Ottavio Serra

Riemann e il fascino dei numeri primi.

1. I numeri primi in Euclide.

Fin dalla matematica greca i numeri primi ebbero un posto importante nello studio dell'aritmetica. Ricordo che un numero (naturale) è detto *primo* se è **maggiore di uno** e non ammette divisori propri. Il numero **1** è escluso per evitare che venga meno il teorema fondamentale dell'aritmetica: "*La scomposizione di un numero in fattori primi è unica, a meno dell'ordine*". I greci avevano notato che i numeri primi si vanno diradando. Ce ne sono **168** fino a 1000, **135** tra 1000 e 2000, **106** tra 10.000 e 11.000, **81** tra 100.000 e 101.000, **79** tra 500.000 e 501.000, **75** tra 1.000.000 e 1.001.000, ecc.

Non credo però che i greci fossero riusciti a trovare numeri primi maggiori di 1000.

Euclide, nel IX° libro degli ***Elementi***, proposizione 20, dimostra un fondamentale teorema, semplice da enunciare e anche da dimostrare: "Comunque si prendano dei numeri primi a, b, c, esiste un numero primo diverso da a, da b, da c". Si faccia infatti il prodotto X=a.b.c e si aggiunga 1: Y=X+1; Y è maggiore di X e perciò di a, di b e di c. Se Y è primo, la tesi è dimostrata; se Y è composto, è divisibile per qualche numero primo q diverso da **a**, da **b** e da **c**, perché altrimenti q dividerebbe X oltre che Y e quindi la loro differenza, che è **1**, il ché è impossibile; per conseguenza **q** è diverso da **a**, da **b**, da **c**.

[1] Corollario: "**Il numero dei numeri primi è infinito**". Siano $p_1=2$, $p_2=3$, ,… p_n i primi n numeri primi, in ordine crescente, X sia il loro prodotto, Y=X+1. Y è maggiore di tutti gli n numeri primi $p_1=2$, $p_2=3$, …p_n ,perciò se Y è primo, esso è un numero primo maggiore di p_n, se è composto ha un divisore primo q maggiore di p_n e perciò in ogni caso esiste un numero primo q maggiore di p_n.

N.B. Il teorema di Euclide **non dimostra** che $Y=p_1.\ p_2,\ \ldots.\ p_n+1$ sia un numero primo, ma che può esserlo e, se non lo è, è prodotto di numeri primi **maggiori di p_n .**

Per esempio, 2+1=3 è primo, 2.3+1=7 è primo, 2.3.5+1=31 è primo, 2.3.5.7+1=211 è primo, e ancora 2.3.5.7.11+1=2311 è primo. Se ci si fermasse qui, si incorrerebbe nella *fregatura di Pierino*, secondo il quale Y è sempre un numero primo, ma 2.3.5.7.11.13+1=30031 è **composto** (prodotto di 59 per 509).

E restano composti i numeri fino a 2.3.5.7.11.13.17.19.23.29+1 =6469693231=331.571.34231, poi 2.3.5.7.11.13.17.19.23.29.31+1=200560490131 è di nuovo primo, poi il prossimo è composto, ecc.

Un altro semplice teorema, alla portata di Euclide, è che i numeri primi, pur essendo infiniti, si vanno diradando, nel senso preciso del seguente

[2] Teorema: Per ogni numero naturale n, esiste una sequenza di n numeri naturali consecutivi nessuno dei quali è primo. Per dimostrarlo, si considerino i seguenti numeri consecutivi:

$a_1=(n+1)!+2$
$a_2=(n+1)!+3$
$a_3=(n+1)!+4$
……
$a_n=(n+1)!+(n+1)$.

(Ricordo che k!=1.2.3…k).

Essi sono in numero di n e nessuno è primo, perché a_1 è divisibile per 2, a_2 per 3,…, a_n per (n+1).

