

Itinerari nel Mondo dei Numeri Primi

Umberto Cerruti, Università di Torino

Indice:

Ci sono infiniti numeri primi

Euclide

Eulero

Chaitin

Complessità

La classe P

La classe NP

Complessità dei primi

Test di primalità

Il mondo del +1

Successioni lineari ricorrenti

Il mondo del -1

Test probabilistici

Il Piccolo Teorema di Fermat

Miller e Fibonacci

Un criterio condizionato

Distribuzione dei numeri

primi

Il Teorema dei Numeri Primi

La Congettura di Riemann

Gap tra i Primi

Conclusioni

An equation means nothing to me unless it expresses a thought of GOD."

Srinivasa Ramanujan

Una visione ...

Questo articolo è dedicato ai numeri primi. Un numero primo è numero divisibile soltanto per se stesso e per uno. L'importanza dei numeri primi è ben nota, non solo per la Matematica in sé ma anche per le potenziali applicazioni, non ultima l'applicazione alla crittografia. In particolare le applicazioni di crittografia hanno assunto enorme importanza in vari campi, dal bancario al militare per lo sviluppo della guerra elettronica (si veda la nota redazionale). Nel corso dell'articolo ci impareremo in un paio di "problemi del Millennio", per la cui soluzione viene offerto un milione di dollari. Inaspettatamente, nel contesto dei numeri primi, incontreremo anche la successione dei numeri di Fibonacci, salita recentemente alla ribalta con il film sul "Codice Da Vinci".

In Figura 1 vediamo un triangolo formato da righe di lunghezza crescente. Ogni riga è interamente costituita di numeri primi. Si nota subito che la differenza D tra due primi consecutivi è costante per ogni riga: a partire dalla seconda riga abbiamo $D = 1, 2, 6, 6, 30$.

I primi, in ogni riga, sono in *progressione aritmetica*. L'ultima riga contiene una progressione aritmetica di primi di lunghezza 6 e differenza 30. Se si aggiunge 30 si trova 187, che non è primo. Esiste una progressione aritmetica di primi che abbia lunghezza 7? O addirittura lunghezza qualsiasi k ? Ovvero il triangolo si può estendere all'infinito? Risponderemo più tardi a questa domanda ...

Fig. N° 1 - Una visione

2
 2, 3
 3, 5, 7
 5, 11, 17, 23
 5, 11, 17, 23, 29
 7, 37, 67, 97, 127, 157

(Nota di redazione)

La dimostrazione di Euclide

Consideriamo un insieme P di k numeri primi: $P = \{p_1, p_2, \dots, p_k\}$: Definiamo $n = p_1 p_2 \dots p_k + 1$. Per il teorema fondamentale dell'aritmetica esiste un fattore primo q di n. Ovviamente q è diverso da tutti i p_i . Dunque dato un qualsiasi insieme finito P di primi, esiste sempre un primo al di fuori di P:

{2, 3, 5, 7, 11, 13} → {59, 509}
 {2, 3, 5, 7, 11, 13, 59, 509} → {901830931}
 {2, 3, 5, 7, 11, 13, 59, 509, 901830931} → {139, 379, 2221, 6951006331}

Questo significa che $2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1 = 30031 = 59 \times 509$, etc.

La dimostrazione di Eulero

Consideriamo un insieme P di k numeri primi $P = \{p_1, p_2, \dots, p_k\}$. Utilizzando la serie geometrica si può trasformare il prodotto a sinistra, nella espressione sottostante, in un prodotto finito di serie (al centro) e utilizzando la proprietà distributiva questo prodotto diventa la serie a destra.

$$\prod_{i=1}^k (1 - p_i^{-1})^{-1} = \prod_{i=1}^k \sum_{h=0}^{\infty} \frac{1}{p_i^h} = \sum_{n \in \mathcal{G}} \frac{1}{n}$$

dove:

$$\mathcal{G} = \{n \in \mathbb{N} : n = p_1^{h_1} p_2^{h_2} \dots p_k^{h_k}\}.$$

Per il Teorema Fondamentale dell'Aritmetica ogni intero n si decompone in modo unico come prodotto di primi. Segue che se P è l'insieme di tutti i numeri primi, allora $\mathcal{G} = \mathbb{N}$ e pertanto:

$$\prod_{i=1}^k (1 - p_i^{-1})^{-1} = \sum_{n \in \mathbb{N}} \frac{1}{n}$$

Poiché la serie armonica diverge, il prodotto non può essere finito.

