Il postulato di Bertrand e i primi di Ramanujan

Umberto Cerruti
Università di Torino

1 Quanti sono i numeri primi?

Denotiamo con $\pi(x)$ il numero dei primi $\leq x$, dove x è un numero reale > 1. Sappiamo tutti che

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

Questo limite esprime il fatto, noto fin dai tempi di Euclide, che esitono infiniti primi.

Il famoso Teorema dei Numeri Primi (TNP), dimostrato nel 1896 da Hadamard e, indipendentemente, da de la Valleé Poussin, asserisce che

$$\pi(x) \sim \frac{x}{\log(x)} \tag{2}$$

Il TNP si può esprimere equivalentemente così

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\log(x)} = 1 \tag{3}$$

Il TNP ci dice che $\pi(x)$ tende all'infinito come $\frac{x}{\log(x)}$.

Il primo risultato pubblicato (sotto forma di ipotesi non provata) che si avvicina al TNP è dovuto a Legendre (1798):

$$\pi(x) \sim \frac{x}{A\log(x) + B} \tag{4}$$

Sebbene Legendre sia il primo ad avere pubblicato una congettura sulla distribuzione dei numeri primi analoga al TNP, Gauss aveva precedentemente eseguito (pare per puro diletto) imponenti calcoli sulla densità dei primi in un intorno di n, al crescere di n. Nella prima tavola compilata da Gauss ci si occupa dei primi fino a 50000. Nella tavola appaiono questi numeri: ci sono 168 primi tra 1 e 1000, 135 tra 1001 e 2000, $\cdots$, 89 tra 48001 e 49000, 98 tra 49001 e 50000. Questi dati convinsero Gauss che la densità dei primi in un intorno di x deve essere dell'ordine di $\frac{1}{\log(x)}$. Conseguentemente tra a e b ci devono essere circa $\int_a^b dt/\log(t)$ numeri primi. Gauss, per confermare la sua ipotesi, calcolò i numeri primi fino a 3000000, compilando altre tavole e confrontando i risultati. La precisione della formula di Gauss è impressionante. Per esempio si constata che tra 2900000 e 3000000 ci sono 6707 primi, mentre $\int_{2900000}^{3000000} dt/\log(t)$ vale circa $6712,64$.

Quindi la congettura di Gauss (non pubblicata esplicitamente) è questa:

$$\pi(x) \sim \int_2^x \frac{dt}{\log(t)} \tag{5}$$

La (5) è equivalente al TNP, ma dà un'approssimazione migliore della (2).

Il TNP ci dà informazioni assai utili sui numeri primi. Per esempio

1. La probabilità che un intero casuale N sia primo è circa $\frac{1}{\log(N)}$
2. La grandezza dell'n-esimo numero primo è dell'ordine di $n\log(n)$

Per esempio, fino a 10^{12} ci sono 37607912018 primi. Quindi la probabilità effettiva che un intero $N < 10^{12}$ casuale sia primo è $\frac{37607912018}{1000000000000} = 0.0376079$ mentre il valore approssimato prevedibile dal TNP è $\frac{1}{\log(10^{12})} = 0.0361912$.

Se ci chiediamo quanto sia grande il miliardesimo primo nella sequenza $p_1 = 2, p_2 = 3, p_3 = 5, \cdots$, dal TNP otteniamo questa previsione: sarà dell'ordine di $10^9\log(10^9) \simeq 2.07 \times 10^{10}$ mentre $p_{1000000000} = 22801763489 \simeq 2.28 \times 10^{10}$.

IL TNP è un teorema che potremmo dire *qualitativo*, che ci dà informazioni di carattere fondamentale sull'andamento asintotico della sequenza dei numeri primi, dice che il rapporto tra $\pi(x)$ e $\frac{x}{\log(x)}$ tende a 1 per x che tende all'infinito.

Ma sappiamo qualcosa di preciso su *quanti* sono i primi, ovvero sul valore di $\pi(x)$, quando x è un ben preciso numero reale assegnato?

Nel 1852 ([4]) Chebyshev dimostrò che

Teorema 1. Teorema di Chebyshev

Esiste un x_0 tale che per ogni $x \geq x_0$ si ha

$$c_1\frac{x}{\log(x)} < \pi(x) < c_2\frac{x}{\log(x)}$$

dove

$$c_1 = \log(2^{1/2}3^{1/3}5^{1/5}30^{-1/30}) \simeq 0.921292022934091$$

e

$$c_2 = \frac{6}{5}c_1 \simeq 1.10555042752091$$

In [1] si osserva che questo risultato è stato spesso riportato erroneamente nella letteratura. Per esempio si è detto che il Teorema 1 vale con $x_0 = 30$. Invece se prendiamo $x_0 = 100$, si ha $\pi(x) = 25$ ma

$$c_2\frac{x}{\log(x)} \simeq 24.0067225069056 < 25$$

In [1] si prova che $\pi(x) < c_2\frac{x}{\log(x)}$ per ogni $x \geq 96098$. Quindi si può porre $x_0 = 96098$.

Da un calcolo che ho fatto al computer, tra $x = 2$ e $x = 96097$ la diseguaglianza destra di 1 risulta falsa ben 83425 volte! Per $x = 96097$ abbiamo $\pi(96097) = 9260$ e $c_2\frac{96097}{\log(96097)} \simeq 9259.91715958754$. E' l'ultima volta che accade a $\pi(N)$ di superare $c_2\frac{N}{\log(N)}$.

Per il TNP al posto di c_2 si può mettere qualsiasi costante > 1. Se la costante è più piccola bisogna aumentare x_0, e viceversa. Per esempio si prova che

$$\text{Per ogni } x \geq 17 \quad \pi(x) < 1.25506\frac{x}{\log(x)} \tag{6}$$

Per quanto riguarda invece la disequaglianza di sinistra in 1 tutto è chiarito, grazie a un notevole risultato di Rosser e Schoenfeld del 1962, in base al quale c_1 può essere sostituita con il suo massimo valore possibile: 1.