2. Arriva Eulero.

Considero ora la seguente serie, dove s è(per il momento) un numero reale:

[3] $\zeta(s)=1+\frac{1}{2^s}+\frac{1}{3^s}+\ldots\frac{1}{n^s}+\ldots=\sum_{k=1}^{\infty}\frac{1}{k^s}$. Come è noto, questa converge per s>1 e diverge a $+\infty$ per $s\leq 1$. In particolare, per s=1 si ottiene la serie armonica, divergente notoriamente a $+\infty$ e, meno notoriamente, divergente come Log(n).[1]

[1] Ottavio Serra, La costante C di Eulero Mascheroni e la funzione Gamma, Annuario dello Scorza n° 18, a.s. 2007-2008

Moltiplicando la **[3]** per $\frac{1}{2^s}$ si ottiene

[4] $\frac{1}{2^s}\zeta(s)=\frac{1}{2^s}+\frac{1}{4^s}+\frac{1}{6^s}+...$ e sottraendo la **[4]** dalla **[3]**, si elidono tutti i denominatori pari e si ottiene:

[5] $(1-\frac{1}{2^s})\zeta(s)=1+\frac{1}{3^s}+\frac{1}{5^s}+\frac{1}{7^s}+\frac{1}{9^s}+...$ Moltiplicando la **[5]** per $\frac{1}{3^s}$ e sottraendo ciò che si ottiene dalla **[5],** si ha $(1-\frac{1}{2^s})(1-\frac{1}{3^s})\zeta(s)=1+\frac{1}{5^s}+\frac{1}{7^s}+...$ (si elidono i denominatori multipli di 3).

Così continuando, nella serie a 2° membro, dopo 1, si elidono i multipli di 5, di 7, eccetera e restano gli inversi, (elevati ad s), di numeri primi sempre più grandi e perciò il 2° membro si approssima sempre più ad 1. Si conclude perciò che

[6] $(1-\frac{1}{2^s})(1-\frac{1}{3^s})(1-\frac{1}{5^s})(1-\frac{1}{7^s})(1-\frac{1}{11^s})...(1-\frac{1}{p^s})\zeta(s)=1$, ovvero

[7] $\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s}=\prod_{p\in P}(1-\frac{1}{p^s})^{-1}$, la somma essendo estesa a tutti i numeri naturali e il prodotto a tutti i numeri primi.

Questa splendida formula è dovuta ad Eulero[2].

L'uso della lettera greca ζ fu in seguito usata da Riemann e la serie, estesa dal campo reale al campo della variabile complessa s, è nota come *funzione Zeta di Riemann.*

Si noti che, per s=1, la serie armonica diverge, perciò anche il prodotto a 2° membro della **[7]** deve divergere, il ché è possibile solo se l'insieme dei numeri primi è infinito. Si ottiene così una elegante dimostrazione, alternativa a quella di Euclide, dell'infinità dei numeri primi.

3. Primo prolungamento analitico.

Abbiamo detto che la serie ζ(s) non converge per s<1 (s reale). E' possibile però prolungare il dominio di convergenza all'intervallo]0, 1[mediante un bell'artificio di calcolo dovuto al solito Eulero.

Considero la serie

[8] $\eta(s)=1-\frac{1}{2^s}+\frac{1}{3^s}-...+\frac{(-1)^{n-1}}{n^s}...=\sum_{n=1}^{\infty}\frac{(-1)^{n-1}}{n^s}$, che, essendo a segni alterni, converge per tutti gli s>0 (assolutamente per s>1, semplicemente per s≤1). (*In particolare, per s=1 converge a Log(2)*).

Ora, notiamo che $\eta(s)=\zeta(s)-2(\frac{1}{2^s}+\frac{1}{4^s}+\frac{1}{6^s}+...)=\zeta(s)-\frac{2}{2^s}\zeta(s)$ e quindi

[9] $\zeta(s)=\frac{\eta(s)}{1-\frac{1}{2^{s-1}}}$, che mostra come ζ(s) converga per ogni **s>0**, **escluso 1**.

Che la **[9]** sia veramente un prolungamento della serie originale ζ(s) (formula **[3]**), si verifica calcolando con la **[9]** e con la **[3]** il valore di ζ(s) per alcuni valori di s>1, per esempio s=2 ($\pi^2/6$), s=4 ($\pi^4/90$), s=6 ($\pi^6/945$).[3]

[2] Leonard Euler, Introductio in Analysin infinitorum, Vol. I, cap. XV, Lione 1797.

[3] Vedi il mio articolo "*π è dappertutto*" sull'Annuario dello Scorza o scaricandolo dal mio sito: *digilander.libero.it/ottavioserra0*, cartella "Articoli".

Il teorema dei numeri primi.

