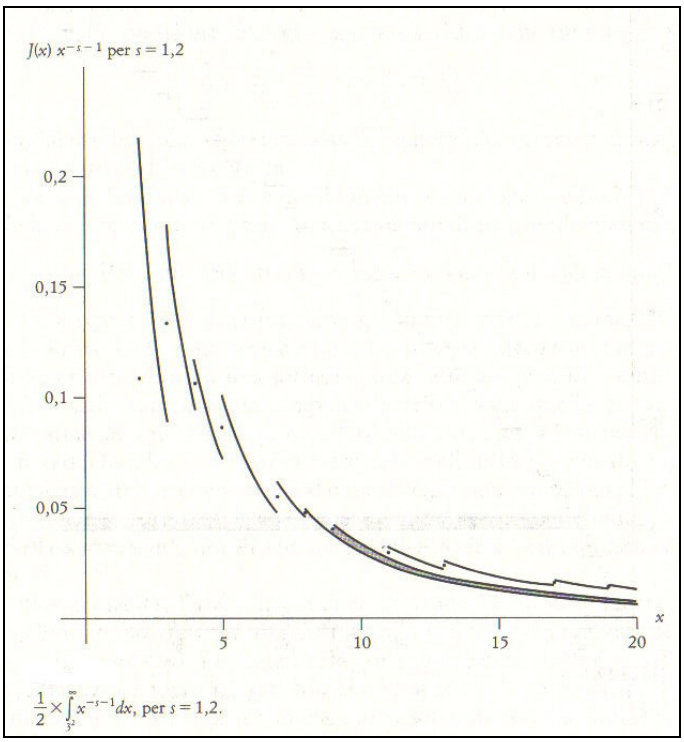


Figura 15 – Schiacciamento con J(x)

Una sommatoria di termini come quello espresso dalla (60), quindi, equivale a:

$$\frac{\ln \varsigma(s)}{s} = \int_0^{\infty} J(x) x^{-s-1} dx \qquad (61)$$

Si vede che $\frac{\ln \varsigma(s)}{s}$ è la *trasformata di Mellin* di $J(x)$. La *trasformata di Mellin inversa* dà $J(x)$ in termini di $\frac{\ln \varsigma(s)}{s}$:

$$J(x) = \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} \frac{\ln \varsigma(s)}{s} x^{-s} ds \,. \qquad (62)$$

Inoltre è possibile esprimere la funzione zeta come se fosse una *funzione intera* (ovvero definita in tutto il suo dominio complesso ma con un "trucchetto matematico") e quindi in funzione delle sue radici ρ (gli zeri non banali):

$$J(x) = Li(x) - \sum_{\rho} Li(x^{\rho}) - \ln(2) + \int_x^{\infty} \frac{dt}{t(t^2-1)\ln(t)} \qquad (63)$$

Dove $Li(x) = \int_{\mu}^{x} \frac{du}{\ln(u)}$ è il Logaritmo integrale e $\mu = 1.45136...$ è la *costante di Soldner*.

Il termine $\sum_{\rho} Li(x^{\rho})$ sono i cosiddetti "termini periodici" così come li denominò Riemann. Il termine "periodico"è dovuto alla chiusura della serie attorno ad un valore πi o $-\pi i$.

In [1] viene mostrato il comportamento dei "termini periodici" per bassi valori e con l'ipotesi di partenza che la RH sia vera. Questa precisazione è dovuta al fatto che i grafici ivi presentati sono una conseguenza di tutto quanto discende dalla RH.

I numeri primi però, suddividendoli con i filtri di Chebyscev in due categorie di resto, si nota che al crescere di N, i due gruppi tendono a variare lentamente di numerosità, l'uno rispetto a l'altro, e quindi la loro differenza cambia di segno molte volte in vari intervalli (all'infinito).

Nella tabella successiva si riportano pochi valori di esempio e da essa si comprende quanto sopra; infatti si nota che per un intervallo grande i numeri primi con resto 1 sono in numero inferiore a quelli con resto 3 ma che la violazione avviene poi ad un determinato valore (p=26861).

In realtà ciò avviene infinite volte. Col filtro a 2 si ottiene resto a 1 (vero anche per un numero dispari). Con filtro a 3 le differenze sono addirittura maggiori con resti 1 e 2.

Filtro divisore 4 Regola: # primi resto 1 < # primi resto 3		
P	**Resto 1**	**Resto 3**
101	12	13
1009	81	87
10007	609	620
26861	violazione	

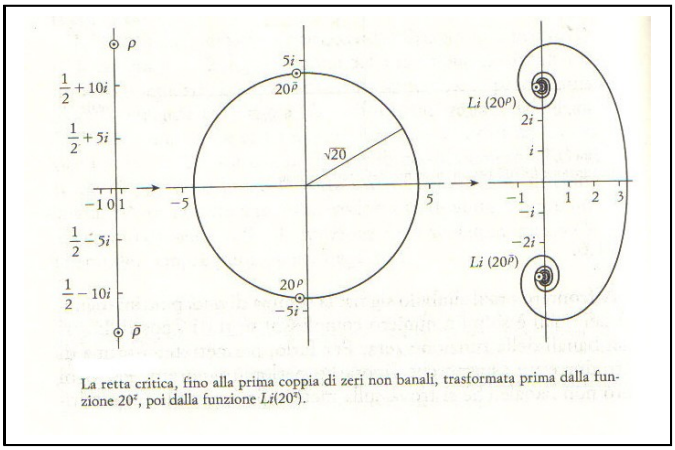
Tabella 8 – Filtro di Chebyscev

Analoghe considerazioni, con lievi differenze, potrebbero essere fatte suddividendo i numeri primi nelle due forme generatrici 6n-1 e 6n+1 (escludendo i composti e il 2 ed il 3) con n che varia da 0 a infinito.

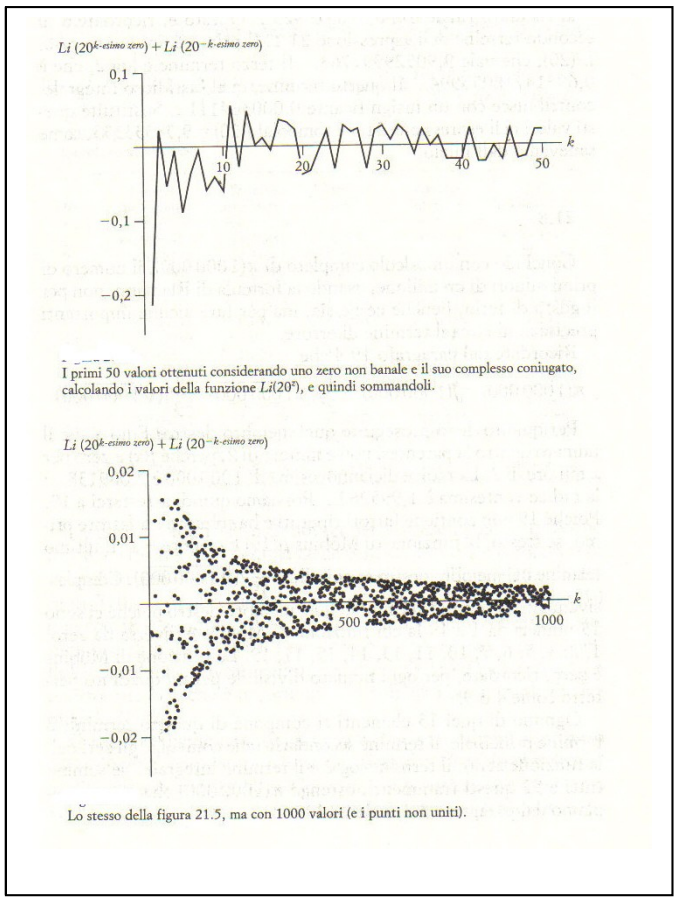
In realtà tutto ciò si ripete alternativamente all'infinito anche per la differenza $\pi(x) - Li(x)$ (risultato di Littlewood) e ciò influisce sui termini periodici attraverso gli zeri non banali.

Come sia legato tutto ciò non è del tutto chiaro. Sicuramente nella (63) i termini periodici potrebbero giungere ad un valore superiore agli altri termini, causando che le spirali in gioco, che si chiudono sempre su πi e $-\pi i$, diventano sempre più grandi e si sovrappongono, arrivando ad una situazione estremamente complessa.

Nel seguito vengono mostrate figure, tratte da [1], relative ai termini periodici, che evidenziano quanto detto sopra.

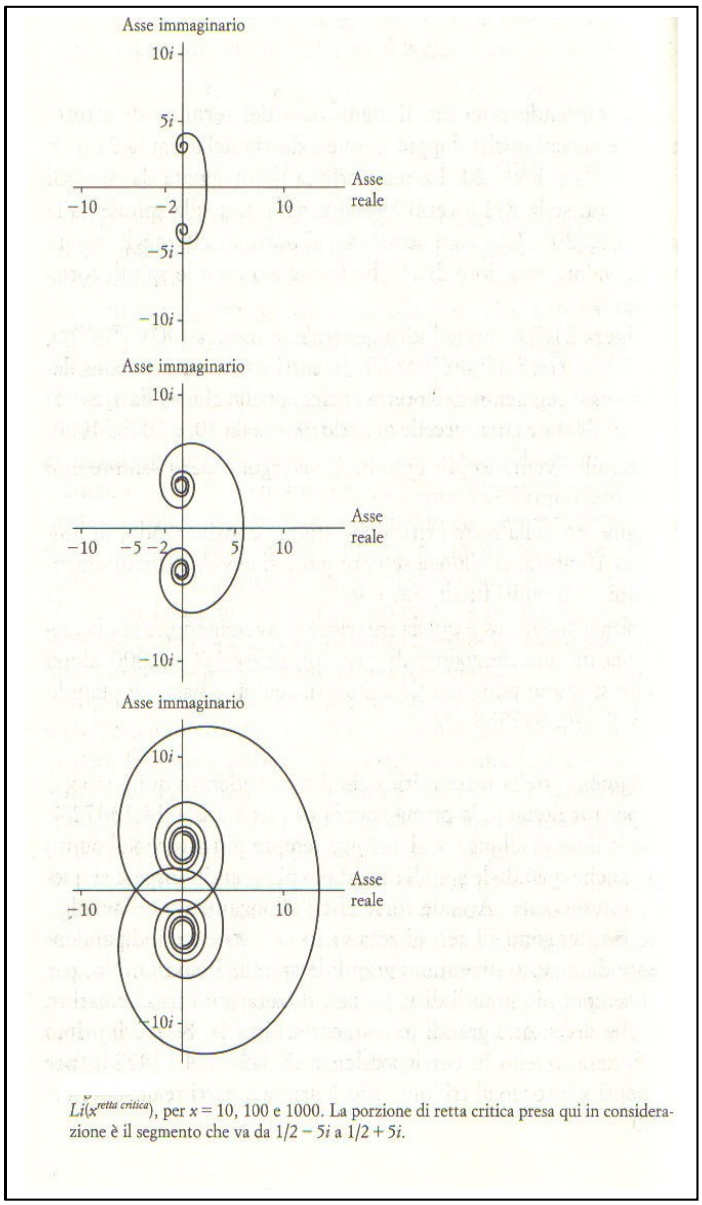


La retta critica, fino alla prima coppia di zeri non banali, trasformata prima dalla funzione 20^z, poi dalla funzione $Li(20^z)$.



I primi 50 valori ottenuti considerando uno zero non banale e il suo complesso coniugato, calcolando i valori della funzione $Li(20^z)$, e quindi sommandoli.

Lo stesso della figura 21.5, ma con 1000 valori (e i punti non uniti).



$Li(x^{\text{retta critica}})$, per $x = 10$, 100 e 1000. La porzione di retta critica presa qui in considerazione è il segmento che va da $1/2 - 5i$ a $1/2 + 5i$.

Figura 16 – Termini periodici di Riemann

Ritornando ai legami, poiché $\pi(x)$ è legata a $J(x)$ e $J(x)$ a sua volta agli zeri della $\varsigma(s)$ allora il conteggio dei numeri primi dipende dagli zeri non banali della funzione $\varsigma(s)$. Questo fu il risultato proposto da Riemann e dimostrato, nel 1895, da *von Mangoldt*.

RH1 equivalente a RH (risultato di Lagarias)

L'ipotesi di Riemann è equivalente a certe congetture legate ad altre funzioni moltiplicative. Ad esempio chiamando con $\sigma(n) = \sum_{d \backslash n} d$ la somma dei divisori di un numero, allora è:

$$\sigma(n) < e^{\gamma} n \ln \ln n \quad n > 5040 \qquad (64)$$

La (64) è il Teorema di Robin.

Dalla (64) Lagarias ha recentemente mostrato che la RH è equivalente a provare la seguente relazione tra il "*numero armonico*" e la somma dei suoi divisori :

$$\sigma(n) \le H_n + e^{H_n} \log(H_n) \quad n \in \{1, 2, 3, ...\} \qquad (65)$$

dove $\sigma(n) = \sum_{d \backslash n} d$ *e* $H_n = \sum_{k=1}^{n} \frac{1}{k}$ *è il numero armonico o serie armonica di n termini.*

La formula di Eulero fornisce un prodotto che rappresenta la funzione zeta; però è possibile nella rappresentazione del prodotto coinvolgere anche gli zeri della funzione (Hadamard) :

$$\varsigma(s) = \frac{e^{(\ln(2\pi) - 1 - \frac{\gamma_0}{2})s}}{2(s-1)\Gamma(1 + s/2)} \prod_{\substack{\varsigma(\rho)=0 \\ \mathrm{Im}(\rho)>0}} (1 - \frac{s}{\rho}) e^{\frac{s}{\rho}} \qquad (66)$$

Dove il prodotto è su ρ, le radici non banali della funzione zeta. ρ_k, può essere usato per definire serie simili alla serie armonica che in quel caso sono convergenti. Definendo $Z(n) := \sum_k \rho_k^{-n}$, allora $Z(n)$ è convergente e $Z(1)$ fu determinata dallo stesso Riemann ed è pari a $\frac{1}{2}(2 + \gamma_0 - \ln(4\pi))$.

Nella RH1 si rimane stupiti della non presenza di numeri complessi o di numeri primi, ma in realtà il legame esiste ed è molto sottile!

E' da osservare che

$$\frac{d}{dt} \ln t = \frac{1}{t} \Rightarrow H_n > \ln(n+1)$$

H_n diverge e cresce come ln n e vale il seguente *limite fondamentale* :

$$\lim_{n \to \infty} H_n - \ln n = \gamma$$

dove γ è la costante di Eulero Mascheroni, ritenuta sicuramente irrazionale e forse trascendente (finora non dimostrato).

RH2 equivalente a RH (funzione di Mertens)

La RH2 contrariamente alla RH1 è direttamente connessa ai numeri primi, attraverso la funzione di Mobius μ.

In [1] si vede che se si considera l'inverso della zeta di Riemann risulta che:

$$\frac{1}{\zeta(s)} = (1-\frac{1}{2^s})(1-\frac{1}{3^s})(1-\frac{1}{5^s})...$$

Se si fanno tutte le combinazioni di prodotti possibili dei termini tra le varie parentesi si ottiene una somma di termini dove non sono presenti tutti i numeri naturali. In pratica rimangono solo i numeri naturali che sono:

- il prodotto di un numero dispari (compreso 1) di numeri primi differenti e con segno negativo,
- il prodotto di un numero pari di numeri primi differenti e con segno positivo,

Spariscono i numeri naturali che sono divisibili per qualche numero primo al quadrato (o potenza). Introduciamo la funzione di Mobius μ definita nel seguente modo:

- $\mu(1)=1$
- $\mu(n) = 0$ se n è divisibile per il quadrato di un numero
- $\mu(n) = -1$ se n è un numero primo o il prodotto di un numero dispari di numeri primi distinti
- $\mu(n) = 1$ se n è il prodotto di un numero pari di numeri primi distinti

In tal caso è:

$$\frac{1}{\zeta(s)} = \sum_n \frac{\mu(s)}{n^s} \qquad (67)$$

Ora introduciamo la *funzione di Mertens M(k):* essa è il *valore cumulativo di $\mu(n)$*:

$$M(k) = \sum_k \mu(\kappa) \qquad (68)$$

Ora la **RH2** equivalente a RH è:

$$M(k) = O(k^{1/2+\varepsilon}) \qquad (69)$$

con ε piccolo a piacere.

Tenendo conto della definizione della *funzione O grande*: allora la (69) equivale a dire:

$$M(k) < c\, k^{1/2+\varepsilon} \quad (70)$$

In realtà la (70) è anche esprimibile nel seguente modo:

$$M(k) = O\,(k^{1/2} \ln k)$$

Ora poiché è noto che ln k cresce più lentamente di una qualsiasi potenza (vedi capitolo relativo al logaritmo), anche non intera, quindi con ε piccolo a piacere, si può sostituire il termine ln k con il termine k^{ε} e per la regola delle potenze con stessa base discende la (70).

Una **congettura più debole**, proposta da Derbyshire, è:

$$M(k) = O\,(k^{1/2}) \qquad (71)$$

La (71) equivale a dire:

$$M(k) < ck^{1/2}$$

Anch'essa da dimostrare. Pensiamo che, nonostante tale congettura sia più debole, sia, invece, un po' più difficile da dimostrare (o che sia vera), perché in pratica si afferma che il log k si deve comportare, nonostante già i suoi grandi sforzi, proprio come la potenza x^0, il che è difficile. Sostanzialmente siamo convinti che purtroppo $M(k) \neq O\,(k^{1/2})$.

L'interpretazione probabilistica di Denjoy

Denjoy propose una interpretazione statistica effettivamente valida. Ad esempio consideriamo tutti i numeri naturali a partire da 2 e sotto ognuno scriviamo anche i suoi fattori primi e trascuriamo tutti i numeri che hanno un fattore quadrato o potenza e proseguiamo a segnare con T (testa) i numeri che hanno un numero pari di fattori primi e con C (croce) quelli con numeri dispari di fattori primi.

Dalla statistica ci aspetteremmo che al tendere di N tende ad un valore grande di numero di lanci di una moneta perfettamente equilibrata, si ottengano N/2 teste e N/2 croci ma con un errore a favore di testa o di croce (Jakob Bernoulli) che è rappresentato *circa* dalla radice quadrata di N! In altri termini al crescere di N, l'errore è minore di $N^{1/2+\varepsilon}$ con ε piccolo a piacere. In realtà l'ipotesi della RH potrebbe discendere anche da qua ed essere dimostrata (ma non è così semplice) nel settore della probabilità.

Quello di cui sopra si potrebbe anche riassumere semplicisticamente dicendo che un numero senza fattori primi ripetuti è una T (testa) o una C (croce) con probabilità ½.

RH3 equivalente a RH (risultati di Von Kock)

La RH3 riporta in ballo, ed era questo il vero scopo di Riemann, la differenza $\pi(x)$ – Li(x) ed il suo errore assoluto e relativo. D'altra parte il logaritmo integrale si può espandere in serie nel seguente modo:

$$Li(x) \sim \frac{x}{\ln x} \sum_{k=0}^{\infty} \frac{k!}{(\ln x)^k} = \frac{x}{\ln x} + \frac{x}{(\ln x)^2} + \frac{2x}{(\ln x)^3} + \ldots \quad (72)$$

Da qui :

$$\pi(x) \sim Li(x), x \to \infty$$

Già Hadamard con la dimostrazione del TNP aveva mostrato un termine d'errore tra $\pi(x)$ e Li(x):

$$\pi(x) = Li(x) + O(xe^{-a\sqrt{\ln x}}), x \to \infty$$

con a>0.

Nel libro di Bachmann, Von Kock esprimeva tale relazione nel seguente modo:

$$\pi(x) - Li(x) < k (\sqrt{x} \log x) \qquad (73)$$

Oggi si esprime semplicemente attraverso la O grande (come visto nella RH2) nel seguente modo:

$$|\pi(x) - Li(x)| = O(x^{1/2+\varepsilon}) \qquad (74)$$

Per comprendere come la (74) discende dalla (73) occorre ricordare i ragionamenti precedenti della O grande, e che il log varia più lentamente delle potenze di x, allora è vera la seguente espressione:

$$\log x = O (x^{\varepsilon})$$

da cui per le regole delle potenze discende la (74).

