EMMECI quadro
Scienza Educazione E Didattica

n. 55
dicembre 2014

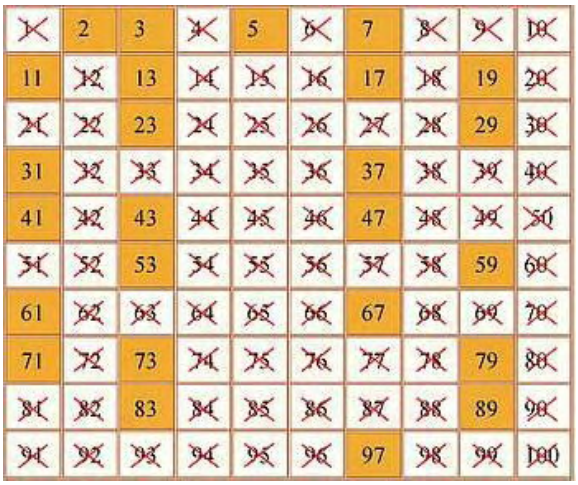
IL CONTEGGIO DEI NUMERI PRIMI

di Loïc Grenié*

* Ricercatore di Matematica presso l'Università di Bergamo

I numeri primi sono infiniti? Si, lo ha dimostrato Euclide. Ma molte altre questioni si possono affrontare sul loro comportamento, e di questo tratta l'articolo, esaminandone alcune.
Si può costruire un diagramma che rappresenta il loro numero in funzione del valore dei numeri interi e ci si può domandare quale si il suo comportamento asintotico, cercando di approssimarlo con una funzione; si può tentare di introdurre nel campo complesso un analogo del numero primo; ci si può infine chiedere se sono infinite le coppie di numeri primi «gemelli» (numeri primi che differiscono di due unità, come 17 e 19).

Lo studio dei numeri primi ha da sempre affascinato i matematici fin da quando Euclide nel 300 a.C. dimostrò che ve ne sono infiniti. Uno dei problemi più semplici riguarda l'esistenza di infinite coppie di numeri primi «gemelli», ovvero di numeri primi distanziati di 2, come ad esempio 3 e 5, 11 e 13, 17 e 19.
Questa congettura è a tutt'oggi irrisolta, nonostante numerosi matematici vi ci siano cimentati. Tuttavia, nell'aprile del 2013 Yitang Zhang (1955 -…), un matematico americano di origine cinese, perlopiù sconosciuto alla comunità scientifica internazionale, ha annunciato di avere dimostrato che esistono infinite coppie di numeri primi che differiscono meno di 70 milioni.
Grazie all'intuizione di Zhang, che per la sua scoperta ha seguito una strada che molti ritenevano sterile, si è aperto tra gli esperti di teoria analitica dei numeri un rinnovato interesse attorno all'argomento; sono state trovate dimostrazioni alternative e più semplici di quella di Zhang e il limite di 70 milioni è stato abbassato a circa 300.
In questo articolo intendiamo fare un approfondimento sui numeri primi e dare al lettore alcune idee di quali siano gli strumenti utilizzati per studiarne la distribuzione.



La funzione enumeratrice dei primi

Che cos'è un numero primo?

Tutti sanno che cos'è un numero primo: «facile: è un intero divisibile solo per 1 e se stesso». Un po' facile infatti.
La prima domanda che uno si può chiedere a questo punto è: ma 1 lui, è primo o no? Se si prende la definizione data sopra, la risposta sembra essere «sì».
Ricordiamoci però di un risultato molto importante: ogni intero positivo può essere scritto come prodotto di primi e, se si ordinano i numeri primi in ordine crescente, la scrittura è unica. A questo punto diventa chiaro che 1 non può essere un numero primo. Infatti se lo fosse avremmo:

$$6 = 2 \cdot 3 = 1 \cdot 2 \cdot 3 = 1 \cdot 1 \cdot 2 \cdot 3 = \cdots$$

e quindi non ci sarebbe più unicità. Una definizione corretta potrebbe essere quindi la seguente: un numero primo è un intero diverso da 1 divisibile solo per 1e se stesso.
La situazione si complica un po' se vogliamo includere gli interi negativi. La scrittura di un intero è sempre unica purché si decomponga il valore assoluto in prodotto di primi e si aggiunga il segno:

$$6 = +1 \cdot 2 \cdot 3$$

$$-6 = -1 \cdot 2 \cdot 3$$

Una domanda un po' più insidiosa sorge allora: infatti 2 diventa divisibile per -1e -2 oltre che 1 e 2. Rimane primo? Certo.
Quindi 2 è primo ed è divisibile per 4 interi: ±1 e ±2. Ma anche -2 è divisibile per questi 4 interi, quindi anche lui è primo? Stranamente la risposta a questa domanda non è univoca.
Se decidiamo che -2 (e quindi anche -3, -5, e tutti gli altri) sono primi anche loro, non serve più il segno:

$$6 = 2 \cdot 3$$

$$-6 = -2 \cdot 3$$

ma perdiamo apparentemente l'unicità:

$$6 = 2 \cdot 3 = -2 \cdot (-3)$$

$$-6 = 2 \cdot (-3) = -2 \cdot 3$$

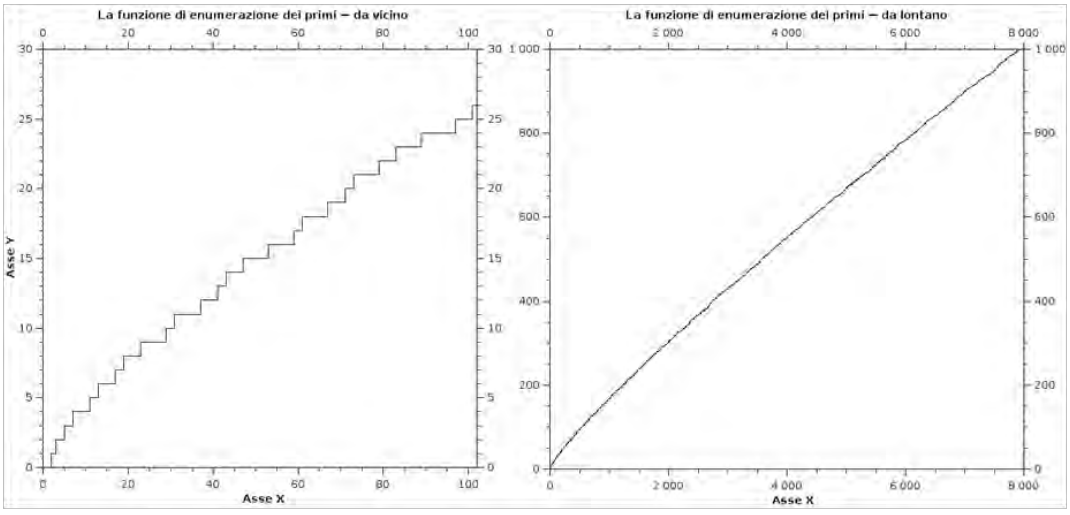
Tuttavia la possiamo riottenere dicendo che la scrittura è unica a meno del prodotto di (alcuni) termini per -1. Nel caso degli interi, se soltanto uno deve essere primo tra -2 e 2 c'è una scelta naturale: è chiaramente 2 che dobbiamo scegliere.
Ci sono casi in cui la scelta però non è così ovvia, anzi, è arbitraria. Se ci limitiamo agli interi la definizione corretta (e naturale) è «un numero primo è un numero p maggiore di 1 e divisibile soltanto per ±1 e ±p». Se invece siamo in un ambito un po' più esteso, per esempio il caso dei campi di numeri che introdurremo nell'ultima sezione, la definizione può essere «un numero primo è un numero p diverso da ±1 divisibile solo per ±1 e ±p».
Per il momento ci teniamo la definizione classica: un intero p è primo se e solo se $p \geq 2$ ed è divisibile soltanto per ±1 e ±p.

La funzione $\pi(x)$

Una delle funzioni preferite della teoria analitica dei numeri è la cosiddetta funzione enumeratrice dei primi π. Se $x \in \mathbb{R}$ allora $\pi(x)$ è il numero di primi p tali che $2 \leq p \leq x$.
È immediato che se $x < 2$ allora $\pi(x) = 0$, se $2 \leq x < 3$, allora $\pi(x) = 1$ e così via.
La funzione è discontinua (ma continua a destra), con discontinuità a salto, con un salto di 1 negli interi primi. Il grafico della funzione, da vicino e da un po' più lontano, è mostrato nella seguente figura.

Andamento generale di $\pi(x)$

È ben chiaro che, a parte 2, i numeri primi saranno tutti dispari per cui la distanza minima tra due primi è 2 (tranne all'inizio). È anche abbastanza intuitivo che man mano che si va avanti nei numeri, i primi si diradano: infatti quando verifichiamo se un intero è primo o no, dobbiamo verificare se è divisibile per ciascuno dei primi precedenti e quindi più è grande, più ci sono primi minori di lui e quindi maggiori sono le probabilità che non sia primo.



La distanza tra due primi successivi tende quindi ad aumentare, ma soltanto in media. Il fatto che la distanza non sia in aumento costante si osserva sul grafico della funzione $\pi(x)$.
Infatti, poiché quest'ultima rimane costante tra due primi successivi, le irregolarità della crescita di $\pi(x)$ corrispondono alle irregolarità delle distanze tra due primi successivi. Il diradamento dei primi ha come conseguenza che la funzione è sostanzialmente concava, cioè con una curvatura aperta verso il basso.