Teorema 2. Teorema di Rosser e Schoenfeld (1962)
Per ogni $x \geq 17$

$$\pi(x) > \frac{x}{\log(x)}$$

Mettendo insieme la 6 e il Teorema 2 otteniamo

$$\text{Per ogni } x \geq 17 \quad \frac{x}{\log(x)} < \pi(x) < 1.25506\frac{x}{\log(x)} \tag{7}$$

Risultati come questo fanno toccare con mano il fatto che la sequenza dei primi all'interno di quella dei numeri interi non ha proprio nulla di casuale. Se io dipingo di blu o di rosso la sequenza dei numeri interi in conseguenza del lancio di una moneta, nessun teorema mi potrà mai garantire la presenza di almeno un numero blu (o rosso) $\leq x$. Si può conoscere soltanto una *probabilità*. Qui invece abbiamo una *certezza*. Fino a 1000, per esempio, la 7 ci garantisce che esistono non meno di 1086 e non più di 1362 primi (il valore esatto è 1229).

D'altra parte la sequenza dei primi *finge* assai bene di essere casuale, si veda per esempio [2].

Possiamo utilizzare la 7 per determinare un confine inferiore al numero dei primi compresi tra x e $2x$, in quanto sappiamo che fino a $2x$ ci sono almeno $\frac{2x}{\log(2x)}$ primi, e fino a x ci sono al più $1.25506\frac{x}{\log(x)}$ primi. Pertanto

$$\text{Per ogni } x \geq 17 \quad \pi(2x) - \pi(x) \geq \frac{2x}{\log(2x)} - 1.25506\frac{x}{\log(x)} \tag{8}$$

Possiamo dunque sapere che tra 1000000 e 2000000 ci sono almeno 47004 numeri primi (il numero esatto è 70435).

Dalla 8 si deduce che $\pi(2x) - \pi(x)$ tende all'infinito al tendere di x all'infinito.

Del resto dal TNP possiamo supporre che, per x grande, tra x e $2x$ ci siano $\frac{2x}{\log(2x)} - \frac{x}{\log(x)}$ primi. Poiché $\log(2x) = \log(x) + \log(2)$ e al crescere di x $\log(2)$ diventa trascurabile, si ha che per x grande $\frac{2x}{\log(2x)} \simeq 2\frac{x}{\log(x)}$. Quindi, anche se può sembrare strano, il TNP prevede che, asintoticamente, ci siano tanti primi tra x e $2x$ quanti tra 1 e x.

I dati confermano, ovviamente, le previsioni.

Per $x = 10^6$ si ha

- $\pi(x) = 78498$
- $\pi(2x) - \pi(x) = 70435$

Per $x = 10^7$ si ha

- $\pi(x) = 664579$

- $\pi(2x) - \pi(x) = 606028$

Per $x = 10^k$, con $k = 6 \cdots 12$, il rapporto $\frac{\pi(x)}{\pi(2x)-\pi(x)}$ vale

$$1.11447,\ 1.09661,\ 1.08349,\ 1.0733,\ 1.06531,\ 1.05888,\ 1.05362$$

Al crescere di x il rapporto tende a 1.

Concludendo, in base al TNP ci sono veramente *tanti* primi tra x e $2x$.

Come si è detto il TNP venne dimostrato solo nel 1896, con metodi di analisi complessa introdotti nel famoso lavoro di Riemann del 1892 sulla funzione $\zeta(s) = \sum_{n=1}^{\infty} 1/n^s$ (per una storia del TNP si veda [6]).

Esistono dimostrazioni elementari di questo teorema, ma sono assai complesse e difficili. L'interesse dei metodi elementari non sta solo nell'aver mostrato che si può arrivare al TNP per strade diverse: essi hanno in seguito condotto ad una maggiore comprensione della struttura dell'insieme dei numeri primi, e alla dimostrazione di teoremi nuovi, per i quali i metodi analitici sono assai meno efficaci (si veda a questo proposito [5]).

Viene allora da chiedersi, che cosa possiamo dire sul numero dei primi presenti in certi intervalli utilizzando soltanto l'aritmetica, o poco più?

2 Il postulato di Bertrand

Nel 1845 Joseph Bertrand congetturò che, per ogni intero $n > 1$, tra n e $2n$ c'è sempre almeno un numero primo.

Dopo quanto abbiamo visto, questa ipotesi sembra una gigantesca sottovalutazione. Però all'epoca nessuno sapeva come provarla. Non c'è poi da stupirsi troppo. Anche oggi (2009) nessuno sa dimostrare che esista sempre, per ogni n, un primo compreso tra n^2 e $(n+1)^2$. Un solo povero singolo primo. Eppure sperimentalmente si osserva una regolare presenza.

Per $k = 1, 2, 3, 4, 5, 6$, $\pi((10^k + 1)^2) - \pi(10^{2k})$ vale rispettivamente

$$5, 23, 152, 1081, 8668, 72413$$

Ammettiamo dunque la nostra ignoranza e torniamo al postulato di Bertrand.

Esso venne dimostrato nel 1850 da Pafnuty Chebyshev. Nel 1919 Ramanujan semplificò la dimostrazione [7]. Il postulato di Bertrand venne poi provato con metodi elementari da Erdös nel 1932.

Diamo in questo paragrafo una idea della linea di attacco di Erdös.

I personaggi principali della storia sono i coeffienti binomiali $\binom{n}{h}$, e in particolare quelli *centrali*, $\binom{2n}{n}$.

Il binomiale $\binom{n}{h}$ possiede un fondamentale significato combinatorico: è il numero dei sottoinsiemi di ordine h presi in un insieme di ordine n.

Esplicitamente si ha che per ogni $n > 0$ e per ogni $0 \leq h \leq n$

$$\binom{n}{h} = \frac{n!}{h!(n-h)!} \tag{9}$$

Ricordiamo che $n! = 1 \times 2 \times 3 \cdots \times n = \prod_{k=1}^{k=n} k$. L'intero $n!$ è il prodotto degli interi positivi $\leq n$. Poichè un numero primo p, per sua stessa definizione, non può essere scritto come prodotto di interi $\leq p$, otteniamo immediatamente il Lemma che segue.

(Notazione: $a|b$ signica che a divide b; viceversa $a \not| b$ significa che a non divide b.)

Lemma 3. *Se p è primo e $n < p$ allora $p \not| n!$*

I coefficienti binomiali appaiono ovunque in matematica (si veda per esempio il Blog [3]). Il primo luogo ove li incontriamo è la famosa formula di Newton.

Teorema 4. Formula del binomio di Newton

$$(a+b)^n = \sum_{h=0}^{n} \binom{n}{h} a^h b^{n-h}$$

Da 4 ricaviamo subito due utili diseguaglianze.