Il termine d'errore di Von Kock $O(\sqrt{x} \log x)$ implica il termine d'errore $O(^{x1/2+\varepsilon})$ ma non è vero il viceversa; infatti i due risultati non sono del tutto equivalenti: sebbene log x cresce più rapidamente di qualsiasi potenza di x, questo è anche vero per $(\log x)^N$, con N positivo.

In altri termini la (74) sarebbe vera lo stesso anche se il termine d'errore nella (73) fosse stato del tipo $O(\sqrt{x} (\log x)^N)$ con N qualsiasi valore positivo. La (74) quindi è una forma debole della (73).

Riguardando la (74) attraverso la (73), sono stati proposti anche dei valori di k. Nel 1976 *Lowell Schoenfeld* ha proposto l'equivalente della (73) con $k=1/(8\pi)$ per $x \geq 2567$.

RH4 equivalente a RH (funzione Θ)

Se poniamo $\Theta(x) = \Sigma \log(p)$ dove la sommatoria è estesa a tutti i numeri primi minori o uguali a (x), troviamo i risultati della tabella seguente.

Θ(n)	Valore
Θ(100)	83,72
Θ(1000)	956,24
Θ(10000)	9895,99
Θ(100000)	99685,4
Θ(1000000)	998484

Tabella 9 – Valori di Θ(x)

Anche in questo caso, per stimare l'errore commesso, cioè la differenza tra Θ(x) e x, ci viene in aiuto la RH, in un'altra equivalente formulazione, la RH4.

Dato un qualsiasi $\varepsilon > 0$, esiste un intero tale che per ogni t

$$| \Theta(t) - t | < t^{\varepsilon} \sqrt{t} \quad (75)$$

RH5 equivalente a RH (sequenza di Farey)

Se F_n è la sequenza di Farey di ordine n, che inizia con 1/n fino a 1/1, allora per tutti gli e>1/2 è

$$\sum_{i=1}^{m} |F_n(i) - \frac{i}{m}| = O(n^e) \qquad (76)$$

Allora la (76) è una forma equivalente della RH, dove $m = \sum_{i=1}^{n} \phi(i)$ è il numero di termini della sequenza di Farey di ordine n.

Per e > -1 è anche equivalente alla RH la seguente espressione:

$$\sum_{i=1}^{m} \left(F_n(i) - \frac{i}{m} \right)^2 = O(n^e) \qquad (77)$$

RH6 equivalente a RH (teoria dei gruppi e funzione di Landau)

La RH è equivalente a certe congetture della Teoria dei gruppi. Ad esempio se si indica con g*(n) il massimo ordine di elementi di un gruppo di Simmetria* S_n, di grado n, nota come *funzione di Landau*, allora la RH è equivalente per qualche n > M

$$\ln g(n) < \sqrt{Li^{-1}(n)} \qquad (78)$$

RH7 equivalente a RH (Derivata della zeta di Riemann)

La RH è equivalente al fatto che la *derivata della funzione zeta di Riemann* ζ'non ha zeri nella striscia 0 < Re(s) < ½.

Questo risultato è molto più importante di quanto si pensi. Dire che ζ ha solo zeri non banali sulla retta critica, mentre la ζ' non ha zeri nella striscia 0 < Re(s) < ½, ci permette di estendere la zona-libera di zeri a: 0 < Re(s) < ½. Questo risultato è servito a *Norman Levinson* per mostrare un Teorema sulla Linea critica.

Considerazioni sulle ipotesi equivalenti della RH

In realtà quelle presentate sono le principali più note, ma ne esistono altre ancora. E' evidente che la dimostrazione di una sola delle RH equivalenti ci porterebbe ad una conoscenza teorica maggiore e a saper prevedere il valore π(N) qualsiasi sia N e senza conteggiare i numeri primi. A quel punto avremo la conoscenza della vera distribuzione dei numeri primi.

Sappiamo che la (44) è il cuore di tutta la teoria e della filosofia del problema di Riemann. Essa mette in relazione una sommatoria dell'inverso di una potenza complessa di numeri naturali, con un prodotto di potenze di numeri primi. Di conseguenza la (44) mette in relazione una struttura additiva nel quale si sommano numeri positivi, incrementati di 1, ad una struttura moltiplicativa. Questo è anche il "nocciolo" della strategia degli attacchi che si stanno sviluppando all'ipotesi di Riemann, aggirando la struttura moltiplicativa dei numeri primi con quelle additiva dei numeri naturali. Solo pensando a questo si intuisce l'importanza del problema di *Goldbach*, della congettura di *Polignac*, di *Chen* e dei lavori di *Vinogradov*, *Lagarias*, etc ed il contributo anche di vari gruppi come quello ERATOSTENE.

Finora non è stata trovata la soluzione definitiva. Probabilmente se le ipotesi equivalenti sono troppo legate alla RH o alla stessa tecnica di soluzione ci si ritrova di nuovo in uno stallo. In ogni caso queste non sono le uniche strade battute, molte altre coinvolgono strumenti matematici ben più complessi: trasformate di *Fourier*, analisi probabilistiche, gli operatori di *Laplace*, etc che non esamineremo in questa sede.

Conseguenze deboli della RH (LH: l'ipotesi Lindelhof)

L'ipotesi di *Lindelhof* dice che per ogni ε>0 è:

$$\zeta(\frac{1}{2}+it)=O(t^{\varepsilon}),\ \text{per t all'infinito} \quad (79)$$

Se indichiamo con p_n l'n-esimo numero primo, *Albert Ingham* mostrò che l'ipotesi di Lindelhof implicava che per ε>0 ed n sufficientemente grande:

$$p_{n+1}-p_n < p^{\frac{1}{2}+\varepsilon} \quad (80)$$

Ma cosa afferma esattamente la LH? Se si indica un numero complesso come σ + i t , la LH si chiede come, per un valore fissato σ, varia il modulo $|\zeta(\sigma+it)|$ al variare di t. Meglio di tutto parlano le figure che mostriamo di seguito.

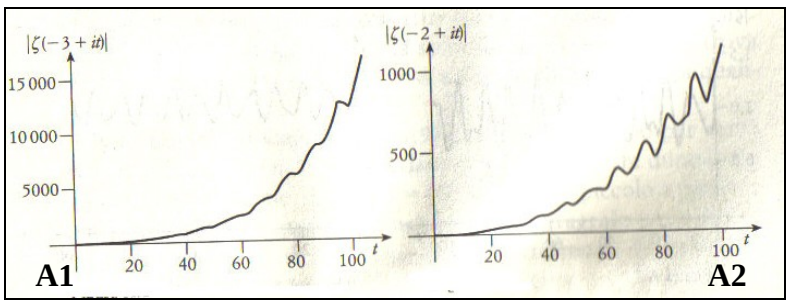


Figura 17 - Andamento LH (a)

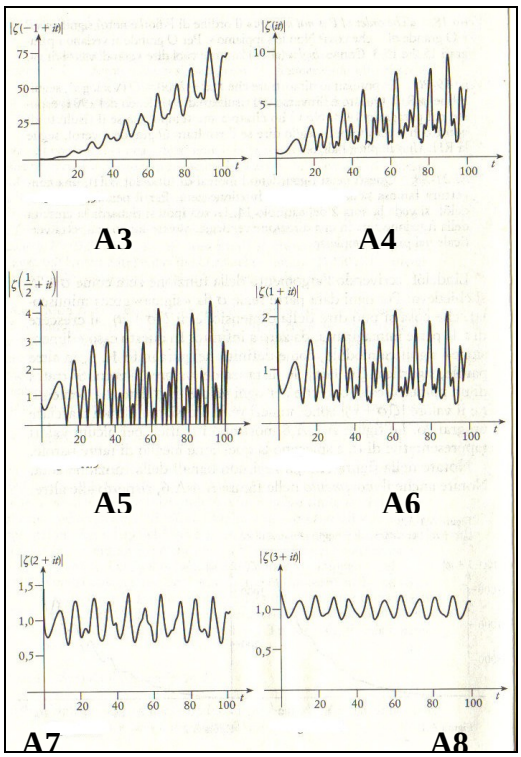


Figura 18 – Andamento LH (b)

I diagrammi mostrano, ad esempio:

- in A4 $|\zeta(0)|=\frac{1}{2}$ (per la verità è $\zeta(0)=-\frac{1}{2}$);
- in A5 abbiamo gli zeri non banali della funzione, cioè a t=0 e σ=1/2;
- in A6 c'è la divergenza della serie armonica;
- in A7 c'è il valore 1,644934… (soluzione della serie di Basilea)
- in A8 il numero di Apéry: 1,202056…
- in A2 c'è uno zero banale per t=0;
- in A1 e A3 ci sono falsi zeri: le approssimazioni erano così piccole che sono stati registrati come zeri.

L'obiettivo della LH è quello di individuare dai grafici una O grande! Dai grafici si nota difatti che:

- Per σ=-1,-2,-3 il grafico ha l'aspetto di una O (t^2) oppure O(t^3), a causa del fatto che c'è una rapida crescita di σ verso sinistra lungo l'asse negativo;
- Per σ=2, 3 il grafico sembra quello di O(1) ovvero O (t^0) infatti le curve oscillano al di sotto di un certo valore;
- Nella striscia critica per σ=0, ½ e 1 è difficile comprendere l'andamento o dire che O grande possa essere.

La LH ipotizza che, in generale, per ogni σ esista un valore μ tale che:

$$|\zeta(\sigma+it)|=O(t^{\mu+\varepsilon}) \quad (81)$$

Ma che succede quando siamo nella striscia critica con σ=0, ½ e 1 ? Attualmente la teoria ipotizza che μ sia funzione di σ: μ(σ) detta *funzione di Lindelhof*, mostrata in figura 19.

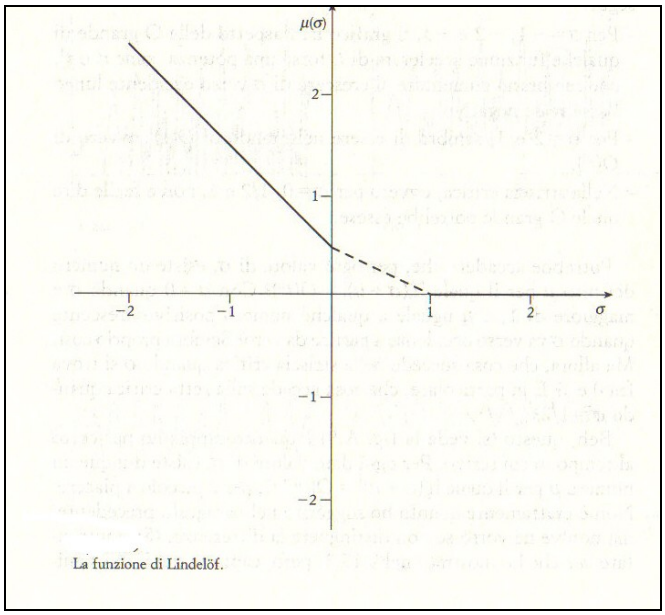


Figura 19 – Funzione di Lindelhof

Questa funzione si comporta in questo modo:

- $\sigma \leq 0$, $\mu(\sigma) = ½ - \sigma$
- $\sigma \geq 1$, $\mu(\sigma) = 0$
- $0 \leq \sigma \leq 1$, $\mu(\sigma) < ½(1-\sigma)$; in poche parole si è sotto la linea tratteggiata della funzione.
- Per tutti i valori di σ, $\mu(\sigma)$ è convessa verso il basso, anche nella striscia critica per cui nella striscia critica $\mu(\sigma)$ è nulla o positiva.

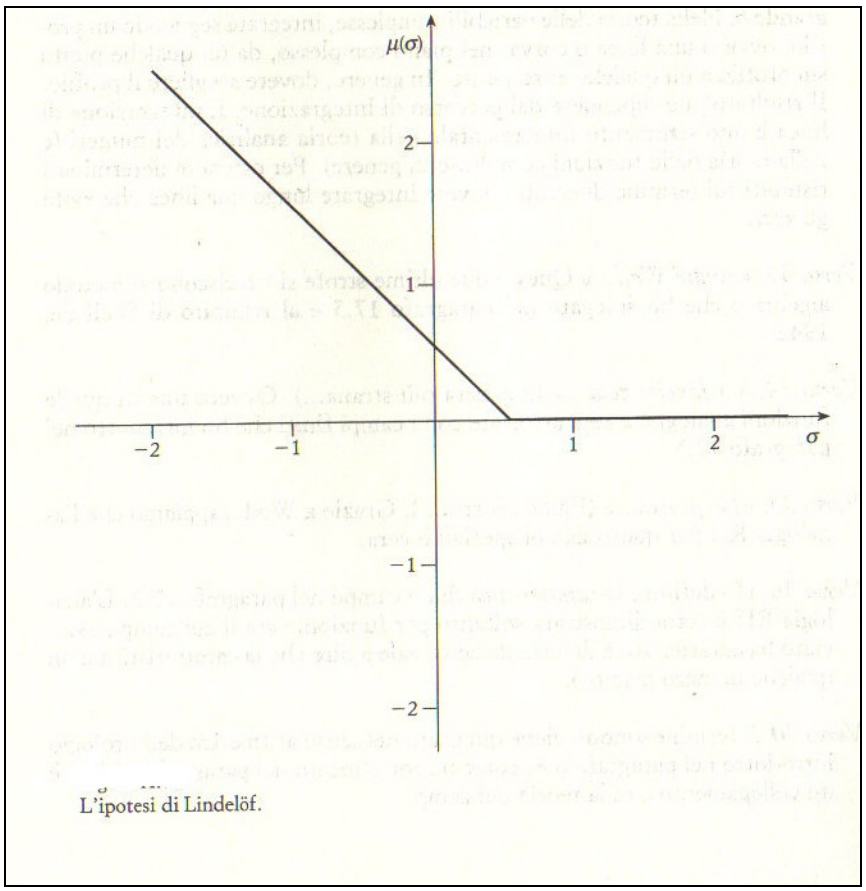


Figura 20 – Ipotesi di Lindelhof

Dalla figura 20 si vede che:

- per $\sigma=1/2$, $\mu(1/2)=0$ da cui discende che: $\mu(\sigma)=1/2-\sigma$ provenendo da $-\infty$ a $\sigma=1/2$ e $\mu(\sigma)=0$ per $\sigma>1/2$.

In realtà finora non si conoscono valori di $\mu(\sigma)$ nella striscia critica. *Anche la LH è una grossa sfida, alla pari di RH*. Se la RH è vera automaticamente lo è anche la LH, ma non è vero il contrario; difatti la LH è una congettura più debole della RH.

Generalized Riemann Hypotesis (GRH)

E' possibile far riferimento alle **L-funzioni** generali, che sono formalmente simili alla funzione zeta. In generale le *L-function* possono essere associate a curve ellittiche, alla teoria dei campi (in questo caso si parla di *Dedekind L-function*); inoltre ve ne sono altre come le *Dirichlet L-function*.

Le Dedekind L-function sono di interesse della ERH Extended Riemann Hypotesis), che non esamineremo poiché coinvolge la teoria dei campi; mentre le Dirichlet L-function afferiscono alla GRH.

La GRH fu formulata da Piltz nel 1884 ed ha legami e conseguenze sui numeri primi.

Formalmente una "*caratteristica di tipo Dirichlet*" è una funzione aritmetica moltiplicativa χ tale che esiste un intero k positivo con $\chi(n + k) = \chi(n)$ per tutti gli n; mentre è $\chi(n)=0$ se il MCD(n,k)>1.

Da dove discende e cosa significa tutta questa definizione? E' nient'altro che la generalizzazione formale di quello che *Dirichlet* aveva trovato.


L. Dirichlet, 1805-1859

Analizziamo quello detto sopra: $\chi(n)=0$ se il MCD(n,k)>1. Quindi per avere una caratteristica di tipo Dirichlet dobbiamo innanzitutto considerare un n e un k che non abbiamo fattori in comune (sono coprimi) ovvero tali che il MCD(n,k)=1.

Ad esempio prendiamo k=6 e n=15. Hanno almeno un fattore comune, il 3 e significa che MCD(6,15)=3>1.

Se adesso sommiamo sempre k a n che otteniamo?

15, 21, 27, 33, 39, 45, 51, 57, …

In questo caso è proprio difficile ottenere nella successione di numeri generata un numero primo.

Guardiamo che succede se n e k non hanno fattori in comune, ad esempio prendiamo k=6 e n=35 cioè tali che MCD(n,k)=1. In tal caso nella successione si ottengono numeri primi:

35, 41, 47, 53, 59, 65, 71, …

La successione o progressione numerica, inoltre, può contenere una infinità di numeri primi, al tendere di n all'infinito. Una cosa ulteriormente interessante è la seguente.

Consideriamo un numero qualsiasi, ad esempio il 9. Tutti i numeri inferiori di 9 e che non hanno fattori in comune con esso sono: 1, 2, 4, 5, 7, 8
Se ad ognuno di essi aggiungiamo 9 si ottengono sei progressioni numeriche, di cui sottolineando i numeri primi:

1: 10, 19, 28, 37, 46, 55, 64, 73, 82, 91, 100, 109, 118, 127 …
2: 11, 20, 29, 38, 47, 56, 65, 74, 83, 92, 101, 110, 119, 128 …
4: 13, 22, 31, 40, 49, 58, 67, 76, 85, 94, 103, 112, 121, 130 …
5: 14, 23, 32, 41, 50, 59, 68, 77, 86, 95, 104, 113, 122, 131 …
7: 16, 25, 34, 43, 52, 61, 70, 79, 88, 97, 106, 115, 124, 133 …
8: 17, 26, 35, 44, 53, 62, 71, 80, 89, 98, 107, 116, 125, 134 …

Ogni successione contiene infiniti numeri primi e sempre nella stessa proporzione.
Supponiamo N = 134. Ora ognuna delle 6 successioni quanti numeri primi contiene?
Per il TNP ognuna ne contiene:

$$1/6 * (N/ \ln N) = 4,\ 55983336\ldots$$

E se ci fate caso effettivamente il valore calcolato si avvicina molto a quello del numero dei primi sottolineato in ogni successione: 5, 5, 4, 5, 4, 5. Con un errore del 2,3%.

Ritornando alla teoria, possiamo ora definire una Dirichlet L-function.

Sia per ogni s complesso con parte reale >1:

$$L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \quad (82)$$

Ora per continuazione analitica essa si può estendere ad una funzione meromorfica definita in tutto il piano complesso. *La GRH afferma che ogni caratteristica di Dirichlet χ ed ogni numero complesso s per il quale $L(\chi,s)=0$, se la parte reale di s è tra 0 e 1, allora essa è ½.*

Il caso $\chi(n)=1$ è la RH.

Conseguenze della GRH

Siano *a* e *d* due numeri coprimi; chiamiamo con π(x,a,d) il numero di numeri primi in una progressione numerica (una successione) generata con a e d e tale che la progressione sia minore di x, allora *se la GRH è vera* si ottiene che:

$$\pi(x, a, d) = \frac{1}{\varphi(d)} \int_2^x \frac{1}{\ln t} dt + O(x^{\frac{1}{2}+\varepsilon}), \quad x \to \infty \quad (83)$$

dove *φ(d) è la funzione totiente di Eulero* e l'integrale è Li (Logaritmo integrale).

Se la GRH è vera seguono varie cose, alcune delle quali sono:

- la congettura debole di Goldbach è vera
- l'algoritmo di *Shank-Tonelli* termina in un tempo polinomiale
- il test di primalità Miller-Rabin termina in un tempo polinomiale

Capitolo 8. Teoria dei campi, degli operatori e legge di Montgomery-Odlyzko

La teoria dei campi è stata ed è, forse, uno dei settori maggiormente promettenti della matematica circa l'attacco all'ipotesi di Riemann. Ma è anche uno dei più complessi da studiare, comprendere e specialmente spiegare o divulgare.

E' un settore che va dall'ambito delle funzioni, a permutazioni, anelli, gruppi, sottogruppi, numeri p-adici, operatori di Riemann, curve ellittiche fino alla crittografia. Per spiegare il tutto in maniera rigorosa, ammesso di averne tutta la necessaria competenza, solo per cercare di coprire tutti gli argomenti principali con esempi, occorrerebbero migliaie di pagine. Un campo usato, ad esempio, da Andrew Wiles per la dimostrazione dell'Ultimo Teorema di Fermat.