Andamento asintotico

La funzione $\pi(x)$ ha un comportamento noto per x che tende all'infinito. Nel seguito useremo la «solita» notazione per l'asintotico, cioè $f \sim g$ se e solo se

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$$

Vari matematici dalla fine del 1700 alla metà del 1800 hanno cercato una funzione semplice (o, piuttosto, nota) f che approssimi bene π per x tendente a $+\infty$. Presentiamo nella tabella seguente alcuni di questi (famosi) matematici e la funzione da loro proposta:

Anno, Persona	Funzione proposta
1792 o 1793, Gauss	qualcosa di simile a $\frac{x}{\ln(x)}$
1797 o 1798, Legendre	$\frac{x}{A\ln(x)+B}$ con A e B ignoti
1808, Legendre	$\frac{x}{\ln(x) - 1{,}08366}$
1838, Dirichlet	$\mathrm{Li}(x)$

dove $\mathrm{Li}(x) = \int_2^x \frac{dt}{\ln(t)}$ è una variante del logaritmo integrale.

Tutte le funzioni da loro proposte sono asintotiche una all'altra, almeno se si sceglie $A=1$ nella prima funzione proposta da Legendre. L'ultima proposta, $\mathrm{Li}(x)$, è quella che approssima meglio $\pi(x)$.
Nel 1848 e 1850, Pafnutij L. Chebyshev (1821-1894) tentò di dimostrare una tale formula. Non vi riuscì, ma introdusse l'uso della funzione ζ di Riemann (1826-1866), di cui parleremo sotto, e di due funzioni che portano il suo nome: le funzioni θ e ψ di Chebyshev.
Anche se non riuscì a dimostrare che

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

dimostrò che se il limite esiste, è per forza 1.
Inoltre provò che, se x è sufficientemente grande, si ha

$$0{,}92 \le \pi(x)\frac{\ln(x)}{x} \le 1{,}11$$

(quindi non troppo lontano da 1).

Riemann stesso, nel 1859, fece un tentativo per dimostrare lo stesso risultato, estendendo l'uso della sua funzione ζ, ma senza riuscire a dimostrare l'esistenza del limite di cui sopra.
Finalmente nel 1896 due articoli pubblicati indipendentemente da Jacques Hadamard (1865-1963) e Charles J. de la Vallée–Poussin (1866-1962) riuscirono a dimostrare che $\pi \sim \mathrm{Li}$, usando ed estendendo le idee di Riemann. Questo risultato viene chiamato *Teorema dei numeri primi*.

La distribuzione asintotica dei primi

Il significato del teorema dei numeri primi sulla distribuzione dei primi è il seguente. Denotiamo p_n l'n-esimo numero primo cosicché $p_1=2$, $p_2=3$, … Il teorema dei numeri primi ha come conseguenza che $p_n \sim n \ln(n)$ o che, vicino ad un intero relativamente grande N ,gli interi primi sono circa $1/\ln(N)$ del totale (è sostanzialmente quello che aveva osservato Gauss).
Per dare un'idea della regolarità e dell'irregolarità del comportamento riportiamo sotto il numero d_k di primi tra N-$10\ln(N)$ e N+$10\ln(N)$ per $N=10^k$ e $k=1,\ldots,100$.

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
d_k	6	18	22	16	16	19	19	17	16	19	28	22	16	21	18	13	22	22	24	24
k	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40
d_k	26	22	17	14	15	16	23	19	19	18	21	15	19	16	22	16	22	24	22	30
k	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59	60
d_k	17	20	23	18	20	23	16	15	20	19	22	16	20	9	19	13	17	23	20	20
k	61	62	63	64	65	66	67	68	69	70	71	72	73	74	75	76	77	78	79	80
d_k	17	16	20	14	20	18	22	17	17	19	15	21	23	21	19	14	14	19	14	21
k	81	82	83	84	85	86	87	88	89	90	91	92	93	94	95	96	97	98	99	100
d_k	17	18	22	18	23	18	17	16	27	26	21	13	24	14	12	18	20	20	17	11

L'asintotico prevede che i numeri primi nell'intervallo $[N\text{-}10\ln(N);\ N\text{+}10\mathrm{Ln}(N)]$ siano

circa $\frac{1}{\ln(N)}(10\ln(N)+10\ln(N))=20$

Dalla tabella si osserva che d_k (che è tale numero di primi per $N=10^k$) rimane intorno a 20, come previsto dall'asintotico, ma che comunque varia abbastanza, tra il 9 per $k=54$ e il 30 per $k=40$. Il primo termine vale però 6, ma non lo abbiamo considerato non solo perché $k=1$ è piccolo e quindi il limite per x tendente all'infinito è poco rilevante, ma anche perché $10\text{-}10\mathrm{Ln}(10)$ è negativo, essendo quasi uguale a $-13{,}25$.

