Università degli studi di Messina
SISSIS
Scuola Interuniversitaria Siciliana di Specializzazione
per l’Insegnamento Secondario
VI ciclo – classe 49A

Storia della Matematica

I buchi neri della matematica:
I numeri primi

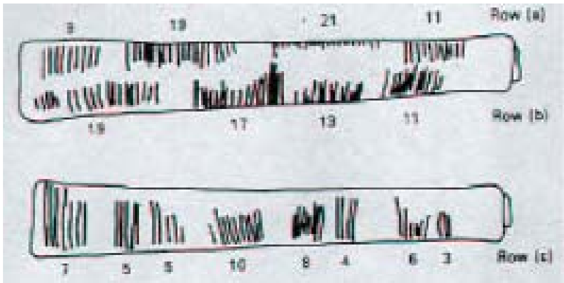
Prof. V. Carfì

a cura di:
Giulio Stringelli

E-mail: giuliostring@alice.it

Ad Ishango conoscevano già i numeri primi?

Il Belgio e la comunità scientifica internazionale hanno spolverato un ossicino scuro, dimenticato da oltre 50 anni negli archivi del museo delle scienze naturali di Bruxelles, che potrebbe essere la prima calcolatrice della storia umana.



L`"osso di Ishango", scoperto nel 1950 dall`archeologo Jean de Heinzelin in Congo, durante degli scavi nell`area dell`antica città di Ishango, è stato riscoperto grazie fra l`altro alla Cnn, che ha ricostruito la sua probabile storia.

L`ossicino, coperto da 168 segnetti regolari, isolati o a gruppi, sarebbe la più antica testimonianza di un ragionamento matematico umano, e costringerebbe ad una revisione delle teorie che finora facevano risalire la nascita della matematica agli egiziani, 5000 anni or sono. I primi matematici conosciuti sarebbero stati quindi gli abitanti di Ishango, allora fiorente centro commerciale africano situato nella zona oggi al confine fra Congo e Rwanda (sul lago Edoardo al confine tra Zaire e Rwanda), 15.000 anni fa.

L`ossicino è attualmente al centro di uno studio per decifrarne il sistema e il criterio in cui sarebbero stati posti i 168 segni.
La suddivisione delle tacche è così disposta:

- riga a): 9 19 21 11 - totale 60
- riga b): 19 17 13 11 - totale 60
- riga c): 7 5 5 10 8 4 6 3 - totale 48

Una mappa astronomica?

Le 168 tacche descritte sono suddivise come sopra secondo il Marshack rappresenterebbe una sequenza di calcoli per la registrazione di giorni che comprendono circa cinque lunazioni e mezze, avute all'incirca nel 8500 a.c..

E se fossero un sistema di numerazione?

Sebbene non vi sia accordo tra gli studiosi sulla natura delle incisioni, si può quasi sicuramente affermare che la popolazione neolitica di Ishango possedeva il *concetto di numero*.
Esaminiamo attentamente la riga b (19, 17, 13, 11) contiene tutti i numeri primi compresi tra 10 e 20!

Era un pezzo di un puzzle composto da ossi che rappresentava una tavola di numeri primi ed un sistema si numerazione? Sembra proprio di si, ed allora dovremmo shiftare all'indietro almeno 3500 anni la nascita del concetto di numero, e forse anche l'odissea, ancor non conclusa, della ricerca dei primi e della loro struttura.

I greci e gli "Atomi della matematica"

Da Ishango fino ai greci sono trascorsi più di otto millenni, e il concetto di numero ebbe di certo una definizione migliore (almeno documentabile in modo migliore), e per primi i greci furono affascinati dalla proprietà singolare che avvolgeva di mistero i numeri primi, cioè il non essere prodotto di due interi primi minori, oppure un prodotto finito di numeri primi minori, ecco che fa capolino il concetto di fattorizzazione. Fattorizzazione che esordisce come semplice esercizio matematico per scomporre i numeri i fattori primi, ma che nella storia è diventata un tormento che ha turbato le notti insonni dei matematici e le notti criminali degli *Hacker*. Illustriamo un pò cosa i greci erano riusciti ad ottenere in materia di fattorizzazione, e presso le scuole filosofiche era noto, ancor prima di Euclide che:

Ogni intero è esprimibile come prodotto di primi

Ed la dimostrazione veniva fatta così:

Sia n non primo $\Rightarrow\ n = a \cdot b$ *. Se a e b sono primi, la tesi è dimostrata.*

Se a e b non primi $\Rightarrow\ a = c \cdot d\ ,\ b = e \cdot f$ *con c,d < a e e,f < b.*

Se c,d,e,f sono primi la tesi è dimostrata; altrimenti si continua a scomporre in fattori finchè alla fine si ottiene che:

$n = p_1 \cdot p_2 \cdots p_r$ *con* $p_1 \cdot p_2 \cdots p_r$ *numeri primi.*

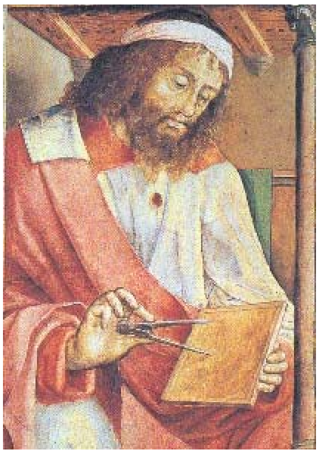
Da qui nacque un'idea che poteva risultare fondamentale per la risoluzione di tutte le problematiche legate all'aritmetica. L'idea fu che i numeri primi fossero in numero finito. Ciò avrebbe permesso di costruire una sorta di schema o "Tavola di Mendelev" capace di descrivere tutti i paesaggi dei numeri. Insomma con i numeri primi finiti, atomi della matematica si poteva costruire tutte le molecole ricorrendo sempre agli stessi atomi. Questo sogno greco si collocava nel desiderio di controllare l'anima sfuggente dei numeri, l'anima della stessa natura delle cose che si esprime tramite essi, l'anima dell'universo e degli astri che pulsano. Appena nata (si fa per dire) già destava preoccupazione nell'affrontarla, e costringeva ad un "superlavoro" coloro che tentavano di dipingerne le sembianze. Sembrava che si potesse conoscere la grande "tastiera" dei numeri e poter suonare il ritmo della matematica, ritmo che si ascoltava quando si tentava di filosofare sulla risoluzione dei problemi con riga e compasso.

Quanti erano i primi era la domanda fondamentale, ma i più si chiedevano se fosse possibile individuare una qualche relazione nel loro presentarsi in mezzo a tutti gli altri numeri, e quindi interpretarne e seguirne il ritmo del loro presentarsi. Già in molti si interrogavano circa quale cosa, divina o diabolica, si celasse dietro tali numeri che improvvisamente comparivano a raffica nello scacchiere dei numeri e che altrettanto improvvisamente si rendevano difficili da trovare. M. du Sautoy definisce in "L'enigma dei numeri primi" questo altalenante comportamento come i colpi dati su un tamburo, e ciò che ne scaturiva era il ritmo della matematica, improvviso, sfuggente, ma presente sempre.

0 1 **2 3** 4 **5** 6 **7** 8 9 10 **11** 12 **13** 14 15 16 **17** 18 **19** 20 21 22 **23** 24 25 26 27 28 **29** 30 **31** 32 34 35 36 **37** 38 39 40 **41** 42 **43** 44 45 46 **47** 48 49 50 51 52 **53** 54 55 56 57 58 **59** 60 **61**

Ecco allora il primo matematico della storia che spezza un sogno dell'umanità, parimenti a quello che fece Godel 2300 anni più tardi: Euclide.

Euclide e numeri primi infiniti



Euclide (350 – 300 a.C. circa) spezzò dunque il sogno di poter controllare la matematica tramite una “tastiera” finita, ma spalancò le porte ad uno dei concetti che ha caratterizzato per altri versi la matematica, l’infinito. La particolarità dell’infinito scoperta da Euclide era quella che una parte dei numeri naturali sia infinita come i numeri naturali stessi (per dirla con le nostre conoscenze, aveva scoperto un sottoinsieme proprio dei naturali con cardinalità infinita). Questo problema non fu percepito dai greci come tale ma di certo gettò ancor più nel mistero questi oggetti speciali fatti di una materia “pregiata”. La stessa cosa causò molta speculazione da parte dei matematici di tutti i tempi e motivò i loro studi alla scoperta dell’infinito, fin quando George Cantor aprì le porte del “paradiso” e Riemann si accorse di una qualche “magia” che legava tra loro tutte le perle della collana dei numeri.
Euclide nel VII libro degli *Elementi* enuncia quello che in seguito passerà alla storia come il ***teorema fondamentale dell’aritmetica***, è il seguente:

Ogni numero intero maggiore di 1 si decompone in un unico modo come prodotto di numeri primi.

Secondo la Definizione XI del **Libro VII** degli *Elementi* di Euclide,

Definizione XI: *un numero primo è un numero intero maggiore di 1 che ammette come divisori (positivi) solo se stesso e 1.*
Si può dimostrare che il teorema in questione è conseguenza di due enunciati euclidei, tratti dallo stesso

Libro VII:

Proposizione 30: *Se un numero primo è un divisore del prodotto di due numeri, è divisore di uno dei due numeri.*

Proposizione 31: *Ogni numero composto (cioè, non primo) ha per divisore un numero primo.*
Questo primo passo permise di affermare l’esistenza e l’unicità della scomposizione in fattori primi, ma lascia aperta la questione di quanti fossero i numeri primi. Questo problema solleticò a tal punto Euclide che cimentandosi in questo problema, non riuscì a generare esplicitamente numeri primi e dimostrarne così l’infinità, ma avvalendosi della potente dimostrazione greca *per assurdo* riuscì ad affermare:

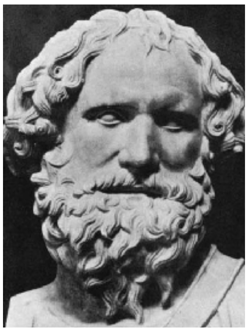
Libro IX

Proposizione 20**:** *Esistono infiniti numeri primi. (Teorema di Euclide)*

La dimostrazione del Teorema di Euclide è considerata una delle “gemme” della matematica antica. Supponiamo dunque per assurdo che esista solamente un numero finito di primi e che questi siano esattamente $p_1<p_2<\cdots<p_k$. *Allora il numero* $N=p_1p_2\cdots p_k + 1$ *non può essere anch'esso primo (perché non è presente nell'elenco precedente); d'altronde, siccome* N *non è divisibile per alcun* p_i, $i=1, \ldots, k$, *deve anch'esso essere primo. Il che è chiaramente una contraddizione. Dunque l'insieme dei numeri primi non può essere finito e quindi il Teorema di Euclide è dimostrato.*

Così Euclide lasciò la imponente eredità della prova dell'esistenza dei numeri primi, ma non riuscì a risolvere il problema della generazione degli stessi, così la rincorsa verso il trampolino di lancio di una qualche struttura d'ordine o di qualche legge che regolasse la scansione del tempo dei numeri primi cominciò.