Cercheremo solo di farvi comprendere la loro importanza, ma per approfondimenti ulteriori dovrete leggere testi più "voluminosi".

Il termine "campo" ha un significato che abbiamo già incontrato, quando abbiamo dimostrato la necessità di introdurre i numeri complessi.

Un insieme di elementi è un campo se tutte le operazioni di addizione, sottrazione, moltiplicazione, divisione fatti su essi producono un risultato contenuto nell'insieme.

Ad esempio **N** non è un campo né rispetto alla sottrazione che alla divisione. **Z** non è un campo rispetto alla divisione. **Q** è un campo per certe divisioni (risultato razionale) ma non lo è per altre (risultato irrazionale).

R è un campo e lo è anche **C**. Q è campo solo per certe divisioni. I tre campi Q, R e C sono un esempio di *campi infiniti,* perché hanno infiniti elementi.

Sappiamo costruire altri campi infiniti? E' semplice, ad esempio con:

$$a + b\sqrt{2}$$

con a, b $\in$ Q. Se b$\neq$0, allora $a+b\sqrt{2}$ non è razionale. Se b=0, allora $a+b\sqrt{2}$ è razionale. In altri termini il campo include sia razionali che irrazionali particolari e poiché a e b possono assumere infiniti valori, il campo ottenibile è un campo infinito. Tutte e quattro le operazioni in ogni caso danno un risultato appartenente al campo.

Sembrerebbe che tutti i campi siano infiniti. In realtà esistono anche i *campi finiti*.

Prendiamo un insieme con due soli elementi: 0 e 1. Ora su 0 e 1 possiamo definire tutte le operazioni:

Addizione
0+0=0, 0+1=1, 1+0=1, 1+1=0 (ho solo due elementi per cui 1+1=0!)
Sottrazione
0-0=0, 0-1=1 (stesso motivo di prima), 1-1=0, 1-0=1
Moltiplicazione
0x0=0, 0x1=0, 1x0=0, 1x1=1
Divisione
Si esclude la divisione per 0.
0:1=0 1:1=1

Un campo con due soli elementi viene chiamato F_2.

Si possono creare campi finiti per un qualsiasi numero primo e anche per potenze di numeri primi. In altri termini se p è un numero primo esiste un campo finito con p elementi; un campo finito con p^2 elementi, uno con p^3 elementi etc. Se ad esempio p=2 i campi verranno chiamati F2, F4, F8 etc e sono tutti i campi finiti possibili che esistono.

L'aritmetica del modulo però funziona bene solo con i campi finiti con numero primo di elementi, perché il campo finito in tal caso è anche un anello e viceversa (anello che effettivamente si comporta come un orologio che ritorna sui valori precedenti). Altrimenti non è un campo! Ricordate la definizione di campo e facciamo un esempio.

Se considero N=4: numero non primo, siamo di fronte ad un anello **Z/4Z** con elementi finiti 0,1,2,3 ma non è un campo; perchè non possiamo ad esempio fare la divisione per 2 degli elementi 1 oppure 3. Per convincervi basta pensare che se potessi fare la divisione ½ = x allora significherebbe che esiste un x tale che 1 = 2 x, il che è assurdo!

In un anello si può solitamente sommare, sottrarre, moltiplicare ma non necessariamente dividere. Vale l'aritmetica modulo ma non è un campo, per cui non va indicato F4: è un errore!

Vediamo la tabella che ne esce fuori con l'aritmetica del modulo applicata all'anello Z/4Z.

+	0	1	2	3
0	0	2	3	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Tabella 10 - Anello Z/4Z

L'aritmetica sottostante i campi con numero di elementi potenza di un numero primo è diversa: è un po' più complessa ed in questa sede non la mostriamo, ma consigliamo di approfondirla a parte.

Ogni campo finito o infinito ha una *caratteristica*. La caratteristica *rappresenta il numero di volte che occorre sommare uno a sé stesso per ottenere zero.*

Per F2 la caratteristica è 2.

Ci sono campi come Q, R, C che sommando 1 non otteniamo mai 0, allora si dice che hanno *caratteristica zero*. In generale ogni campo ha caratteristica 0 oppure p (numero primo).

Con Q, R e C abbiamo anche un esempio di campi infiniti con caratteristica zero.

Gli elementi di un campo devono essere per forza numeri? No, possono essere oggetti matematici qualsiasi definiti in algebra.

Prendiamo l'insieme di tutti i polinomi $ax^n + bx^{n-1} + cx^{n-2} + ...$ con a, b, c etc numeri interi; ora creiamo delle *funzioni razionali* (divisione di due polinomi): anche questo è un campo, perchè ammette tutte e quattro le operazioni il cui risultato è nel campo. Tale campo ha infiniti elementi.

Possiamo anche generalizzare ulteriormente. Per i coefficienti del polinomio leviamo il vincolo che siano numeri interi e pensiamoli come gli elementi di un campo finito F2 di caratteristica 2 (gli elementi 0 e 1). Ora il campo che abbiamo creato si dice: "*campo delle funzioni razionali su F2*". Abbiamo un campo infinito con caratteristica finita.

Come usare la teoria dei campi con l'ipotesi di Riemann? Non è semplice, però vi illustreremo l'idea.

Emil Artin, nel 1921, mostrò che è possibile, partendo da un campo finito, costruire un campo estensione a cui potervi associare una funzione zeta, cioè di argomento complesso. Nello studio di tali funzioni si sono trovate strette somiglianze alla zeta di Riemann ed anche qui valgono i prodotti di Eulero, le ipotesi di Riemann e analoghe formule.

Weil successivamente estese ancora di più il risultato ad una classe più ampia di oggetti.

Attualmente è una parte della matematica che potrebbe dare risultati interessanti, ma porta con sé soprattutto complessità e astrattezza.

La *teoria degli operatori* è un particolare settore dell'algebra. In essa si utilizzano i concetti di *matrici, polinomio caratteristico*, *traccia*, *autovalori* e *autovettori.*

Le matrici nel seguito la daremo come conoscenza scontata per motivi anche di spazio.

In generale nella teoria degli operatori interessano matrici quadrate N x N come:

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

Quella di sopra è una matrice $M_{2x2.}$ I termini a11, a12, a21, a22 possono essere di qualsiasi tipo: interi, reali, razionali, irrazionali e complessi. Nel seguito per semplicità li consideriamo interi:

$$\begin{pmatrix} 5 & 1 \\ 2 & 6 \end{pmatrix}$$

Come si trova la traccia? La *traccia è costituita dalla somma dei termini sulla diagonale a11+a22*. Nell'esempio vale 11.

Lo stesso valore deve corrispondere anche alla somma degli autovalori del polinomio caratteristico.

Il *polinomio caratteristico* dell'esempio è $x^2 - 11x + 28$. Il 28 lo ricaviamo come 5*6-2*1=28.

Gli *autovalori sono le radici dell'equazione associata al polinomio*. In realtà dovrebbero essere quelle la cui somma dà 11 e il cui prodotto dà 28, per cui gli autovalori sono 4 e 7 (4+7=11 corrisponde alla traccia).

Ovviamente la cosa si deve estendere anche a matrici quadrate di dimensioni maggior di 2x2, dove diventa un po' più lungo il procedimento, ma non difficile, di ricerca del polinomio caratteristico e degli autovalori (siamo certi che approfondirete a parte questo argomento).

Tali matrici sono usate per rappresentare gli *operatori*. In realtà più matrici quadrate possono afferire allo stesso operatore, perché possono avere lo stesso polinomio caratteristico, la stessa traccia e gli stessi autovalori.

La sorpresa però proviene dalla matrici *hermitiane*, cioè quelle matrici che presentano tutti gli elementi come numeri complessi e caratterizzati dal fatto che se l'elemento a_{mn}=a+ib allora l'elemento a_{nm}=a-ib. Mentre sulla diagonale principale a11, a22 etc sono tutti interi proprio perché a+ib=a-ib per cui b=0.

Esiste un *Teorema che dice: "Tutti gli autovalori di una matrice hermitiana sono reali*".

Come conseguenza *anche i coefficienti del polinomio caratteristico di una matrice hermitiana sono reali*. Questo perché essendo gli autovalori zeri del polinomio caratteristico associato alla matrice hermitiane, allora possiamo sfruttare gli zeri per scomporre il polinomio in (x-a)(x-b)(x-c)… Ora se a,b,c secondo il Teorema sono reali allora le moltiplicazioni dei termini tra parentesi ci portano a coefficienti reali.

Qual è ora il legame con la zeta di Riemann?

Il ragionamento è il seguente: da una parte abbiamo delle matrice hermitiane con numeri complessi, i cui autovalori o zeri del polinomio caratteristico sono reali.

Dall'altra abbiamo la zeta di Riemann, rappresentata da numeri complessi e legata agli zeri non banali. Gli zeri sono simmetrici rispetto alla retta critica e la parte reale degli zeri non banali è ½; per cui l'ipotesi di Riemann porta al fatto che la parte immaginaria degli zeri è reale.

Da qui nasce la *congettura di Hilbert-Polya*:"Gli zeri non banali della funzione zeta di Riemann corrispondono agli autovalori di un operatore hermitiano".

Fisica nucleare, Meccanica Quantistica e zeri non banali della zeta di Riemann

Che c'entra Riemann con la Meccanica Quantistica? Ne daremo solo un cenno. Occorre anche dire che Riemann era anche un fisico (fisico e matematico erano due mestieri connessi), anzi molti suoi lavori erano proprio rivolti alla Fisica.

In Meccanica Quantistica si studia il comportamento dell'atomo e dei livelli di energia in gioco; ad esempio ci si pongono domande del tipo: che succede se un atomo passa da un livello di energia ad un altro? Come sono spaziati i livelli di energia? Perché sono spaziati in quel modo? Si studiano però *sistemi dinamici* cioè insiemi di particelle che sono dotate in un certo istante di posizione, velocità, direzione, verso etc.

Eugen Wigner e *Freeman Dyson*, dimostrarono che dietro a questi concetti di fisica ci sono degli oggetti matematici rappresentati dalle *matrici casuali*.

Abbiamo già visto prima cosa sono le matrici hermitiane. Ora supponiamo che i *valori* di tali matrici hermitiane *siano causal*i. Ma la casualità come è intesa? Secondo una legge *gaussiana* (la famosa curva a campana)! Difatti, ma non lo dimostreremo (vi invitiamo a leggere qualche libro di statistica e di probabilità), se scegliessimo a caso una serie di valori reali per comporre i numeri appartenenti alla matrice, da una gaussiana disegnata su carta millimetrata con migliaia di quadratini, rispettando la regola di ottenere una matrice hermitiana, con buona probabilità la maggior parte di essi sarebbero sotto la campana e in quantità minore ai lati.

Scegliendo a caso i quadratini, il loro valore reale potrebbe essere rappresentato dalla sua distanza dalla linea centrale del picco della gaussiana. A questo punto si avrà a che fare con una *matrice hermitiana gaussiana* (GUE).

La legge di Montgomery-Odlyzko

Montgomery studiò la spaziatura degli zeri non banali della zeta di Riemann, argomento molto connesso alla teoria dei campi numerici del tipo $a+b\sqrt{2}$.

Durante questo studio giunse alla conclusione che *la distribuzione degli zeri era legata all'integrale seguente*:

$$\int\left[1-\left(\frac{\sin \pi u}{\pi u}\right)^2\right]du$$

Montgomery, scoprì, con l'intervento Dyson che l'integrale corrispondeva col *fattore di forma per la correlazione di coppia degli autovalori delle matrici casuali hermitiane* [17, 18, 19].

Purtroppo Montgomery non aveva gli strumenti per dimostrarla. A causa della divisione delle materie, provocate da una giusta specializzazione, questo per anni è stato un difetto difficilmente superabile: gli specialisti non avendo entrambe le specializzazioni non riuscivano a correlare i diversi argomenti. Oggi si preferisce creare team con persone aventi specializzazioni diverse e si sono promossi ambiziosi programmi come il *Langlands*.

Odlyzko sfruttò l'idea di Montgomery giungendo ad una congettura. Vediamo il ragionamento.

Con Montgomery si era accertato che gli zeri non banali della zeta seguono una legge statistica come visto prima (la distribuzione e il fattore di forma …).

La stessa legge era presente anche nello studio dei sistemi dinamici conformi agli operatori GUE (cioè dietro ai quali ci sono le matrici hermitiane gaussiane).

Mentre i sistemi dinamici e le matrici GUE erano stati studiati moltissimo, gli zeri banali, sotto questo aspetto all'epoca, molto meno. Per cui Odlyzko con un potente computer (il Cray) analizzò 100 mila zeri non banali della funzione zeta di Riemann, con accuratezza fino a 8 cifre decimali, con la formula Riemann-Siegel.

In base a questa analisi enunciò la seguente *Legge di Montgomery-Odlyzko: La distribuzione delle spaziature tra zeri non banali successivi della funzione zeta di Riemann (normalizzata) è identica, dal punto di vista statistico, alla distribuzione delle spaziature degli autovalori in un operatore GUE.*

Spieghiamo la tecnica usata da Odlyzko. A cosa gli serviva la normalizzazione? Il problema era che gli zeri con parte reale ½, salendo sulla retta critica variavano la parte immaginaria T (l'altezza) e risultavano sempre più ravvicinati in media. Per vederli meglio occorreva espandere in qualche modo la loro distanza. Un modo semplice era di moltiplicare T per log T . Se T aumenta, aumenta anche log T . Si ottiene, quindi, una normalizzazione semplice e ammissibile perché lo stiamo facendo su tutti gli zeri non banali.

Ad esempio prendiamo una successione di zeri tra 90mila-esimo e il 100mila-esimo. I numeri complessi associati sono al 90mila-esimo: ½ + 68194,3528i; mentre al 100mila-esimo: ½ + 749208275i.

Se normalizzo con il log T e considerando solo la parte immaginaria, otteniamo, invece, che la successione parte da: 759011,1279 e termina a 840925,3931.

Visto che si è interessati alla distribuzione dei valori della successione, anzicché lavorare con grandi valori, possiamo interessarci solo alla loro distanza relativa (non ci interessa la loro posizione assoluta). Per cui adesso, se sottraggo il primo valore ad ogni valore della successione, la nuova successione diventa va da 0 a 81914,2653.

Ultimo step è quello di passare ad una scala dimensionale diversa. Ridurre la scala non mi altera la spaziature. Divido per il numero di zeri a disposizione: 10mila, allora adesso la successione va da 0 a 8,19142653.

A questo punto Odlyzko aveva 10mila valori tra 0 e 9 e poteva studiarseli statisticamente: con la distribuzione di Poisson, con lo scostamento dalla media, etc.

Gli zeri non sono spaziati a caso ma sono concentrati maggiormente intorno alla spaziatura media (poco superiore a 1). Alla fine riportando su un istogramma le spaziature comprese tra 0 e 0,1, tra 0,1 e 0,2, tra 0,2 e 0,3 etc si arriva ad approssimare l'istogramma con una curva a campana, sbilanciata più a sinistra.

L'equazione che dà luogo ad una curva a campana, ipotizzata da Eugene Wigner per le spaziature per un operatore GUE, è simile alla seguente:

$$y = \frac{(320000)}{\pi^2} x^2 e^{-\frac{4x^2}{\pi}}.$$

La conclusione è che i numeri primi e gli zeri non banali della zeta di Riemann sono legati agli autovalori di una matrice GUE che rappresentano anche i sistemi dinamici delle particelle subatomiche!

Il caos e i sistemi caotici classici

Se si fa passare un atomo attraverso un forte campo elettromagnetico, ed è proprio questo un sistema dinamico modellabile con un operatore GUE, si ottiene che gli elettroni passano a livelli energetici alti tali da portare l'atomo ad un comportamento caotico: un sistema caotico quantistico!

A questo punto *Michael Berry* ipotizzò che se esiste un operatore di Riemann esso allora modella un sistema caotico e i suoi autovalori, le parti immaginarie degli zeri non banali della funzione zeta, sono i livelli energetici di quel sistema.

Campo p-adico e spazio adelico

Alain Connes, anzicchè cercare un operatore del genere di cui sopra, lo ha costruito su *spazi bidimensionali*. E qui arriviamo ad una parte matematica piuttosto complessa che introduce innanzitutto il *campo dei numeri p-adici* $\mathbf{Q_p}$ fino agli *spazi adelici*.

I numeri p-adici del tipo $a + b\sqrt{2}$ li avevamo già introdotti. Un campo di numeri p-adici è detto ***campo*** $\boldsymbol{Q_p}$ e serve per estendere Q e completarlo (in modo abbastanza complicato). Uno spazio adelico contiene tutti i campi Qp e l'operatore di Riemann di Alain Connes è in uno spazio adelico.

La RH a questo punto si dovrebbe ridurre (come se fosse facile!) a dimostrare una formula della traccia, che mette in relazione gli autovalori di un operatore nello spazio adelico di Connes con le orbite periodiche di un sistema dinamico classico.

Il metodo però non ha dato indizi se esistono zeri fuori della retta critica!

Capitolo 9. Sottoproblemi della RH

Congettura di Cramer

La congettura di Cramer è legata alla non ancora provata congettura per cui è:

$$\textbf{lim sup}_{\,n\to\infty} \quad (p_{n+1} - p_n) / (\ln p_n)^2 \quad = \quad 1 \qquad (84)$$

dove p_n è l'ennesimo numero primo. La (84) porta anche alla formula di Cramer – Shanks (*Cramer Shanks ratio*), che afferma che R(p) non deve superare il valore di 1 affinché la congettura di Cramer sia vera. Nella (84) il simbolo "ln" va inteso come logaritmo naturale (neperiano).

Ricordiamo che se indichiamo con p_n l'ennesimo numero primo e con pn+1 il numero primo successivo, allora possiamo definire il gap *g(p) sia come il numero di composti + 1 esistenti tra p_n e p_{n+1}, sia come la funzione $d_k = p_{n+1} - p_n$. In altri termini se g è il gap allora g-1 sono i composti nel gap.*

In pratica tale gap è sempre un numero pari (eccetto per $p_1=2$), da Goldbach.

Esempio: 7-5=2, 29-23=6. Eccezione: 3-2=1.

Un gap G si dice poi gap massimale se i precedenti gap erano minori.

Da nostri calcoli risulta che Rp è minore o uguale a 0,5 per soli sei valori di gap (5, 7, 17, 19, 21 e 35); per valori maggiori di gap tale rapporto cresce in media lentamente, fino ad un massimo di 0,92063 per il gap 1132 tra i numeri primi:

1 693 182 318 746 370 e 1 693 182 318 746 370 + 1132;

per i tre valori di gap successivi 1184, 1198 e 1220 rispettivamente dopo i numeri primi:

a) 43 841 547 845 541 059 e tale numero + 1184
b) 55 350 776 431 903 243 e tale numero + 1198
c) 80 873 624 627 234 849 e tale numero + 1220

i rispettivi valori di R(p) sono:

$R(a) = 1184/(\ln a)^2 = 1184/1468{,}37 = 0{,}8063 < 1$
$R(b) = 1198/(\ln b)^2 = 1198/1486{,}29 = 0{,}8060 < 1$
$R(c) = 1220/(\ln c)^2 = 1220/1\,515{,}67 = 0{,}8049 < 1$

Fin qui la congettura è vera. Il rapporto medio cresce lentamente al crescere dei valori dei gap e, fino al gap 381, il valore medio di R(p) è 0,575. Una lista di valori di gap noti e ancora più grandi di 381 è data dai siti:

http://mathworld.wolfram.com/CramerConjecture.htlm
http://www.maa.org/editorial/mathgames_01_25_04.html

Nel secondo link proposto, però, i valori di gap sono rappresentati con una unità in più rispetto ad altre liste; per es. 381 viene indicato con 382. Nel seguito mostriamo il tutto nella Tabella 11, aggiungendo per ogni gap il relativo R(p).