Il termine di errore

Una volta noto un asintotico per $\pi(x)$, la fase successiva è capire come si comporta $\pi(x)-f(x)$ dove f è l'asintotico che abbiamo scelto.
Qui, la funzione conveniente è $\mathrm{Li}(x)$. Infatti, nel 1914 John E. Littlewood (1885-1977) dimostrò che la funzione $\pi(x)-\mathrm{Li}(x)$ cambia segno infinite volte (non si sa ancora dov'è il suo primo cambiamento di segno, ma sicuramente precede 10^{316}).
Questo implica che la differenza non tende all'infinito. Purtroppo non si sa molto di più su questa differenza; la funzione ψ, una cugina di π, è invece meglio nota.

La funzione ζ di Riemann

Prima di parlare di ψ conviene introdurre la funzione ζ di Riemann, che in teoria dei numeri è una regina.

L'espressione come serie

Questa famosa funzione si definisce per i reali $s>1$ così.

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

La convergenza della serie è molto semplice da studiare, tutti gli studenti che hanno affrontato le serie hanno visto che questa serie converge se (e solo se) $s>1$.
Si può dare un senso naturale a questa serie se (e solo se) s è un numero complesso di parte reale maggiore di 1.

Il prodotto di Eulero

Osserviamo che, se s è un qualsiasi numero reale (o complesso), il prodotto delle potenze da 0 a 3 di $1/p^s$ per i primi p da 2 a 5 ha la seguente espressione:

$$\left(1+\frac{1}{2^s}+\frac{1}{4^s}+\frac{1}{8^s}\right)\left(1+\frac{1}{3^s}+\frac{1}{9^s}+\frac{1}{27^s}\right)\left(1+\frac{1}{5^s}+\frac{1}{25^s}+\frac{1}{125^s}\right)=$$
$$1+\frac{1}{2^s}+\frac{1}{3^s}+\frac{1}{4^s}+\frac{1}{5^s}+\frac{1}{6^s}+\frac{1}{8^s}+\frac{1}{9^s}+\frac{1}{10^s}+\frac{1}{12^s}+\frac{1}{15^s}+\frac{1}{18^s}+\frac{1}{20^s}$$
$$+\frac{1}{24^s}+\frac{1}{25^s}+\frac{1}{27^s}+\frac{1}{30^s}+\frac{1}{36^s}+\frac{1}{40^s}+\frac{1}{45^s}+\frac{1}{50^s}+\text{altri termini}$$

Otteniamo una parte della somma che definisce la funzione ζ. Si può capire che man mano che aumentano il numero dei primi e le potenze di questi, la somma a destra si completa. Ogni termine della somma $1/n^s$ si ottiene purché i primi che compongono n appaiano nel prodotto, fino (almeno) alla potenza con la quale compaiono in n.
Dobbiamo far tendere all'infinito sia il numero di primi che le loro potenze, per cui il procedimento analitico è un po' delicato. Per fortuna la convergenza di tutto è sufficientemente veloce per ovviare a tutti i problemi e si ottiene:

$$\forall s>1,\ \zeta(s)=\prod_{p\ primo}\sum_{n=0}^{\infty}p^{-ns}=\prod_{p\ primo}\frac{1}{1-p^{-s}}$$

Quest'ultima presentazione si chiama *il prodotto di Eulero* della funzione ζ e rimane valido per ogni complesso s con parte reale maggiore di 1.

Il prolungamento analitico

Chiunque ha studiato le serie sa che:

$$\forall x,\ |x|<1\Rightarrow\sum_{n=0}^{\infty}x^n=\frac{1}{1-x}$$

Ora, la serie a sinistra è definita se e solo se $|x|<1$ mentre la funzione a destra è definita per ogni x (diverso da 1). Si dice che la funzione di destra è un *prolungamento analitico* di quella di sinistra.
Per passare «attraverso» 1, si deve utilizzare il caso in cui x è complesso per «girare attorno» a 1 (invece di passare attraverso). Succede un fenomeno analogo per la funzione ζ di Riemann.
La funzione, definita inizialmente per i complessi s di parte reale maggiore di 1 può essere estesa a tutti gli $s\in\mathbb{C}$ diversi da 1.