Gauss aveva notato che approssimativamente il numero dei numeri primi ≤ n era $\pi(n) \approx \frac{n}{\log n}$, approssimazione tanto migliore quanto più grande è n. Si noti che il rapporto tende ad 1, la differenza Δ supera invece ogni limite: è la differenza relativa Δ / π(n) che tende a zero.

n	π(n)	n/log n	π(n)/(n/log n)	[π(n)–n/log(n)]/ π(n)
1.000	168	145	1,1586	0,1369
10.000	1.229	1.086	1,1317	0,1164
100.000	9.592	8.686	1,1043	0,0945
1000.000	78.498	72.382	1,0845	0,0779
10.000.000	664.579	620.421	1,0712	0,0664
100.000.000	5.761.455	5.428.681	1,0613	0,0578
1.000.000.000	50.847.534	48.254.942	1,0537	0,0510

Né Gauss, né altri fino al 1896 riuscirono a dimostrare il teorema intuito da Gauss; verso il 1850 il russo Cebicev dimostrò solo che, se $\pi(n) = \frac{A.n}{\log n}$, allora A deve essere 1. Riemann lo usò nelle sue ricerche sulla funzione Zeta, ma non tentò di dimostrarlo. Finalmente il francese Hadamard e il belga De La Vallèe Poussin, indipendentemente uno dall'altro, lo dimostrarono nel 1896 utilizzando strumenti di analisi complessa e il teorema affermante che la funzione Zeta di Riemann, ζ(s), considerata nel campo complesso, non ha zeri sulla retta x=Re(s)=1. Il legame tra la funzione Zeta e il teorema dei numeri primi è molto profondo. In particolare, ogni risultato sull'**assenza** di zeri nella striscia aperta 1/2< Re(s) <1 ha **conseguenza** sulla bontà dell'approssimazione di π(x) con Li(x), *logaritmo integrale di* x : $Li(x) = \int_2^x \frac{dt}{\log t}$,che in ogni caso dà un'approssimazione migliore di x /log x. Nel 1901 Von Kock dimostrò che ***se l'assenza di zeri nella striscia suddetta (***1/2< Re(s) <1) ***è vera***, allora π(x) = Li(x)+O($\sqrt{x}$.log x). Perciò dimostrare la congettura di Riemann, che ancora resiste, equivarrebbe a dimostrare il teorema di Von Kock, che probabilmente rappresenta la migliore approssimazione possibile per π(x).

Nota sul simbolo "O". f(x)=g(x)+O(h(x) significa che, per x→∞, |f(x)-g(x)|<|h(x)|.

La congettura (o ipotesi) di Riemann, dice che tutti gli zeri complessi *non banali* di ζ(s) hanno parte reale =1/2 (zeri non banali sono quelli diversi dagli interi negativi pari, come vedremo).

Riporto per comodità la tabella precedente completata con i valori di Li(x).

n	π(n)	n/log n	π(n)/(n/log n)	Li(n)	π(n)/Li(n)
1.000	168	145	1,1586	174	0,9655
10.000	1.229	1.086	1,1317	1.243	0,9887
100.000	9.592	8.686	1,1043	9.626	0,9965
1.000.000	78.498	72.382	1,0845	78.624	0,9984
10.000.000	664.579	620.421	1,0712	664.914	0,9995
100.000.000	5.761.455	5.428.681	1,0613	5.762.205	0,99987
1.000.000.000	50.847.534	48.254.942	1,0537	50.849.231	0,999967

Come si vede, n/log n dà un valore approssimato per difetto di π(n), Li(n) approssimato per eccesso, ma molto migliore. Però per numeri n immensamente grandi, dell'ordine di 10^{316}, Li(x) non dà sempre valori per eccesso (Per il calcolo di Li(x), si scarichi dal mio sito, cartella *Eseguibili*, sottocartella *calcolo*, il programma *Funzioni integrali speciali*. Nella stessa cartella il programma *Riemann* consente di calcolare valori di ζ(s) per s reale).

Risultati della scuola inglese. Nel 1914 Hardy dimostrò che esistono infiniti zeri sulla retta x=1/2; ma ciò non significa che **tutti abbiano parte reale 1/2.**

Nello stesso anno Lettlewood dimostrò che, se la congettura di Riemann è vera, Li(x)– π(x) oscilla infinite volte da valori positivi a valori negativi.

Solo nel 2000 Richard Hudson e Carte Bays dimostrarono che la prima inversione (Li(x)< π(x)) avviene in prossimità di $1{,}39822.10^{316}$.