Eratostene (290 -195 a.c. circa) e il suo crivello.



Nato a Cirene, colonia greca in Libia, intorno al 290 a.C., fu allievo di Callimaco ad Alessandria, per poi proseguire gli studi ad Atene, dove si accostò allo Stoicismo e all'Accademia platonica.

Nel 245, dopo la morte di Callimaco, Eratostene venne richiamato alla corte di Alessandria da Tolomeo III Evergete, come direttore della Biblioteca dopo Apollonio Rodio e precettore dell'erede al trono, Tolomeo IV. Eratostene, anche per la sua carica di bibliotecario, intrattenne rapporti con i maggiori scienziati del tempo, tra cui il siracusano Archimede, che gli dedicò un trattato. Si ritiene che sia morto intorno al 195.

La sua vita fu costellata di studi di carattere geografico-climatico, filosofico, critica letteraria e poesia, ma fu il primo a dettare un algoritmo possibile per la ricerca dei numeri primi, il suo celeberrimo algoritmo è conosciuto in letteratura come il crivello di Eratostene. Egli produsse una tavola dei numeri primi che si trovano nei primi 1000 numeri interi, il tutto fu fatto con un algoritmo semplice, ma di onerosa complessità computazionale, ecco i passi:

- si scrivono tutti gli interi fino a N;

- si cancellano i multipli di 2, poi i multipli di 3 (il primo intero non cancellato), poi i multipli di 5 (il nuovo primo intero non cancellato), e così via;

- arrivati a $\sqrt{N}$ *ci si ferma: i numeri non cancellati sono tutti e soli i primi fino a N.*

Supponiamo, ad esempio, di voler trovare i numeri primi minori di 100. Scriviamo tutti i numeri compresi tra 2 e 100 in una tabella.

	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100

Ora cancelliamo tutti i multipli di 2

	2	3		5		7		9		11		13		15		17		19	
21		23		25		27		29		31		33		35		37		39	
41		43		45		47		49		51		53		55		57		59	
61		63		65		67		69		71		73		75		77		79	
81		83		85		87		89		91		93		95		97		99	

Ora cancelliamo tutti i multipli di 3 (nota che alcuni, quelli pari, sono già scomparsi):

	2	3		5		7				11		13				17		19	
		23		25				29		31				35		37			
41		43				47		49				53		55				59	
61		63				67				71		73				77		79	
		83		85				89		91				95		97			

Ora cancelliamo tutti i multipli di 5 e di 7 (quelli rimasti, almeno):

	2	3		5		7				11		13				17		19	
		23						29		31						37			
41		43				47						53						59	
61						67				71		73						79	
		83						89								97			

Chi ebbe a misurarsi con la tavola dei primi prodotta da Eratostene sicuramente rimase turbato dalla disposizione dei numeri primi nelle tavole, dal loro raggrupparsi e dilatarsi improvvisamente, come dei colpi di tamburi dati dal fato, casualmente, che scandiscano il tempo della matematica.

Il lavoro di Eratostene rimane l'unico algoritmo di generazione dei numeri primi che dall'antichità giunse nel medioevo tramite l'era oscurantista. Dunque il problema rimase sopito per più di mille anni, per riaffiorare significativamente nel XVII secolo dove i primi matematici "giocherelloni" congetturarono alcune possibili soluzioni, delegando ad altri di dimostrare le loro asserzioni.

Fermat (1601 – 1665) e la ripresa della sfida

Forse il più brillante matematico del suo tempo, Fermat era in realtà un dilettante; dopo gli studi in diritto svolse infatti l'attività di avvocato, dedicando allo studio della matematica il tempo libero. Tale era però il suo talento che riuscì a dare numerosissimi contributi allo sviluppo di questa scienza, assai più dei matematici di professione. Purtroppo pubblicò poco dei suoi lavori e anzi spesso il merito delle sue scoperte fu inizialmente attribuito ad altri. Si occupò da principio della traduzione di alcune opere matematiche dell'antichità. Trattò poi di numerose questioni di geometria analiticia, dei luoghi geometrici nel piano cartesiano e si occupò delle proprietà delle rette e delle coniche.

Elaborò un ingegnoso metodo per la ricerca dei massimi e minimi di una funzione, introducendo i concetti fondamentali del calcolo differenziale. Ideò un metodo per il calcolo delle aree, anticipatore dei metodi del calcolo integrale. Diede importanti contributi anche nella teoria dei numeri, tra cui il famosissimo "ultimo teorema di Fermat" sulla scomponibilità delle potenze di numeri interi.

Pierre Fermat incarna forse lo spirito puro del matematico che si occupa di teoria dei numeri, infatti egli amava giocare e trastullarsi con i numeri per trovare sempre nuove relazioni. In questo secolo di certo la comunicazione tra studiosi dello stesso argomento era alquanto difficoltosa, ma lo scambio epistolare era molto diffuso, Fermat utilizzava questo mezzo per comunicare all’amico Mersenne i risultati ottenuti. Proprio in una di queste lettere evidenzia una questione importante su come poter generare dei numeri primi (anche se non tutti gli elementi potevano essere coperti) e quindi anche se parzialmente dare una prima struttura d’ordine a questi “sfuggenti tesori”. Mersenne, matematico e filosofo, vissuto nello stesso periodo di Fermat non era un semplice amico, ma era colui che a quell’epoca di occupava dei “dispacci scientifici” e delle “pubblicazioni”, ma questo argomento lo tratterò in seguito.

Tra i suoi vari giochi Fermat, ebbe a scontrarsi con un risultato che apparentemente poteva essere accettabile, ma funzionò limitatamente; questo tipo di congettura prese in letteratura il nome di ***numeri di Fermat*** e fu comunicata per via epistolare a Mersenne il quale stuzzicato nella sua curiosità si occupò personalmente dei numeri primi, come vedremo.

Numeri di Fermat: $F_N = 2^{2^N} + 1$ *con N naturale è un numero primo*. (n-ennesimo numero di Fermat)

Non fu data una dimostrazione, ma nelle sue notti insonni Fermat aveva provato che:

per N = 0 $F_0 = 2^{2^0} + 1 = 2 + 1 = 3$ Numero primo

per N = 1 $F_1 = 2^{2^1} + 1 = 4 + 1 = 5$ Numero primo

per N = 2 $F_2 = 2^{2^2} + 1 = 16 + 1 = 17$ Numero primo

per N = 3 $F_3 = 2^{2^3} + 1 = 256 + 1 = 257$ Numero primo

per N = 4 $F_4 = 2^{2^4} + 1 = 65536 + 1 = 65537$ Numero primo

Provata l’esistenza dei primi quattro numeri di Fermat per N = 1,2,3,4 (quindi provato il fatto che fossero realmente dei numeri primi), con solo carta e penna e tanta tanta passione, il “giocherellone” non resistette di comunicare tale

Ecco i primi cinque:
$F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$.
Questi cinque interi sono primi, e ciò condusse Fermat a formulare l'ipotesi che gli F_n siano primi per ogni n.
Questa ipotesi fu comunicata all'amico Mersenne dunque, e per i mezzi di quel tempo sembrò resistere. Questo primo risultato attivò tutte le intelligenze eccellenti in campo matematico, fin quando Leonard Eulero finì con lo scomporre il quinto numero di Fermat.

Ecco il primo problema della congettura di Fermat,
$F_5 = 2^{2^5} + 1 = 4294967296 + 1 = 4294967297$
Trovare i fattori primi di questo naturale era un impresa titanica nel XVII secolo e si pensò che fosse un primo, ma all'inizio del XVIII secolo, esattamente nel 1732 Eulero però scoprì che

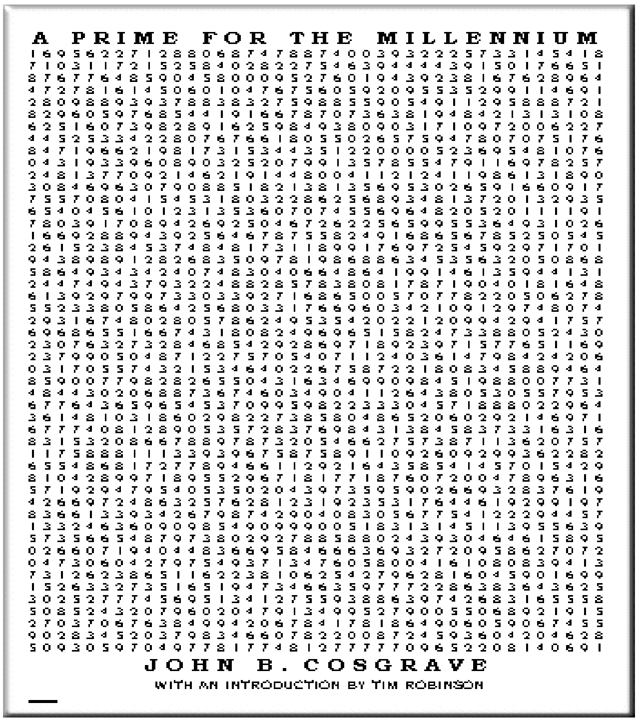
ogni divisore primo di F_n è della forma $k \cdot 2^{n+2} + 1$.

Nel caso di F_5, per k=1,2,3,4,5 troviamo 129, 257, 385, 513, 641; solo 257 e 641 sono primi, e 641 divide F_5, infatti

$F_5 = 4294967297 = 641 \cdot 6700417$

Questo non precluse però la strada alla ricerca dei numeri di Fermat, infatti si ritiene molto probabile che i numeri di Fermat primi siano in numero finito.

Altri importanti risultati li ottenne Gauss grazie ai numeri di Fermat; Gauss dimostrò che si può costruire con riga e compasso un poligono regolare con n lati se e solo se n è il prodotto di una potenza di 2 per un prodotto finito di numeri di Fermat primi e distinti.