Gap	Numero primo p_n	$(\ln p)^2$	R(p)
…			
382	10 726 904 659	533,42	0,71
384	20 678 048 297	564,17	0,68
394	22 367 084 959	567,90	0,69
456	25 056 082 087	573,33	0,79
464	42 652 618 343	599,09	0,77
466	127 976 334 671	654,08	0,77
474	182 226 896 239	672,28	0,70
486	241 160 624 143	686,89	0,70
490	297 501 075 799	697,94	0,70
500	303 371 455 241	698,97	0,71
514	304 599 508 537	699,19	0,73
516	416 608 695 821	715,85	0,72
532	461 690 510 011	721,36	0,73
534	614 487 453 523	736,79	0,72
540	738 832 927 927	746,83	0,72
582	1 346 294 310 749	779,99	0,74
588	1 408 695 493 609	782,52	0,75
602	1 968 188 556 461	801,35	0,75
652	2 614 941 710 599	817,51	0,79
674	7 177 162 611 713	876,27	0,76
716	13 829 048 559 701	915,53	0,78
766	19 581 334 192 423	936,70	0,81
778	42 842 283 925 351	985,24	0,78
804	90 874 329 411 493	1033,01	0,77
806	171 231 342 420 521	1074,13	0,75
906	218 209 405 436 543	1090,08	0,83
916	1 189 459 969 825 483	1204,94	0,76
924	1 686 994 940 955 803	1229,32	0,75
1132	1 693 182 318 746 371	1229,58	0,92
1184	43 841 547 845 541 059	1468,37	0,80
1198	55 350 776 431 903 243	1486,29	0,80
1220	80 873 624 627 234 849	1515,67	0,80

Tabella 11 – Gap e Rp

Osservazioni su R(p)

La media aritmetica dei valori di R(p) va crescendo lentamente, infatti per gli ultimi 10 valori è di 7,96/19 = 0,796 ≈ 0,80, mentre per i primi 10 valori di questa tabella è 7,22/10 = 0,722; mentre fino al valore di gap 382 la media è 0,575; quindi essa aumenta lentamente ma non sembra ancora tendere ad un numero preciso come limite massimo minore di 1. La tabella suggerisce anche un modo per individuare il successivo numero primo p_{n+1}.

Ad esempio preso il numero primo p_n: 1693182318746371, per esso si ha.

$$p_n + (\ln p_n)^2 = 1693182318746371 + 1229.58$$

E in effetti il successivo primo p_{n+1} è

1693182318747503 = 1693182318746371 + 1132

Per esso è:

$$R(p) = [\ p_{n+1} - p_n\ ] / (\ln p_n)^2 = 1132 / 1229.58 = 0.92086$$

abbastanza prossimo al valore 1.

Se si trovasse un contro-esempio per cui R(p)>1 la congettura di Cramer verrebbe in pratica smentita. Ma questo ce lo possono dire, eventualmente, ulteriori valori per gap ancora sconosciuti e più grandi. In tal caso occorrerebbe cercare, anche in modalità informatica (qui per una volta il "guiness dei primati" potrebbe dare una indicazione utile!), partendo dai gap già noti (es. 1220 o superiori), dei <u>contro-esempi</u>, che se esistessero, dovrebbero essere tali che:

$$R(p) > 1 \Rightarrow p_{n+1} - p_n > (\ln p_n)^2$$

Ma esiste un gap per cui è vera questa diseguaglianza?

La difficoltà sta soprattutto nel fatto che R(p) dipende da due cose:

- gap
- il numero primo più piccolo del gap

E' evidente che per trovare dei controesempi, il gap dovrebbe crescere molto di più del quadrato del logaritmo del numero primo inferiore del gap. Nella Tabella 11 fino al gap 1220 ciò non avviene, anzi avviene il contrario R(p)<1.

L'alternativa alla ricerca dei contro-esempi è una dimostrazione; anche attraverso un teorema correlato (esempio la RH) che evidenzi tale possibilità o tale impossibilità. Finora è stato vano anche questo tentativo.

Congettura di Cramer come sottoproblema della RH

La congettura di Cramer è anche un sottoproblema della RH poiché, secondo lo stesso Cramer, se l'ipotesi di Riemann è vera, allora avremo il più debole risultato:

$$g(p) < k \sqrt{p} \log p \qquad (85)$$

Se ponessimo k = 1, avremmo la seguente Tabella 12, che soddisfa la (85); in realtà la (85) è soddisfatta anche con valori di k>1 e k<1. Per k<1, si potrebbe avere qualche problema, anche se è ammissibile, come vedremo nel seguito quando introdurremo la funzione O grande.

g(p)	√p	ln p	√p* ln p = d > g(p)	d/g(p)
0	1,41	0,69	0,97	-
1	1,73	1,09	2,58	2,58
3	2,64	1,94	5,12	1,70
5	4,79	3,13	14,99	2,99
7	9,43	4,48	42,24	6,03
13	10,63	4,72	50,17	3,85
17	22,86	6,25	142,87	8,40
19	29,78	6,78	201,90	10,62
21	33,60	7,02	235,87	11,23
…	…	…	…	…
381	32752,01	23,09	756243,91	1984,89
…	…	…	…	…

Tabella 12 – Andamenti di g(p)

Se k = 1 è il valore minimo considerabile, allora la RH è vera in base alla (85), anche se non è questa una dimostrazione rigorosa.

Il termine evidenziato nella parte destra della (85), ricordando quanto visto con il risultato di **Von Kock** del 1901 è possibile riscriverla in:

$$g(p) = O(\sqrt{p} \log p) \qquad (86)$$

La (85) può anche essere vista in un altro modo:

$$g(p)/d < k$$

Tale rapporto è sempre soddisfatto per $k \geq 1$, mentre per k<1 occorre che anche il termine d faccia la sua parte.

Tenendo conto che log x cresce più lentamente di una qualunque potenza positiva di x, anche la più piccola ad esempio ε piccolo a piacere, allora è possibile dire, per i ragionamenti precedenti della O grande, che è vera la seguente espressione:

$$\log x = O(x^{\varepsilon})$$

per cui la (86) potrebbe diventare la (87) con vari passaggi:

$$g(p) = O(\sqrt{p}\, p^{\varepsilon})$$

$$g(p) = O(p^{1/2+\varepsilon}) \qquad (87)$$

Il termine d'errore $O(\sqrt{p} \log p)$ implica il termine d'errore $O(p^{1/2+\varepsilon})$ ma non è vero il viceversa. Infatti i due risultati non sono del tutto equivalenti: sebbene log x cresce più rapidamente di qualsiasi potenza di x, questo è anche vero per $(\log x)^N$, con N positivo. In altri termini la (87) sarebbe vera lo stesso anche se il termine d'errore nella (86) fosse stato del tipo $O(\sqrt{p}\, (\log p)^N)$ con N qualsiasi valore positivo. *La (87) quindi è una forma debole della (86)*. Se fossimo in grado di dimostrare rigorosamente la (87) con un ε piccolo a piacere (o nullo) ovvero tale che:

$$\mathbf{g(p) = O(p^{1/2})}$$

avremmo dimostrato anche la RH! Ma non è semplice.

Considerazioni sul termine d'errore

Sarebbe possibile considerare che:

$$p_{n+1} = p_n + (\ln pn)^2 \qquad (88)$$

Se nella (88) consideriamo il $(\ln pn)^2$ come termine di errore, confrontato con la (86) si vede che si tenta di approssimare la radice quadrato col log. Tuttavia, in termini di O grande, questo significa abbassare il limite superiore (vedi figura 21); il che comunque non porta ad escludere a priori che esistano o no valori di primi e gap controesempi, cioè che cadono al di sopra del $(\ln pn)^2$.

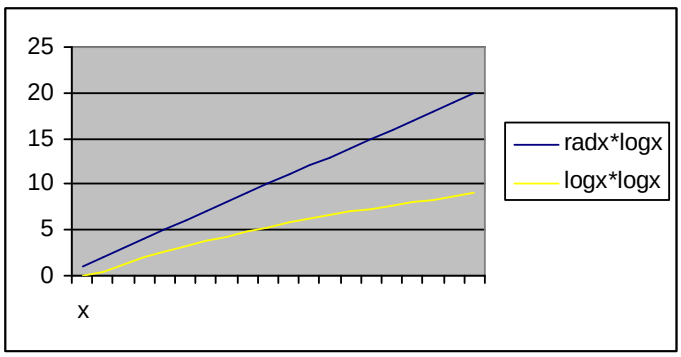


Figura 21 – radx*logx vs logx*logx

Ci poniamo anche la seguente domanda: è necessario che il tutto sia legato all'ipotesi di Riemann? In realtà no. Basta pensare all'interpretazione probabilistica di Denjoy già vista precedentemente.

Tecniche informatiche per i gap massimali

Finora non è stata approntata nessuna tecnica efficace per individuare un gap massimale ed il numero primo di partenza, tranne che esaminare tutti i primi e tracciarne la differenza, il gap e R(p). E' chiaro che in tal modo si perdono molte settimane solo per vedere un gap soddisfacente. L'idea semplice per evitare la scansione brutale dei primi è basarsi su un numero primo molto grande da cui partire, ad esempio con l'aiuto magari delle formule di Mersenne, o partire al contrario da un gap corrispondente agli intervalli rarefatti individuabili con dei fattoriali, ad esempio tra n! +1 a n!+n. Tale tecnica ha però il seguente vantaggio e difetto: da una parte si accelera, dall'altra poiché non si sa quando R(p) possa aumentare (la sua dipendenza non è matematicamente così ovvia perché dipende dal gap e contemporaneamente dall'estremo inferiore del gap) e potremmo perderci qualche valore interessante.

Secondo un risultato mostrato da Cramer, Shanks ha congetturato che il maximal gap di magnitudo (=dimensione) M si ha intorno a $e^{\sqrt{M}}$. Riesel misurò la verità di questa congettura con $R = \ln(p_{k+1}) / \sqrt{M}$ (attenzione: non è R(p)), R che ci si aspetta che vada ad 1 appena crescono M e p_{k+1}.

A questo punto si può fare una stima per avvicinarsi al gap desiderato. Se si conoscono i valori di R in forma tabellare o R viene calcolato dalle tabelle precedenti si può fare l'ipotesi interessante che il maximal gap da cercare è all'incirca a $e^{R\sqrt{M}}$.

Ad esempio se nell'intervallo fino a 1220 calcoliamo R = 1,12 dalle tabelle precedenti, allora la prima occorrenza di gap di 4000 o più potrebbe stare su $e^{1,13\sqrt{4000}} \approx 1,912 * 10^{31}$. Forza accendete PARI e cercate!!!

Capitolo 10. Osservazioni, calcoli e disquisizioni

Questo capitolo è effettivamente una serie di appunti, disquisizioni e note. Uno zibaldone di idee e spunti da analizzare e, se validi, da far evolvere.

Accendiamo i motori

Esaminiamo due affermazioni:

1. per ogni n, tra n e 2n c'è almeno un numero primo.
2. tra n! +2 e n! + n non ci sono numeri primi.

L'affermazione 1. è detta Postulato di Bertrand, che la verificò nel 1845 per n fino a 3000000 e venne dimostrato da Chebyscev nel 1850. Il grande Erdös ne diede una dimostrazione assai elegante e semplice nel 1932.

La tecnica di Erdös può essere estesa per dimostrare che dato qualsiasi k esiste un N tale che, se n è maggiore di N, ci sono tra n e 2n almeno k primi (in vari lavori ed anche in questo il gruppo ERATOSTENE[5] mostra che ci sono almeno $k = \pi(2n) - \pi(n)$ primi, vedi formula (91)).

La 2. è ovvia:
n! + 2 è divisibile per 2,
n! + 3 è divisibile per 3,
……
n! + n, che è divisibile per n.

Pur essendo poco più di una banalità la 2. dà un'argomentazione fortissima a favore della non-casualità della successione dei primi. In una successione casuale esisteranno spazi lunghi quanto si vuole privi di un certo simbolo, ma non sapremo mai dove si trovano.

Nel caso dei numeri primi invece in parte lo sappiamo, e anche in due modi diversi: infatti, oltre che nel suddetto intervallo tra n! +2 ed n! + n, altri intervalli rarefatti (con pochissimi numeri primi o anche privi del tutto di numeri primi) si trovano in intervalli, per es. di 100 unità, privi di coppie di numeri primi gemelli: questo perché, per molti N = 12n, esclusi i valori negli intervalli rarefatti (ad es. 12!+12 multiplo di 12) l'ultima soluzione di Goldbach è proprio una coppia di gemelli (Vedi Teorema del gruppo ERATOSTENE e [11]).

E per una conseguenza di una soluzione positiva della congettura di Goldbach (gruppo ERATOSTENE), per i numeri pari N di forma N = 6n (e quindi anche N = 12n) ci sono molte più coppie di Goldbach (circa il doppio) rispetto ai numeri pari adiacenti N = 6n-2 ed N = 6n +2, essendo facilmente verificabile la relazione di Goldbach:

$$G(N - 2) + G(N + 2) \approx G(N) \quad (89)$$

dove $G(N \pm 2)$ è il numero delle coppie di primi p e q tali che $p + q = N \pm 2$, oppure $p + q = N$.

Quindi, essendo le coppie di Goldbach simmetriche alla semisomma $s = N/2$, una coppia di gemelli è la più vicina ad s, infatti è data da $p = s-1$ e $q = s + 1$, ed

[5] Il gruppo ERATOSTENE è un gruppo di Caltanissetta, fondato dal prof. Francesco Di Noto e a cui aderiscono il dott. Michele Nardelli, il prof. Giovanni Di Maria, la prof. Annarita Tulumello. Con tale gruppo, per taluni articoli, in diverse occasioni hanno collaborato anche l'ing Rosario Turco e la prof. Maria Colonnese.

essendoci più coppie di Goldbach per N = 12n, ne consegue che attorno ad s c'è un intervallo denso di numeri primi; e, viceversa, per numeri N = 12n $\pm$ 2 ci sono intervalli meno densi di numeri primi (o del tutto privi) intorno ad N/2, e tali intervalli possono essere anche maggiori di quelli tra n!+2 ed n! + n.

Questo spiega la formazione di altri intervalli più o meno densi di numeri primi, legati alla presenza o meno di coppie di gemelli al centro di tali intervalli.

Anche tutto ciò (Goldbach e gemelli) influisce in qualche modo sulla distribuzione non casuale dei numeri primi, al pari del Postulato di Bertrand e degli intervalli riguardanti i fattoriali.

Per fare un solo esempio, nell'intervallo di 100 unità tra 10000019 e 10000079 ci sono 60 unità senza alcun numero primo (e quindi anche senza coppie di numeri primi gemelli); mentre per il precedente intervallo, pure di 100 unità, tra 9 999 900 e 10000000, ci sono ben nove numeri primi, tra i quali ben due coppie di gemelli ravvicinate, causa prima di tale densità di numeri primi (vedi, tra l'altro, il nostro lavoro "Progressioni Aritmetiche di numeri primi PAP1, PAP2 e PAP dense e teoremi di Green, Tao e Goldston" sul sito del gruppo ERATOSTENE.

In altre parole la distribuzione delle coppie di numeri primi gemelli, regolata dalla formula:

$$g(N) \approx \frac{N}{(\ln N)^2} * 1,32032... \qquad (90)$$

dove 1,32032… è una costante, regola l'esistenza di intervalli numerici densi di numeri primi (dove ci sono coppie di gemelli ravvicinate) o rarefatti o privi di numeri primi (dove le coppie di gemelli sono più distanti tra loro rispetto alla loro frequenza media, circa $1/(\ln N)^2$).

Calcolo dei numeri primi tra n e 2n

Il postulato di Bertrand già l'abbiamo citato prima, è stato dimostrato Teorema da Chebyscev, e ci assicura che tra n e 2n c'è almeno un numero primo. Ma solo un numero primo? Quanti ve ne sono tra n e 2n?

Se dovessimo calcolare in modo approssimato? Formula di Gauss sui numeri primi e TNP ci suggeriscono:

$$k = \pi(2n) - \pi(n) \approx \frac{2n}{\ln(2n)} - \frac{n}{\ln n} \qquad (91)$$

Ci aspettiamo però che i valori che otterremo sono minori di quelli reale. Questo perché il calcolo con il logaritmo dà un valore per difetto rispetto a quello del Logaritmo integrale, per valori bassi di n.

Ad esempio, n = 100 e 2n = 200:

$k \approx 200/\ln(200) - 100/\ln(100) = 200/5{,}20 - 100/4{,}60 = 37{,}80 - 21{,}73 = 16{,}07$

in realtà da 100 a 200 ci sono 21 > 16,07 numeri primi.

Goldbach e Riemann

Una relazione tra la fattorizzazione dei semiprimi e la RH si può mostrare facilmente, tramite la RH1. La RH1 è connessa alla funzione $\sigma(n)$, la somma dei divisori di n.

Per un semiprimo $N=p*q$ è:

$$\sigma(N) = 1 + N + p + q \quad (92)$$

e contiene tutti i fattori propri e impropri di N.

Togliendo i fattori impropri banali, 1 ed N, rimangono solo p e q, la cui somma è un numero pari $S = p + q$.

Dai nostri lavori su Goldbach, sappiamo che tale numero S è minimo solo per i quadrati perfetti, ed equivale a $S = p + q = n + n = 2n$ solo se N è un quadrato perfetto, $N = n^2$.

Nei numeri N non quadrati perfetti, S è compreso tra 2n ed N – 3, e quindi $S = p + q$ dovremmo cercarlo tra tutti i numeri pari compresi in tale intervallo, costruire tutte le coppie di Goldbach per ognuno dei vari possibili numeri pari S, e infine tra queste trovare la coppia di Goldbach tale che $p + q = S$, e $p * q = N$.

Ecco perché tale ricerca è laboriosa e praticamente non conveniente, ed è molto meglio usare il metodo dei quadrati perfetti s^2 e d^2 (rispettivamente semisomma e semidifferenza tra i numeri primi p e q, tali che

$$\mathbf{p = s - d} \quad \text{e} \quad \mathbf{q = s + d,}$$

metodo tanto più veloce quanto più p e q sono vicini ad $n = \sqrt{N}$, e quindi anche S più vicina a 2n (sempre per una conseguenza della congettura di Goldbach: mentre la somma e la semisomma sono costanti, la differenza decresce e il prodotto cresce, a partire dalla prima coppia di Goldbach fino all'ultima, e tutte simmetriche rispetto a N/2 , cioè con p e q sempre equidistanti da N/2).

Un'altra relazione tra Goldbach, la RH1 e σ(n), è la somiglianza dei rispettivi grafici, e dei relativi contro esempi per quanto riguarda Goldbach (G(N) = 0) e la RH1 (L(n) $\leq$ 0). Ecco perché la congettura di Goldbach (Vedi [11]) potrebbe essere molto importante per la RH1, e quindi indirettamente anche la RH: si potrebbe aggirare la funzione moltiplicativa zeta di Riemann con la funzione additiva σ(n), come in questo caso, oltre che con le altre funzioni additive collegate alle altre ipotesi equivalenti alla RH.

Congettura per forme chiuse G(N) e g(N) – ipotesi equivalenti RH

In [9] si presenta un algoritmo nuovo per il calcolo di G(N), che rappresenta il numero di soluzioni della congettura di Goldbach.

In questa parte di lavoro ci si pone un'ulteriore domanda: Se la congettura di Goldbach è legata alla RH in generale, come visto nel paragrafo precedente, qual è l'equazione analitica in forma chiusa in gioco? Ne esiste una? In realtà sì.

Ci eravamo appuntati qualcosa … Ecco! Qualche scarabocchio passato, scritto da "Block Notes Matematico" ed ERATOSTENE, riportava:

"… Una *nostra congettura* è che:

$$\left|\frac{G(x)}{x} - \int_2^x \frac{dt}{t(\ln t)^2}\right| = O(x^{\frac{1}{2}+\varepsilon})$$

che *è la nostra ulteriore ipotesi equivalente della RH*! (**R. Turco, M. Colonnese, gruppo ERATOSTENE**)".