Teorema 5. *Per tutti gli interi positivi n si ha*

$$\binom{2n}{n} < 4^n$$

Dimostrazione. Da 4 ricaviamo che $2^{2n} = (1+1)^{2n} = \sum_{h=0}^{2n} \binom{2n}{h}$. Il binomiale centrale $\binom{2n}{n}$ è uno degli addendi di $\sum_{h=0}^{2n} \binom{2n}{h}$. Quindi

$$\binom{2n}{n} < \sum_{h=0}^{2n} \binom{2n}{h} = 2^{2n} = 4^n$$

□

Teorema 6. *Se n è dispari allora per ogni $0 \leq k \leq n$*

$$\binom{n}{k} \leq 2^{n-1}$$

Dimostrazione. Ricordiamo che si ha sempre $\binom{n}{k} = \binom{n}{n-k}$.

Se n è dispari nella somma di Newton c'è un numero pari di addendi che si possono associare a due a due. Allora per ogni $0 \leq k \leq n$ si ha

$$2^n = (1+1)^n = \sum_{h=0}^{n} \binom{n}{h} = 2 \sum_{h=0}^{(n-1)/2} \binom{n}{h} \geq 2 \binom{n}{k}$$

Pertanto $\binom{n}{k} \leq 2^{n-1}$

□

La diseguaglianza appena vista ci serve per provare un risultato essenziale.

Teorema 7. *Sia x un numero reale. Se $x \geq 2$ allora il prodotto dei numei primi $\leq x$ è minore di 4^x. In simboli*

$$\prod_{p \leq x} p < 4^x$$

Dimostrazione. Il teorema è banalmente vero per ogni $2 \leq x \leq 3$. Dimostriamo che se il teorema è vero per ogni intero dispari $n \geq 3$ allora è vero per ogni numero reale $y \geq 3$. Dato un qualsiasi $y \geq 3$ esiste sempre un intero dispari $n \geq 3$ tale che $n \leq y < n+2$. Poiché y viene prima di $n+2$ i primi che sono $\leq y$ sono gli stessi che sono $\leq n$. Dunque

$$\prod_{p \leq y} p = \prod_{p \leq n} p < 4^n \leq 4^y$$

Proviamo allora il teorema per ogni intero dispari $n \geq 3$. La dimostrazione è per induzione.

Il teorema è vero per $n = 3$, in quanto $6 < 64$. Questa è la base della induzione.

Consideriamo ora un qualsiasi intero dispari $n \geq 5$ e facciamo l'ipotesi induttiva che il teorema sia vero per ogni intero dispari $k < n$. Dobbiamo dimostare il teorema per n.

Poich n è dispari ≥ 5, possiamo scegliere un segno $\pm$ in modo tale che $k = (n \pm 1)/2$ sia dispari. Certamente l'intero k risultante è ≥ 3. Si ha $n = 2k \mp 1$ e quindi $n - k = 2k \mp 1 - k \leq k + 1$, ovvero $k + 1 \geq n - k$.

Supponiamo $k < p \leq n$. Allora $p|n!$ ma (per 3) $p \not| k!$. Se $p > k$ allora $p > k+1$, perché sono entrambi dispari. Segue $p > n - k$. Pertanto $p \not| (n-k)!$ Riassumendo

- $p|n!$
- $p \not| k!$
- $p \not| (n-k)!$

Conclusione: $p | \binom{n}{k} = \frac{n!}{k!(n-k)!}$. Questo vale per ogni $k < p \leq n$. Pertanto

$$\prod_{k<p\leq n} p \,|\, \binom{n}{k}$$

A maggior ragione

$$\prod_{k<p\leq n} p \leq \binom{n}{k}$$

Dal 6 segue allora che

$$\prod_{k<p\leq n} p \leq 2^{n-1} \quad (*)$$

Dividiamo il prodotto dei primi $p \leq n$ in due parti: il prodotto dei primi $p \leq k$ e quello dei primi $k < p \leq n$:

$$\prod_{p \leq n} p = \prod_{p<k} p \prod_{k<p\leq n} p$$

Poiché k è dipari ed è $< n$, per ipotesi induttiva il primo prodotto è $< 4^k$. Per $(*)$ il secondo prodotto è $\leq 2^{n-1}$. Quindi

$$\prod_{p \leq n} p < 4^k 2^{n-1} = 2^{2k+n-1} \leq 2^{2n} = 4^n$$

Per vedere che $2^{2k+n-1} \leq 2^{2n}$ si osserva che $2k \leq n+1 \Rightarrow 2k-1 \leq n \Rightarrow 2k+n-1 \leq 2n$. Quindi il teorema è dimostrato.

□

Ragionando ancora per induzione si dimostra la seguente diseguaglianza

Teorema 8. *Se* $n > 1$ *allora* $\binom{2n}{n} > \frac{4^n}{2\sqrt{n}}$

Le diseguaglianze provate in 8 e in 7 sono fondamentali per conseguire il risultato finale.

Per il nostro scopo è necessario anche sapere quali primi p dividano $\binom{2n}{n}$, e con quale esponente appaiano.

Per quanto riguarda $n!$, un risultato classico è il seguente

Teorema 9. Potenze prime che dividono n!

Se p *è primo, il più grande esponente* v *che divide* $n!$ *è*

$$v = \sum_{j=1}^{\infty} \lfloor \frac{n}{p^j} \rfloor$$

La funzione $\lfloor \alpha \rfloor$ è il più grande intero $\leq \alpha$. Si noti che la somma in 9 è sempre finita, perché per j abbastanza grande $p^j > n$ e $\lfloor \frac{n}{p^j} \rfloor = 0$.

Per esempio la più grande potenza di 2 che divide 55! è 2^{50} in quanto

$$\lfloor \frac{55}{2} \rfloor + \lfloor \frac{55}{4} \rfloor + \lfloor \frac{55}{8} \rfloor + \lfloor \frac{55}{16} \rfloor + \lfloor \frac{55}{32} \rfloor = 27 + 13 + 6 + 3 + 1 = 50$$

Denoteremo nel seguito con e_p il più grande intero tale che $p^{e_p} | \binom{2n}{n}$. Naturalmente e_p dipende da n, e più correttamente dovrebbe essere denotato con $e_p(n)$. Però questo non dovrebbe creare confusioni dal momento che n sarà ogni volta fissato. Si noti che e_p è definito per ogni primo p, fissato n, ed vale 0 per tutti i p tranne un numero finito.