Questo è un risultato straordinario e sorprendente (a soli 18 anni). Per esempio ne segue che si può costruire con riga e compasso un poligono regolare con 17 lati, ma non un con 13 o 19 lati! Ma ancor di più Gauss così riuscì a provare che con riga e compasso fosse possibile disegnare una figura con 65537 lati, equivalente al quarto numero di Fermat.
La difficoltà nel trattare i numeri di Fermat sta nel fatto che crescono in modo doppiamente esponenziale e diventano grandissimi con estrema rapidità al crescere di n.
Alcuni fattori primi dei numeri di Fermat hanno dimensioni spettacolari! Recentemente ***John B. Cosgrave***[1] ha trovato un divisore primo di $\boldsymbol{F_{2145351}}$ (sic). Questo numero primo possiede ben 645817 cifre, ed è $3 \cdot 2^{2145353}+1$. E' il quinto numero primo oggi noto (in ordine di grandezza ovviamente) ed è il più grande oggi noto tra i primi non - **Mersenne**

[1] Ordinario presso St Patrick College in Dublino, presidente del dipartimento di Matematica. Inoltre Cosgrave detiene il record con il numero di primo con il maggior numero di cifre, però non si tratta si un numero di Fermat, bensì di un numero di Mersenne.

La storia di questo primo tentativo di trovare dei numeri primi tramite una determinata formula non si è ancora fermata, o quanto meno è ancora ambito di ricerca, vuoi per la generazione di numeri primi (sempre che ne esistano per n > 4), vuoi per la generazione di divisori primi di numeri di Fermat.

L'opera di Fermat non si fermò a questo primo passo, scoprì ancora un risultato che portava alla luce delle proprietà sui numeri primi, la più famosa è:

i numeri primi che divisi per 4 ammettevano resto 1 , posso essere scritti in modo unico come somma di due quadrati

dunque la questione numericamente si può impostare così:

se 4n + 1 è un numero primo, per n naturale $\Rightarrow$ *esistono e sono unici a,b naturali tali che* $a^2 + b^2 = 4n + 1$

Verifichiamo l'affermazione:

se n = 7 $4(7) + 1 = 29 = 2^2 + 5^2$

se n = 9 $4(9) + 1 = 37 = 1^2 + 5^2$

se n = 13 $4(13) + 1 = 53 = 2^2 + 7^2$

scrisse durante il giorno di Natale 1640 di possedere la dimostrazione di questa proprietà, ma fu una grande beffa aggravata dal fatto che proprio a Mersenne indicò i primi ipotetici passi di una dimostrazione. (burlone!)

Più importante fu invece il celeberrimo PTF (Piccolo Teorema di Fermat), congetturato e parzialmente dimostrato dallo stesso Fermat, che costituisce tutt'oggi un test attendibile per la primalità di n numero. La dimostrazione del teorema e l'estensione dello stesso fu effettuata da Eulero.

<u>Piccolo Teorema di Fermat</u>: *se p è un numero primo, allora per ogni numero naturale b appartenente all'intervallo aperto (0,p) si ha:*

$$b^p \equiv b(\mathrm{mod}\, p)$$

oppure nella forma equivalente

$$b^{p-1} \equiv 1(\mathrm{mod}\, p)$$

questo teorema può essere facilmente verificato con alcuni esempi:

i numeri 2,3,5 sono primi e soddisfano il PTF

$1^2(\mathrm{mod}\, 2) = 1;$

$1^3(\mathrm{mod}\, 3) = 1;$ $2^3(\mathrm{mod}\, 3) = 2;$

$1^5(\mathrm{mod}\, 5) = 1;$ $2^5(\mathrm{mod}\, 5) = 2;$ $3^5(\mathrm{mod}\, 5) = 3;$ $4^5(\mathrm{mod}\, 5) = 4$

Alcune sfaccettature di questo teorema hanno permesso di creare un test, usato ancora nelle *release* avanzate.

Test di Fermat

Dal PTF discende una equivalenza logica del teorema che è:
se esiste un numero naturale b appartenente all'intervallo aperto (0,p), per il quale:

$$b^p \pmod p$$

è diverso da b, allora p è un numero composto.

Così ad esempio per il numero *p=4* è:

$$1^4 \pmod 4 = 1; \quad 2^4 \pmod 4 = 1; \quad 3^4 \pmod 4 = 1$$

per cui *4* è, come ci attendeva, composto.

E' lecito a questo punto chiedersi:

se per ogni b, appartenente all'intervallo aperto (0,p), è:

$$b^p \pmod p = b$$

si può affermare che p è un numero primo ?
Purtroppo no.

Esistono infatti numeri composti come:
- *561* (il prodotto di *3*, *11* e *17*)
- *1729* (il prodotto di *7*, *13* e *19*)

che, in relazione al piccolo teorema di Fermat, *si comportano come se fossero primi.*
Siffatti numeri sono detti ***numeri di Carmichael***.

Esistono anche numeri composti che, in relazione al piccolo teorema di Fermat, si comportano come se fossero primi, ***ma non per tutti i valori di b dell'intervallo aperto (0,p).***

Per il numero composto *341* (il prodotto di *11* e *31*), è infatti:

$$1^{341} (\mathrm{mod}\, 341) = 1$$
$$2^{341} (\mathrm{mod}\, 341) = 2$$
$$3^{341} (\mathrm{mod}\, 341) = 168$$
$$4^{341} (\mathrm{mod}\, 341) = 4$$
$$5^{341} (\mathrm{mod}\, 341) = 335$$
$$6^{341} (\mathrm{mod}\, 341) = 336$$
$$7^{341} (\mathrm{mod}\, 341) = 51$$
$$8^{341} (\mathrm{mod}\, 341) = 8$$
$$9^{341} (\mathrm{mod}\, 341) = 262$$

…………………………

In tal caso si dice che ***341*** è uno ***pseudoprimo*** in base 1 - 2 - 4 - 8 - 15 - 16 - 23 - 27 - 29 - 30 - 31 - 32 - 33 - 35 - 39 - 46 - 47 - 54 - 58 - 60 - 61 - 62 - 63 - 64 - 66 - 70 - 77 - 78 - 85 - 89 - 91 - 92 - 93 - 94 - 95 - 97 - 101 - 108 - 109 - 116 - 120 - 122 - 123 - 124 - 125 - 126 - 128 - 132 - 139 - 140 - 147 - 151 - 153 - 154 - 155 - 156 - 157 - 159 - 163 - 170 - 171 - 178 - 182 - 184 - 185 - 186 - 187 - 188 - 190 - 194 - 201 - 202 - 209 - 213 - 215 - 216 - 217 - 218 - 219 - 221 - 225 - 232 - 233 - 240 - 244 - 246 - 247 - 248 - 249 - 250 - 252 - 256 - 263 - 264 - 271 - 275 - 277 - 278 - 279 - 280 - 281 - 283 - 287 - 294 - 295 - 302 - 306 - 308 - 309 - 310 - 311 - 312 - 314 - 318 - 325 - 326 - 333 - 337 - 339 - 340.
In tutto dunque ***120*** **basi su 340.**

Il numero composto ***91*** (il prodotto di *7* e *13*), è uno ***pseudoprimo*** in base 1 - 3 - 4 - 9 - 10 - 12 - 13 - 14 - 16 - 17 - 22 - 23 - 25 - 26 - 27 - 29 - 30 - 35 - 36 - 38 - 39 - 40 - 42 - 43 - 48 - 49 - 51 - 52 - 53 - 55 - 56 - 61 - 62 - 64 - 65 - 66 - 68 - 69 - 74 - 75 - 77 - 78 - 79 - 81 - 82 - 87 - 88 e 90.
In tutto dunque ***48 basi su 90.***
Il numero composto ***15*** (il prodotto di *3* e *5*), è uno ***pseudoprimo*** in base 1 - 4 - 5 - 6 - 9 - 10 - 11 e 14.
In tutto dunque ***8 basi su 14.***
Fortunatamente, se confrontati con i numeri primi, i numeri di Carmichael, numeri pseudoprimi in ogni base, sono molto rari, non altrettanto i numeri pseudoprimi per alcune basi (come i numeri di cui sopra: *341*, *91* e *15*).
Scegliamo adesso a caso una base, ad esempio del numero pseudoprimo *15*.
La probabilità che quest'ultimo non venga riconosciuto come numero composto dal test di Fermat vale: *8/14=0,57*.
Se risottoponiamo al test di Fermat, con una nuova base, di nuovo il numero pseudoprimo *15*, la probabilità che quest'ultimo non venga ancora una volta riconosciuto come numero composto vale ora: *7/13=0,54*.
Se si continua, le probabilità che si ottengono sono:

- *6/12=0,5*
- *5/11=0,45*
- *4/10=0,4*
- *3/9=0,3*
- *2/8=0,25*
- *1/7=0,14*.

Che, come si vede, tendono a decrescere**.**
E' importante a questo punto chiedersi:
se il numero pseudoprimo 15 non viene riconosciuto come numero composto per 4 volte consecutive, che probabilità ha di superare per la quinta volta il test di Fermat ?
La risposta è: ***0,07****=0,57*0.54*0.5*0,45*.

Esclusi i numeri di Carmichael, risulta che i

numeri pseudoprimi per alcune basi, sono tali, per un numero di basi b, che, al più, è circa la metà di quelli compresi nell'intervallo aperto (0,p).

Se dunque il controllo della primalità è su un numero *p* molto grande, scegliendo a caso *100* basi differenti, la probabilità che un numero pseudoprimo non venga riconosciuto come numero composto, nemmeno al 101-esimo test, è all'incirca minore o uguale di:

$$\frac{1}{2^{100}} = \frac{1}{2^{10^{10}}} = \frac{1}{1024^{10}} \cong \frac{1}{10^{30}}$$

Un numero dunque che non venga, ***dopo 100 tentativi***, riconosciuto come numero composto, dal test di Fermat, è ***quasi certamente un numero primo***.