E' possibile dimostrarla? Sì. In vari lavori [vedi anche gruppo ERATOSTENE] è mostrato che:

$$G(N) \approx c\frac{N}{(\ln N)^2} \quad (93)$$

Ora senza voler tener presente la costante *c* e sapendo che è vero il TNP nella forma semplice:

$$\pi(N) \approx \frac{N}{\ln N}, \quad N \to \infty$$

Dalla (93) e dal TNP è:

$$\frac{G(N)}{N} \approx \frac{1}{(\ln N)^2}, \quad \frac{\pi(N)}{N \ln N} \approx \frac{1}{(\ln N)^2}$$

ci si riconduce all'ipotesi fatta con la relazione del tipo:

$$\left|\frac{G(N)}{N} - \frac{\pi(N)}{N\ln N}\right| < KC(N), \text{ con } K=1 \text{ e } C(N)=\frac{1}{\ln N} \quad (94)$$

Introducendo ora la funzione O grande, la precedente espressione diventa:

$$\left|\frac{G(N)}{N} - \frac{\pi(N)}{N\ln N}\right| = O((\ln N)^{-1}) \qquad (95)$$

e di conseguenza se al posto di $\pi(N)$ introduciamo il Logaritmo integrale:

$$\left|\frac{G(x)}{x} - \int_2^x \frac{dt}{t(\ln t)^2}\right| = O((\ln x)^{-1}) + O(x^{\frac{1}{2}+\varepsilon}) = O(x^{-\varepsilon}) + O(x^{\frac{1}{2}+\varepsilon}) \approx O(x^{\frac{1}{2}+\varepsilon}) \qquad (96)$$

La (96) è interessante, perchè è un'espressione analitica in forma chiusa che lega il numero di soluzioni di Goldbach G al logaritmo integrale e alla RH e dove la (96) è un'ipotesi equivalente della RH. Inoltre con essa asseriamo che G(N)>0 e disponiamo di una funzione e la sua inversa, possiamo cioè da $\pi(N)$ risalire a G(N) e viceversa con la (94).

Passiamo intanto a fare qualche calcolo con excel e settiamoci anche una regola che, in automatico ci verifichi la disuguaglianza ABS(A-B) < k, cioè scriva SI se verificata. Di seguito i risultati in tabella.

N	G(N)	A = G(N)/N	π(N)	B = π(N)/N*LN(N)	ABS(A-B)	K	ABS(A-B)<K?
4	1	0,25	2	0,36067376	0,11067376	0,72134752	SI
6	1	0,166666667	3	0,279055313	0,112388647	0,558110627	SI
8	1	0,125	4	0,240449173	0,115449173	0,480898347	SI
10	2	0,2	4	0,173717793	0,026282207	0,434294482	SI
12	1	0,083333333	5	0,167679002	0,084345668	0,402429604	SI
14	2	0,142857143	6	0,162395649	0,019538506	0,378923182	SI
16	2	0,125	6	0,13525266	0,01025266	0,36067376	SI
18	2	0,111111111	7	0,134546322	0,023435211	0,345976256	SI
20	2	0,1	8	0,13352328	0,03352328	0,333808201	SI
22	3	0,136363636	8	0,117641983	0,018721653	0,323515453	SI
24	3	0,125	9	0,117996743	0,007003257	0,31465798	SI
26	3	0,115384615	9	0,106244196	0,00914042	0,306927676	SI
28	2	0,071428571	9	0,096461238	0,025032666	0,300101629	SI
30	3	0,1	10	0,098004701	0,001995299	0,294014104	SI
100	6	0,06	25	0,05428681	0,00571319	0,217147241	SI
200	8	0,04	46	0,043410008	0,003410008	0,188739166	SI
300	21	0,07	62	0,036233266	0,033766734	0,175322254	SI
400	14	0,035	78	0,0325463	0,0024537	0,1669041	SI
500	13	0,026	95	0,030573127	0,004573127	0,160911192	SI
600	32	0,053333333	102	0,026575249	0,026758084	0,156324996	SI
1000	28	0,028	168	0,024320491	0,003679509	0,144764827	SI
10000	128	0,0128	1229	0,013343698	0,000543698	0,10857362	SI
100000	754	0,00754	9592	0,008331505	0,000791505	0,086858896	SI
1000000	5239*	0,005239	78498	0,005681875	0,000442875	0,072382414	SI

*Calcolato con la formula di ERATOSTENE

Tabella 13 – G(N) : ipotesi equivalente RH

Il termine d'errore 1/ln N, numericamente, funziona benissimo; tuttavia ci segniamo di verificare per ulteriori valori il suo comportamento! E' mezzanotte. Ma ad occhio ci riteniamo già soddisfatti del risultato!

Con la (96) è **G(N)>0**; difatti G(x) ha senso per $x \geq 4$ per cui l'integrale ha un valore positivo.

La (94) è quasi un "*tool alla Chebyscev*" che mette insieme vari concetti di probabilità (Vedi TNP al primo capitolo) e su cui si dovrebbe verificare una possibile interpretazione. La formula difatti è come se dicesse: "*La differenza, in valore assoluto, tra il numero di soluzioni di Goldbach G(N), rapportata al numero N pari in gioco, ed il conteggio di numeri primi fino ad N incluso, rapportato all'N-esimo numero primo ($\sim N \ln N$), è inferiore alla probabilità che N sia un numero primo ($\sim 1/\ln N$)*". Questa ce l'appuntiamo sul Block Notes Matematico!

E' da osservare poi che ln N nella (94) è circa H_n.

La relazione trovata per G(N) va bene anche per il calcolo *g(N) del numero di coppie di numeri primi gemelli*:

$$\left|\frac{g(N)}{N} - \frac{\pi(N)}{N \ln N}\right| < KC(N), \text{ con } K=1 \text{ e } C(N)=\frac{1}{\ln N}$$

$$\left|\frac{g(x)}{x} - \int_2^x \frac{dt}{t(\ln t)^2}\right| = O(x^{\frac{1}{2}+\varepsilon}) \quad (97)$$

Una verifica immediata numerica ce ne può dare effettivo convincimento.

Nel seguito abbiamo usato solo numeri pari di g(N) ma il discorso non cambia nemmeno con valori dispari N. L'obiettivo era solo qualitativo per verificare l'andamento a bassi ed alti valori di N.

N	g(N)	A=g(N)/N	π(N)	B=π(N)/N*LN(N)	ABS(A-B)	K	ABS(A-B)<K?
3	0	0	2	0,606826151	0,606826151	0,910239227	SI
4	0	0	2	0,36067376	0,36067376	0,72134752	SI
5	1	0,2	3	0,372800961	0,172800961	0,621334935	SI
6	1	0,166666667	3	0,279055313	0,112388647	0,558110627	SI
7	2	0,285714286	4	0,293656196	0,00794191	0,513898342	SI
8	2	0,25	4	0,240449173	0,009550827	0,480898347	SI
9	2	0,222222222	4	0,202275384	0,019946839	0,455119613	SI
10	2	0,2	4	0,173717793	0,026282207	0,434294482	SI
11	2	0,181818182	5	0,189560178	0,007741996	0,417032391	SI
12	2	0,166666667	5	0,167679002	0,001012335	0,402429604	SI
13	3	0,230769231	6	0,179940575	0,050828656	0,389871245	SI
14	3	0,214285714	6	0,162395649	0,051890065	0,378923182	SI
15	3	0,2	6	0,147707749	0,052292251	0,369269373	SI
16	3	0,1875	6	0,13525266	0,05224734	0,36067376	SI
17	3	0,176470588	7	0,145334875	0,031135714	0,352956124	SI
18	3	0,166666667	7	0,134546322	0,032120345	0,345976256	SI
19	4	0,210526316	8	0,142999272	0,067527043	0,339623272	SI
20	3	0,15	8	0,13352328	0,01647672	0,333808201	SI
21	4	0,19047619	8	0,125127139	0,065349052	0,328458739	SI
22	4	0,181818182	8	0,117641983	0,064176199	0,323515453	SI
23	4	0,173913043	9	0,1247983	0,049114743	0,318928989	SI
24	4	0,166666667	9	0,117996743	0,048669924	0,31465798	SI
25	4	0,16	9	0,111840288	0,048159712	0,310667467	SI
26	4	0,153846154	9	0,106244196	0,047601958	0,306927676	SI
27	4	0,148148148	9	0,101137692	0,047010456	0,303413076	SI
28	4	0,142857143	9	0,096461238	0,046395905	0,300101629	SI
29	4	0,137931034	10	0,102404898	0,035526136	0,296974204	SI
30	4	0,133333333	10	0,098004701	0,035328632	0,294014104	SI
100	8	0,08	25	0,05428681	0,02571319	0,217147241	SI
200	15	0,075	46	0,043410008	0,031589992	0,188739166	SI
300	19	0,063333333	62	0,036233266	0,027100067	0,175322254	SI
400	21	0,0525	78	0,0325463	0,0199537	0,1669041	SI
500	24	0,048	95	0,030573127	0,017426873	0,160911192	SI
600	26	0,043333333	102	0,026575249	0,016758084	0,156324996	SI
1000	35	0,035	168	0,024320491	0,010679509	0,144764827	SI

Tabella 14 – g(N) ipotesi equivalente RH

Per cui anche per g(N) valgono considerazioni analoghe. In pratica abbiamo appena descritto la RH8 e la RH9 e la (97) è *la soluzione della congettura sui numeri primi gemelli senza far riferimento a nessuna costante ma a funzioni note*.

La congettura sui numeri primi gemelli diceva:"[Twin prime conjecture"] Per grandi valori di n le due equivalenti approssimazioni sono congetturate:

$$g(n) = 2C_2 Li_2(n) \sim 2C_2 \int_2^n \frac{dt}{(\log t)^2}$$

$$g(n) \sim 2C_2 \frac{n}{(\log n)^2}$$

".

Goldbach e la fattorizzazione dei semiprimi e del RSA

Se si utilizza una equazione di secondo grado e la congettura forte di Goldbach si trova un semplice metodo per fattorizzare i semiprimi RSA; metodo individuato da James Constant (math@coolissues.com).

Il problema di Goldbach come abbiamo visto è connesso a Riemann e mostreremo che non avremo bisogno della funzione totiente $\varphi(x)$ di Eulero e che è possibile fattorizzare un semiprimo N a partire solo da N.

Siano a e b due numeri primi, che non conosciamo a priori, allora otteniamo il semiprimo:

$$p=a*b \quad (98)$$

Poniamo

$$a+b=s \quad (99).$$

Ora per la congettura di Goldbach se a e b sono primi allora s è un numero pari.

Poniamo:

$$b=s-a \quad (100)$$

Dalla (98) si ottiene l'equazione di secondo grado:

$$a^2 - a\,s + p = 0 \quad (101)$$

Da cui è:

$$a = \frac{1}{2}(s \pm c) \qquad c = \sqrt{s^2 - 4p} \quad (102)$$

Ora se a e b sono primi ed s pari, poiché $2a = (s \pm c)$ allora anche c è pari!!!

Ora se c è pari e c >0 significa che

$$s^2 > 4p \quad (103)$$

Deve quindi essere:

$$s^2 = c^2 + 4p \quad (104)$$
$$c^2 = s^2 - 4p \quad (105)$$

Metodo algoritmico per fattorizzare in base a Goldbach

- Step 1: si cerca un valore di $s^2 > 4p$ tale che sia un quadrato
- Step 2: si determina $c^2 = s^2 - 4p$.

- Si estrae la radice quadrata di c^2. Se c risultante è intero e numero pari ci si arresta perché con la (102) e la (100) si sono trovati a e b
- Altrimenti si ritorna allo step 1 per il quadrato successivo

Esempio
p=55
4p=220

Un quadrato successivo è $s^2=16^2= 256$

Ora dalla (101) è $c^2 = 256 – 220 = 36$, da cui c=6 è pari e intero.

Dalla (102) è a = ½(16±6) ovvero le due soluzioni a=11, b=5. Soluzione trovata e Fattorizzazione effettuata!

E' generalizzabile il metodo ad un numero di fattori qualsiasi?

Sì, ma con qualche problema come vedremo.

La generalizzazione del metodo significa poter fattorizzare un numero $N=p_1p_2p_3p_4…p_m$ di cui non conosciamo a priori né *m, che chiamiamo grado di fattorizzazione o bigomega*, né i vari p_i.

Inoltre si dovrebbe aggiungere una equazione sugli m fattori primi, attraverso una congettura di Goldbach o una sua variante (*Vinogradov*) o qualche altra proprietà che coinvolge gli m fattori, sia nel caso di risultato pari o dispari. In tal caso si otterrebbe una equazione di grado m qualsiasi (da non risolvere), i cui coefficienti dell'equazione però devono sottostare a m-1 disequazioni. Le disuguaglianze su cui basano le disequazioni sono dedotte a partire dalla somma dei fattori. La soluzione del sistema di disequazioni fornisce alla fine soluzioni che rappresentano i fattori primi di N.

Il problema è risolvibile se, nell'ordine, rimuoviamo due difficoltà:

- esiste un modo per sapere a priori dato N, quanti m fattori ha N ivi comprese le molteplicità (ad esempio se $N=2*3^2*5^3$ allora m è la somma degli esponenti di tutti i numeri, m=6) ?
- possiamo usare Goldbach o varianti con la somma di m fattori per avere delle condizioni da imporre nel sistema di disequazioni?

Il primo punto non è impossibile, fidatevi! Se siete avvezzi al programma PARI/GP e alla Teoria dei numeri saprete che esiste una *funzione bigomega(x)*, molto veloce, che fornisce il numero di divisori di x, tenendo conto anche della loro molteplicità.

Ad esempio N=90:
m = bigomega(90)=4, perché $90=2*3^2*5$

inoltre anche con numeri con molte cifre si ottiene una risposta in pochi millisecondi. Dov'è l'inconveniente in tutto ciò? Se ad esempio m=200 avremo un'equazione di grado 200 e quindi da risolvere un sistema di 199 disequazioni (questo non è un problema per un calcolatore): il problema sono le ipotesi sulle 199 disequazioni da formulare e generalizzare per ogni m. In teoria è possibile. Conviene tale metodo in pratica? Per l'RSA si usano i metodi economici visti prima, per la fattorizzazione basta scomporre in fattori… Forse la generalizzazione del metodo, al momento, non ha un'applicazione per cui convenga usarlo. Ma ce lo segniamo sul Block Notes Matematico, non si sa mai in futuro!

Fattorizzazione e quadrati perfetti

In [6][7] sono mostrati algoritmi per la fattorizzazione basata sui quadrati perfetti e sulle forme generatrici di numeri primi $6n\pm1$. In particolare in [6] sono anche mostrati test di primalità e calcolo di $\pi(N)$ sfruttando le forme generatrici di numeri primi $6n\pm1$.

L'algoritmo del quadrato perfetto permette, per esempio, di fattorizzare istantaneamente il prodotto di due numeri primi gemelli p e q, poiché, per motivi legati alle forme $6k\pm1$, tali prodotti sono di forma $p * q = (6k-1)(6k+1) = N$ e in tali casi:

$$p = \sqrt{(N+1)} - 1 \quad q = \sqrt{(N+1)} + 1$$

dove 1 è il quadrato della semidifferenza tra due numeri gemelli; per numeri primi non gemelli, ovviamente la semidifferenza è maggiore e quindi anche il suo quadrato;

un esempio per tutti $p = 11$, $q = 13$ (primi gemelli)

$$N = p * q = 11*13 = 143$$

$$p = \sqrt{(143+1)} - 1 = \sqrt{144} - 1 = 12 - 1 = 11$$

$$q = \sqrt{(143+1)} + 1 = \sqrt{144} + 1 = 12 + 1 = 13,$$

il tutto senza aver bisogno di dimostrare la RH!

Fattorizzazione dei semiprimi e del RSA col modulo

Una fattorizzazione basata sull'equazione $x^2=a^2$ mod N dove N=p*q è il semiprimo, quindi, dello stesso genere RSA, è mostrata in [8].

L'RSA è attaccabile? In pratica sì e senza RH!

Se si usano dei quadrati perfetti per le chiavi si facilita di molto la vita al hacker, perché è possibile implementare facilmente un algoritmo abbastanza veloce in C o altro linguaggio secondo la teoria esposta in [6], [7] e [8].

L'unica barriera che pone l'RSA non è né la funzione totiente di Eulero, né il tipo di matematica sottostante, ma solo la lunghezza dei numeri primi (centinaia di cifre). In tal caso maggiore è la lunghezza dei due numeri primi, maggiore è il tempo necessario a risolvere il problema di ottenere le chiavi di codifica e decodifica. Questo semplice espediente permette alla società di ampliare la lunghezza dei numeri primi, osservando in ambito mondiale e scientifico quanto i crittoanalisti e gli hacker si siano avvicinati al limite di sicurezza del sistema crittografico in gioco. Oggi, per sistemi critici, sono preferibili sistemi di crittografia diversi dal RSA, non basati sulla fattorizzazione, problema matematico troppo comprensibile da tutti, anche per diminuire la platea di persone che potrebbero attaccare il sistema crittografico.

Il problema di Basilea e le costanti zeta

Eulero non ci ha tramandato una forma chiusa per N dispari, esistono solo i valori approssimati. Ma esiste una forma chiusa per N dispari?

La bellezza e l'armonia della matematica indurrebbe a dire che se è vera la tabella 4 già vista prima nel capitolo delle serie, allora i "buchi" vuoti della tabella per N dispari dovrebbero essere colmati con delle forme chiuse, tali da ottenere il valore reale disponibile della colonna successiva.

N	Valore in forma chiusa	Valore
2	$\pi^2/6$	1,644934066848
3	?	1,202056903159
4	$\pi^4/90$	1,082323233711
5	?	1,036927755143
6	$\pi^6/945$	1,017343061984
…	…	…

Fissiamo l'attenzione su N=3. Volendo essere romantici e credendo alla poesia della matematica, ci illudiamo che il valore di convergenza sia π^3/t, dove t oppure 1/t non è intero e andrebbe ricercata una forma chiusa per esso, come pure potrebbero essere

coinvolte anche costanti famose come l' *e di Nepero*, o valori di *Fibonacci* o il *Rapporto Aureo* o *i fattoriali* etc. (Vedi in Appendice – Costanti Matematiche)

Facciamoci qualche conto con il calcolatore. Per N=3, in base al valore reale disponibile e immaginando che il risultato **sia** π^3/t, ne consegue che t=25,7943501888831436… (irrazionale) o che 1/t = 0,038768179602897632 32... Per N=5, invece, c = 300,8028424438149839… e 1/c=0,00332443667046… Non ci viene in mente nessuna costante famosa con questi valori … Quindi il legame non è semplicemente di fattore moltiplicativo rispetto a π^3 o rispetto a π^5 .

Se, invece, ricordiamo che e = 2,7182818284590452353… e per N=2 il valore 1,644934066848 $\approx \sqrt{e}$ = 1,6487212707001281468… Inoltre sempre per N=3, il numero 1,2020… è circa la media aritmetica tra $\sqrt{1,6449…}$ = 1,2825…e $\sqrt{1,2825…}$

E quest'ultima radice è in realtà la radice quarta del primo valore 1,6449…

Se usiamo il numero di *Nepero*, stiamo in ogni caso facendo una approssimazione e non abbiamo ancora ottenuto una forma chiusa del valore, ma solo una misura approssimata e quindi un numero irrazionale con un elevato numero di cifre.

Se consultiamo le costanti matematiche ad oggi note su Wikipedia, **balza con sorpresa all'occhio** che per N=3 del problema di Basilea c'è la *costante di Apèry* = *1,202056903159 = ξ(3)*. Ma esistono forme chiuse volendo anche per ξ(2n+1), solo che all'epoca del problema di Basilea lo studio completo sui valori di zeta non erano stati fatti, anche se Eulero aveva introdotto la serie corrispondente.

Ad oggi, quindi, l'unica forma chiusa nota è solo attraverso la funzione zeta di Riemann, però quella reale di variabile reale (e funzioni correlate a quella di Riemann), o meglio ancora attraverso le cosiddette **costanti zeta**. In sostanza il problema di Basilea non è un problema … Lo è se non si vogliono usare i risultati della zeta di Riemann.

Costanti zeta

Simon Plouffe ha trovato che:

$$\zeta(3)=\frac{7}{180}\pi^3-2\sum_{n=1}^{\infty}\frac{1}{n^3(e^{2\pi n}-1)}$$

$$\zeta(5)=\frac{1}{294}\pi^5-\frac{72}{35}\sum_{n=1}^{\infty}\frac{1}{n^5(e^{2\pi n}-1)}-\frac{2}{35}\sum_{n=1}^{\infty}\frac{1}{n^5(e^{2\pi n}+1)}$$

$$\zeta(7)=\frac{19}{56700}\pi^7-2\sum_{n=1}^{\infty}\frac{1}{n^7(e^{2\pi n}-1)}$$

Con sorpresa vediamo che la nostra idea di base non era male: c'è la potenza di π (N=3, N=5, N=7) e troviamo anche il numero di Nepero!