Inoltre questo prolungamento ha una proprietà molto strana, detta *equazione funzionale*, che dice che:

$$\forall s\in\mathbb{C},\zeta(s)=2^s\pi^{s-1}\sin(\tfrac{\pi s}{2})\Gamma(1-s)\zeta(1-s).$$

Nell'equazione precedente, Γ è una funzione nota che, tra varie proprietà, è una funzione definita ovunque che «interpola» il fattoriale nel senso che se è intero, allora $\Gamma(n+1)=n!$; la definizione precisa della funzione gamma è:

$$\forall s\in\mathbb{C}\ \text{t.c.}\ \Re s>0,\Gamma(s)=\int_0^{\infty}t^{s-1}e^{-t}dt$$

con un prolungamento analitico a tutto $\mathbb{C}$ usando il fatto che $\Gamma(s+1)=s\,\Gamma(s)$.

Gli zeri

Osservando l'equazione funzionale della funzione ζ, vediamo che per $n<0$ intero:

$$\zeta(2n)=0$$

Infatti, le definizioni di ζ e Γ fanno sì che $\zeta(1-2n)$ e $\Gamma(1-2n)$ sono definiti e quindi prendendo $s=2n$ nell'equazione funzionale si vede subito che $\zeta(2n)=0$ perché, $\forall n\in\mathbb{Z}$ $\sin(\pi n)=0$.

Si dice che gli interi negativi pari sono gli *zeri banali* della funzione ζ. Ci sono altri numeri complessi ρ, tali che $\Re\rho \in (0,1)$ e tali che $\zeta(\rho) = 0$.

Questi numeri sono detti *zeri non banali* della funzione ζ. Usando l'espressione come prodotto di Eulero della funzione ζ, si può intuire – e, come vedremo più avanti, dimostrare – che gli zeri della funzione ζ sono legati alla distribuzione dei numeri primi.

Le funzioni di Chebyshev

Definizione delle funzioni θ e ψ

Chebyshev ha introdotto due funzioni importanti, la funzione θ e la funzione ψ. La prima è una versione «pesata» di π. Precisamente,

$$\vartheta(x) = \sum_{p \le x} \ln(p)$$

dove la somma è sui numeri p primi. Si dice che è una versione pesata di π perché la funzione π può essere riscritta come:

$$\pi(x) = \sum_{p \le x} 1$$

Visto che la funzione $\ln$ cresce lentamente, si capisce facilmente (e si dimostra senza difficoltà) che:

$$\pi(x) \sim \frac{\vartheta(x)}{\ln(x)}$$

La funzione più semplice da studiare è l'ulteriore variante:

$$\psi(x) = \sum_{n \le x} \Lambda(n)$$

Dove $\Lambda(n) = \ln(p)$ se e solo se n è una potenza (non nulla) del primo p, e 0 altrimenti. In modo analogo a quanto detto sopra, abbiamo:

$$\psi(x) \sim \vartheta(x) \text{ e quindi } \pi(x) \sim \frac{\psi(x)}{\ln(x)}.$$

Il teorema dei numeri primi è quindi equivalente a $\psi(x) \sim x$.

Il legame con la funzione ζ

Informazioni sul comportamento di $|\pi(x) - \mathrm{Li}(x)|$ possono essere ottenute a partire da analoghe informazioni su $|\psi(x)-x|$, la quale risulta più facile da studiare poiché direttamente collegata alla funzione ζ di Riemann.
Più precisamente, se $x > 1$,

$$\psi(x) = -\frac{1}{2i\pi}\int_{\sigma-i\infty}^{\sigma+i\infty} \frac{\zeta'(s)}{\zeta(s)} \cdot \frac{x^s}{s}\,\mathrm{d}s$$

per qualsiasi $\sigma > 1$, dando il significato seguente all'integrale: $s=\sigma+it$ con $t \in \mathbb{R}$ quindi $\mathrm{d}s=i\mathrm{d}t$ e l'integrale deve essere inteso come l'integrale della parte reale più i volte l'integrale della parte immaginaria.

La stima dell'integrale

Per riuscire a dimostrare una maggiorazione per $|\psi(x)-x|$, usiamo un ulteriore parametro $T > 0$ per approssimare il termine con l'integrale con:

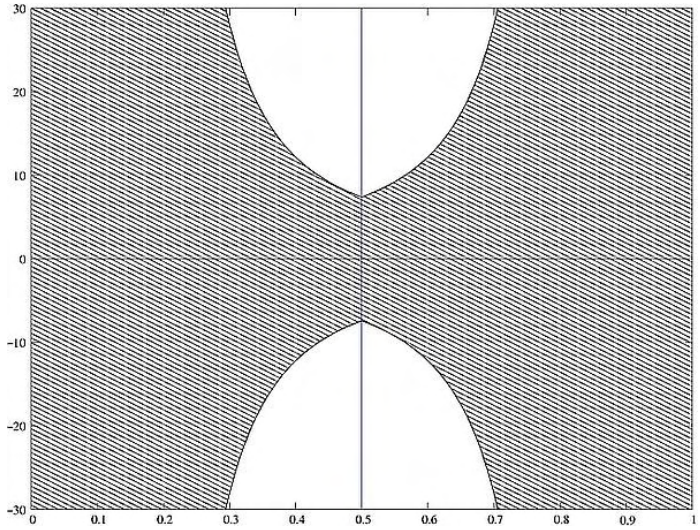
$$I = -\frac{1}{2i\pi}\int_{\sigma-iT}^{\sigma+iT} \frac{\zeta'(s)}{\zeta(s)} \cdot \frac{x^s}{s}\,\mathrm{d}s$$