Martin Mersenne (1588 – 1648) e l'influenza di Fermat

Scienziato e filosofo francese, Marin Mersenne nacque a La Soultière, presso Oizé, Maine nel 1588, e morì a Parigi nel 1648**.** Dopo un biennio di teologia alla Sorbona, entrò, nel 1611, nell'ordine religioso dei Minimi per insegnare filosofia, e, dal 1619, si stabilì nel convento parigino dell'Annunziata, in cui rimase,fatta eccezione per alcuni brevi viaggi - fino alla morte. Insegnò a Nevers e, dal 1620, si stabilì a Parigi. Amico e corrispondente dei principali esponenti della cultura del tempo (Cartesio, Hobbes, Fermat, Huygens, Torricelli, Gassendi), divenne il centro di collegamento di quanti, al di fuori della vecchia cultura universitaria, si occupavano con serietà di ricerche e dibattiti in largo senso scientifici.

Nelle vesti informali di segretario della repubblica delle lettere dell'epoca , grazie alle periodiche riunioni da lui tenute nel 1666, presso il convento dell'Annunziata, trasse origine l'Accademia delle Scienze. I contributi scientifici di Mersenne spaziano su un ampio fronte di argomenti, estendendosi dall'esegesi biblica alla filosofia, dalla meccanica alla teorica musicale e all'acustica, dalla geometria all'ottica, dalla pneumatica alla linguistica. Al di là degli esiti specifici di questa intensa attività di ricerca, Mersenne svolse un ruolo particolarmente rilevante nell'organizzare la cultura europea del tempo. Il Minimo francese favorì le relazioni tra i dotti, mettendoli in contatto e promuovendone il dibattito e la cooperazione scientifica. Mersenne è noto anche per essere stato in Francia, a lungo, il punto d'incontro di un gruppo di studiosi che per suo mezzo si comunicavano le principali scoperte scientifiche che venivano fatte in Europa e i principali contributi filosofici che si venivano elaborando nei vari paesi. Nelle vesti informali di segretario della repubblica delle lettere dell'epoca, Mersenne partecipò attivamente al dibattito sui problemi del vuoto, soprattutto a partire dal viaggio in Italia effettuato nel 1644. In quella occasione, egli ebbe modo di assistere ad alcuni esperimenti barometrici e di discutere con i principali esponenti del movimento scientifico italiano, diffondendone, poi, in ambiente francese, le acquisizioni.

I dialoghi epistolari tenuti con Fermat e con altre grandi menti illustri fece si che Mersenne si accorse di una relazione capace di generare numeri primi, meglio di quella ideata dallo stesso Fermat, anche coadiuvato dallo studio dei numeri perfetti di Euclide.

Mersenne, nella prefazione alla sua ***Cogitata Physico Mathematica***, affermò che:
$M_n = 2^n - 1$ *è primo per* n_p*= 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257 e per nessun'altro numero n minore di 257. (*M_n *sarà chiamato n-esimo numero di Mersenne)*

Tale affermazione si è però rivelata successivamente inesatta in quanto si è scoperto che $2^{67}-1$ e $2^{257}-1$ non sono primi. Inoltre, altri esponenti inferiori a 257, danno luogo a numeri primi: n = 61, 89, 107.

La ricerca dei numeri di Mersenne da Eulero in poi ebbe una risonanza planetaria, e tutti gli algoritmi e test di primalità si cimentarono con questi elefantiaci numeri con un numero di cifre impressionanti.

L'ultima svolta della ricerca dei numeri di Mersenne si ebbe negli anni 90, quando partì il Great Internet Mersenne Prime Search (GIMPS), un progetto che vede impegnati computer di tutto il mondo a testare la primalità dei numeri di Mersenne. Il progetto prevede la decomposizione di un algoritmo di primalità in N parti, e sfrutta la potenza di calcolo di tutti i computer che aderisco al progetto bandito dall'Elettronic Frontier Found. Il progetto consiste nel processare la primalità dei numero primi con un test simile a quello di Fermat, dunque tutti i numeri minori di p vengono suddivisi in tranche e si inizia a processare. Chi avrà la fortuna provare che sia prima avrà scritto il suo nell'albo d'oro di coloro che hanno trovato dei numeri di Mersenne per primi, ed inoltre al momento del rilascio del software condiviso, l'Electronic Frontier Foundation offre un premio di $100,000 alla prima persona o gruppo di persone che scopra un numero primo di Mersenne con almeno 10 milioni di cifre. Chiunque può avere un posto nella lista dell'immortalità. Si pensa che i numeri di Mersenne siano infiniti, ma manca ancora una dimostrazione di ciò. La ricerca continua...

##	*n*	Cifre in M_n	year	Discovered
1/4	2-3-5-7	1-2	----	----
5	13	4	1456	Anonymous
6/7	17-19	6	1588	Castaldi
8	31	10	1772	Euler
9	61	19	1883	Pervushin
10/11	89/107	27/33	1911/14	Powers
12	127	39	1876	Lucas
13/14	521/607	157/183	1952	Robinson
15/16	1279/2203	386/664	1952	Robinson
17	2281	687	1952	Robinson
18	3217	969	1957	Riesel
19	4253	1281	1961	Hurwitz
20	4423	1332	1961	Hurwitz
21	9689	2917	1963	Gillies
22	9941	2993	1963	Gillies
23	11213	3376	1963	Gillies
24	19937	6002	1971	Tuckerman
25	21701	6533	1978	Noll & Nickel
26	23209	6987	1979	Noll
27	44497	13395	1979	Nelson & Slowinski
28	86243	25962	1982	Slowinski
29	110503	33265	1988	Colquitt & Welsh
30	132049	39751	1983	Slowinski
31	216091	65050	1985	Slowinski
32	756839	227832	1992	Slowinski & Gage
33	859433	258716	1994	Slowinski & Gage
34	1257787	378632	1996	Slowinski & Gage
35	1398269	420921	1996	Armengaud, Woltman, et. al. (GIMPS)
36	2976221	895932	1997	Spence, Woltman, et. al. (GIMPS)
37	3021377	909526	1998	Clarkson, Woltman, Kurowski et.al. (GIMPS, PrimeNet)
38	6972593	2098960	1999	Hajratwala, Woltman, Kurowski et.al (GIMPS, PrimeNet)
??	13466917	4053946	2001	Cameron, Woltman, Kurowski et. al. (GIMPS, PrimeNet)
??	20996011	6320430	2003	Shafer, Woltman, Kurowski et. al. (GIMPS, PrimeNet)
??	24036583	7235733	2004	Findley, Woltman, Kurowski et. al. (GIMPS, PrimeNet)
??	25964951	7816230	2005	Nowak et al. (GIMPS, PrimeNet)

Leonard Eulero e nuovi numeri primi

L. Eulero (Basilea 1707 - San Pietroburgo 1783), matematico svizzero, operò soprattutto nel campo della matematica pura; la sistematizzazione e la riformulazione dell'analisi che si trova nelle sue opere è alla base della matematica moderna e della teoria delle funzioni. Studiò all'università di Basilea come allievo del matematico svizzero Johann Bernoulli. Nel 1727, su invito dell'imperatrice russa Caterina I, entrò a far parte dell'Accademia delle Scienze di San Pietroburgo dove fu nominato professore di fisica (1730) e poi di matematica (1733). Nel 1741 accolse la proposta del re di Prussia Federico il Grande e si trasferì all'Accademia delle Scienze di Berlino dove rimase fino al 1766, anno in cui fece ritorno a San Pietroburgo. Sebbene fosse ostacolato fin dall'età di 30 anni da una progressiva perdita della vista, Eulero redasse un gran numero di importanti opere matematiche e centinaia di appunti che provano la sua straordinaria produttività scientifica.

Nella sua *Introduzione all'analisi infinitesimale* (1748), diede la prima trattazione completa dell'algebra, della teoria delle equazioni, della trigonometria e della geometria analitica; precisò la definizione di funzione e affrontò la teoria delle serie. Inoltre studiò le superfici di secondo grado e le curve di secondo e terzo grado; dimostrò che le sezioni coniche sono rappresentate dall'equazione generale di secondo grado purché sussistano alcune relazioni tra i coefficienti della variabile. In altre opere si occupò di calcolo (compreso il calcolo delle variazioni), della teoria dei numeri, dei numeri immaginari. Sebbene fosse soprattutto un matematico, Eulero fornì anche notevoli contributi di astronomia, meccanica, ottica e acustica. Tra le numerosissime opere: *Istituzioni di calcolo differenziale* (1755), *Istituzioni di calcolo integrale* (1768-1770).

Il lavoro di Eulero ha avuto un grande impatto sulla teoria dei numeri in generale e sui numeri primi in particolare. Egli ha esteso il Piccolo Teorema di Fermat ed ha introdotto la funzione φ di Eulero, come già detto ha fattorizzato il quinto numero di Fermat $2^{32}+1$.

Fu il primo a riconoscere che la teoria dei numeri poteva essere studiata con gli strumenti dell'analisi e così facendo diede origine alla Teoria Analitica dei Numeri. Fu in grado di mostrare che non solo la cosiddetta *serie armonica* $\Sigma(1/n)$ diverge, ma anche la serie

$$1/2 + 1/3 + 1/5 + 1/7 + 1/11 + ...$$

formata sommando i reciproci dei numeri primi. La somma dei primi n termini della serie armonica cresce circa come log (n), mentre la seconda serie diverge più lentamente, circa come log(log (n)). Questo significa, ad esempio, che sommando i reciproci di tutti i primi finora noti, anche con i più potenti calcolatori, si ottiene una somma di circa 4, mentre se potessimo sommare tutti i primi esistenti otterremmo infinito. Questo tipo di studio avrà un peso inaspettato in seguito nella teoria dei numeri

Andando per ordine, ottenne un grande risultato, anche se forse ne rimase ignaro, quando riuscì ad ottenere una funzione generatrice di numeri primi. Non una semplice funzione che fornisse pochi esempi, ma in relazione alla sua struttura “una grande quantità di numeri primi”.

Eulero studiando la funzione, chiamata la parabola di Eulero,

$$x^2 + x + 41$$

scoprì che per qualunque valore di x assegnato tra 0 e 39, la formula restituiva un numero primo.

Si verifica facilmente che per x = 0 si ottiene 41; per x = 1 43; per x = 2 47; per x = 4 53; ……; per x = 38 1523; per x = 39 1601; tutti i numeri ottenuti risultano essere primi.

In generale riuscì a dimostrare la validitá della funzione generatrice di primi $x^2 + x + q$ per q = 2, 3, 5, 11, 17, e generano primi per i valori di x compresi tra 0 e q-2.