Formula generale delle costanti zeta ζ(2n+1)

Se definiamo con $S_{\pm}(s)=\sum_{n=1}^{\infty}\frac{1}{n^s(e^{2\pi n}\pm 1)}$

Si dimostra (ma non lo mostriamo. Consultate Wikipedia) che:

$$0=A_n\zeta(n)-B_n\pi^n+C_nS_{-}(n)+D_nS_{+}(n)$$

dove A_n, B_n, C_n, D_n sono coefficienti interi.

Plouffe fornisce una tavola di valori come in figura 22:

Coefficienti

n	A	B	C	D
3	180	7	360	0
5	1470	5	3024	84
7	56700	19	113400	0
9	18523890	625	37122624	74844
11	425675250	1453	851350500	0
13	257432175	89	514926720	62370
15	390769879500	13687	781539759000	0
17	1904417007743250	6758333	3808863131673600	29116187100
19	21438612514068750	7708537	42877225028137500	0
21	1881063815762259253125	68529640373	3762129424572110592000	1793047592085750

Figura 22 – Coefficienti costanti zeta

Formula generale delle costanti zeta ζ(2n)

Si possono esprimere tramite i numeri di Bernoulli, su una relazione già trovata da Eulero:

$$\zeta(2n)=(-1)^{n+1}\frac{B_{2n}(2\pi)^{2n}}{2(2n)!}$$

Alcuni di questi valori sono registrati su OEIS (www.research.att.com) e sono rappresentati in figura 23, dove A è il denominatore e B il numeratore per cui B / A.

Coefficienti

2n	A	B
2	6	1
4	90	1
6	945	1
8	9450	1
10	93555	1
12	638512875	691
14	18243225	2
16	325641566250	3617
18	38979295480125	43867
20	1531329465290625	174611
22	13447856940643125	155366
24	201919571963756521875	236364091
26	11094481976030578125	1315862
28	5646536601700762736718 75	6785560294
30	5660878804669082674070015625	6892673020804
32	6249022057102234120726640625 0	7709321041217
34	1213045458143374858729289062 5	151628697551

Figura 23 – costanti zeta per 2n

I numeri di Bernoulli, invece, si possono calcolare in varie forme; ma la più sorprendente è quella in forma determinante associata alla matrice:

$$B_{2n} = (2n)!\begin{pmatrix} \frac{1}{2!} & 1\dots & 0 \\ \vdots & \ddots & 0 \\ \frac{1}{(2n+1)!} & \frac{1}{(2n)!} \dots & \frac{1}{2!} \end{pmatrix}$$

La dimostrazione di Eulero per N pari

Ma facciamo un passo indietro. Eulero come trovò i valori per N pari?

Occorre ricordare lo sviluppo in serie di Taylor della funzione seno (e avremo a che fare ancora con una serie):

$$\sin(x) = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \dots$$

Dividendo per x entrambi i membri si ottiene:

$$\frac{\sin(x)}{x} = 1 - \frac{x^2}{3!} + \frac{x^4}{5!} - \frac{x^6}{7!} + \dots$$

Eulero assunse che il secondo membro lo potesse trattare normalmente come un polinomio finito anche se in realtà è infinito (assunzione che non dimostrò, ecco perché la sua dimostrazione sebbene porti ad un risultato valido non è rigorosa. Oggi

si dimostra rigorosamente: vedi Wikipedia) e trovò che le *radici del polinomio* sono: $\pm\pi$, $\pm 2\pi$, $\pm 3\pi$ … Sostituiamo ora $z=x^2$

Ora diventa:

$$\frac{\sin(x)}{x}=1-\frac{z}{3!}+\frac{z^2}{5!}-\frac{z^3}{7!}+...$$

Ora le radici di questo polinomio, per le sostituzioni fatte, sono π^2, $4\pi^2$, $9\pi^2$, …

Per il *Teorema di Viète* (vedi Wikipedia) sapendo che se un polinomio ha il termine costante pari a 1, la somma degli inversi delle sue radici è uguale al coefficiente del termine lineare, cioè x, ma cambiato di segno. Ad esempio se il polinomio è del tipo con costante pari a 1: $a_n x^n+...+a_2 x^2+bx+1$, allora stiamo cercando il valore –b.

Ora supponendo di poter applicare le stesse regole dei polinomi finiti a quelli infiniti, allora è:

$$+\frac{1}{3!}=\frac{1}{6}=\frac{1}{\pi^2}+\frac{1}{4\pi^2}+\frac{1}{9\pi^2}+...$$

Moltiplicando per π^2, primo e secondo membro, si ottiene il valore finale cercato e abbiamo completato la dimostrazione:

$$\frac{\pi^2}{6}=1+\frac{1}{4}+\frac{1}{9}+...$$

Funzioni correttrici

In riferimento alla RH3, il gruppo ERATOSTENE in vari lavori ha presentato delle correzioni connesse alla funzione $\pi(n)$. Nell'articolo "Due formule più precise per il calcolo dell'n-esimo numero primo e di $\pi(N)$") il gruppo ha introdotto le funzioni correttrici c e c' (con $c' \approx \sqrt{c}$) utili fino a $N = 10^{23}$) che permettono di abbattere l'errore percentuale in modo simile a Li(x).

Ad esempio, per $\pi(50000000)$, il valore reale è 3001143. Le funzioni correttrici sono 1,0711 per 10^7 e 1,0612 per 10^8:

$\pi(50000000) \approx$ 50000000/ ln 50000000 · 1,0711 = 3021006
$\pi(50000000) \approx$ 50000 000/ln 50000000 · 1,0612 = 2993084

con discrepanze di 19872 e 8049 rispetto al valore reale 3001134.

Usando invece la media aritmetica tra i due valori di c', avremo:

1,0711 + 1 0612/2 = 1,06615

e $\pi(50000000) \approx 50000000/\ln 50000000 \cdot 1{,}06615 = 3007045$ (poiché 50000000 è a metà strada tra i due numeri 10^7 e 10^8) con discrepanza di sole 5 911 unità, e quindi con un 'errore percentuale di 5911/30011,34 = 0,1969 ; mentre con Li(x) si ottiene un errore percentuale di 5485/30011,34 = 0,1827, valore vicinissimo allo 0,1969 ottenuto con la media dei due valori della funzione correttrice c', data dal rapporto tra il valore reale di $\pi(n)$ e il valore stimato col la formula n/ ln (n), dove n è, nelle tabelle di ERATOSTENE, una potenza di 10 fino a 10^{23}, idem per la funzione c per il calcolo dell'n-esimo numero primo, con c tale che n-esimo $\approx$ N ln (N) c.

Congettura sulla funzione media cumulativa di Mertens

M(k) è una funzione un po' irregolare, oscillante sopra e sotto lo zero con un andamento che i matematici chiamano *random walk o cammino aleatorio*.

Per argomenti pari a 1000, 2000,… fino a 10mila (*Archimede* direbbe una miriade!) la funzione assume i valori: 2, 5, -6, -9, 2, 0, -25, -1, 1, -23.

Per argomenti 1 milione, 2 milioni,…fino a 10 milioni, la funzione assume i valori: 212, -247, 107, 192, -709, 257, -184, -189, -340, 1037.

Se non si tiene conto dei segni, è abbastanza chiaro che la dimensione di M(k) aumenta (vedi *Prof. Cerruti ed il suo famoso blog*), , ma i più considerano poco chiaro come possa essere sfruttato il tutto.

In realtà qualcosa si osserva chiaramente: la media aritmetica di tali valori può essere un valore sempre più piccolo, in percentuale, rispetto ai valori della serie degli argomenti o alla loro media.

Ad esempio, per la serie da 1000 a 10000, la media aritmetica è

$$(2+5-6-9+2+0-25-1+1-23)/10 = 54/10 = 5{,}4$$

che rispetto a 5500 (media dei dieci valori), costituisce il 5,4/55 = 0,098% circa lo 0,9 per 10mila e quindi un 55 millesimo; mentre per la serie dei milioni da uno a dieci milioni, la media aritmetica è:

$$(212-247+107+192-709+257-184-189-340+1037)/10 = 136/10 = 13{,}6$$

che rispetto a 5 500 000 (media dei dieci valori) costituisce il 13,6/55000 = 0,0002472%, circa il 2 per milione sulla media dei valori 5 500 000 (il cui 1% è già 55 000).

La media per i primi valori di M(k) da 1 a 10 è (1+0-1-1-2-2-2-2-2-1)/10 = -12/10 = -1,2 che costituisce il -1,2/0,055 = 21,81 % (in valore assoluto) rispetto alla media dei numeri da 1 a 10 (valori dei primi dieci argomenti).

Quindi, la media dei valori della funzione M(k) cumulativa è una percentuale sempre più piccola della media dei valori argomenti, e variabile dal 21,81 % per i valori di k da 1 a 10, allo 0,098 % per i valori da 1000 a 10000, (per migliaia), allo 0,0002472 % per i valori da 1000000 a 10000000 (per milioni interi).

Si potrebbe introdurre, quindi, una *funzione di Mertens media cumulativa*, in base alla suddetta idea della media aritmetica dei valori di M(k) e dei valori degli argomenti, che potrebbe dare luogo alla **congettura sulla *funzione di Mertens media cumulativa*** formulabile come segue: "La media aritmetica dei valori successivi di M(k) è una percentuale sempre più piccola della media dei corrispettivi valori di k; e quindi tendente a zero, come differenza tra i valori di "testa" e "croce", (+1) e (-1) dei valori di M(k) al crescere di k." Però pensiamo ad un ulteriore miglioramento che scaturisce dall'osservazione che la percentuale si potrebbe calcolare anche sul valore finale degli argomenti, ottenendo valori simili:

1,2 / 0,1	=	12 %,
5,4 /100	=	0,054 %
13,6 / 10 000	=	0,00136 %
10 / 1,2	=	8,33
10000 / 5,4	=	1851,85
10000000 / 13,6	=	735 294,11

sempre crescenti tra il valore massimo di k e la media dei valori di M(k).

Inoltre sarebbe:

$$1,2 \approx \sqrt[8]{10} = 1,33$$

$$5,4 \approx \sqrt[8]{10000} = 3,16$$

$$13,6 \approx \sqrt[8]{10000000} = 7,49$$

Se questa valutazione della media risultasse attendibile da più approfonditi calcoli futuri, per argomenti prossimi a 1000000000000 avremmo una media di circa $\sqrt[8]{1000000000000} = 31,62$, dimostrando che è sottostante a questi numeri una qualche nuova funzione, che chiameremo M'(k), cresce molto lentamente al crescere di n, poiché i valori positivi e negativi di M(k) (funzione $\mu(n)$ cumulativa) tendono ad annullarsi reciprocamente, lasciando valori molto bassi di M'(n), per esempio -247 e 257, con differenza 257 - 247 = 10, -709 e 1037, con differenza 1037 – 709 = 328, per gli argomenti da 1 milione a 10 milioni.

Potrà servire tale idea alla dimostrazione della RH2? Per il momento questa provvisoria relazione trovata, e da accertare ulteriormente, la registriamo nel nostro block notes come "*congettura ERATOSTENE sulla funzione media cumulativa di Mertens*":

$$M'(k) \approx \sqrt[8]{k} \quad (101)$$

Tale formula è comunque interessante per la RH2 ed in ogni caso M'(k) della (101) è legata a M(k) della (69).

Altra osservazione
Tenendo conto della sola somma algebrica S di -12, 54 e 136, constatiamo che -12 è minore di √10= 3,16, 54 è minore di √1000 =100 e 136 è minore di √10000000 = 3262,27, e infine il rapporto M'(k)/k , cioè tra la somma algebrica e l'argomento k è, rispettivamente per i tre gruppi di numeri:

-12 / 10 = -1,2 (unico valore negativo)
54 / 10000 = 0,0054
136 / 10000 000 = 0,0000136

e quindi tendente a 0 per k sempre più grandi.

Lo stesso fenomeno, in misura simile, si verifica con il rapporto tra il valore più alto di M(K) e k per i tre esempi:
-2 / 10 = - 0,2
-25 / 10000 = - 0,0025
1037 / 10000000 = 0,00001037

Questo potrebbe influire, ma occorre verificare fino a che punto, sulla funzione M(k) per k molto grandi: la somma algebrica o il valore più alto di M(k) cumulativa è sempre vicina allo zero come differenza tra valori negativi e positivi di M(k).

Capitolo 11. Grafici e tabelle funzioni coinvolte con la RH

Dedicheremo questo capitolo ad alcuni grafici e tabelle, tratti anche da INTERNET, relative alle funzioni coinvolte nelle varie ipotesi RH equivalenti, data la somiglianza tra alcuni grafici relativi a funzioni differenti, anche con qualcuna (per es. Goldbach) non direttamente interessata ad una particolare ipotesi.

Qui ci si chiede se, ad esempio, la notevole somiglianza potrebbe essere utile ad eliminare possibilità di contro esempi (per es. per Goldbach e RH1), poiché entrambi i relativi grafici presentano aree libere da valori, compresi i possibili contro esempi, e quindi verificare se possono contribuire a dimostrare la verità della congettura interessata, in questo caso Goldbach ed RH1.

Le tabelle invece evidenziano particolari andamenti comuni ad alcune funzioni, per esempio la tendenza a 0 oppure ad 1; andamenti con caratteristiche comuni, per esempio un valore come radice quadrata per es. nel problema di Basilea, connesso alla RH3) o quarta (per es. la funzione Θ(n) nella RH4) del valore precedente, etc e, forse, potenzialmente utili per una migliore comprensione dei meccanismi matematici che si celano dietro.

Cominciamo con la figura 22 e la figura 23 entrambe connesse alla funzione μ(n) di Moebius sulla quale si basa la RH2. Entrambe le figure sono tratte dal blog del Prof. Umberto Cerruti: http://alpha01.dm.unito.it/personalpages/cerruti/luglio04-gennaio28 articolo Congettura di Riemann e sicurezza mondiale, al quale si rimanda per la descrizione dei grafici.

Nella figura 22 si nota una maggiore regolarità del grafico, dove la somma algebrica dei valori positivi e negativi tendono ad annullarsi sulla retta centrale con valore zero; e la loro media cresce lentamente con n come visto nel capitolo precedente.

Mentre nella figura 23 (distribuzione casuale dei lanci di una moneta) ciò non è possibile, mancando le regolarità del primo grafico (distribuzione solo apparentemente casuale dei numeri primi).

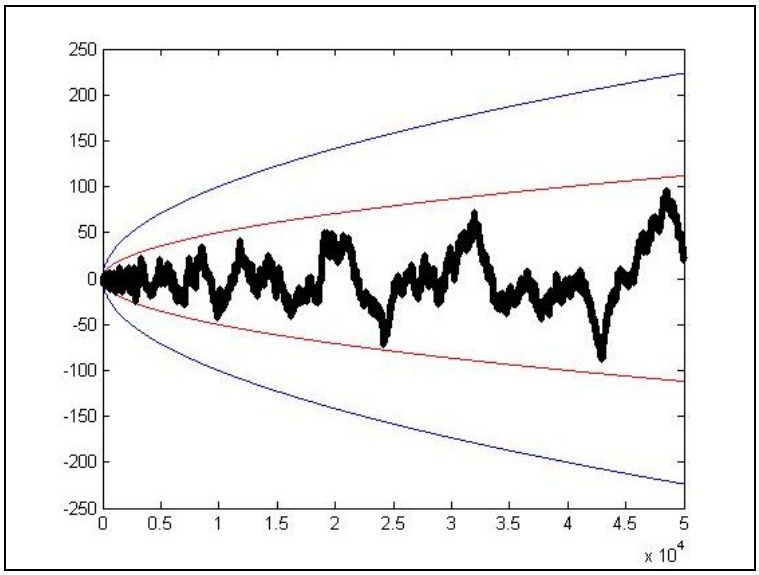


Figura 24 – funzione di Moebius (a)

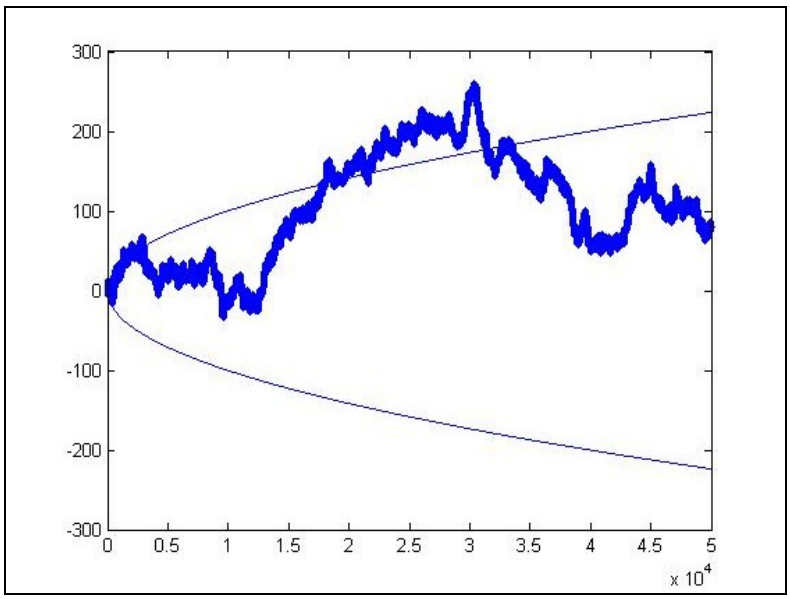


Figura 25 – funzione di Moebius (b)

Guardando tali figure viene in mente una somiglianza notevole tra i grafici della funzione L(n), connessa alla funzione σ(n), vedi figura 24, ed il grafico della funzione φ totiente di Eulero, vedi figura 25. Dove la linea tratteggiata è nostra, per evidenziare l'angolo inferiore privo di valori, e quindi di contro esempi $L(n) < 0$ per la RH1 (equivalenza di Lagarias RH1 = RH vedi [5]).

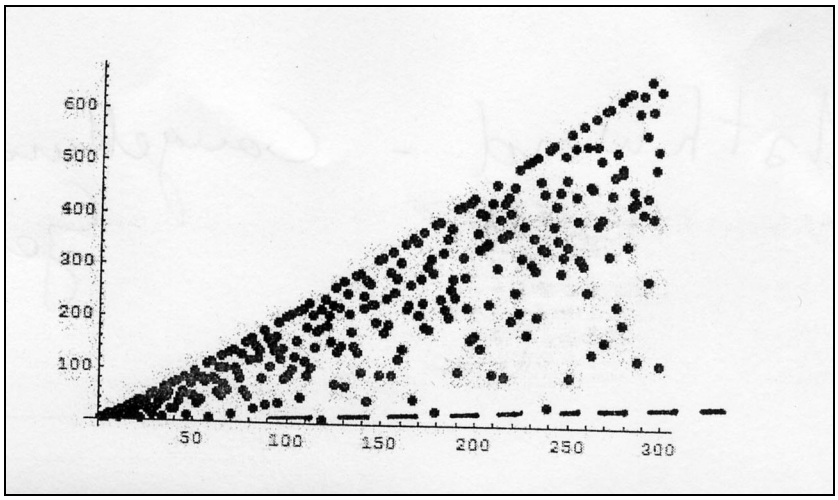


Figura 26 – L(n)

Nella figura 25 ci sono invece i grafici simili della funzione φ di Eulero, tratti dai siti web Wikipedia e Mathworld, con voce di ricerca "Mathworld Goldbach" su Internet.