una scelta classica è $\sigma = 1+1/\ln(x)$ e $T = \sqrt{x}$. Rimangono poi da stimare $\psi(x) - I$, e ciò non è molto difficile, e I che risulta più sottile da affrontare.
Senza entrare troppo nei dettagli, per calcolare l'integrale invece di andare direttamente da $\sigma - iT$ a $\sigma + iT$, si fa un giro lungo verso la sinistra.

A questo punto entrano in gioco gli zeri della funzione ζ. La parte più sottile del lavoro di Hadamard e de la Vallée–Poussin consiste nel dimostrare che gli zeri non banali stanno in una zona del piano complesso della forma:

$$\left|\mathrm{Re}\, s - \frac{1}{2}\right| \leq \frac{1}{2} - \frac{c}{\ln(|\mathrm{Im}\, s|)}$$

per una certa costante c, non esplicita. Con questo risultato di localizzazione si riesce a dimostrare che $\psi(x) \sim x$.
La zona senza zeri dimostrata da Hadamard e de la Vallée–Poussin, scegliendo c=1, è la parte strisciata nel seguente grafico.



Poiché il logaritmo cresce piano la zona rimane relativamente larga quando $\mathrm{Im}\, s$ è piccolo ma invece, per $\mathrm{Im}\, s$ che tende all'infinito, la zona diventa infinitesimale.
L'ipotesi di Riemann dice che gli zeri non banali sono tutti contenuti nella retta verticale $\mathrm{Re}\, s = 1/2$ e sotto questa ipotesi si riesce a dimostrare che

$$|\psi(x) - x| \leq \frac{1}{2\pi}\sqrt{x}\ln^2(x) + r(x)$$

con una funzione $r(x)$ esplicita e tale che.

$$\lim_{x\to\infty} \frac{r(x)}{\sqrt{x}\ln^2(x)} = 0$$

Questa stima è la «migliore» che si può ottenere nel senso che Chebyshev ha dimostrato che l'ipotesi di Riemann è vera se e solo se esiste una costante positiva c tale che:

$$\forall x \geq 2, |\psi(x) - x| \leq c\sqrt{x}\ln^2(x)$$

Sviluppi ulteriori

Primi gemelli, cugini e sexy

Abbiamo visto l'andamento generale, all'infinito, della distribuzione dei primi. Cosa si può dire invece della ripartizione specifica dei primi?
Come abbiamo visto, a parte all'inizio, la distanza tra due primi successivi è come minimo 2. Due primi a distanza 2 si dicono gemelli. Quante coppie di numeri primi gemelli esistono? Sono note tali coppie circa fino a 10^{200000}.
Si suppone, ma non si sa dimostrare, che esistano infinite coppie di primi gemelli. Le coppie di primi a distanza diversa da 2 sono meno studiate. Ad esempio si dice che i primi a distanza 4 uno dall'altro sono primi «cugini» mentre quelli a distanza 6 sono primi *sexy* (gioco di parole con l'inglese "six"). Questo argomento si chiama: *primi in intervalli corti*.

L'argomento è in grande fermento in questo periodo (Dicembre 2014). Per darne una spiegazione, ricordiamo che p_n è l'n-esimo numero primo. Nel 2005, Dan Goldston (1954-…), János Pintz (1950-…) e Cem Yıldırım (1961-…) dimostrarono che, facendo una congettura ancora più complicata dell'ipotesi di Riemann, detta EH, si poteva dimostrare che esistono infiniti primi p_n tali che $p_{n+1} - p_n \leq 16$. Il 14 Maggio 2013, Yitang Zhang ha trovato un modo per dimostrare, senza ipotesi, che esistono infiniti primi p_n tali che $p_{n+1} - p_n \leq 70000000$.
Sotto l'impulso di Terence Tao (1975-…) e grazie a un risultato dovuto a James Maynard, che ha trovato una dimostrazione decisamente migliore di quella di Zhang, questo limite scende quasi quotidianamente. Dopo un anno il limite è sceso da 70000000 a 246, mentre si sono dimostrati (e abbassati) i limiti per $p_{n+m} - p_n$ per alcuni $m \geq 1$.
Durante questo periodo, è stato dimostrato che supponendo EH allora esistono infiniti primi p_n tali che $p_{n+1} - p_n \leq 12$ e, supponendo una sua versione più generale, si scende a $p_{n+1} - p_n \leq 6$ (quindi ci sono infiniti primi gemelli, cugini e/o sexy). Nel retroscena, Yoichi Motohashi ha riconosciuto di aver provato una strada simile a quella di Zhang ma di averla abbandonata prima di aver capito che poteva portare al risultato desiderato. Ulteriori sviluppi si possono trovare cercando *primes in small gaps* su Internet.