L'obiettivo quindi adesso si spostò su di una formula che potesse generare tutti i numeri primi; questa impresa dallo stesso Eulero fu descritta come improba, e si ha prova di ciò quando nel 1751 scrisse:

"Ci sono alcuni misteri che la mente umana non penetrerà mai. Per convincersene non dobbiamo far altro che gettare un'occhiata alle tavole dei numeri primi. Ci accorgeremo che non vi regna né ordine né legge."

Eulero dunque amava calcolare numeri primi, e come lavoro di esordio presentò una tavola che conteneva tutti i primi contenuti nei numeri da 1 a 100.000; certo è che questo primo lavoro gli permise di osservare in larga scala quel ritmo vitale che caratterizza i numeri primi, ritmo che solleticò la sua mente nella bramosa voglia di dominare questi numeri "divini" e "creatori". Tale brama fece costruire all'"Aquila" di Basilea quel terreno di caccia che riusciva a dominare dall'alto, ma in cui non riusciva ad orientarsi, pur conoscendone alcune linea guida.

Goldbach ed Eulero: congetture da 2.000.000 di dollari

Christian Goldbach (Königsberg, Prussia orientale, 18 marzo 1690 - Mosca, 20 novembre 1764), matematico prussiano molto noto per la sua congettura sui numeri primi formulata nel 1742 e ancora aperta.
Nato nella città ora chiamata Kaliningrad ed enclave della Russia, figlio di un pastore, Goldbach studiò diritto e matematica. Viaggiò molto attraverso l'Europa e incontrò molti matematici famosi, come Leibniz, Leonhard Euler, Nicolas I Bernoulli, Nicolas II Bernoulli, Daniel Bernoulli, Abraham de Moivre ed Hermann. Nel 1725 Goldbach divenne professore di matematica e storico della Accademia delle Scienze di San Pietroburgo, appena aperta. Nel 1728 divenne tutore del successivo Zar Pietro II. Nel 1742 divenne membro dello staff del Ministero degli esteri russo.

I maggiori contributi di Goldbach riguardano la teoria dei numeri. Altri suoi lavori hanno come argomenti lo studio delle curve, le serie infinite e l'integrazione delle equazioni differenziali.

Nel 1742, il matematico prussiano scrisse una lettera a Leonard Eulero in cui propose la seguente congettura:

Ogni numero dispari maggiore di 5 può essere scritto come somma di tre numeri primi.

Eulero, interessandosi al problema, rispose con una versione più forte della congettura:

Ogni numero pari maggiore di 2 può essere scritto nella somma di due numeri primi.

La prima delle due è oggi conosciuta come ***congettura "debole" di Goldbach***, la seconda come ***congettura "forte" di Goldbach***. (L'enunciato della versione forte implica quello della congettura debole, poiché ogni numero dispari maggiore di 5 può essere ottenuto aggiungendo 3 ad ogni numero pari maggiore di 2). Si conviene che il termine *congettura di Goldbach* sia sinonimo di congettura forte di Goldbach. Entrambi i problemi sono rimasti irrisolti fino ad oggi.

Andiamo a verificare brevemente la *congettura "debole"* e scriviamo così:
$n = q_1 + q_2 + q_3$ *dove n è un numero dispari maggiore di 5, e* q_1, q_2, q_3 *sono numeri primi*

Verifichiamo la congettura per

n = 11 = 3 + 3 + 5

n = 535 = 31 + 131 + 373

Per la congettura forte si usi la formula:

$n = q_1 + q_2$ *dove n è un numero pari maggiore di 2, e* q_1, q_2 *sono numeri primi*

anche qui si può avere una semplice verifica,

n = 16 = 11 + 5

n = 456 = 317 + 139

Durante il corso degli anni molti matematici ha espresso un disaccordo per la congettura di Goldbach, ma nessuno ha mai potuto provare che sia falsa; ma nessuno altresì ha mai potuto dimostrarne la validità.

Nel 2000, allo scopo di pubblicizzare il libro "*Lo zio Petros e la congettura di Goldbach"* di Apostolos Doxiadis, l'editore britannico Tony Faber offrì un premio di 1.000.000 di dollari per una dimostrazione della congettura. Il premio sarebbe stato assegnato solo per dimostrazioni inviate per la pubblicazione entro aprile 2004. Il premio non fu mai reclamato. Mentre dal 2004 una università americana mise in palio 2.000.000 di dollari per stimolare la ricerca matematica… Anche 2.000.000 è un numero pari chissà potendo trovare i numeri q_1e q_2 che lo compongano si possa avere la giusta illuminazione.

Ancora una volta la sfida all'universo dei numeri non è mossa da un intelletto solitario, ancora una volta si cercano compagni di ventura per l'esplorazione del paesaggio che Riemann dipinse in seguito, tutt'oggi si ricorre alla gratificazione economica per scardinare un passaggio obbligato che aprirà le porte a chissà che tipo di realtà.

Gauss, solutore innovativo

Nato il 30 Aprile 1777 a Brunswick, Duchy di Brunswick. All'età di sette anni Carl Friedrich Gauss cominciò a frequentare la scuola elementare, e le sue potenzialità furono subito notate Nel 1788 Gauss andò al Ginnasio, dove studiò anche il Latino.Nel 1792, dopo aver ricevuto un compenso dal Duca di Brunswick, Gauss entrò al Collegio Carolino di Brunswick. All'accademia Gauss da solo scoprì il teorema binomiale, la legge della reciprocità quadratica e il teorema dei numeri primi. Nel 1795 Gauss lasciò Brunswick per studiare all'Università di Gottingen e lì divenne grande amico di Farkas Bolyai.

Gauss lasciò Gottingen senza il diploma, ma in quel periodo fece molte importanti scoperte; la costruzione del 17-agono con riga e compasso, questa fu la più grande costruzione di un poligono regolare fin dai tempi dei matematici greci e fu pubblicata come Lezione VII del più importante scritto di Gauss, *Disquisitiones Arithmeticae.* Nell'estate del 1801 pubblicò il testo *Disquisitiones Arithmeticae* composta da sette sezioni, tutte, tranne l'ultima, riguardanti la teoria dei numeri. Gauss si interessò anche di astronomia; con una buona approssimazione stabilì l'orbita del pianeta Cerere e nel 1802 cominciò a studiare quella del pianeta Pallade e in quel periodo gli fu proposta la direzione dell'osservatorio di Gottingen, ma egli rifiutò. Il suo benefattore, il Duca di Brunswick morì combattendo nell'esercito prussiano, e nel 1807 Gauss accettò il posto all'osservatorio di Gottingen. Nel 1809 pubblicò il suo secondo libro che trattava del moto dei corpi celesti: *Theoria motus corporum coelestium in sectionibus conicis Solem ambientium.* Il lavoro era diviso in due volumi; il primo includeva equazioni differenziali, sezioni coniche e orbite ellittiche, mentre nel secondo Gauss mostrò i metodi di approssimazione dell'orbita di un pianeta. Sebbene continuò a fare osservazioni fino a settanta anni, il contributo di Gauss sulla teoria astronomica terminò nel 1817. Fin dal 1800 Gauss si interessò sulla possibile esistenza di una geometria non euclidea e parlò dell'argomento con Farkas Bolyai che più tardi gli rivelò le scoperte del figlio Jànos. Gauss si dedicò maggirmente alla geometria differenziale e pubblicò alcuni lavori in merito. *Disquisitiones generales circa superficies curva*(1828) fu il suo più importante scritto sull'argomento.Dal 1845 al 1851 Gauss si impegnò ad ampliare i fondi dell'Università di Gottingen. Questo lavoro gli consentì di avere una pratica esperienza in materia finanziaria e fece la sua fortuna investendo in compagnie private. Dal 1850 in poi il lavoro di Gauss fu pressoché di natura pratica sebbene approvò la tesi di Riemann e ascoltò la sua discussione. Morì il 23 Febbraio 1855 a Gottingen, Hannover.

Di certo se si venissero a considerare anche le ricerche in campo astronomico e fisico non citate, la sola lettura di una breve biografia di Gauss forse conterrebbe un numero parole in numero uguale al più grande numero di Mersenne trovato. Per questo motivo si tratterò esclusivamente le sue ricerche sui numeri primi, e i metodi utilizzati.

Fin a l’avvento di Gauss, si era adottata la strategia di sviscerare una formula che potesse generare tutti i numeri, e che mettesse la parola fine ad un problema così rilevante. Gauss abile solutore di problemi numerici, già a quindici anni durante le lezioni di matematica al ginnasio era stato capace si calcolare la somma dei primi n numeri naturali avvalendosi di una semplice formula, $\frac{n(n+1)}{2}$, beffando sia l’insegnante che i suoi compagni in un tempo brevissimo. Aveva semplicemente, per Gauss, cambiato le regole del gioco semplificandosi la vita. Venuto a contatto con i numeri primi, decise che era il momento di una svolta e decide di cambiare strategia nell’affrontare “l’armata invincibile” .

La nuova strategia fu quella di non localizzare l'attacco alla posizione dei numeri, ma alla loro densità (distribuzione) tra i naturali. Usò per questo scopo uno strumento a lui molto familiare come i logaritmi con cui, grazie a Nepero, era in grado di effettuare calcoli onerosi in brevissimo tempo. Vuoi per le note proprietà dei logaritmi, vuoi per la sua viscerale passione verso questo tipo di calcolo che fin da bambino lo stimolò, tanto da fargli ampliare in tenera età la tavola degli stessi.