La dimostrazione di Chaitin

Siamo tutti convinti che esistono infiniti primi. Però, nel 1995 Chaitin si è chiesto, forse per la prima volta: Perché i primi sono infiniti?

La risposta di Chaitin è sorprendente e straordinariamente interessante:

È proprio la infinità dei primi quella che garantisce la complessità dell'universo... o, più modestamente, la complessità delle stringhe binarie.

Comprimibilità delle stringhe

Se ci mostrassero queste tre stringhe di 30 bit:

1, 1, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 0, 1, 0, 0, 0, 0, 1, 1, 1 (rosso)
 1, 1 (verde)
 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1, 0, 0, 1, 1, 1 (blue)

e ci chiedessero di indicare quella più casuale, indicheremmo tutti, forse, quella rossa. E' ovvio però che nessuna di queste stringhe è più (o meno) probabile di un'altra. Tutte hanno probabilità $1/2^{30}$ di essere selezionate da un grande, grandissimo cestino che contenga (ben rimescolate) le 2^{30} stringhe di 30 bit. E' altrettanto ovvio che la stringa verde e quella blu possono essere compresse molto facilmente, sostituendole rispettivamente (per esempio) con (30)(1) o (6)(00111). Per Chaitin la complessità di una stringa s è la lunghezza minima di un programma che genera s . Se pensiamo a stringhe autoscompattanti la complessità di s è la minima lunghezza di una stringa t che (quando si scompatta) genera s . Chiediamoci ora: Quante sono le stringhe di lunghezza n che hanno complessità strettamente inferiore a $n - k$?

Le stringhe sono quasi sempre poco comprimibili

Le stringhe di lunghezza n che hanno complessità strettamente inferiore a $n - k$ non possono essere più delle stringhe di lunghezza minore o uguale a $n - k - 1$ (un fatto che potremmo dire lapalissiano). Esclusa la stringa vuota (di 0 bit) che non genera nulla, ci sono 2 stringhe di 1 bit, 2^2 stringhe di 2 bit e ...

$$N = \sum_{h=1}^{n-k-1} 2^h = 2^{n-k} - 2$$

stringhe di lunghezza minore o uguale a $n - k - 1$. Pertanto (tra le stringhe di lunghezza n) meno di

$$\frac{2^{n-k}}{2^n} = \frac{1}{2^k}$$

si possono comprimere più di k bit!!

Ci devono essere infiniti primi!

Supponiamo che l'insieme dei primi P sia finito:

$$P = \{p_1, p_2, \dots, p_k\}.$$

Allora ogni intero n si potrebbe scrivere, in modo unico nella forma:

$$n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$$

Sarebbe pertanto possibile identificare n con la sequenza dei k esponenti (e_1, e_2, \dots, e_k) . La lunghezza di questa sequenza è dell'ordine di $k \log(\log(n))$, quindi: le stringhe di lunghezza n potrebbero sempre essere espresse da stringhe di lunghezza circa

$$k \log(\log(n))$$

Come abbiamo visto una compressione così grande è assolutamente impossibile! Pertanto:

L'infinità dei numeri primi è la causa della famosa incomprimibilità della informazione.

Tempo polinomiale deterministico

Consideriamo la famiglia dei problemi decisionali. Diciamo che un problema decisionale A è polinomiale se esiste un algoritmo che, data una qualsiasi istanza a di A , termina in un tempo che è limitato superiormente da $|a|^k$, rispondendo correttamente sì o no. Con $|a|$ intendiamo il peso dei dati di ingresso.

Per esempio se si tratta di interi, il peso sarà il numero delle cifre, se si tratta di grafi sarà il numero dei vertici ... La classe P è la classe di tutti i problemi decisionali polinomiali.