Campi di numeri

Chiameremo *numero algebrico* un numero complesso z per il quale esistono un intero $n \geq 1$ e degli interi $a_0, \ldots, a_n$ (con $a_n \neq 0$) tali che:

$$a_n z^n + \ldots + a_1 z + a_0 = 0$$

Se possiamo inoltre prendere $a_n = 1$, si dice che z è un *intero algebrico*.
Sia z un numero algebrico (non necessariamente intero) e consideriamo:

$$K = \mathrm{Q}[z] = \left\{ \sum_{i=0}^{k} b_i z^i \right\}$$

con $k \geq 0$ e tutti i b_i razionali. Un tale K si dice *campo di numeri*.
Si può verificare senza difficoltà che tutti gli elementi di un campo di numeri sono numeri algebrici. L'insieme degli interi algebrici in K si chiama *anello degli interi* di K e si denota O_K. L'insieme O_K gioca per K il ruolo di $\mathbb{Z}$ per $\mathbb{Q}$

In alcuni di questi insiemi O_K, ma non in tutti, esiste una nozione di numero primo analoga a quella degli interi primi p di cui abbiamo parlato fin qui. In questi casi c'è sempre un'ambiguità analoga a quella tra 2 e -2 di cui abbiamo parlato all'inizio e non c'è quasi mai una scelta naturale. In questi casi si sceglie come definizione di numero primo la seconda versione, cioè il caso in cui -2 è ancora un numero primo.
Per dare un po' più di concretezza a questo discorso consideriamo il caso in cui $z = i$.
In questo caso $K = \mathbb{Q}[i] = \{a + ib \mid a, b \in \mathbb{Q}\}$ e $O_K = \mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$
gli elementi di $\mathbb{Z}[i]$ si chiamano *interi di Gauss*. A ciascun numero primo p corrispondono una o due famiglie di interi di Gauss primi. Sono della forma $a+ib$ con $a^2 + b^2 \in \{p, p^2\}$

Per $p = 2$ c'è una famiglia di interi primi di Gauss corrispondenti: $\{1+i, 1-i, -1+i, -1-i\}$. In questo caso $a^2+b^2=2$.

Se $p=4k+3$ con $k \in \mathbb{N}$ c'è di nuovo una famiglia di interi primi di Gauss corrispondenti a p: $\{p, -p, ip, -ip\}$. In questo caso $a^2+b^2=p^2$.

Se $p=4k+1$ con $k \in \mathbb{N}$ si può dimostrare che esistono allora due interi u e $v \in \mathbb{N}$ tali che $u^2+v^2=p$ e ci sono allora due famiglie corrispondenti a p: $\{u+iv, -u-iv, -v+iu, v-iu\}$ e $\{u-iv, -u+iv, v+iu, -v-iu\}$. In questo caso $a^2+b^2=p$.

L'equivalente del segno ± 1 degli interi è per il segno complesso $\{1, -1, i, -i\}$ e spiega perché le famiglie di cui sopra siano costituite da quattro elementi. Nel caso di $\mathbb{Z}[i]$ se volessimo l'unicità della decomposizione in primi bisognerebbe scegliere un primo in ciascuna famiglia. Una scelta vagamente naturale sarebbe prendere quello dei

quattro che sta nel primo quadrante. In realtà questa scelta non è poi così naturale e comunque questo è l'unico altro campo, oltre a $\mathbb{Q}$ in cui una qualche scelta naturale sia possibile. È la ragione per la quale, quando si considerano i campi di numeri, si lascia perdere l'unicità.

Nei casi più generali la nozione di numero primo non esiste più e bisogna sostituirla con la nozione di ideale primo. Per capire da dove viene la nozione, possiamo considerare il caso di $K = \mathbb{Q}[i\sqrt{5}]$ per il quale $O_K = \mathbb{Z}[i\sqrt{5}] = \{a + ib\sqrt{5} \mid a, b \in \mathbb{Z}\}$

Abbiamo allora:

$$6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$$

Per avere una decomposizione unica servirebbero quattro elementi x, y, z e t in tali che:

$$\begin{aligned} 2 &= x \cdot y \\ 3 &= z \cdot t \\ 1 + i\sqrt{5} &= x \cdot z \\ 1 - i\sqrt{5} &= y \cdot t \\ 6 &= x \cdot y \cdot z \cdot t \end{aligned}$$

ma si può verificare che tali elementi sono impossibili da ottenere.