Infatti Gauss sorprendentemente elaborò la propria congettura sulla densità dei primi avvalendosi dei logaritmi, ma ancor più delle tavole di numeri primi disponibili all'epoca. L'approccio allo studio della densità, di per se stesso innovativo, fu condotto da un punto di vista medio (o per dirla in un linguaggio più attuale statistico). All'uopo fu introdotta una funzione particolare chiamata $\pi(n)$ che rappresentasse il numero dei primi presenti nei primi n elementi dei naturali. Brevemente questa funzione era così fatta:

$$\pi(x) = /\{p \text{ numero primo tale che } p \leq x\}/$$

$\pi(1) = 0$; $\pi(10) = 4$; $\pi(20) = 8$; $\pi(30) = 10$ ……

Studiando l'andamento di questa funzione, "il ribelle" poté notare una regolarità nella distribuzione irregolare dei primi, una singolare regolarità. E' immediato constatare che la distribuzione dei primi tra gli interi è estremamente irregolare ma questa irregolarità "in piccolo" (relativa cioè alla comparsa dei singoli primi), sparisce se si considera la distribuzione media dei primi data da $\pi(n)/n$. Questo rapporto soddisfa una legge che per la sua semplicità ed eleganza è sbalorditiva! Tale legge può essere intuita e congetturata scorrendo tabelle di primi ti questo tipo:

n	$\pi(n)$	$\pi(n)$ /n	**Scarto tra due potenze di 10 consecutive**
10	4	2,5	
100	25	4,0	1,5
1.000	168	6,0	2,0
10.000	1229	8,1	2,1
100.000	9592	10,4	**2,3**
1.000.000	78.498	12,7	**2,3**
10.000.000	664.579	15,0	**2,3**
100.000.000	5.761.455	17,4	**2,4**
1.000.000.000	50.847.534	19,7	**2,3**
10.000.000.000	455.052.511	22,0	**2,3**

La congettura iniziale di Gauss, basa sul fatto che log 10 ≈ 2,3, è stata la seguente

Per i numeri compresi fra 1 e n, ogni log n numeri ce ne sarà grossomodo 1 che è primo

da ciò dunque, la formulazione di una prima congettura definitiva, che il numero dei primi fino ad N, con N molto "grande", fosse possibile approssimarlo, in media, con una funzione analitica, la seguente:

$$\pi(n) \approx \frac{n}{\log n} \quad \text{per n} \to \infty$$

Il risultato ottenuto non fu mai pubblicato, forse perché l'Accademia di Parigi aveva rifiutato di pubblicare *Disquisitiones arithmeticae*, quindi Gauss tentò di mettere al posto giusto tutti i tasselli prima di proporre un nuovo lavoro. Comunque questo risultato comparì in fondo alle tavole dei Suoi logaritmi e proprio tramite quelle si riuscì a dar la paternità della scoperta a Gauss, quando Legendre in seguito, e autonomamente migliorò la formula. La dimostrazione della congettura di Gauss, fu effettuata nel 1896 da De la Vallè Poussin e Hadamard, con i potenti metodi dell'analisi complessa e grazie ad una dimostrazione probabilistica.

Un miglioramento della formula di Gauss lo ottenne il francese Legendre, membro dell'Accademia di Parigi, ottenne autonomamente un risultato simile a quello di Gauss.

"*La distribuzione apparentemente caotica dei numeri primi nasconde un certo ordine, dato dal comportamento della funzione π(n) che esprime il numero di primi minori o uguali a n",*
come specifica K. Devlin in *"Dove va la matematica".*

Nel suo libro *Essai sur la Théorie des Nombres* del 1798, Legendre osservò che $\pi(n)$ è approssimativamente uguale al numero

$$\pi(n) \approx \frac{n}{\log n - 1{,}03866}$$

Non c'è niente di particolare nel numero 1,08366: Legendre ottenne questo risultato esaminando le tavole dei numeri primi fino a 400.000 e scelse questo numero semplicemente per dare un'approssimazione il più precisa possibile.

n	$\pi(n)$	$\frac{n}{\log n}$	$\frac{n}{\log n - 1{,}03866}$	**Li**(n)
1.000	168	145	172	178
10.000	1.229	1.086	1.231	1.246
100.000	9.592	8.686	9.592	9.630
1.000.000	78.498	72.382	78.534	78.628
10.000.000	664.579	620.420	665.138	664.918
100.000.000	5.761.455	5.428.681	5.769.341	5.762.209

L'evidenza della migliore approssimazione della formula data da Legendre non bastò ai matematici. La critica dell'Accademia e di tutto il mondo scientifico di quel periodo si accanì sul fatto che il numero 1,03866 (numero magico) non provenisse da "nulla" o per meglio dire fu introdotto nella formula empiricamente. L'eleganza dei matematici di razza, non permise loro di accettare un risultato così "*costruito*", quindi erano dell'idea che come molto spesso accade in matematica, ed anche il natura, le formule devono essere (relativamente) semplici e non di recondita provenienza. Ma Gauss ancora un volta tirò fuori dal cilindro qualcosa di alternativo, un'idea che spinse tutti ad aggirare ulteriormente l'ostacolo, e che poi spedì Riemann a contemplare il suo famoso "*Paesaggio*".

Nel 1863, Gauss, avanzato negli anni, pubblicò i suoi lavori sui numeri primi indicando sia il suo vecchio lavoro, che uno nuovo lavoro con nuovi concetti. L'idea fondante della nuova formula scaturiva da una semplice osservazione della probabilità che si venisse a presentare un numero primo, partendo da un naturale qualsiasi. Nell'intervallo da 1 a 100 ad esempio abbiamo la presenza di 25 primi, e dunque la probabilità era di 1 a 4; se si consideriamo i primi 1000 numeri era di 1 a 6 e così via. Quindi la casualità della distribuzione portò Gauss a pensare il presentarsi dei numeri primi, come il lancio di una moneta "non bilanciata" , e pensò proprio che la Natura giocasse a testa o croce con in numeri, questa è solo un'ipotesi.

Così penso bene di dare un peso ad "ogni lancio" nella misura di $\frac{1}{\log(n)}$, e di creare così un modello per la stima dei numeri primi nei naturali da 1 a n in questo modo

$$\pi(n) \approx \frac{1}{\log 2} + \frac{1}{\log 3} + ... + \frac{1}{\log n} \qquad \text{per meglio dire} \qquad \pi(n) \approx \sum_{i=2}^{n} \frac{1}{\log i}$$

Il gusto dell'eleganza e della ricerca spinse Gauss ancora più avanti , e avvalendosi dei potenti mezzi dell'Analisi Matematica, appena nata, scrisse la sua celeberrima funzione ***Logaritmo Integrale***

$$\pi(n) \approx Li(n) = \int_2^n \frac{1}{\log x} dx$$

Subito Gauss stesso riuscì a provare la validità della sua nuova formula, e considerando i numeri primi fino a 3.000.000 provò che tale funzione si discostava di un settecentesimo dell'un percento dalla realtà. Il confronto proposto nella tabella precedente evidenzia come già per valori di 10^8 numeri primi analizzati la funzione approssimi in maniera molto più esatta delle funzioni considerate precedentemente e che poteva essere considerata in buona misura "aderente" a π(n).

In effetti dalla tabella sembra che Li(*n*), sia lievemente maggiore di π(*n*), e se si dovesse proseguire nella tabulazione è probabile che si continuerebbe a mostrare la stessa cosa. Sarebbe da scettici non concludere che Li(*n*) approssima π(*n*) per eccesso. Ma se si arrivasse a tale conclusione si sarebbe in errore, poiché nel 1914 il matematico inglese J. E. Littlewood (un collega di G. H. Hardy) dimostrò che la differenza Li(*n*) - π(*n*) passa da un valore positivo a uno negativo infinite volte all'aumentare di *n* negli interi positivi. Così, ci saranno certamente valori di *n* per i quali Li(*n*) è minore di π(*n*), e S. Skewes mostrò nel 1955 che un tale *n* dovrà apparire prima del cosiddetto *numero di Skewes*:

$$e^{e^{e^{79}}} \approx 10^{10^{10^{34}}}$$

un valore incomprensibilmente grande. Molto più piccolo, ma ancora ben al di fuori della nostra immaginazione, è il numero nel 1966 Lehman mostrò che esso sostituisce il numero di Skewes, nel senso che Li(*n*) - π(*n*) cambierà segno per qualche valore inferiore a quel numero. Più piccolo ancora è il numero e nel 1986 Hermann J. J. te Riele dimostrò che un cambiamento di segno avverrà per qualche *n* al di sotto di questo limite. Ma questi sono ancora numeri estremamente grandi, e ciò ha portato a concludere che è possibile che non si arrivi mai a scoprire un numero *n* per il quale Li(*n*) sia effettivamente minore di π(*n*) (quel che è certo è che una ricerca al calcolatore fatta fino a un miliardo non è approdata a nulla).

E' da notare tuttavia che tale modello implica la nozione di infinito e i concetti di analisi. Il lavoro di entrambi i matematici era scaturito da un importante saggio di otto pagine, pubblicato dal tedesco Bernhard Riemann nel 1859, dal titolo *Sul numero di primi minori di una grandezza data*. In questo scritto, l'unico di Riemann sulla teoria dei numeri, egli suggerì alcune linee di ricerca che ancora oggi risultano estremamente produttive. Si potrebbe addirittura affermare che la pubblicazione di questo scritto ha segnato l'inizio di tutta la teoria analitica dei numeri, nella quale le tecniche dell'analisi sono applicate a problemi relativi ai numeri naturali.»

Riemann e il panorama dell'universo dei numeri.

Nato il 17 Settembre 1826 a Breselenz, Hannover**.** Seguito nei primi studi dal padre, nel 1840 Georg Riemann entrò direttamente nella terza classe del Liceo di Hannover e durante gli studi si trasferì al Ginnasio di Luneburg ove mostrò un particolare interesse per la matematica e il direttore del Ginnasio lo invitò a studiare i testi matematici della sua biblioteca personale.

Nel 1846 si iscrisse all'Università di Gottingen per studiare teologia, ma poi si dedicò alla matematica sotto la guida di Gauss.

Nel 1847 si recò a Berlino dove ebbe come insegnanti Dirichlet, Jacobi, Steiner. Ritornato a Gottingen, nel 1851 presentò la tesi di laurea su Fondamenti di una teoria generale delle funzioni di variabile complessa, grandemente apprezzata da Gauss, che ne fu il relatore.

Nel 1854 scrisse un articolo *Sulle ipotesi che sono alla base della geometria*, che è diventato un classico della storia della matematica, in cui presentò metodi e concetti che sarebbero stati poi utilizzati nella teoria della relatività di Einstein. Altro grande lavoro del 1854 fu *Sulla rappresentabilità di una funzione mediante una serie trigonometrica*, in cui studiò le condizioni perché una funzione sia integrabile.

Nel 1859, morto Dirichlet, Riemann gli successe nella cattedra che era stata di Gauss e poi di Dirichlet dal 1855.

Nel 1863, ammalatosi di tubercolosi, si recò in Italia per curare la sua malattia, ma nel 1866 morì a Selasca, sul lago Maggiore.

Con tutti i maestri illustri avuti, Riemann non ha avuto carenza di modelli e strumenti per attuare e consacrare le sue geniali intuizioni. Proprio una di queste strabilianti frecce scagliate verso il futuro, fu l'aver discusso in sede di esame per il dottorato, presso l'università di Gottinga, la sua creativa, fantasiosa e musicale Ipotesi. Ipotesi che ha donato a lui l'immortalità e a tutti gli altri matematici il sogno di poter risolvere il più grande problema matematico affrontato dall'uomo, i numeri primi.