P sembra piccola

I problemi:

1. L'intero a è una potenza perfetta?
2. Gli interi a e b sono coprimi?

appartengono a P . Purtroppo nessuno sa se, tra infiniti altri, i seguenti problemi stiano in P :

3. Il grafo F contiene una cricca con k vertici?

(una cricca è un grafo nel quale tutti i vertici sono connessi)

4. Il grafo F è Hamiltoniano?

(un grafo Hamiltoniano è un grafo che possiede un percorso chiuso che passa per ogni vertice una e una sola volta, detto *percorso Hamiltoniano*)

5. L'equazione diofantina $ax^2 + by - c = 0$ ha soluzioni?

(si dice diofantina una equazione della quale si ammettono soltanto soluzioni intere)

Tempo polinomiale non deterministico

Supponiamo di avere un grafo F con 1000 vertici, e che ci chiedano se è Hamiltoniano. Non sappiamo rispondere, in generale, ci vorrebbe davvero troppo tempo. Ora, il signor O (un Oracolo). ci dice sì, è Hamiltoniano. So che sei incredulo, eccoti la prova:

$$V_1, V_2, \dots, V_{1000}$$

La lista $V_1, V_2, \dots, V_{1000}$ che ci viene data dall'Oracolo è un ordinamento dei 1000 vertici di F .

A noi rimane soltanto da verificare che la risposta è corretta, percorrendo la strada proposta $V_1 - V_2 - \dots - V_{1000} - V_1$. Ovviamente questa verifica è molto veloce da fare, richiede un tempo certamente polinomiale. La classe NP è formata da tutti i problemi per i quali esiste un algoritmo in grado di *verificare, in tempo polinomiale, la correttezza* di una risposta *sì* che ci viene offerta.

La classe co-NP

E' facile constatare che quasi tutti i problemi più difficili, in specie quelli che si incontrano nelle applicazioni, appartengono alla classe NP . E' importante notare una profonda differenza con la classe P . In ambito deterministico rispondere alla domanda:

Il grafo F è Hamiltoniano?

è la stessa cosa che rispondere alla domanda:

E' vero che F non è Hamiltoniano?

In contesto non-deterministico non si tratta affatto del medesimo problema. Pensiamo a questo fatto: come farebbe l'Oracolo a convincerci che un grafo F *non* è Hamiltoniano? Come potremmo verificare in fretta che *non* possiede alcun percorso Hamiltoniano? Ogni problema in NP ha dunque un co-problema, e questo dà luogo alla classe **co-NP**:

Un problema sta nella classe **co-NP** se il suo co-problema è in **NP**. Ovviamente si ha:

$$P \subset NP \cap \text{co-NP}$$

Il primo problema del Millennio

Il Clay Mathematics Institute offre un milione di dollari per la soluzione di questo problema (ci sono altri sei problemi “del millennio”):

$$P = NP ?$$

Si tratta evidentemente di un problema di enorme importanza, sia sul piano epistemologico che su quello delle applicazioni. Infatti se si riuscisse a provare in maniera costruttiva la uguaglianza delle due classi, si otterrebbero algoritmi polinomiali (cioè veloci) per risolvere la maggior parte dei problemi matematici che vengono dal mondo del lavoro.

Torniamo ora ai numeri primi e consideriamo il problema decisionale chiamato **Primes**:

$$N \text{ è primo?}$$

Il co-problema di **Primes** è ovviamente **Composite**:

$$N \text{ è composto?}$$

Evidentemente **Composite** sta in **NP**. Per convincermi che **N** è composto, basta infatti che l'Oracolo mi fornisca un divisore d di **N**. La verifica è immediata, consiste semplicemente nel dividere **N** per d .

$$\text{Pertanto } \text{Composite} \hat{=} NP$$

(il simbolo $\hat{=}$ significa “appartiene a”)

Primes è il co-problema di Composite e dunque, per definizione:

$$\text{Primes} \hat{=} \text{co-NP}$$

Soltanto nel 1974 Pratt riuscì a provare che:

$$\text{Primes} \hat{=} NP$$

con un metodo ricorsivo assai ingegnoso.