Come sappiamo, i fattori primi di $(2n)!$ sono tutti $\leq 2n$. Pertanto, con la notazione introdotta abbiamo che

$$\binom{2n}{n} = \prod_{p \leq 2n} p^{e_p} \tag{10}$$

Esempio 10. Poniamo $n = 17$. Si trova che

$e_2 = 2, \quad e_3 = 3, \quad e_5 = 1, \quad e_{11} = 1, \quad e_{19} = 1, \quad e_{23} = 1, \quad e_{29} = 1, \quad e_{31} = 1$

Questo significa che $\binom{34}{17} = 2^2 \times 3^3 \times 5 \times 11 \times 19 \times 23 \times 29 \times 31$

Poiché $\binom{2n}{n} = \frac{(2n)!}{n!n!}$, dal Teorema 9 si ottiene subito che

Teorema 11. *Dato n si ha che*

$$e_p = \sum_{j=1}^{\infty}(\lfloor\frac{2n}{p^j}\rfloor - 2\lfloor\frac{n}{p^j}\rfloor)$$

Si noti che le differenze che appaiono nella somma di 11 possono valere soltanto 0 o 1. Precisamente valgono 0 se $\lfloor\frac{2n}{p^j}\rfloor$ è pari e 1 altrimenti.

Teorema 12.

$$p^{e_p} \leq 2n$$

Dimostrazione. Se t è il massimo esponente per cui $p^t \leq 2n$, allora per ogni $j \geq t+1$ si ha $p^j > 2n$ e pertanto da $t+1$ in poi tutti gli addendi della somma in 11 sono nulli. Ma gli addendi valgono 0 o 1, perciò $e_p \leq t$. Coseguentemente $p^{e_p} \leq p^t$. La tesi segue dal fatto che per costruzione $p^t \leq 2n$ □

Quindi non soltanto si deve avere $p \leq 2n$, ma anche $p^{e_p} \leq 2n$. Riprendendo l'esempio precedente con $n = 17$, possiamo a priori stabilire che e_3 non può essere maggiore di 3, che per ogni primo $5 < p < 34$, e_p non può essere > 1.

Con questa tecnica possiamo facilmente valutare gli e_p.

Teorema 13. *Supponiamo $n \geq 3$.*

1. *Se $p \geq \sqrt{2n}$ allora $e_p \leq 1$*
2. *Se $2n/3 < p \leq n$ allora $e_p = 0$*
3. *Se $n < p \leq 2n$ allora $e_p = 1$*

Abbiamo ora quanto ci serve per dimostarre il Postulato di Bertrand

(Notazione: nel seguito denotiamo con p_k il $k-$esimo numero primo. Per esempio $p_4 = 7$, $p_{10} = 29$.)

Teorema 14. Postulato di Betrand (dimostrato da Chebyshev)

$$\textit{Per ogni } n > 1 \qquad \pi(2n) - \pi(n) > 0$$

Si noti che 14 ha come immediata conseguenza

Corollario 15.

$$\textit{Per ogni } n \geq 1 \qquad p_{n+1} < 2p_n$$

Il Postulato di Bertrand, e il suo corollario, si ottengono come ovvia conseguenza del Teorema che segue.

Dimostreremo infatti molto di più, determinando per $\pi(2n) - \pi(n)$ un confine inferiore e un confine superiore non banali, in modo del tutto indipendente da quanto detto nel primo paragrafo, e, in particolare dal TNP.

Teorema 16. *Per ogni $n > 1$ si ha*

$$\frac{n}{3\log(2n)} < \pi(2n) - \pi(n) < \frac{7n}{5\log(n)}$$

Dimostrazione. Possiamo spezzare il prodotto che ci dà $\binom{2n}{n}$ in due parti

$$\binom{2n}{n} = \prod_{p\leq 2n} p^{e_p} = \prod_{p\leq n} p^{e_p} \prod_{n<p\leq 2n} p^{e_p}$$

Per il punto (3) di 13, quando $n < p \leq 2n$, si ha $e_p = 1$. Dunque

$$\binom{2n}{n} = \prod_{p\leq n} p^{e_p} \prod_{n<p\leq 2n} p$$

Per il punto (2) di 13, se $2n/3 < p \leq n$ allora $e_p = 0$. Pertanto

$$\binom{2n}{n} = \prod_{p\leq 2n/3} p^{e_p} \prod_{n<p\leq 2n} p = Q_n P_n$$

Ove si è posto

$$Q_n = \prod_{p\leq 2n/3} p^{e_p}$$

$$P_n = \prod_{n<p\leq 2n} p$$

Vogliamo trovare un confine superiore per Q_n. Scomponiamo il prodotto Q_n in due parti, $Q_n = AB$, dove $A = \prod_{p\leq 2n/3} p$ è il prodotto dei primi $p \leq 2n/3$ tali che $e_p = 1$, e $B = \prod_{p\leq 2n/3} p^{e_p}$ è il prodotto dei primi $p \leq 2n/3$ tali che $e_p > 1$. Per il punto (1) di 13, se $e_p > 1$ allora $p < \sqrt{2n}$. Pertanto $B \leq \prod_{p<\sqrt{2n}} p^{e_p}$. In conclusione

$$Q_n \leq \prod_{p\leq 2n/3} p \prod_{p<\sqrt{2n}} p^{e_p}$$

Per il Teorema 7 sappiamo che $\prod_{p\leq 2n/3} p < 4^{2n/3}$. Per quanto riguarda il secondo prodotto, ricordiamo che $p^{e_p} \leq 2n$. Perciò $\prod_{p<\sqrt{2n}} p^{e_p} \leq (2n)^z$ dove z è il numero dei primi $p < \sqrt{2n}$. Poiché i primi (a parte 2) sono dispari, il numero dei primi minori di un dato numero Y è ampiamente minore di $Y/2$. Pertanto $z \leq \sqrt{2n}/2$. Quindi $\prod_{p<\sqrt{2n}} p^{e_p} \leq (2n)^{\sqrt{2n}/2}$.