Leibniz disse: "la musica è il piacere che la mente umana prova quando conta senza esser conscia di contare". Ebbene, Riemann invece riuscì ad ascoltare la musica dell'universo, attraverso quella aritmia che è caratteristica del cuore dei naturali che pulsando per mantenere in vita l'infinità grandiosa dei numeri stessi. Un battito come armoniche fondamentali che sovrapposte costituiscono la sinfonia della matematica. Adesso è importante capire come il battito sia stato interpretato da Riemann. Chi e come ha influenzato la sua opera? Come ha poggiato le basi della rivoluzione riemanniana nella teoria dei numeri?

La funzione ζ di Eulero

La funzione ζ costituisce un importate campo di ricerca nella teoria dei numeri. Tale funzione fu introdotta e studiata nel 1737 da Eulero. Lo studio di Eulero si basava sullo studio di tale funzione come funzione reale di variabile reale. E' opportuno sviscerarne le caratteristiche già notate da Eulero, per consentirne un approccio migliore all'interpretazione di Riemann nel voler scoprire un filo conduttore tra tutte le "gemme" dei numeri.

La definizione data per la funzione zeta è, $\zeta : D \to \Re \quad (D \subset \Re)$

$$\zeta(x) = \sum_{n=1}^{+\infty} \frac{1}{n^x} = 1 + \frac{1}{2^x} + \frac{1}{3^x} + \frac{1}{4^x} + \dots$$

Eulero osservò che la serie al secondo membro è convergente per tutti i reale x > 1, di conseguenza la funzione ζ gode delle seguenti proprietà:

1. $D = \{x \in \Re : x > 1\}$
2. $\lim_{x \to 1^+} \zeta(x) = +\infty$
3. la funzione è continua e derivabile infinitamente in D
4. Inoltre la funzione per valori interi pari da 2 a 26 ammette valore del tipo $\alpha\pi^x$ infatti
   - $\zeta(2) = \sum_{n=1}^{+\infty} \frac{1}{n^2} = 1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + ... = \frac{\pi^2}{6}$
   - $\zeta(4) = \sum_{n=1}^{+\infty} \frac{1}{n^4} = 1 + \frac{1}{2^4} + \frac{1}{3^4} + \frac{1}{4^4} + ... = \frac{\pi^4}{90}$
   - $\zeta(6) = \sum_{n=1}^{+\infty} \frac{1}{n^6} = 1 + \frac{1}{2^6} + \frac{1}{3^6} + \frac{1}{4^6} + ... = \frac{\pi^6}{945}$
   - ………………………………………………
5. Infine la funzione può essere scritta

$$\zeta(x) = \frac{2^x}{2^x - 1} \cdot \frac{3^x}{3^x - 1} \cdot \frac{5^x}{5^x - 1} \cdot \frac{7^x}{7^x - 1} \cdot \frac{11^x}{11^x - 1} \cdot ...$$

Queste cinque proprietà, ed in particolare l'ultima, stimolarono le grandi menti facendo assumere a questa funzione una importanza cardinale nella teoria dei numeri, e nella caratterizzazione dei numeri primi in seno ai naturali. Appena nata, la funzione zeta, sembrava essersi creata dal nulla per mezzo del grande intelletto di Eulero, ma dopo pochi mesi di vita apparvero di prepotenza i geni di cui era costituita; un prodotto infinito con pioli i numeri primi, che descrive le sue caratteristiche e che forse un giorno svelerà quelle di tutti i numeri.

Fondamentale, infatti, fu l'applicazione di concetti e di procedimenti analitici nella ricerca in teoria dei numeri, caratteristica metodologica propria del XIX secolo. Senza dubbio, le radici della *teoria analitica dei numeri* non furono idealmente distanti dal punto di vista euleriano che, come vedremo, sarà ripreso, almeno per quanto riguarda lo studio delle proprietà della funzione ζ, da Riemann. Sono note molte applicazioni della funzione ζ: ad esempio, si dimostra che

a) la probabilità che due numeri interi, scelti a caso, non abbiano alcun fattore comune e la probabilità che un numero, scelto a caso, non sia divisibile per un quadrato sono entrambe

$$\frac{1}{\zeta(2)} = 0{,}607927...$$

b) Analogamente, la probabilità che tre numeri interi, scelti a caso, non abbiano alcun fattore comune è

$$\frac{1}{\zeta(3)} = 0{,}831907...$$

c) per x=3 [2]*la funzione ζ assuma come valore un numero irrazionale, e probabilmente trascendente (ma ciò è un ipotesi).*

$$\zeta(3) = \sum_{n=1}^{+\infty} \frac{1}{n^3} = 1 + \frac{1}{2^3} + \frac{1}{3^3} + \frac{1}{4^3} + ... = 1{,}202056...$$

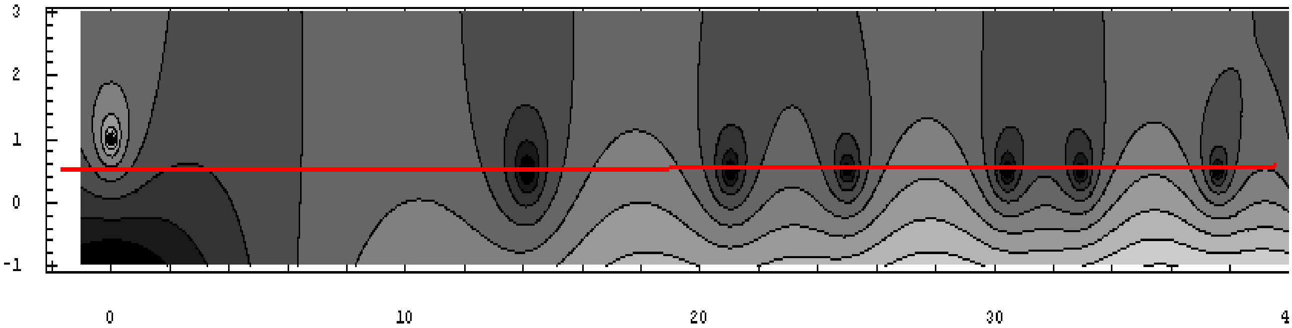
[2] La dimostrazione fu eseguita da Roger Apérey nel 1978

Bernhard Riemann cambia prospettiva

Una fase di notevole importanza nello studio della funzione ζ è associata agli studi di Riemann, il quale propose (1859) di definire tale funzione per $x \in \boldsymbol{C}$ e si occupò del prolungamento analitico di ζ all' intero piano complesso.
Gli zeri della funzione ζ così prolungata (ζ ammette un polo per $z = 1$) sono:

- $x = -2$, $x = -4$, $x = -6$, ... detti *zeri banali* di ζ;
- alcuni numeri complessi (non reali) x, con parte reale $0 \leq \mathrm{Re}(x) \leq 1$.

Riemann suppose che *tutti gli zeri non banali* di ζ siano caratterizzati dalla proprietà di avere parte reale Re(x)=½. La congettura indicata da Riemann non è ancora stata provata né smentita; nel 1914, G.H. Hardy giunse a dimostrare che z ha infiniti zeri non banali per i quali risulta verificata la supposizione Riemanniana.



In figura il modulo della funzione ζ con in rosso la retta "magica"

Molte verifiche della congettura in casi particolari sono state condotte sugli zeri di ζ: il primo lavoro in tale direzione fu condotto nel 1903 da J.P. Gram, il quale calcolò i primi 15 zeri non banali di ζ; nel 1935, E.C. Titchmarsh giunse alla determinazione dei primi 1041 zeri non banali di z ([5], p. 182).
Con la diffusione dei mezzi per il calcolo automatico, questo genere di ricerche subì un impulso notevole: nel 1986, grazie all' utilizzo di un elaboratore per più di 1000 ore di tempo-macchina, la congettura di Riemann è stata verificata da J. Van de Lune, H.J.J. te Riele e D.T. Winter per il primo miliardo e mezzo di radici non banali della funzione z, ma evidentemente tutto ciò non comporta alcunché per quanto riguarda la validità in generale della supposizione in esame. Nel 1984, una dimostrazione della congettura, annunciata dal giapponese Matzumoto, si è rivelata errata.

L'ipotesi di Riemann

Tuttora risulta uno dei principali problemi aperti della matematica; un premio da 1.000.000 di dollari è stato offerto dal Clay Mathematics Institute per chi scoprirà una dimostrazione della congettura. Molti matematici pensano che l'ipotesi di Riemann sia vera (non tutti però, J. E. Littlewood e Atle Selberg sono molto scettici al riguardo). Ciò rende molto più bella la sfida! Si narra che Riemann avesse la dimostrazione della sua ipotesi, ma purtroppo dopo la sua morte una domestica provetta ha abbia fatto pulizia tra le confuse carte di Riemann cestinando quella che poteva essere la chiave si volta di un mistero millenario.