Riassumendo, nel 1974, si sapeva che:

$$\text{Primes} \hat{=} NP \subset \text{co-NP}$$

(il simbolo \subset significa “intersezione”: il problema **Primes** sta sia in **NP** che in **co-NP**) ma nessuno sapeva provare che **Primes** $\hat{=} P$, sebbene tutti gli esperti concordassero su questa ipotesi.

Fu solo nel 2002 che l'ipotesi venne dimostrata vera da Agrawal, Kayal e Saxena. Prima del loro teorema, chiamato AKS, per testare la primalità di un intero N si avevano a disposizione:

1. Algoritmi polinomiali per numeri di forma *particolare*.
2. Algoritmi polinomiali *probabilistici*.
3. Algoritmi polinomiali deterministici ma *condizionati*.

Al contrario AKS è *polinomiale, universale, deterministico e incondizionato*.

Cominciamo a vedere come si può verificare la primalità di numeri di forma particolare.

Teorema di Pocklington

Supponiamo $N = RF + 1$.

Se $F > \sqrt{N}$, ed esiste un a tale che $\forall q$ primo che divide F si ha:

1. $a^{N-1} \equiv 1 \pmod{N}$
2. $a^{\frac{N-1}{q}} \not\equiv 1 \pmod{N}$

allora N è primo.

Questo teorema permette di trovare primi molto grandi della forma, per esempio, $N = k2^n + 1$.

I candidati più ovvi sono gli interi $N = 2^n + 1$. Per essi il Teorema di Pocklington ha una forma equivalente assai più semplice:

sia $N = k2^n + 1$, allora N è primo $\Leftrightarrow \exists a$ tale che $a^{(N-1)/2} \equiv -1 \pmod{N}$.

Sembra un metodo semplice, efficace e diretto, sembra che potremo trovare facilmente tanti grandi primi della forma $N = 2^n + 1$.

Forse... Purtroppo, però, se $N = 2^n + 1$ è primo, allora necessariamente:

$$n = 2^k \text{ e quindi } N = 2^{2^k} + 1$$

$$\text{Il numero } F_n = 2^{2^n} + 1$$

si dice n -esimo numero di Fermat.

Teorema di Pepin:

$$F_n \text{ è primo } \Leftrightarrow 3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$$

Il Teorema di Pepin è estremamente elegante e consente di verificare la primalità dei numeri di Fermat in un colpo solo. Purtroppo non è efficace, perché gli esponenti crescono troppo velocemente.

Primi di Fermat

I numeri F_n primi si dicono primi di Fermat. Sono primi di Fermat i numeri F_0, F_1, F_2, F_3, F_4 . Non se ne conoscono altri. Eulero dimostrò che 641 divide F_5 , distruggendo così l'illusione di Fermat, che riteneva fossero tutti primi. E' un peccato che non se ne siano trovati altri, perché hanno una proprietà assai notevole. Infatti Gauss dimostrò che un poligono regolare con N lati è costruibile con riga e compasso se e solo se

$$N = 2^m q_1 q_2 \dots q_t$$

dove i q_i sono primi di Fermat distinti.

E' possibile, per esempio, costruire con il solo ausilio di riga e compasso un poligono regolare con 17 lati, perché $17 = F_2$.

Le successioni di Fibonacci

Poniamo:

$$\forall n > 1 \quad \begin{aligned} W_0(a, b, h, k) &= a, & W_1(a, b, h, k) &= b & \text{ e} \\ W_n(a, b, h, k) &= hW_{n-1}(a, b, h, k) - kW_{n-2}(a, b, h, k) \end{aligned}$$

Le $W_n(a, b, h, k)$ sono successioni ricorrenti lineari, dove ogni elemento è combinazione lineare dei due precedenti.