3. Secondo prolungamento analitico.

La funzione ζ(s) non è definita per s<0. E'possibile, però, utilizzando un importante risultato di Eulero, estendere il dominio ai numeri reali negativi, per cui la funzione sarà calcolabile per tutti i numeri reali, escluso 1. La formula di Eulero è la seguente:

[10] $\zeta(s) = \frac{(2\pi)^s}{\pi} sen(\frac{s\pi}{2})\Gamma(1-s)\zeta(1-s)$, essendo **Γ** la funzione euleriana

$\Gamma(x) = \int_0^{+\infty} t^{x-1}e^{-t}dt$, che per x = n, intero positivo, dà il fattoriale di n-1. (Vedi nota 1 a pag.1)

La **[10]** consente di calcolare ζ(s) per valori negativi di s a partire da valori di s>1. In particolare, per **s intero negativo pari**, ζ(s)=0, perché si annulla il seno (**zeri *banali* della funzione ζ**).

Come abbiamo detto, la congettura di Riemann afferma che tutti gli zeri non banali di ζ(s) sono numeri complessi con parte reale=1/2. Fino ad oggi la congettura ha resistito ad ogni tentativo di dimostrazione. E'stato dimostrato che esistono infiniti zeri sulla retta x=1/2, ma non che questi esauriscano tutti gli zeri non banali. Tra l'altro il calcolo effettivo di tali zeri è molto difficile. I primi 15 furono calcolati dal danese Gram nel 1903. Riporto, a titolo di esempio, i primi tre:[4]

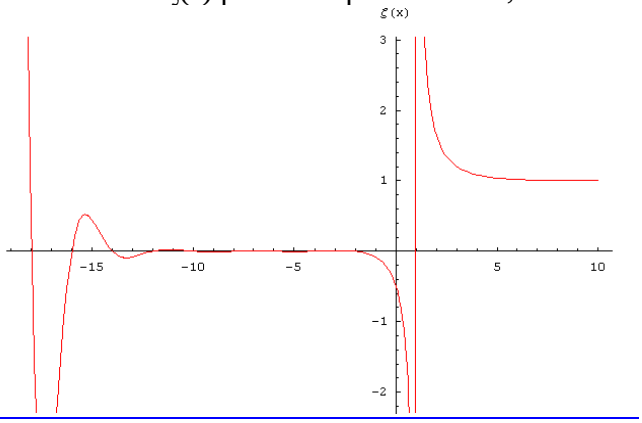
1/2 ± 14,134725i
1/2 ± 21,022040i
1/2 ± 25,010858i.

In seguito Andrew Odlyzko calcolò milioni di zeri, dei quali riporto i primi 20.

14.134725142	
21.022039639	52.970321478
25.010857580	56.446247697
30.424876126	59.347044003
32.935061588	60.831778525
37.586178159	65.112544048
40.918719012	67.079810529
43.327073281	69.546401711
48.005150881	72.067157674
49.773832478	75.704690699
	77.144840069

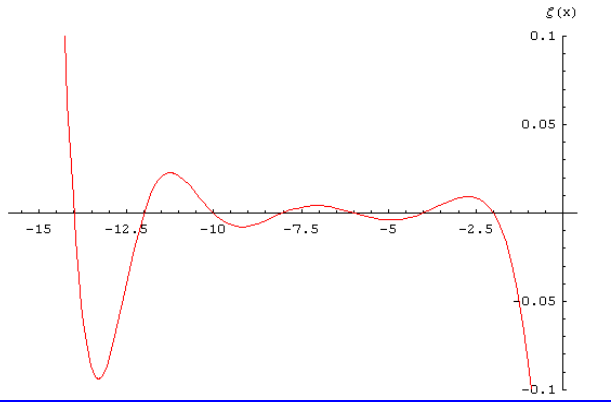
Nel 2004 Gourdon e Demichel hanno raggiunto i 10 mila miliardi di zeri, tutti con Re(Z)=1/2.

Il seguente è un grafico della funzione ζ(s) per s compreso tra -18,5 e 10:



Si noti che ζ(0)= -0,5. Per ottenerlo, occorre usare la formula di Laurent (vedi il mio programma *Riemann*, nel sito citato).

[4] John Derbyshire: "L'ossessione dei numeri primi", La biblioteca di Le Scienze, 2009.



Particolare del grafico precedente, per s compreso tra -15,5 e 0. [5]

Per il calcolo di ζ(s) per valori reali di s si può usare il mio programma "*Riemann*" nella cartella "*Calcolo*", sottocartella di *"Eseguibili"*, del mio sito.