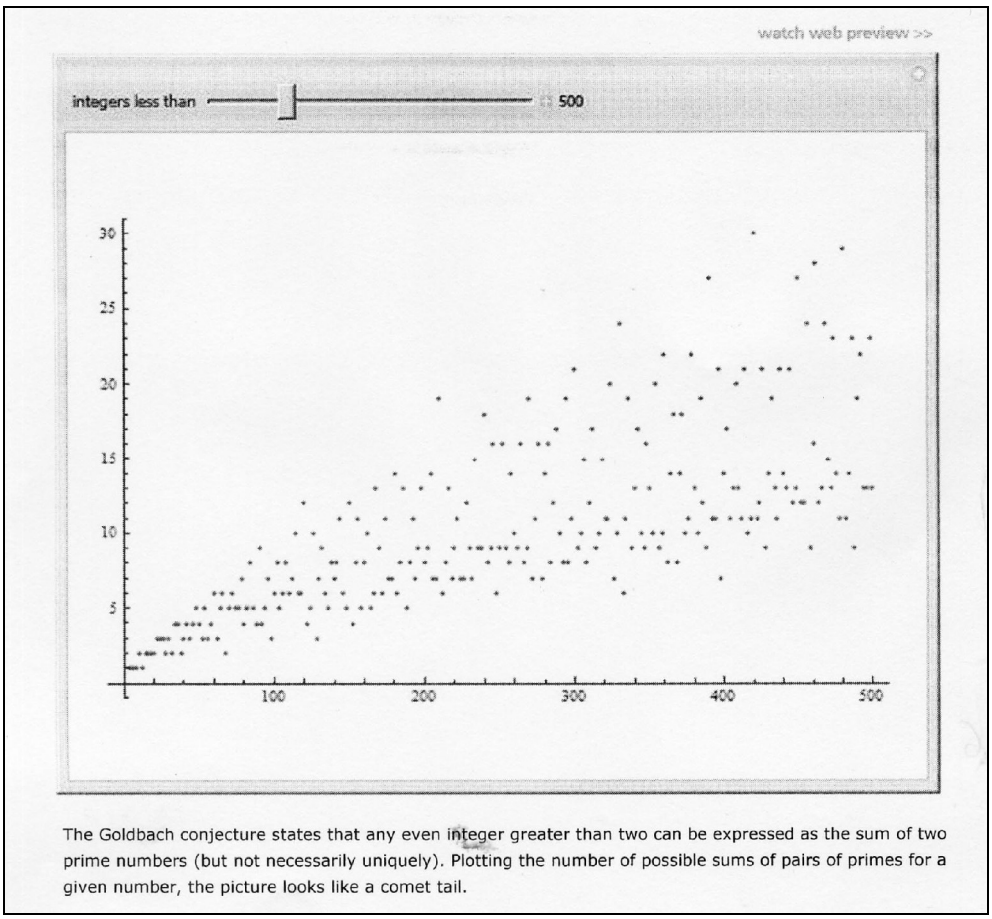


Figura 27 - Goldbach

Anche qui si nota, come nel grafico precedente, un angolo superiore libero da valori come nel grafico precedente della Fig. 24, un angolo centrale con i valori di φ e un angolo inferiore pure libero da valori come l'angolo superiore; poiché, come vedremo in seguito, φ(p) = p +1 se p è primo e per i numeri primi si hanno i valori più alti (e quindi sulla linea superiore del grafico), mentre per gli altri numeri composti si hanno i valori intermedi, e comunque minori di n/2, e cioè $\varphi(n) \leq n/2$. I valori minori di φ(n) si hanno per i numeri n multipli di 6, e quindi di forma n = 6k:

φ(12) = 4,
φ(18) = 6,
φ(24) = 8,
φ(30) = 8,
φ(36) = 12,
φ(42) = 12,
etc.

Ciò collega indirettamente la funzione φ(n) alla funzione G(N), di Goldbach, anch'essa collegata ai multipli di 6, con N = 6k, ma con la differenza che ora i multipli di 6 hanno più elevati valori di G(N), numero delle coppie di primi la cui somma è N. E anche i relativi grafici così si somigliano molto, anche se per opposti motivi: per i multipli di 6 la funzione φ(n) assume i valori minimi, mentre la funzione G(N) assume i valori massimi rispetto a numeri vicini ma non multipli di 6.

Un risultato del gruppo ERATOSTENE è la relazione di Goldbach:

$$G(6k-2) + G(6k+2) \approx G(6k)$$

come è esposto in vari lavori (vedi “Numeri primi in cerca d’autore” [11]).

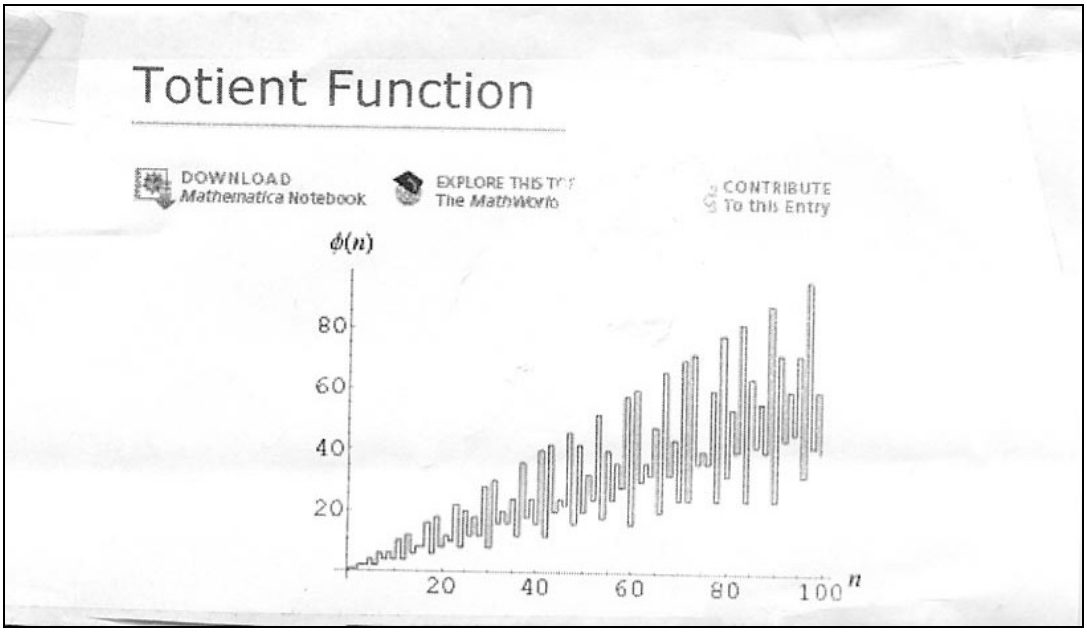


Figura 28 – Funzione totiente di Eulero

Tranne che per le figure 22 e 23 che riguardano la RH3 e la funzione μ(n), notiamo una certa somiglianza generale tra tutti le figure viste, che chiameremo “tri-angolari”, poiché sono costituiti da un angolo superiore libero di valori, un angolo centrale in cui si concentrano i valori della funzione interessata, e un angolo inferiore libero da valori, e quindi anche di contro esempi per le congetture interessate (ricordiamo la RH1 e Goldbach). Figure con comportamenti del genere gli inglesi le chiamano “*comet*” perché somigliano molto alle code delle comete.

Circa invece i numeri primi p, la funzione φ(p) assume i valori più alti, essendo di più i numeri fino a p coprimi con p, rispetto ai numeri composti. E quindi per i numeri primi la funzione φ(p) assume ovviamente i valori più alti (contrariamente alla funzione somma di divisori, σ(p, avendo p i due soli divisori 1 e se stesso).

Per i numeri primi, com’è noto, abbiamo $\varphi(p) = p - 1$ (valori alti rispetto ai numeri composti) mentre per la funzione σ(p) abbiamo $\sigma(p) = p + 1$ (valori bassi rispetto ai numeri composti) che rivedremo in seguito collegando la funzione φ(p) alla congettura di Goldbach.

Ricordiamo anche brevemente che nella funzione L(n) della RH1 è coinvolta la funzione σ(n), specialmente per i numeri abbondanti (tipo i fattoriali e i loro multipli), con la formula $L(n) = H_n + e^{Hn} \cdot \log Hn - \sigma(n)$, e affinché la RH1 sia vera deve essere $L(n) > 0$. Solo i numeri abbondanti sembrano pericolosi per la RH1, ma non lo sono, poiché la funzione σ(n) per i numeri abbondanti

H_n cresce meno velocemente di $H_n + e^{Hn} \cdot \log Hn$, e quindi la loro differenza L(n) sarà sempre positiva e maggiore di 1, come mostrato in [5].

Ma torniamo alla funzione $\varphi(p) = p-1$.

Osserviamo che $\varphi(n)$ e $\sigma(n)$ sono in qualche modo complementari, nel senso che i coprimi di n sono i numeri diversi dai divisori di n; per esempio, se n = 8, $\varphi(8) = 4$ = numero dei coprimi 1, 3, 5, 7 di 8, $\sigma(8) = 15$ = somma dei quattro divisori di 8, e cioè 1, 2, 4, e 8 con in comune soltanto l'unità, insieme coprimo e divisore di tutti i numeri n. Ovviamente 2, 4 e 8 sono diversi dai coprimi 1, 3, 5, e 7. Insomma, i numeri fino a n si dividono in coprimi con n e divisori di n.

I grafici per $\varphi(n)$ e $\sigma(n)$, o meglio i loro valori, sono quindi capovolti, cioè con i valori di $\varphi(p)$ più alti per i numeri primi, e più bassi per i numeri multipli di 6 (avendo questi più divisori e meno coprimi); e, viceversa, per $\sigma(n)$, con i valori ora più bassi per i numeri primi (avendo essi due soli divisori e quindi somme minori) e più alti per i multipli di 6 (con più fattori e più divisori e quindi con somme maggiori), e inoltre i multipli di 6 hanno un maggior numero G(N) di coppie di Goldbach (vedi Figura 26).

In sostanza le quatto funzioni $\varphi(n)$, $\sigma(n)$, L(n) e G(N) sono tra loro interconnesse tramite i multipli di 6, connessioni rese evidenti dai rispettivi grafici**.**

Una quasi somiglianza della funzione $\varphi(p)$ con la funzione G(N) è questa, seguita da un esempio numerico:

$\varphi(p-1) + \varphi(p+1) \approx \varphi(p)$ con p primo:

$\varphi(16) + \varphi(180) \approx \varphi(17)$

$8 + 6 = 14 \approx 16 = 17 - 1,$

idem per qualsiasi altro numero primo.

$G(N-2) + G(N+2) \approx G(N)$ con N = 6k

$G(454) + G(458) \approx G(456)$ con 456 = 76 x 6

$12 + 9 = 21 \approx 24.$

In genere $\varphi(p-1) + \varphi(p+1)$ è sempre minore di $\varphi(p)$ e $\varphi(n)$ è sempre minore di n/2. Altre stime (Mathworld) danno $\varphi(n) > \sqrt{n}$, per cui è: $\sqrt{n} > \varphi(n) < n/2$.

Segue Tabella di $\varphi(n)$ ed n divisa in sei colonne

6k+2 6k+3 6k+4 6k+5 6(k+1) 6(k+1)+1

n; **φn**	n; **φ(n)**	n;(**φ(n)**	n; **φ(n)**	n; **φ(n)**	n; **φ(n)**
					1 **1**
2 **1**	3 **2**	4 **2**	5 **4**	6 **2**	7 **6**
8 **4**	9 **6**	10 **4**	11 **10**	12 **4**	13 **12**
14 **6**	15 **8**	16 **8**	17 **16**	18 **6**	19 **18**
20 **8**	21 **12**	22 **10**	23 **22**	24 **8**	25 **20**
26 **12**	27 **18**	28 **12**	29 **28**	30 **8**	31 **30**
32 **16**	33 **20**	34 **16**	35 **24**	36 **12**	37 **36**
38 **18**	39 **24**	40 **16**	41 **40**	42 **12**	43 **42**
…	…	…	…	…	…

Tabella 15 - φ(n) ed n

Nella tabella di cui sopra sono sottolineate le coppie con rapporto N/φ(N) = 2 oppure 3.

Più in generale, nella prima colonna il rapporto medio è > 2;
nella seconda colonna, il rapporto medio è < 2;
nella terza colonna, il rapporto medio è > 2;
nella quarta colonna (esclusi i numeri primi) < 2;
nella quinta colonna > 3;
nella sesta colonna (esclusi i numeri primi) < 2.

Per i numeri primi, com'è noto, il rapporto p/φ(p) = p/(p-1) ≈ 1. Il suddetto rapporto quindi varia tra valori leggermente superiori a 1 quando n = p = primo, a 3 o a valori superiori a 3 per n 0 multipli di 6, giacenti sulla quinta colonna (n=6k). Segue la Tabella dei valori di φ(n) fino ad n = 42 con φ(n) ≈ n/2, e con φ (n) ≈ n/3 se n è di forma 6k (i numeri primi sono sottolineati).

k	n	φ(n)	≈ n/3 per n = 6k
	1	1	
	2	1	
	3	2	
	4	2	
	5	4	
1	**6**	**2**	= **6/3 = 2** (Valori bassi per n = 6k)
	7	6	= p – 1 (valori alti se n = p primo)
	8	4	
	9	6	
	10	4	
	11	10	
2	**12**	**4**	**= 12/3 = 4**
	13	12	
	14	8	
	15	8	
	16	8	
	17	16	
3	**18**	**6**	**= 18/3 = 6**
	19	18	
	20	8	
	21	12	
	22	10	
	23	20	
4	**24**	**8**	**= 24/3 = 8**

	25	20	
	26	12	
	27	18	
	28	12	
	29	28	
5	**30**	**8**	**≈ 30/3 = 10**
	31	30	
	32	16	
	33	20	
	34	16	
	35	24	
6	**36**	**12**	**= 36/3 = 12**
	37	36	
	38	18	
	39	24	
	40	16	
	41	40	
7	**42**	**12**	**≈ 42/3 = 14**
	…	**…**	

Tabella 16 - Tabella dei valori di φ(n)

Per i valori successivi vedi alla voce di Wikipedia "Funzione φ(n) di Eulero".

Come si può facilmente notare, i valori minori della funzione si riferiscono ai numeri n multipli di 6 (importanti, come abbiamo già accennato, per la funzione L(n) della RH1 e per la congettura di Goldbach), per i quali invece la funzione σ(n) assume i valori più alti, e viceversa per i numeri primi.

Più in generale, $\varphi(6k) \approx 6k/3 \approx 2k$ per i multipli di 6, e con $\varphi(n) \approx n/2$ per tutti gli altri numeri; mentre per i numeri primi, il rapporto è $p/p-1 \approx 1$ e tendente a 1 come limite inferiore, al crescere di p.

In conclusione, rapporto $n/\varphi(n)$ massimo (circa 3) per i multipli di 6, rapporto medio (circa 2) per tutti gli altri numeri composti, e minimo (circa 1) per i numeri primi. Inoltre, per i numeri di forma 6k, $\varphi(6k) < 2k$;

per es. , per $n = 42 = 6 \times 7$, $\varphi(42) = 12 < 2 \times 7 = 14$, mentre per $n = 36 = 6 \times 6$, $\varphi(36) = 12 = 2 \times 6 = 2k$.

Legami tra formule e griglia delle connessioni

Le connessioni matematiche individuate sono appresso elencate.

funzione φ(n) e funzione μ(n)

$$\sum d\mu\left(\frac{n}{d}\right) = \varphi\left(\frac{n}{d}\right)$$

con d = divisori di n

funzione φ(n) e funzione σ(n)

$n \cdot \sigma(n) \equiv 2 \pmod{\varphi(n)}$
$\equiv 0 \pmod{\varphi(n)}$ se $\varphi(n) \equiv 2$
$\equiv 2 \pmod{\varphi(n)}$ se altrimenti

altra relazione tra φ(n) e σ(n)

$\varphi(\sigma(n)) = n$

Le prime soluzioni trovate da *Helnius* sono per

2, 8, 12, 240, 720, 6912, 32768.

Per es. per n = 12: $\sigma(12) = 28$, $\varphi(\sigma(12)) = \varphi(28) = 12$

Qui notiamo che tutti i numeri trovati da Helnius sono di forma n = 6k oppure n = 6k +2, esempi:

2 = 6 x 0 +2
8 = 6 x 1 +2
12 = 6 x 2
240 = 6 x 40
720 = 6 x 120
6912 = 6 x 1 152
32768 = 6 x 5 461 + 2

Anche qui riappare la forma n = 6k, anche se questa volta insieme alla forma n = 6k + 2, e quindi non da sola come per σ(n) e G(N) dove queste funzioni assumono i valori maggiori rispetto a numeri di forma diversa).

funzione φ(n) e funzione G(N) (Goldbach)

Se la congettura di Goldbach fosse vera, come sostiene il gruppo ERATOSTENE, allora per ogni intero positivo m, esistono due primi p e q tali che:

$\varphi(p) + \varphi(q) = 2m$ (numero pari, quale che sia m)

Infatti, poiché $\varphi(p) = p - 1$ = numero pari (con eccezione per p =2) e $\varphi(q) = q - 1$ = altro numero pari, (sempre con eccezione per q = 2) la somma di due pari è sempre pari (p-1) + (q-1) = p + q – 2, anche questo pari da cui deriva che p + q - 2 = 2m, e che p + q = 2m – 2 anch'esso numero pari, e corrisponde ad N pari = p + q della congettura di Goldbach; per esempio, per p = 23 e q = 37: $\varphi(23) + \varphi(37) = 22 + 36$

= 58 = 2m, mentre p + q = 23 + 37 = 60 = 22 + 36 + 2 = 2m + 2 = N pari somma di due numeri primi diversi da 2, proprio come vuole la congettura di Goldbach (unica eccezione N = 2 + 2 = 4, il numero minimo richiesto per N pari). Infatti, tutti i numeri pari N $\geq$ 4 sono la somma, e anche più volte (esattamente G(N) volte), di G(N) coppie di Goldbach p + q = N; per esempio per N =100 ci sono 6 coppie di Goldbach (e quindi G(100) = 6, e G(N) cresce quasi regolarmente al crescere di N in base ai multipli dispari di 3, dei numeri primi e dei numeri compositi esistenti fino ad N, e non regredisce mai fino a G(N) = 0, contro esempio - peraltro inesistente - della congettura (vedi Figura 25, con l'angolo inferiore privo di valori, zero compreso) e nostra ultima dimostrazione in "Numeri primi in cerca d'autore"). Ricordiamo che per N = 6k, G(N) assume valori di circa il doppio rispetto ai numeri pari vicini di forma N = 6k $\pm$ 2, a causa del ruolo dei multipli dispari di 3 nella formazione delle coppie di Goldbach, ruolo ora perfettamente compreso e che ci ha permesso di dimostrare la congettura forte di Goldbach, e di conseguenza anche della congettura debole (N $\geq$ 7 come somma di tre numeri primi), e questa è, com'è noto, un sottoproblema della GRH.

Segue la griglia di queste e delle altre connessioni tra le varie funzioni e con una delle ipotesi RH equivalenti (indicate nell'ultima colonna a destra)

Griglia delle connessioni

	φ(n)	μ(n)	σ(n)	π(n)	ζ(n)	Θ(n)	Li(n)	L(n)	G(N)	RH
φ(n)	-	si (1)	**si (2)g**	si(9)	si(3)	no	no	si(g)	si(4)g	RH1
μ(n)	-	-	no	si(6)	no	no	no	no	no	RH2
σ(n)	-	-	-	no	no	no	no	si(5)g	si(g)	RH1
π(n)	-	.	-	-	si (**8,10**)	si(7)	no	no	no	RH3
ζ(n)	-	-	-	-	-	no	no	no	no	RH
Θ(n)	-	-	-	-	-	-	no	no	no	RH4
Li(n)	.	.	.	.	.	.	-	no	no	RH
L(n)	-	-	-	-	-	.	.	.	si(g)	RH1
G(N)	-	-	-	-	-	-	-	-	.	RH
										(Tramite GHR e Goldbach deb.)