Diciamo successione generalizzata di Fibonacci la sequenza $W_n(a, b, h, k)$ con valori iniziali 0 e 1:

$$U_n(h, k) = W_n(0, 1, h, k)$$

La classica successione di Fibonacci (quella che conta le coppie di coniglietti) è:

$$\{U_n(1,-1)\} = \{0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, \dots\}$$

Diciamo successione generalizzata di Lucas la sequenza:

$$V_n(h, k) = W_n(2, h, h, k)$$

La classica successione dei numeri di Lucas è:

$$\{V_n(1,-1)\} = \{2, 1, 3, 4, 7, 11, 18, 29, 47, 76, 123, 199, \dots\}$$

I numeri di Lucas e quelli di Fibonacci sono collegati da moltissime relazioni. Si noti per esempio che: $1+2=3$, $1+3=4$, $2+5=7$, $3+8=11$, ..., $U_k + U_{k+2} = V_{k+1}$

Come calcolare rapidamente i numeri di Fibonacci

Nelle applicazioni occorre calcolare numeri di Fibonacci con indice grande. Questo non è possibile, in modo efficace, se si utilizza la formula ricorsiva. Un metodo efficace (tra molti altri) per il calcolo dei numeri di Fibonacci generalizzati è dato dall'uso di una particolare matrice, la matrice M . Valgono infatti le seguenti identità.

$$\mathbf{M} = \begin{pmatrix} 0 & 1 \\ -k & h \end{pmatrix}$$

$$\mathbf{M}^n = \begin{pmatrix} -kU_{n-1}(h, k) & U_n(h, k) \\ -kU_n(h, k) & U_{n-1}(h, k) \end{pmatrix}$$

$$\text{Tr}(\mathbf{M}^n) = V_n(h, k)$$

$$\mathbf{M}^n = T_n(h, k)\mathbf{I} + U_n(h, k)\mathbf{M}$$

dove:

$$T_n(h, k) = W_n(1, 0, h, k)$$

Per esempio:

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^{10} = \begin{pmatrix} 34 & 55 \\ 55 & 89 \end{pmatrix}$$

Questo algoritmo è efficace perché le potenze si calcolano velocemente, per successive quadrature.

Proprietà di divisibilità

I numeri di Fibonacci possiedono notevolissime proprietà di divisibilità (ricordiamo che la notazione $a|b$ significa "a divide b", per esempio $3|48$):

1. Se $m|n$ allora $U_m(h, k)|U_n(h, k)$
2. $p|U_{p-(\Delta/p)}(h, k)$
3. $p|U_p(h, k) - (\Delta/p)$

dove $\Delta = h^2 - 4k$ e (Δ/p) è il simbolo di Legendre, che vale 1 se Δ è un quadrato modulo p e -1 altrimenti (supporremo sempre che p non divida Δ). Per esempio, modulo 7 i quadrati sono

$1 = 1 \times 1 \pmod{7}$, $2 = 3 \times 3 \pmod{7}$, $4 = 2 \times 2 \pmod{7}$ (si ricordi che lavorando modulo 7 prendiamo sempre il resto della divisione per 7). Invece 3 non è il quadrato di alcun numero modulo 7. Pertanto si avrà $(3/7) = -1$ e $(2/7) = 1$. La proprietà 2. ci dice che dato un qualsiasi numero primo p, per quanto grande, p divide almeno un numero di Fibonacci. Dalla 1. si ricava poi che p divide infiniti numeri di Fibonacci!

Teorema di Morrison

Supponiamo $N = RF - 1$. Se $F > \sqrt{N + 1}$ ed esistono h,k tali che $(\Delta/N) = -1$ e $\forall q$ primo che divide F si ha:

1. $N | U_{N+1}(h, k)$
2. $MCD(N, U_{(N+1)/q}(h, k)) = 1$

allora N è primo.

Questo teorema permette di trovare primi molto grandi della forma, per esempio, $N = k2^n - 1$. I candidati più ovvi sono gli interi $N = 2^n - 1$. Questi numeri sono detti numeri di Mersenne.

Numeri primi di Mersenne

Si prova che per $n \geq 3$:

$$M_n = 2^n - 1$$

è primo se e solo se:

$$M_n | V_2^{n-2}(4, 1)$$

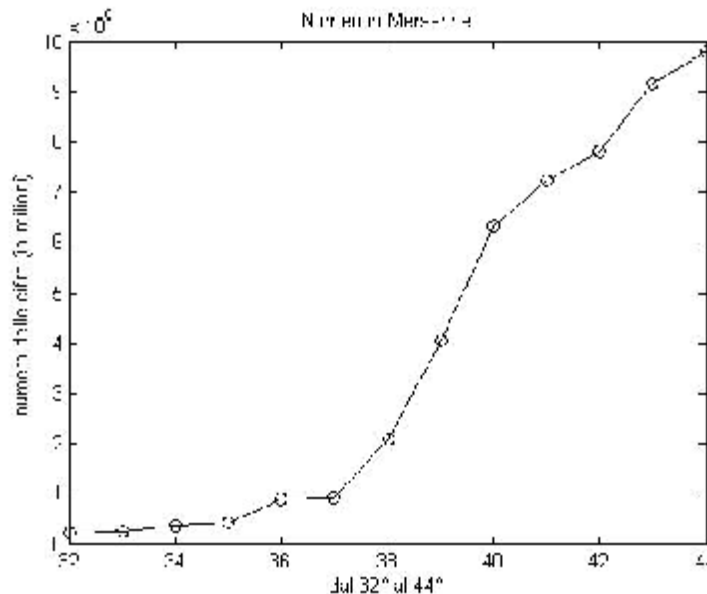
Per esempio $M_7 = 127$ è primo perché $127 | 2005956546822746114 = V_{32}$ e inoltre $V_2^{n-2}(4, 1) \pmod{M_n}$ si calcola velocemente con successive quadrature modulo M_n , in quanto:

$$V_2^{n-2}(4, 1) = L_{n-1}, \text{ dove}$$

$$L_1 = 4, L_n = L_{n-1}^2$$

{4, 14, 194, 37634, 1416317954, 2005956546822746114}

In figura si riporta come aumenta il numero delle cifre dei numeri primi di Mersenne



Attualmente sono noti soltanto 44 primi di Mersenne. Il più grande di essi sfiora il traguardo del milione di cifre.

Pseudoprimi di Fermat

Il piccolo teorema di Fermat (PTF) asserisce che dato un intero N primo:

$$1. \text{ Se } \text{MCD}(N,a)=1, \text{ allora } a^{N-1} \equiv 1 \pmod{N}$$

Purtroppo non vale il viceversa! Gli interi N composti per i quali vale la 1. vengono chiamati pseudoprimi di Fermat (ppf (a)) sulla base a . Si prova che esistono infiniti ppf su qualsiasi base. Se per N vale la 1. si dice che N passa il test di Fermat sulla base a . Se N è molto grande ed è composto ha pochissime possibilità di passare il filtro costituito dal test di Fermat. Infatti se diciamo $P(x)$ la probabilità che un numero random $N \leq x$ sia ppf (a) su random $a < N$, si prova che:

$$P(10^{100}) < 2.77 \times 10^{-18}$$

$$P(x) < (\log x)^{-197} \text{ se } x \text{ ha più di } 100000 \text{ cifre}$$

Numeri di Carmichael

Si dicono Numeri di Carmichael, *gli interi N che sono ppf (a) per ogni base a* . Si noti che le basi sono coprime con N , ed esistono quindi esattamente $\phi(N)$ basi, dove ϕ è la funzione di Eulero e:

$$\phi(N) = |\{a < N : \text{MCD}(a,N) = 1\}|$$

(Il simbolo $|A|$, dove A è un insieme finito, denota il numero di elementi di A)

E' stato dimostrato che esistono infiniti numeri di Carmichael. Questo è sorprendente perché i numeri di Carmichael hanno una forma molto originale.

Infatti si prova che: N è un numero di Carmichael se e solo se:

$$(1) N = p_1 p_2 \dots p_k$$

$$(2) \forall i, p_i - 1 | N - 1$$

Per esempio: 561 è di Carmichael, infatti $561 = 3 \times 11 \times 17$ e 2, 10, 16 dividono 560. I numeri di Carmichael *passano tutti i possibili test di Fermat*. Si può fermarli solo con un filtro più fine.

Pseudoprimi di Miller

Dato N dispari, si ha $N - 1 = 2^s T$ con $s \geq 1$ e T dispari. Le seguenti identità valgono sempre:

$$a^{N-1} - 1 = a^{2^s T} - 1 = (a^T - 1) \prod_{k=0}^{s-1} (a^{2^k T} + 1) =$$

$$(a^T - 1)(a^T + 1)(a^{2T} + 1) \dots (a^{2^{s-1} T} + 1)$$

Se N è primo per il PTF N divide $a^{N-1} - 1$, e pertanto divide, proprio perché è primo, uno almeno dei fattori sopra elencati.