Mettendo insieme questi risultati

$$Q_n < 4^{2n/3}(2n)^{\sqrt{2n}/2}$$

da cui segue per inversione

$$Q_n^{-1} > 4^{-2n/3}(2n)^{-\sqrt{2n}/2} \qquad (**)$$

Ora $\binom{2n}{n} = Q_n P_n \Rightarrow P_n = \binom{2n}{n} Q_n^{-1}$. Utilizzando questo fatto, la $(**)$ e 8 otteniamo

$$P_n = \binom{2n}{n} Q_n^{-1} > 4^n (2\sqrt{n})^{-1} 4^{-2n/3} (2n)^{-\sqrt{2n}/2}$$

e semplificando un poco

$$P_n > 4^{n/3} (2\sqrt{n}(2n)^{\sqrt{2n}/2})^{-1} \qquad (***)$$

Poniamo.

$$(2n)^{w(n)} = 4^{n/3} (2\sqrt{n}(2n)^{\sqrt{2n}/2})^{-1} \tag{11}$$

Si noti che la funzione $w(n)$ è *definita* dalla 11. Infatti applicando log da entrambi i lati si trova

$$w(n) = \frac{\log(4^{n/3}(2\sqrt{n}(2n)^{\sqrt{2n}/2})^{-1})}{\log(2n)}$$

Nel prodotto $P_n = \prod_{n<p\leq 2n} p$, ogni p è $\leq 2n$. Quindi $P_n \leq (2n)^z$, dove z è il numero dei primi in questione. Il numero dei primi $n < p \leq 2n$ è esattamente $\pi(2n) - \pi(n)$, e perciò $P_n \leq (2n)^{\pi(2n)-\pi(n)}$. Utilizzando 11, $(***)$ e quanto appena detto

$$(2n)^{w(n)} < P_n \leq (2n)^{\pi(2n)-\pi(n)}$$

che conduce immediatamente a

$$w(n) < \pi(2n) - \pi(n) \tag{12}$$

Se nella $(2n)^{w(n)} = 4^{n/3}(2\sqrt{n}(2n)^{\sqrt{2n}/2})^{-1}$ prendiamo ancora il logaritmo da entrambi i lati, epandendolo con l'uso delle sue proprietà elementari, otteniamo

$$w(n)\log(2n) = (n/3)\log(4) - \log(2\sqrt{n}) - (\sqrt{2n}/2)\log(2n)$$

Mettiamo in evidenza $n/3$, e teniamo presente il fatto che $\frac{3}{n} \times \frac{\sqrt{2n}}{2} = \frac{3}{\sqrt{2n}}$:

$$w(n)\log(2n) = (n/3)[\log(4) - (3/n)(\log(2\sqrt{n})) - 3\log(2n)/\sqrt{2n}] \qquad (o)$$

Poniamo $g(x) = \log(4) - (3/x)(\log(2\sqrt{x})) - 3\log(2x)/\sqrt{2x}$, che è la funzione tra parentesi quadre.

E' ben noto che la funzione $\log(x)$ tende all'infinito più debolmente di x^t, per qualsiasi $t > 0$. Dunque

$$\lim_{x\to\infty} \frac{\log(2\sqrt{x})}{x} = 0 \quad \text{e} \quad \lim_{x\to\infty} \frac{\log(2x)}{\sqrt{2x}} = 0$$

Le due funzioni $\frac{\log(2\sqrt{x})}{x}$ e $\frac{\log(2x)}{\sqrt{2x}}$ inoltre sono positive e decrescenti per $x > 1$. Pertanto, per $x > 1$, $g(x)$ è crescente e si ha che $\lim_{x\to\infty} g(x) = \log(4) \simeq 1.38629$

Esiste dunque un x_0 tale che per ogni $x > x_0$ si ha $g(x) > 1$. Corrispondentemente esiste un intero n_0 tale che per ogni $n > n_0$ l'espressione tra le quadre di (o) è > 1. Con qualche calcolo troviamo che $g(2190) \simeq 0.999995$ e $g(2191) \simeq 1.00006$. Otteniamo allora dalla (o)

$$\text{Per ogni } n > 2190 \quad w(n) > \frac{n}{3\log(2n)}$$

Con l'uso del computer si constata che la stessa diseguaglianza vale per ogni $1 < n <= 2190$. Infine, ricordando la 12 otteniamo

$$\text{Per ogni } n > 1 \quad \pi(2n) - \pi(n) > \frac{n}{3\log(2n)} \tag{13}$$

Veniamo al confine superiore di $\pi(2n) - \pi(n)$.

Ricordiamo che $P_n = \prod_{n<p\leq 2n} p$. Segue che $\log(P_n) = \sum_{n<p\leq 2n} \log(p)$. Ogni p nella sommatoria è $> n$, pertanto $\log(p) > \log(n)$ e $\sum_{n<p\leq 2n} \log(p) > (\log(n) + \log(n) + \cdots + \log(n))$, ove $\log(n)$ si somma tante volte sono i primi $n < p \leq 2n$, ovvero, come già abbiamo osservato, $\pi(2n) - \pi(n)$ volte. Quindi

$$\log(P_n) = \sum_{n<p\leq 2n} \log(p) > (\pi(2n) - \pi(n)) \log(n) \qquad (i)$$

Per costruzione (si veda l'inizio della dimostarzione) $P_n | \binom{2n}{n}$. In particolare $P_n \leq \binom{2n}{n}$. Ricordiamo che (5) $\binom{2n}{n} < 4^n$. Segue che

$$\log(P_n) \leq \log(\binom{2n}{n}) < \log(4^n) = n\log(4) \qquad (ii)$$

Mettendo insieme (i) e (ii):

$$(\pi(2n) - \pi(n)) \log(n) < n\log(4)$$

e

$$\pi(2n) - \pi(n) < \frac{n\log(4)}{\log(n)}$$

Ora $7/5 = 1.4$ e $\log(4) \simeq 1.38629$, pertanto

$$\text{Per ogni } n > 1 \quad \pi(2n) - \pi(n) < \frac{7n}{5\log(n)} \tag{14}$$

Le 13 e 14 concludono la dimostrazione del Teorema. $\square$

Il risultato di Erdös si ottiene, come abbiamo visto in dettaglio nel Teorema 16, con metodi del tutto elementari. Si tratta però di un risultato tutt'altro che ovvio. Ci assicura dell'esistenza di *moltissimi* primi tra n e $2n$. La funzione $\frac{x}{3\log(2x)}$ che appare in 13 è sempre crescente per $x \geq 2$. Inoltre

$$\lim_{x\to\infty} \frac{x}{3\log(2x)} = \infty$$

Quindi se $\frac{n_0}{3\log(2n_0)} > L$ per un certo $n_0 \geq 2$, per ogni $n > n_0$ si avrà sempre $\frac{n}{3\log(2n)} > L$. Prendiamo per esempio $L = 1000000$. Si vede che $\frac{55580000}{3\log(2\times 55580000)} \simeq 1.00001 \times 10^6$. Possiamo dunque essere *certi* che *per ogni* $n > 55580000$ tra n e $2n$ c'è almeno *un milione* di primi!