Tabella 17 - Griglia delle connessioni

Le formule numerate nella griglia per le varie connessioni "si" sono le seguenti:

(1) $\sum_d d\mu\left(\frac{n}{d}\right) = \varphi\left(\frac{n}{d}\right)$

(2) $\varphi(\sigma(n)) = n$ con n = 2, 8, 12, 128, …

(3) $\sum_{n=0}^{\infty} \frac{\varphi(n)}{n^s} = \frac{\xi(s-1)}{\xi(s)}$

(4) $\varphi(p) + \varphi(q) = 2m; \quad p + q = 2m + 2$

(5) $L(n) = H_n + e^{Hn} \cdot \log Hn - \sigma(n)$, con $L(n) > 0$

(6) $$\pi(n) = \sum_n \frac{\mu(n)}{n} J^n \sqrt{x}$$

(7) $\pi(n) \approx Li(n)$

(8) $$\pi(n) \approx \mathrm{Re}(n) = 1 + \sum_{k=1}^{\infty} \frac{1}{k\xi(k+1)} \cdot \frac{\log n^k}{k!}$$

g = grafico simile

Un'altra relazione tra $\varphi(n)$ e $\pi(n)$ è la formula già vista (83), conseguenza della GRH sulle osservazioni di Dirichlet e le L-functions. Se ci si riferisce alle progressioni a n + b, per esempio 4n + 3 o 6n+5 (quest'ultima equivalente a 6(n+1) -1 = 6k -1, che insieme alla 6k+1, è una delle forme generatrici di numeri primi: P = 6k+1 con eccezione del 2 e del 3, e di tutti i prodotti tra primi (senza fattori 2 e 3) e le potenze dei numeri primi. Tali forme possono essere scritte anche come P = 1 +6n, che danno luogo a numeri primi negativi e positivi, in particolari i numeri gemelli diventano -p e + q = p+2, e ora è la loro somma algebrica ad essere uguale a 2, infatti q + (- p) = q - p = 2, e viceversa è la loro differenza algebrica ad essere: q – (- p) = p + q = N = 12n. Le forme $6k \pm 1$ sono state usate per creare algoritmi in [6][7]. Per la relazione (9) di cui sopra possiamo fare due facili esempi. Poiché fino a x = 40 ci sono 5 primi di forma 4a +3 (7, 11, 19, 23 e 31) (dalla progressione 4n+3, con a = b = 7), applicando la (9) abbiamo:

$$5/(40/\log 40) = 5(40/3{,}58) = 5/10{,}86 = 0{,}4604051 \rightarrow 1/\varphi(7) = 1/6 = 0{,}16$$

Mentre per la forma 6n +5 = 6(n+1)-1 = 6n' -1, (con n'= a = 5) fino a x = 40 ci sono anche qui 5 primi (5, 11, 17, 23 e 29) e anche qui abbiamo 0,4604051 ma con tale valore è $1/\varphi(5) = 1/4 = 0{,}25$. Da notare che la forma 4n + 3 dà in ordine numeri primi di forma 6k+1, numeri primi di forma 6k-1 e numeri dispari composti multipli di 3 (se anche n lo è) o multipli di 5, 7, ecc. Ad esempio:

n	4 n	+	3	=	x	
1	4		3		7	primo (=6 x 1 +1)
2	8		3		**11**	primo (= 6 x 2 -1)
3	12		3		15	composto (= 3 x 5)
4	16		3		**19**	primo (= 6 x 3 +1)
5	20		3		**23**	primo (=6 x 4 -1)
6	24		3		27	composto (= 3 x 9)
7	28		3		**31**	primo (= 6 x 5 + 1)
8	32		3		35	composto (= 5 x 7)
9	36		3		39	composto (= 3 x 13)
10	40		3		**43**	primo (= 6 x 7 +1)
11	44		3		**47**	primo (=6 x 8 -1)
12	48		3		51	composto (= 3 x 17)
13	52		3		55	composto (= 5 x 11)
…	…		…		…	…

Mentre le forme 6k +1 e 6 k -1 danno, per ciascuna di loro, circa metà dei numeri primi fino a x , e composti senza fattori 2 e 3:

k	6k -1	6k +1n	
1	**5**	**7**	
2	**11**	**13**	**gemelli**
3	**17**	**19**	**gemelli**
4	**23**	25 = 5 x 5	
5	**29**	**31**	**gemelli**
6	35 = 5 x 7	**37**	
7	**41**	**43**	**gemelli**
8	**47**	49 = 7 x 7	
9	**53**	55 = 5 x 11	
10	**59**	**61**	**gemelli**
11	65 = 5 x 13	**67**	
12	**71**	**73**	**gemelli**
…	…	…	

In tali forme, i numeri gemelli condividono lo stesso k. Poiché i numeri primi si distribuiscono quasi equamente in entrambe le colonne (con leggera preferenza per la forma 6k-1, Eulero), abbiamo che $\pi(N)/2 + \pi(N)/2 \approx \pi(N)$.

Un'altra relazione che permette risultati esatti per il calcolo di $\pi(N)$ tra funzione zeta e funzione $\pi(N)$ è la (63) già vista.

Capitolo 12. Scarabocchi e calcoli finali sulla RH4

Ci sarebbe piaciuto effettivamente riportare il foglietto quadrettato dei calcoli ("scarabocchi") fatti da uno degli autori sulla RH4, sarebbe stato simpatico…

Ma proseguiamo col "volo pindarico" dell'autore di cui prima e vediamo dove atterriamo:

$t = 100\,000 \quad \Theta(100\,000) = 99685{,}4$
$t - \Theta(t) = 100\,000 - 99\,685{,}4 = 314{,}6$
$\sqrt{t} = \sqrt{100\,000} = 316{,}22$

Fin qui nulla di strano, proseguiamo.

Per $\varepsilon = 0{,}1$: $t^{\varepsilon} = 100\,000^{0{,}1} = 3{,}162$
$314{,}6 < 3{,}1622 * 316{,}22 = 999{,}912$

Per $\varepsilon = 0{,}01$: $t^{\varepsilon} = 100\,000^{0{,}01} = 1{,}1220$
$314{,}6 < 1{,}1220 * 316{,}22 = 354{,}80$

Per $\varepsilon = 0{,}001$: $t^{\varepsilon} = 100\,000^{0{,}001} = 1{,}00115$
$314{,}6 < 1{,}00115 * 316{,}22\ldots = 319{,}88\ldots$

Ora la disuguaglianza per la RH4 $\left| \Theta(t) - t \right| < t^{\varepsilon} \sqrt{t}$ fin qui dai calcoli è vera.

Per $t = 1000000$, $\Theta(1000000) = 998484$, $t - \Theta(t) = 1000000 - 998484 = 1516$ non è più tanto vera; ad esempio per $\varepsilon = 0{,}01$ (per $\varepsilon = 0{,}1$ è vera):

$1\,516 > t\,\sqrt[0{,}01]{\ t} = 1{,}148 * 1000 = 1148{,}15$

che è minore di $1\,516 = \Theta(t) = \Theta(1000000)$, anziché maggiore come prevede la disuguaglianza affinché la RH4 sia vera, ma anche per $\varepsilon = 0{,}001$ non è vera, essendo $1516 > 1\,013{,}91$, e cosi via, anche per $\varepsilon = 0{,}0001$, ecc.

Però il numero $\Theta(1000000) = 998\,484$ segnalato dal Prof. Umberto Cerruti nel suo blog sulle ipotesi RH equivalenti è esatto.

Chiesti chiarimenti al gentilissimo Prof. Umberto Cerruti, ci è stato risposto che non si sa quali valori possa assumere n, sebbene connessi a ε, ed utili a completare il lavoro sulle ipotesi RH equivalenti e le funzioni sulle quali si basano.

A questo punto l'autore ha fatto delle congetture ulteriori ("i voli pindarici!"), soprattutto come appunto sul block notes da vagliare opportunamente in futuri lavori.

La funzione $\Theta(t) = \Sigma \log p$ dove la sommatoria è estesa a tutti i numeri primi minori o uguali a t. Andiamo a trattare la RH4 in modo diverso, come:

$$\Re = \frac{10^n}{\theta(10^n)}$$

Costruiamo ora una tabella dei valori di $\Re$

n	**$t = 10^n$**	**$\Theta(10^n)$**	**$\Re$ n**	**$\Re$ n $\approx \sqrt{\ \Re}$ -1**
2	100	83,72	1,194475	$= \Re 2$
3	1000	956,24	1,045762	$= \Re 3 \approx \sqrt[4]{\ \Re 2}$
4	10000	9895,99	1,0105103	$= \Re 4 \approx \sqrt[4]{\ \Re 3}$
5	100000	99685,4	1,003155	$= \Re 5 \approx \sqrt[4]{\ \Re 4}$
6	1000000	998484	1,001518	$= \Re 6\ \sqrt[4]{\ \Re 5}$

Qui notiamo che $\Re 2 = 1{,}194475$ è circa $\sqrt[4]{2}$, poiché $\sqrt{2} = 1{,}4141213562$ e $\sqrt{2} = 1{,}189207115$ è molto vicino a 1,19475 (cosi come nel problema di Basilea il valore 1,6449… per N = 2 è molto vicino a e = $\sqrt{\ }2{,}728$) . I rapporti $\Re$ n discendono ora dalle 2^{4n} -esime potenze di 2, con buona approssimazione. Ora è:

$\sqrt[4]{1{,}194475} = 1{,}45428333 \approx 1{,}45762 = \Re\,\mathbf{3,}$
$\sqrt[4]{1{,}045762} = 1{,}01116859 \approx 1{,}10105103 = \Re\,\mathbf{4}$
$\sqrt[4]{1{,}0105103} = 1{,}00226172 \approx 1{,}003155 = \Re\,\mathbf{5}$
$\sqrt[4]{1{,}003155} = 1{,}00078781 \approx 1{,}001518 = \Re\,\mathbf{6}$

quest' ultimo valore con soli 8 decimillesimi di differenza dal valore reale 1, 00078781. I rapporti $\Re \mathbf{n}$ sono una nuova funzione correttrice, poiché è chiaro che:

$$10^n \approx \Re n * \theta(10^n)$$

e, viceversa:

$$\theta(10^n) \approx \frac{10^n}{\Re n}$$

Un esempio per tutti:

$10\,000 \approx 9895{,}99 \cdot 1{,}0105103 = 9\,999{,}999 \approx 10\,000$

con piccole differenze finali dovute alle cifre decimali non considerate di $\Re n$. Per valori intermedi di t compresi tra 10^n e 10^{n+1}, $\Theta(t)$ è ovviamente compreso tra $\Theta(10^n)$ e $\Theta(10^{n+1})$, in modo direttamente proporzionale, e si può calcolare in modo approssimativo con $\Re n$ relativo alla potenza di 10 più vicina. Per esempio, per t = 900 poco minore di $1000 = 10^3$, con $\Re \mathbf{3} = 1{,}045762$, per cui:

$$\Theta(900) \approx 900/1{,}045762 \approx 860{,}6164$$

valore sicuramente molto vicino al valore reale.

Osserviamo però facilmente che $\Re n$ tende rapidamente a 1($\Re n \rightarrow 1$) con velocità maggiore a causa delle radici quarte, rispetto a tante altre funzioni correttrici o valori, che decrescono invece tramite radici quadrate.

Tali velocità di tendenza a 1, potrebbe essere utile a possibili dimostrazioni delle ipotesi RH equivalente alla quale sono connessi (ad esempio i valori $\Re n$ alla RH4)?

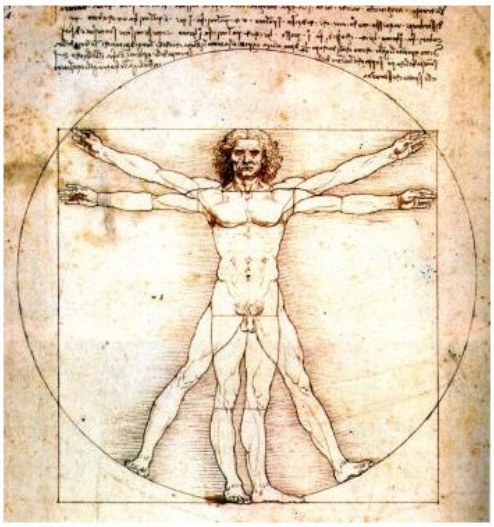
Mentre per la RH1 i valori di $\sigma(n!)$ e di $L(n!)$ tendono all'infinito al crescere di n abbondante come i fattoriali, e i loro multipli, e la somma algebrica S dei valori di M(t) tende lentamente all'infinito con $S \approx \sqrt[8]{t}$ ma il rapporto S/t tende a zero al crescere di t, etc.

Questa tendenza di alcune serie di valori a infinito, a 0 oppure ad 1 va ulteriormente approfondita. Ce l'appuntiamo sul block notes!

Fine dei fogli del block notes . . .

Appendice - Costanti Matematiche

Simbolo	Valore	Nome	Campo	Tipo	Descrizione	Numero cifre conosciute
π	≈ 3,14159 26535 89793 23846 26433 83279 50288	Pi Greco, costante di Archimede o numero di Ludolph	Gen, Ana	*T*	2000 a.C.	1.241.100.000.000
e	≈ 2,71828 18284 59045 23536 02874 71352 66249	Costante di Napier, base dei logaritmi naturali	Gen, Ana	*T*	1618	50.100.000.000
e^{π}	≈ 23,14069 26327	Costante di Gelfond		*T*	1934	
$\sqrt{2}$	≈ 1.41421 35623 73095 04880 16887 24209 69807	Costante di Pitagora, radice quadrata di due	Gen	*A; I*	800 a.C.	137.438.953.444
$\sqrt[3]{2}$	≈ 1,25992 10498 94873 16476 72106 07278	Costante deliana, radice cubica di due	Gen	*A; I*	430 a.C.	
$\sqrt{3}$	≈ 1,73205 08075 68877 29352 74463 41505	Costante di Teodoro di Cirene, radice quadrata di tre	Gen	*A; I*	800 a.C.	1.000.025
γ	≈ 0,57721 56649 01532 86060 65120 90082 40243	Costante di Eulero - Mascheroni	Gen, NuT	I?	1735	108.000.000
ϕ	≈ 1,61803 39887 49894 84820 45868 34365 63811	Rapporto aureo	Gen	*A; I*	III secolo a.C.	3.141.000.000
β^*	≈ 0,70258	Costante Embree-Trefethen	NuT			
δ	≈ 4,66920 16091 02990 67185 32038 20466 20161	Costante di Feigenbaum	ChT	*T*?	1975	1018
α	≈ 2,50290 78750 95892 82228 39028 73218 21578	Costante di Feigenbaum	ChT	*T*?		1018
C_2	≈ 0,66016 18158 46869 57392 78121 10014 55577	Costante dei numeri primi gemelli	NuT			5.020
θ	≈ 1,3063778838630806904 6	Costante di Mills	NuT			7000
M_1	≈ 0,26149 72128 47642 78375 54268 38608 69585	Costante Meissel-Mertens	NuT		1866 - 1874	8.010
B_2	≈ 1,90216 05823	Costante di Brun sui numeri primi gemelli	NuT		1919	10
B_4	≈ 0,87058 83800	Costante di Brun per i numeri primi quadrupli	NuT			
Λ	$> -2{,}7 \cdot 10^{-9}$	Costante Bruijn-Newman	NuT		1950	
K	≈ 0,91596 55941 77219 01505 46035 14932 38411	Costante Catalan	Com	I?		201.000.000
K	≈ 0,76422 36535 89220 66	Costante Landau-Ramanujan	NuT	*I*		30.010
K'	≈ 1,13198 824	Costante di Viswanath	NuT			8
B_L	≈ 1,08366	Costante di Legendre	NuT			
μ	≈ 1,45136 92348 83381 05028 39684 85892 027	Costante Ramanujan-Soldner	NuT			75.500
E_B	≈ 1,60669 51524 15291 763	Costante Erdös-Borwein	NuT	*I*		
β^*	≈ 0,28016 94990	Costante di Bernstein	Ana			
λ	≈ 0,30366 30029	Costante Gauss-Kuzmin-Wirsing	Com		1974	385
e	≈ 0,66274 34193	Limite di Laplace				
λ	≈ 1,30357 72690 34296	Costante di Conway		*A*	1986	
F	≈ 4,52782 95661	Costante di Freiman		*A*		
$e^{e^{e^{79}}}$	$\approx 10^{10^{8.85 \cdot 10^{33}}}$.	Numero di Skewes	Nut		1933	
	≈ 0,11000100000000000000000001	Costante di Liouville	Ana	*T*	1844	
$\zeta(3)$	≈ 1.202056903159594	Costante di Apery	Ana, Nut	I		
i	$=\sqrt{-1}$	Unità immaginaria		*A; C;*		
$\aleph_0$	$= \#\{\mathbb{N}\}$	Aleph-zero, cardinalità dell'insieme dei numeri naturali				



Riferimenti

[1] John Derbyshire, "L'ossessione dei numeri primi: Bernhard Riemann e il principale problema irrisolto della matematica ", Bollati Boringhieri.
[2] J. B. Conrey, "The Riemann Hypothesis", Notices of the AMS, March 2003.
[3] E. C. Titchmarsh, "The Theory of the Riemann Zeta-function", Oxford University Press 2003.
[4] A. Ivic, "The Riemann Zeta-Function: Theory and Applications", Dover Publications Inc 2003.
[5] Proposta di dimostrazione della variante Riemann di Lagarias – Francesco Di Noto e Michele Nardelli – sito ERATOSTENE
[6]Test di primalità, fattorizzazione e $\pi(N)$ con forme $6k\pm1$ - Rosario Turco, Michele Nardelli, Giovanni Di Maria, Francesco Di Noto, Annarita Tulumello – CNR SOLAR Marzo 2008
[7] Fattorizzazione con algoritmo generalizzato con quadrati perfetti in ambito delle forme $6k\pm1$" – Rosario Turco, Michele Nardelli, Giovanni Di Maria, Francesco Di Noto, Annarita Tulumello, Maria Colonnese – CNR SOLAR
[8] Semiprimi e fattorizzazione col modulo – Rosario Turco, Maria Colonnese – CNR SOLAR Maggio 2008
[9] Algoritmi per la congettura di Goldbach - G(N) reale- Rosario Turco – CNR SOLAR (2007)
[10] Il segreto della spirale di Ulam, le forme $6k\pm1$ e il problema di Goldbach – Rosario Turco - R CNR Solar 2008 – The secret of Ulam's spiral, the forms $6k\pm1$ and the Goldbach's problem
http://www.secamlocal.ex.ac.uk/people/staff/mrwatkin/zeta/ulam.htm
[11] Numeri primi in cerca di autore: Goldbach, numeri gemelli, Riemann, Fattorizzazione - Rosario Turco, Michele Nardelli, Giovanni Di Maria, Francesco Di Noto, Annarita Tulumello, Maria Colonnese – CNR SOLAR
[12] Teoria dei numeri e Teoria di Stringa, ulteriori connessioni Congettura (Teorema) di Polignac, Teorema di Goldston –Yldirim e relazioni con Goldbach e numeri primi gemelli" – Michele Nardelli e Francesco Di Noto – CNR SOLAR Marzo 2007;
[13] Teoremi sulle coppie di Goldbach e le coppie di numeri primi gemelli: connessioni tra Funzione zeta di Riemann, Numeri Primi e Teorie di Stringa" Nardelli Michele e Francesco Di Noto- CNRSOLAR Luglio 2007;
[14] Note su una soluzione positiva per le due congetture di Goldbach" - Nardelli Michele, Di Noto Francesco, Giovanni Di Maria e Annarita Tulumello - CNR SOLAR Luglio 2007
[15] Articoli del prof. Di Noto – sito gruppo ERATOSTENE
[16] I numeri primi gemelli e l'ipotesi di Riemann generalizzata", a cura della Prof. Annarita Tulumello

Ripassi veloci e approfondimenti

[17] Super Sintesi "Per chi vuole imparare in fretta e bene" MATEMATICA - Massimo Scorretti e Mario Italo Trioni – Avallardi
[18] Introduzione alla matematica discreta – Maria Grazia Bianchi e Anna Gillio – McGraw Hill
[19] Calcolo delle Probabilità – Paolo Baldi – McGraw Hill

[20] Random Matrices and the Statistical Theory of Energy Level – Madan Lal Metha
[21] Number Theoretic Background – Zeev Rudnick
[22] A computational Introduction to number theory and Algebra – Victor Shoup
[23] An Introduction to the theory of numbers – G.H. Hardy and E.M. Wright
[24] A Course in Number Theory and Crittography – Neal Koblitz

Blog famosi

[25] http://alpha01.dm.unito.it/personalpages/cerruti/luglio04.gennaio28.html **Blog del Prof. Cerruti**

Email per suggerimenti e segnalazioni

mailto:rosario_turco@virgilio.it

Siti vari

CNR SOLAR
http://150.146.3.132/

Aladdin's Lamp (ing. Rosario Turco)
www.geocities.com/SiliconValley/Port/3264 menu' MISC sezione MATEMATICA

gruppo ERATOSTENE
http://www.gruppoeratostene.com o precedente sito http://www.gruppoeratostene.netandgo.eu

dott. Michele Nardelli
http://xoomer.alice.it/stringtheory/