Considerazioni conclusive.

Dai risultati finora ottenuti seguono alcune conseguenze, delle quali riporto alcune.

a) La probabilità che il numero N sia primo è asintoticamente 1/log(N).

b) L'N^{mo} numero primo è asintoticamente Nlog(N).

(*Asintoticamente* vuol dire che l'approssimazione è tanto migliore quanto più grande è N).

c) La dimostrazione della congettura di Riemann potrebbe spianare la strada alla scoperta di metodi polinomiali per la fattorizzazione di numeri primi grandi e ciò potrebbe mettere in crisi la crittografia a *chiave pubblica* che finora ha garantito la sicurezza informatica delle transazioni finanziarie e commerciali. Infatti, mentre è possibile ottenere in tempi ragionevoli numeri primi "*grandi*", dell'ordine delle cento cifre o più, utilizzando il piccolo teorema di Fermat[6] , il prodotto di due numeri primi siffatti (prodotto dell'ordine di 200 cifre) richiede tempi proibitivi per la fattorizzazione, ma la conoscenza dei fattori è necessaria per la decodifica (chiave privata). La fattorizzazione richiede infatti algoritmi di complessità "*esponenziale*" (almeno fino ad oggi).

A titolo di esempio riporto un numero di 64 cifre:

9876543219876543219876543219876543219876543219876543219876543211

che il mio programma (*nota 6*) riconosce essere composto in una frazione di secondo, mentre la fattorizzazione, eseguita col programma "Mathematica 4.2" di Wolfram (Università di Honolulu) richiede circa 6 minuti (e meno male che il primo fattore, 7243, è **molto** piccolo):

```
Timing[FactorInteger[9876543219876543219876543219876543219876543219876543219876543211]]

{338.531 Second, {{7243, 1}, {4717956422034289037345785 9, 1}, {2890231022121151062371079761792 5003, 1}}}
```

Le cose diventano drammatiche per i seguenti numeri primi di 41 cifre l'uno:

```
p =38421491444031199954016219846067329821621
  è probabilmente primo
p =38421491444031199954016219846067329821609
  è probabilmente primo
```

il cui prodotto, di 82 cifre,

```
14762110047837627026685757419429284338111161761502008802861001388474587077212081 89 è certamente composto
```

come riconosce in un secondo il mio programma, ma che "Mathematica" non è riuscito a fattorizzare in un'ora di elaborazione.

[5] Grafici presi da Wikipedia.

[6] Vedi sul mio sito il programma "Test di primalità basato sul piccolo teorema di Fermat", cartella *eseguibili*, sottocartella "*Aritmetica*".

Si verifica facilmente che il test di primalità basato sul piccolo teorema di Fermat ha complessità logaritmica o poco più; si tratta di vedere, infatti, se $Z = y^n = 2^{p-1}$ è congruo ad 1 (mod. p). L'algoritmo è molto semplice e lo riporto qui di seguito:
Posto all'inizio Z=1, b=2,
mentre n>0 **si esegua**:
[se n è dispari si ponga Z: = Z*b; **in ogni caso** si ponga n:=n div 2 e b:=b^2]. Naturalmente, a ogni passo Z e b vanno ridotti all'anello delle classi resto modulo p. Se n è un numero di k cifre, il numero c dei cicli che lo riducono a zero è tale che $2^c \geq 10^k \rightarrow c \geq k/LOG(2) = \approx k/0{,}3$. Per un numero di 100 cifre il numero c dei cicli è circa 333.
La crittografia non si basa soltanto sui numeri primi, c'è, per esempio, il metodo delle sequenze di numeri "*random*" (pseudo casuali). [7]

Per finire, una critica didattica. Trovo assurdo che nella scuola media o nel biennio di scuola secondaria si insegni a trovare il massimo comun divisore di due numeri mediante scomposizione in fattori primi (algoritmo di complessità esponenziale) anziché mediante il metodo euclideo delle divisioni successive, di rara bellezza e semplicità oltre che di complessità logaritmica. Il metodo dei fattori primi va bene per trovare il massimo comune divisore di 12 e 18 o giù di lì, ma provate con numeri dell'ordine delle migliaia o delle decine di migliaia con carta e penna, dell'ordine dei miliardi con un computer!

[7] Vedi sul mio sito il programma "Cripto" nella cartella *eseguibili*, sottocartella "*Vari*".