3 I primi di Ramanujan

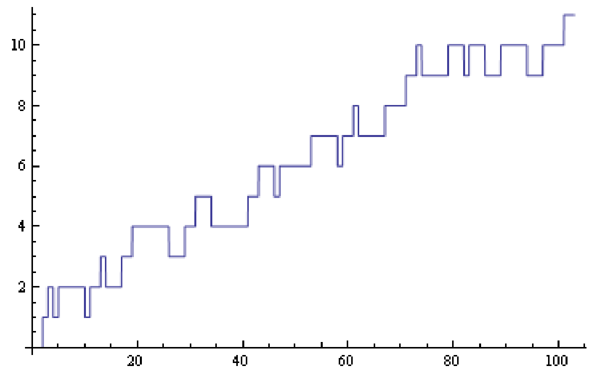
Come abbiamo visto nel paragrafo precedente

$$\lim_{x\to\infty} \pi(2x) - \pi(x) = \infty$$

Se sostituiamo $x/2$ a x otteniamo

$$\lim_{x\to\infty} \pi(x) - \pi(x/2) = \infty \tag{15}$$

Poniamo $\rho(x) = \pi(x) - \pi(x/2)$. La funzione $\rho(x)$ è una fuzione a gradini che tende all'infinito in modo particolare. Cresce e diminuisce infinite volte, e quando cambia il salto è sempre ± 1.



La funzione $\rho(x)$ tra 1 e 103

Vediamo che cosa accade esattamente. Nell'intervallo compreso tra due numeri interi consecutivi, estremi esclusi, la ρ è evidentemente costante. Dobbiamo considerare soltanto i valori interi di x. Distinguiamo i due casi: x pari e x dispari.

- **Caso I**

  Supponiamo $x = 2n, \quad \pi(2n) = s, \quad \pi(n) = t, \quad \rho(x) = s - t.$

  Passiamo da x a $x + 1 = 2n + 1$. Allora $\rho(x+1) = \pi(2n+1) - \pi(n + \frac{1}{2}) = \pi(2n+1) - \pi(n) = s' - t$.

  Se $2n + 1$ è primo allora $s' = s + 1$ e $\rho(x+1) = \rho(x) + 1$, altrimenti $\rho(x+1) = \rho(x)$.

- **Caso II**

  Supponiamo $x = 2n - 1, \quad \pi(2n-1) = s, \quad \pi(n - \frac{1}{2}) = t, \quad \rho(x) = s - t.$

  Passiamo da x a $x+1 = 2n$. Allora $\rho(x+1) = \pi(2n) - \pi(n) = \pi(2n-1) - \pi(n) = s - t'$.

  Se n è primo allora $t' = t + 1$ e $\rho(x+1) = \rho(x) - 1$, altrimenti $\rho(x+1) = \rho(x)$.

Da quanto detto segue che possiamo definire una successione di interi $R_1, R_2, \cdots, R_k, \cdots$ così :

Definizione 17. R_i è il minimo intero tale che per tutti gli $x \geq R_i$ si ha $\rho(x) \geq i$.

La condizione di minimalità implica immediatamente che gli R_i devono essere primi. Chi è R_1? Nella definizione si legge che

$$R_1 \text{ è il minimo intero tale che per tutti gli } x \geq R_1 \text{ si ha } \rho(x) \geq 1.$$

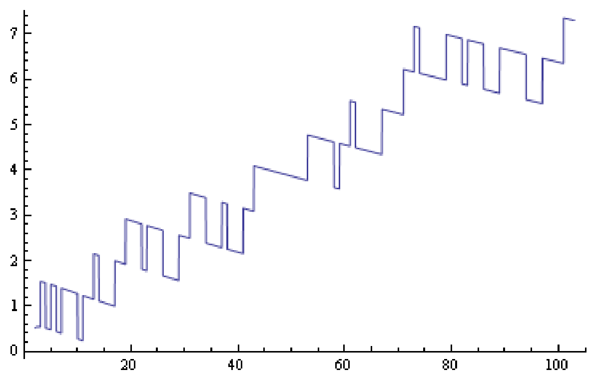
Dunque R_1 è il minimo intero tale che per tutti gli $x \geq R_1$ esiste almeno un primo tra $n/2$ e n. Per il Teorema 14 sappiamo che $R_1 = 2$. Calcoliamo R_2. Dal Teorema 16 sappiamo che

$$\text{Per ogni } x \geq 1 \quad \pi(2x) - \pi(x) > \frac{x}{3\log(2x)}$$

sostituendo $x/2$ a x abbiamo

$$\text{Per ogni } x \geq 2 \quad \rho(x) = \pi(x) - \pi(\frac{x}{2}) > \frac{x}{6\log(x)}$$

Questo è il grafo della differenza $\rho(x) - \frac{x}{6\log(x)}$, per $2 \leq x \leq 103$



La funzione $\rho(x) - \frac{x}{6\log(x)}$ **tra** 2 **e** 103

Per $x = 46$, $\frac{x}{6\log(x)} \simeq 2.00245$. Dunque per ogni $x \geq 46$ ci sono almeno 2 primi tra $x/2$ e x. Calcoliamo $\rho(x)$ all'indietro: troviamo $\rho(46) = 5$, $\rho(44) = 6$, $\rho(45) = 6, \cdots$. La sequenza da $x = 46$ a $x = 2$ è questa

$5, 6, 6, 6, 5, 5, 4, 4, 4, 5, 4, 4, 4, 5, 5, 5, 4, 4, 3, 3, 3, 4, 4, 4, 3, 4, 4, 4, 3, 3, 2, 2, 2, 3, 2, 2, 1, 2, 2, 2$
$1, 2, 1, 2, 1$

Si osserva che $\rho(10) = 1$ e che $\rho(x) \geq 2$ da $x = 11$ a $x = 46$. Da quanto detto segue che per ogni $x \geq 11$ si ha che $\rho(x) \geq 2$, pertanto $R_2 = 11$.