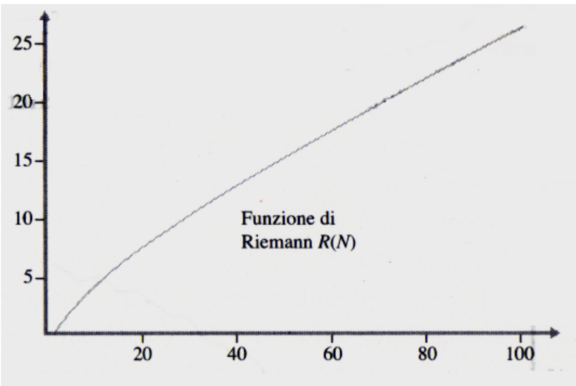
L'espressione $\frac{n}{\log n}$, seguita da una approssimazione più esatta da parte di Legendre, ed ancora migliorata per grandi valori dal Li(n), pur essendo un'approssimazione abbastanza semplice per $\pi(n)$ non è molto stretta e i matematici hanno cercato di migliorarla. Naturalmente il prezzo da pagare è una maggiore complessità dell'espressione approssimante. Una delle approssimazioni più soddisfacenti per $\pi(n)$ è la seguente

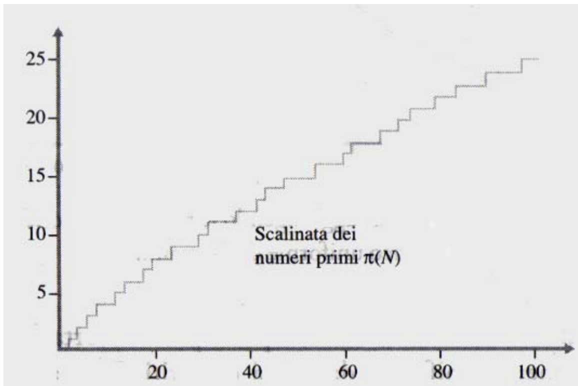
$$R(n) = 1 + \sum_{k=1}^{\infty} \frac{1}{k\zeta(k+1)} \cdot \frac{(\log n)^k}{k!}$$

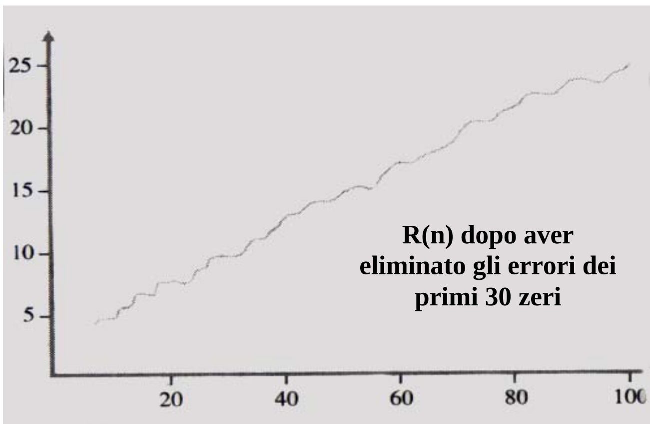
con ζ la funzione zeta di Riemann $\zeta(s) = \sum_{n=1}^{+\infty} \frac{1}{n^s} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \ldots = \prod_p \frac{1}{1-p^{-s}}$

La funzione Riemanniana R(n) per l'approssimazione di $\pi(n)$ produsse subito dei risultati tangibili e ancor più nel tempo si rivelò essere un esatto "Best Featting" del numero dei primi fino a n. Ecco una tabella dei più recenti risultati ottenuti:

n	$\pi(n)$	$\pi(n) - R(n)$	$\pi(n) - Li(n)$
10^7	664.579	88	339
10^8	5.761.455	97	754
10^9	50.847.534	-79	1.701
10^{10}	455.052.511	-1.828	3.104
10^{11}	4.118.054.813	-2.318	11.588
10^{12}	37.607.912.018	-1.476	38.263
10^{13}	346.065.536.839	-5.773	108.971
10^{14}	3.204.941.750.802	-19.200	314.890
10^{15}	29.844.570.422.669	73.218	1.052.619
10^{16}	279.238.341.033.925	327.052	3.214.632







R(n) dopo aver eliminato gli errori dei primi 30 zeri

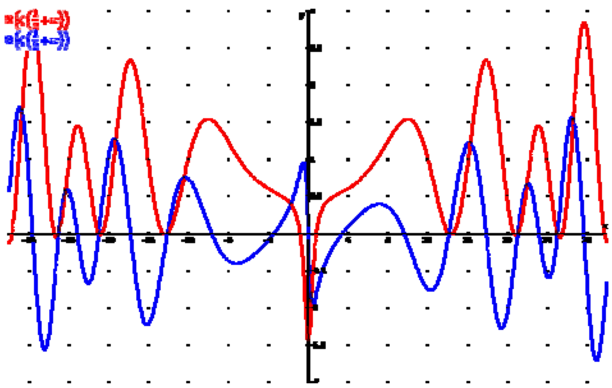
Questi risultati ottenuti comunque presentavano degli errori, anche se relativamente piccoli, e di sicuro molto più piccoli delle approssimazioni effettuate da Gauss. Ed è proprio a questo punto che Riemann ebbe il giusto insight per la risoluzione della questione.

Riemann era sicuro di poter ricostruire tutto il suo paesaggio solo avendo a disposizione i punti che annullano la funzione $\zeta(s)$, ragionando sempre per interpolazione. Quindi ricreare l'intero paesaggio con solo a disposizione i punti "a livello del mare". Questo tipo di intuizione lo portò a servirsi di una equazione perfetta, nel considerare il ruolo degli zeri,

zeri della zeta = numeri primi = onde

Infatti infiniti erano i numeri primi e grazie alla loro composizione (per prodotto) generano tutti i numeri naturali, così la grande prima ipotesi che infiniti fossero i punti a livello del mare e che la composizione delle loro "vibrazione" avrebbero generato tutto il resto del paesaggio. Non solo ipotizzò che avessero tutti una comune proprietà, quelli di esseri allineati sul piano di Gauss secondo una "retta magica". Così ipotizzando Riemann permise di passare dal Caos a l'ordine, solo guardando al di là delle frontiere, fatte di specchi, dei numeri Reali.

Eulero aveva precedentemente dimostrato nella sua pubblicazione di Losanna del 1768, "Introductio analysin infinitorum", che un esponenziale con esponente complesso si poteva esprimere sul piano di Gauss con l'equazione di un'onda sinusoidale. E proprio mettendo a frutto questo risultato Riemann ebbe la geniale idea di "guardare oltre lo specchio reale", ed inserire gli



zeri della $\zeta(s)$ ed ognuno dei complessi della forma $\frac{1}{2}+it$ assumessero la forma di un'onda, l'onda "musicale" relativa ad ogni numero primo.

Le caratteristiche di ciascun onda era dettate dalla posizione occupata nel paesaggio, più lontana era l'onda dall'origine più "vibrava" velocemente, dando la propria componente acuta alla melodia. Riemann riuscì a capire la relazione che generava l'errore tra la sua formula ed il numero dei primi fino ad N e riuscì finalmente ad interpolare al meglio i risultati ottenuti, trovando l'ordine ove non era possibile notarlo, caratterizzando i numeri "sfuggenti" e mettendoli in fila sul piano di Gauss, ed al livello del mare nel "suo paesaggio".

Come si può notare nelle figure proposte i primi "semi" della matematica sono piantati nel "paesaggio" nei punti $z_{1,2}=\frac{1}{2}\pm 14{,}135i$, $z_{3,4}=\frac{1}{2}\pm 21{,}022i$, $z_{5,6}=\frac{1}{2}\pm 25{,}011i$ e la ricerca degli stessi è molto complessa, e come per i numeri di Mersenne la tecnologia ha fatto si che quantomeno si lasci accesa la speranza della validità dell'ipotesi. Tale validità potrebbe stare alla base (e sta alla base di altri risultati in teoria dei numeri) di nuove prospettive e la sua dimostrazione potrebbe dipingere un altro paesaggio matematico.

Come per i numeri di Mersenne, anche per la ricerca degli zeri si è aperta la caccia! Una caccia ai possibili zeri sulla retta magica, e non. Ecco le specifiche del progetto che si prefigge, tramite erogazioni di premi, di trovare il massimo numero di zeri non banali per la funzione zeta.

Cos'è ZetaGrid?
ZetaGrid è un sistema distribuito (*grid system*) *open source* e *platform independent* che utilizza i cicli *idle* delle CPU che aderiscono al progetto. Il *grid computing* può essere utilizzato per qualsiasi applicazione che necessiti di una elevata potenza di calcolo e che può essere divisa in singoli passi separati, ognuno dei quali può richiedere un tempo prolungato di computazione su un singolo computer. *ZetaGrid* può essere eseguito come un processo in *background* a bassa priorità su diverse piattaforme tipo Windows, Linux, AIX, Solaris e Mac OSX. Sui sistemi Windows può inoltre essere eseguito come uno *screen saver*.

***ZetaGrid* in pratica**:
Nel laboratorio di sviluppo della IBM (IBM Development Laboratory) a Böblingen, *ZetaGrid* risolve in pratica un unico problema, girando su 6 piattaforme differenti: La verifica dell'**Ipotesi di Riemann,** che è considerato uno dei problemi più importanti della matematica moderna. L'implementazione coinvolge più di 9000 *workstation* ed ha un picco di performance di circa 5649 GFLOPS. Ogni giorno sono calcolati più di un miliardo di zeri per la funzione zeta.

Dettagli tecnici:
ZetaGrid fornisce un kernel Java protetto, che non permette accessi dall'esterno e rende sicure le comunicazioni e le attività utilizzando un livello d'accesso riservato con una firma digitale (sistema di crittazione a chiave pubblica di ElGamal) e protocolli di scambio delle chiavi (Diffie-Hellman semi-certificato e verifica delle chiavi di ElGamal). Le chiavi hanno una lunghezza di 1024 bit. La struttura di *ZetaGrid* fornisce capacità di management ed è molto semplice da utilizzare. Inoltre, è supportato su piattaforme differenti ed è stata provata la sua stabilità.

Prima che il progetto iniziasse il 28 agosto 2001 l'Ipotesi era stata verificata per i primi 1.500.000.001 zeri. Il 27 ottobre 2001, J. van de Lune verficò l'Ipotesi per i primi 10 miliardi di zeri. Fino ad oggi il risultato è stato esteso fino a 100 miliardi di zeri che hanno reso necessario il calcolo di 1.3×10^{18} operazioni in virgola mobile. Ma *ZetaGrid* vuole andare oltre. I risultati sui primi 100 miliardi di zeri della funzione zeta di Riemann hanno confermato i calcoli effettuati da altri scienziati e gli hanno estesi hai primi 100 miliardi di zeri non banali.

Bibliografia e sitografia

Marc du Sautoy – ***L'enigma dei numeri primi, L'ipotesi di Riemann*** – Rizzoli

Kieth Devlin – ***Dove va la matematica*** – Bollati Boringhieri

Piergiorgio Odifreddi – **La Matematica del Novecento** - Einaudi

Carl B. Boyer - ***Storia della matematica*** - Mondadori

Manfred R. Schroeder - ***La teoria dei numeri*** - Franco Muzzio Editore

Courant-Robbins - ***Che cos'è la matematica*** - Bollati-Boringhieri

H. Meschkowski - ***Mutamenti nel pensiero matematico*** - Boringhieri

Morris Kline - ***Storia del pensiero matematico*** - Einaudi

http://www.mersenne.org/

http://www.utm.edu/research/primes/

http://primes.utm.edu/curios/

http://mathworld.wolfram.com/

http://www.sosmath.com/tables/tables.html

http://digilander.libero.it/bernadgl/critto2.html

Indice