Ernst E.Kummer (1810-1893) li ha quindi chiamati *elementi ideali* e Richard Dedekind (1831-1916) è riuscito a dare la definizione formale di *ideale*, che è quella che si usa in teoria degli anelli, che ha permesso di dare un senso compiuto all'intuizione di Kummer.

L'ideale non è come l'unità immaginaria i, non è un numero da aggiungere, è un concetto diverso ma che si inserisce bene nella teoria. Ciascun gruppo di quattro elementi che abbiamo elencato nel caso di $\mathbb{Z}[i]$ corrisponde a un ideale e sono i suoi *generatori*. Ogni ideale primo ha una norma che è la potenza di un numero primo p; nel caso di $\mathbb{Z}[i]$ sono i p e p^2 che abbiamo indicato. Per il campo K si definisce una funzione π_K, analoga alla funzione π, che conta gli ideali primi la cui norma sta tra 2 e x. Ci sono funzioni θ_K e ψ_K, analoghe di θ e ψ, e la cosa molto strana è che qualunque sia il campo di numeri K,

$$\begin{aligned} \psi_K(x) &\sim \psi(x) \sim x \\ \vartheta_K(x) &\sim \vartheta(x) \sim x \\ \pi_K(x) &\sim \pi(x) \sim \frac{x}{\ln(x)} \end{aligned}$$

e che inoltre, facendo per il campo di numeri K un'ipotesi analoga all'ipotesi di Riemann, si ha

$$\left|\psi_K(x) - x\right| \le \frac{n_K}{2\pi}\sqrt{x}\ln^2(x) + r(x)$$

Dove n_K è la dimensione di K come spazio vettoriale su $\mathbb{Q}$

La funzione $r(x)$ è tale che $\lim_{x\to\infty} \dfrac{r(x)}{\sqrt{x}\ln^2(x)} = 0$

Il comportamento asintotico della distribuzione dei primi è quindi quasi lo stesso in tutti i campi di numeri. Per essere completi, segnaliamo che questo limite non è purtroppo uniforme in K.

L'ipotesi di Riemann

Abbiamo visto che l'ipotesi di Riemann è che gli zeri non banali della funzione ζ siano sulla retta $\mathrm{Re}\, s = 1/2$. Riemann aveva già dimostrato che i primi zeri non banali stanno effettivamente su questa retta. Il fatto che gli zeri siano su questa retta ha l'effetto che la distribuzione dei primi è la migliore possibile, nel senso che soltanto

se tutti gli zeri stanno su questa retta abbiamo che il termine di resto $|\psi(x)-x|$ è al massimo $c\sqrt{x}\ln^2(x)$, altrimenti è di ordine maggiore.

Da quando Riemann ha fatto questa ipotesi, migliaia di matematici e non matematici hanno tentato di dimostrarla. Si è verificata, prima a mano poi con i computer, la posizione di qualche milione dei primi zeri non banali e tutti stanno su questa retta. La fondazione Clay ne ha fatto uno dei suoi problemi del millennio, con un milione di dollari allegato nel caso di una dimostrazione (corretta).
Anche se nessuno è riuscito a dimostrare l'ipotesi di Riemann, ne sono state proposte diverse generalizzazioni. La più comune è la cosiddetta *ipotesi di Riemann generalizzata* che riguarda l'analoga ζ_K della funzione ζ per un campo di numeri K.
Un'altra versione, per i cosiddetti *campi di funzioni* è invece stata dimostrata da Weil nel 1942, il suo metodo però non si può estendere ai campi di numeri.
Enrico Bombieri (1940-…) ne ha dato una dimostrazione diversa nel 1973 ma nessuno è riuscito ad adattare neanche questa dimostrazione.

Diamo una breve bibliografia, in inglese, per chi desiderasse approfondire l'argomento.

Loïc Grenié (*Ricercatore di Matematica presso l'Università di Bergamo)*

Riferimenti bibliografici

[1] B. Fine and G. Rosenberger. *Number theory*. Birkhäuser Boston Inc., Boston, MA, 2007. An introduction via the distribution of primes.

[2] G. Tenenbaum and M. Mendès France. *The prime numbers and their distribution*, volume 6 of *Student Mathematical Library*. American Mathematical Society, Providence, RI, 2000.

EMMECI quadro
Scienza Educazione E Didattica

DIRETTORE RESPONSABILE Mario Gargantini
www.emmeciquadro.eu

Aut. Trib. Milano n. 226 del 24.3.2000
ISSN 2240-0389
Emmeciquadro (online)