I numeri primi R_i vengono detti *primi di Ramanujan*, perché vennero introdotti da Ramanujan stesso in [7].

Nella **On-Line Encyclopedia of Integer Sequences (OEIS)** la sequenza dei primi di Ramanujan appare qui: A104272.

Questi sono i primi 100 primi di Ramanujan

2, 11, 17, 29, 41, 47, 59, 67, 71, 97, 101, 107, 127, 149, 151, 167, 179, 181, 227, 229, 233, 239, 241,263, 269, 281, 307, 311, 347, 349, 367, 373, 401, 409, 419, 431, 433, 439, 461, 487, 491, 503, 569, 571,587, 593, 599, 601, 607, 641, 643, 647, 653, 659, 677, 719, 727, 739, 751, 769, 809, 821, 823, 827, 853,857, 881, 937, 941, 947, 967, 983, 1009, 1019, 1021, 1031, 1049, 1051, 1061, 1063 1087, 1091, 1097, 1103,1151, 1163, 1187, 1217, 1229, 1249, 1277, 1289, 1297, 1301 1367, 1373, 1423, 1427, 1429, 1439

Nel numero di Agosto-Settembre 2009 dell'*American Mathematical Monthly* è uscito un interessante articolo di Jonathan Sondow sui primi di Ramanujan ([9]).

Vediamo alcuni fatti assai iteressanti dimostrati da Sondow, e due congetture che propone.

Teorema 18. (J. Sondow)

1. $$2n\log(2n) < R_n < 4n\log(4n) \quad (n \geq 1)$$

2. *Per ogni $\epsilon > 0$, esiste un $n_0 = n_0(\epsilon)$ tale che*

$$R_n < (2+\epsilon)n\log(n) \quad (n \geq n_0)$$

3. $$\lim_{n\to\infty} \frac{R_n}{p_{2n}} = 1$$

ovvero

$$R_n \sim p_{2n}$$

4. $$R_n > p_{2n} \quad (n \geq 2)$$

Diciamo primo non-Ramanujan un numero primo che non appartenga alla successione degli R_n.

Questi sono i primi non-Ramanujan < 100:

$3, 5, 7, 13, 19, 23, 31, 37, 43, 53, 61, 73, 79, 83, 89$

Sondow osserva che i punti (3) e (4) del Teorema 18 fanno pensare che la probabilità che un numero primo casuale sia un primo di Ramanujan deve essere leggermente inferiore a $\frac{1}{2}$. Chiaramente essa sarebbe $\frac{1}{2}$ se si avesse sempre $R_n = p_{2n}$, perché allora tra i primi $2n$ primi ne avremmo sempre n di Ramanujan. Le cose non stanno proprio così , ma quasi.

- Per $n = 250$, abbiamo $R_{250} = 4013 = p_{554}$, quindi tra i primi 554 numeri primi, 250 sono di Ramanujan, con una percentuale dello 0.451264%.

- Per $n = 500$, abbiamo $R_{500} = 8831 = p_{1100}$, quindi tra i primi 1100 numeri primi, 500 sono di Ramanujan, con una percentuale dello 0.454545%.

- Per $n = 750$, abbiamo $R_{750} = 13901 = p_{1642}$, quindi tra i primi 1642 numeri primi, 750 sono di Ramanujan, con una percentuale dello 0.45676%.

- Per $n = 1000$, abbiamo $R_{1000} = 19403 = p_{2197}$, quindi tra i primi 2197 numeri primi, 1000 sono di Ramanujan, con una percentuale dello 0.455166%.

Sebbene i primi di Ramanujan sembrino molto particolari, il numero dei primi di Ramanujan pare essere di poco inferiore a quello dei primi non-Ramanujan. Queste (e altre) considerazioni hanno portato Sondow alla seguente Congettura.

Congettura 19. Prima Congettura di Sondow *Nella successione* (p_n) *dei numeri primi esistono sequenze arbitrariamente lunghe di primi di Ramanujan consecutivi e sequenze arbitrariamente lunghe di primi non-Ramanujan consecutivi.*

Per esempio si ha $(R_{167}, R_{168}, \cdots, R_{179}) = (p_{384}, p_{385}, \cdots, p_{396}) =$

$$(2657, 2659, 2663, 2671, 2677, 2683, 2687, 2689, 2693, 2699, 2707, 2711, 2713)$$

Le seconda Congettura riguarda i primi gemelli.

Ricordiamo che due primi $p < q$ si dicono gemelli se $q = p+2$. Facciamo una osservazione, utile anche se banale. Sia (p, q) una coppia di primi gemelli diversa dalla coppia $(3, 5)$, allora si ha

$$p \equiv -1 (\mathrm{mod}\ 6) \quad \mathrm{e} \quad q \equiv 1 (\mathrm{mod}\ 6) \tag{16}$$

Il motivo è ovvio: se $p > 3$ è primo, p è coprimo con 6 e quindi diviso per 6 può dare come resto soltanto 1 e $5 \equiv -1 (\mathrm{mod}\ 6)$.

Una coppia di primi gemelli (p, q) è individuata in modo univoco dal suo primo elemento p. Possiamo dunque definire l'isieme Gem

Definizione 20.

$$\mathrm{Gem} = \{p : \ p \ \mathrm{e} \ p + 2 \ \text{sono primi}\}$$

Tutti sono convinti che Gem sia infinito, ma di questo fatto non esiste alcuna dimostrazione.

Questi sono i primi 50 elementi di Gem:

3, 5, 11, 17, 29, 41, 59, 71, 101, 107, 137, 149, 179, 191, 197, 227, 239, 269, 281, 311, 347, 419, 431, 461, 521, 569, 599, 617, 641, 659, 809, 821, 827, 857, 881, 1019, 1031, 1049, 1061, 1091, 1151, 1229, 1277, 1289, 1301, 1319, 1427, 1451, 1481, 1487

Si noti che, per l'osservazione 16, tutti i primi in Gem (tranne 3) sono della forma $6k-1$.

Esistono coppie di primi di Ramanujan gemelli. Queste sono della forma

$$(R_m, R_{m+1}) \quad \text{con} \quad R_{m+1} = R_m + 2 \tag{17}$$

La coppia più piccola è $(149, 151)$.

Possiamo allora definire l'insieme GemRam formato dai primi elementi delle coppie di primi di Ramanujan gemelli

Definizione 21.

$$\mathrm{GemRam} = \{p : \ p \ \mathrm{e} \ p + 2 \ \text{sono primi di Ramanujan}\}$$

Questi sono i primi 50 elementi di GemRam:

149, 179, 227, 239, 347, 431, 569, 599, 641, 821, 1019, 1049, 1061, 1427, 1487, 1607, 1787, 1997, 2081, 2129, 2237, 2267, 2657, 2687, 2711, 2789, 2999, 3167, 3257, 3299, 3359, 3527, 3539, 3581, 3671, 3917, 4091, 4127, 4229, 4241, 4337, 4547, 4637, 4649, 4787, 4799, 4967, 5009, 5021, 5519

Se nell'insieme dei numeri primi prendiamo un elemento casuale, abbiamo osservato che questo sarà un primo di Ramanujan con probabilità leggermente inferiore a $\frac{1}{2}$. Se prendiamo una coppia di primi a caso, ci si aspetta che siano entrambi primi di Ramanujan con probabilità $< \frac{1}{4}$.

Sorprendentemente la probabilità che un primo gemello casuale (un elemento di Gem) sia un primo gemello di Ramanujan (un elemento di GemRam) sembra più alta di $\frac{1}{4}$.

Sondow osserva che nell'elenco dei primi 1100 numeri primi ci sono 168 primi gemelli e 70 primi gemelli di Ramanujan. Il rapporto è $\frac{70}{168} \simeq 0.416667$.

Facendo qualche conto ho trovato che tra i primi 2194 numeri primi ci sono 332 primi gemelli e 119 primi gemelli di Ramanujan. Il rapporto è $\frac{119}{332} \simeq 0.358434$.

Sondow fa una osservazione tendente a spiegare il motivo di questa frequenza apparentemente più elevata.

Proposizione 22. *Siano p e q due primi con $p \geq 5$, $q = p + 2$. Allora*

$$\rho(q) = \rho(p) + 1 \tag{18}$$

Dimostrazione. Poniamo $\pi(q) = t$. Ovviamente segue che $\pi(p) = t - 1$. Dunque

$$\rho(q) = \pi(q) - \pi(\frac{q}{2}) = t - \pi(\frac{p}{2} + 1)$$

$$\rho(p) = \pi(p) - \pi(\frac{p}{2}) = t - 1 - \pi(\frac{p}{2})$$

Da 16 sappiamo che $p = 6k - 1$ $(k \geq 1)$. Quindi

$$\pi(\frac{p}{2} + 1) = \pi(3k + \frac{1}{2})$$

$$\pi(\frac{p}{2}) = \pi(3k - \frac{1}{2})$$

Poiché $3k$ non è primo si ha

$$\pi(3k + \frac{1}{2}) = \pi(3k - \frac{1}{2})$$

e infine

$$\rho(q) = \rho(p) + 1$$

$\square$

La Proposizione appena dimostrata dice che la condizione 18 è una condizione *necessaria* affinché due primi consecutivi p_n e p_{n+1} siano primi gemelli. Naturalmente non è sufficiente. Per esempio $p_{96} = 503$, $p_{97} = 509$ e $\rho(509) = 43$, $\rho(503) = 42$.

Se pensiamo alla condizione 18 come a un filtro che setaccia le coppie di numeri primi (p, q) soltanto una parte delle coppie (p_n, p_{n+1}) passerà, tra le quali le coppie gemelle. Per gran parte delle coppie (p_n, p_{n+1}) accade infatti che $\rho(p_{n+1}) = \rho(p_n)$.

Invece *tutte* le coppie (R_m, R_{m+1}) di primi di Ramanujan consecutivi soddisfano la 18, perché, proprio per la definizione dei primi di Ramanujan, si ha sempre $\rho(R_n) = n$.

Quindi *tutte* le coppie (R_m, R_{m+1}) passano il filtro. Concludendo

Data una coppia di numeri primi, se questi sono primi gemelli è più probabile che siano primi di Ramanujan gemelli.

Ecco, per terminare, l'ultima congettura di Sondow:

(Notazione: $|A|$ denota il numero degli elementi dell'insieme A (ovvero l'ordine di A).)

Congettura 23. Seconda Congettura di Sondow *Poniamo* $\pi_G(x) = |p \leq x : p \in Gem|$. *Analogamente poniamo*

$\pi_{GR}(x) = |p \leq x : p \in GemRam|$. *Allora se* $x \geq 571$ *si ha*

$$\frac{\pi_{GR}(x)}{\pi_G(x)} > \frac{1}{4}$$

La 23 implicherebbe, tra l'altro, che

Esistono infiniti primi gemelli se e solo se esistono infiniti primi di Ramanujan gemelli.

Riferimenti bibliografici

[1] D. Burde, A remark on an inequality for the prime counting function, *Math. Inequal. Appl.* **10**, No. 1, 2007, 9–13.

[2] U. Cerruti, Congettura di Riemann e sicurezza mondiale,

URL:http://www.dm.unito.it/personalpages/cerruti/luglio04-gennaio28.html#riemann

[3] U. Cerruti, La probabilità di sbagliare tutto

URL:http://www.dm.unito.it/personalpages/cerruti/pdfblog/sbagliaretutto.pdf

[4] P. L. Chebyshev, Memoire sur les nombres premiers, *Journal de Math. Pures et Appl.* **17**, 1852, 366–390.

[5] H. G. Diamond, Elementary methods in the study of the distribution of prime numbers, *Bullettin of the American Mathematical Society* **7**, 1982, 553–589

[6] L. J. Goldstein, A History of the Prime Number Theorem, *The American Mathematical Monthly*, **Vol. 80**, 1973, 599–615.

[7] S. Ramanujan, A proof of Bertrands postulate, *J. Indian Math. Soc.* **11**, 1919, 181-182.

URL:http://www.imsc.res.in/~rao/ramanujan/CamUnivCpapers/Cpaper24/page1.htm.

[8] J. B. Rosser - L.Schoenfeld, Approximate Formulas for Some Functions of Prime Numbers, *Illinois J. Math.* **6**, 1962, 64–97.

[9] J. Sondow, Ramanujan Primes and Bertrands Postulate, *The American Mathematical Monthly*, **Vol. 116**, 2009, 630–635.