Diciamo che N composto è uno *pseudoprimo di Miller sulla base a (ppm(a))* se si comporta come se fosse primo, ovvero se:

$$a^T \equiv 1 \pmod{N}, \text{ oppure}$$

$$\exists k \ 0 \leq k \leq s - 1 \ a^{2^k T} \equiv -1 \pmod{N}$$

Per ogni base a ci sono infiniti ppm(a). Però ... Non esistono interi N che siano ppm(a) su tutte le basi. Il test di Miller è un filtro assai più sottile di quello di Fermat.

Primi probabili

Se consideriamo i primi 10 numeri di Carmichael:

$$\{561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341\}$$

Soltanto gli ultimi due sono ppm(2), ma questi stessi non sono ppm(3). Fino a 2.5×10^{10} soltanto 3215031751 è ppm(a) per tutte le basi $a \in \{2, 3, 5, 7\}$. Fino a 10^{12} non ci sono interi che siano ppm(a) simultaneamente sulle basi 2, 13, 23, 1662803.

Un intero N è ppm(a) per meno di 1/4 delle possibili $\phi(N)$ basi. La probabilità che un intero N composto passi il test di Miller su k basi random è $< 1/4^k$.

Pseudoprimi di Fibonacci

Se N è composto, e soddisfa le proprietà di divisibilità per i Fibonacci:

$$N \mid U_N \left(\frac{\Delta}{N} \right) (h, k)$$

$$N \mid U_N(h, k) - \left(\frac{\Delta}{N} \right)$$

dove $\Delta = h^2 - 4k$, e (Δ/N) è il simbolo di Jacobi, che generalizza il simbolo di Legendre, diciamo che N è pseudoprimo di Fibonacci sulla base (h, k) (*ppfi*(h, k))

Considerazioni statistiche

Ci sono 9 ppm(2) minori di 50000:

{2047, 3277, 4033, 4681, 8321, 15841, 29341, 42799, 49141}

Ci sono 7 ppfi(1,-1) minori di 50000:

{4181, 5777, 6721, 10877, 13201, 15251, 34561}

Come si vede la intersezione delle due liste è vuota! La combinazione del Test di Miller e di quello di Fibonacci sembra molto efficace!

Praticamente primi

Varianti di questo Test sono utilizzate da Mathematica, Maple, Pari etc... Sia N il numero da testare. Si scelgono Δ, h, k in modo che:

- Δ sia il minimo intero della forma $5 + 4k$ tale che $(\Delta/N) = -1$
- h sia il minimo dispari maggiore di $\sqrt{\Delta}$
- $k = (h^2 - \Delta)/4$.

Se N $\mid U_{N+1}(h, k)$ e passa il test di Miller sulla base 2, allora N è dichiarato primo. Non si conoscono controesempi, anche se si dà per certo che esistano.

Certamente primi a condizione che ...

Se è vera la Extended Riemann Hypothesis (ERH) si riesce a dimostrare che:

se N è composto:

$$\exists a < 2\log^2(N) \text{ tale che } N \text{ non è ppm}(a)$$

Questo fornisce un criterio di primalità universale, deterministico e polinomiale. Però questo criterio ha il difetto di essere condizionato (cioè funziona a patto che la ERH sia vera).

Quanti sono i primi?

La funzione $\pi(x)$ conta il numero dei primi $\leq x$. Sappiamo che $\lim_{x \rightarrow \infty} \pi(x) = \infty$. Sappiamo che i numeri primi sono più frequenti dei quadrati, infatti è:

$$\sum_p \frac{1}{p} = \infty, \text{ mentre } \sum_n \frac{1}{n^2} = \frac{\pi^2}{6}.$$

Del resto, poiché $\lim_{x \rightarrow \infty} \pi(x)/x = 0$

la sequenza dei primi ha **densità** nulla. *Come tende all'infinito la somma dei reciproci dei primi?*
 Posto

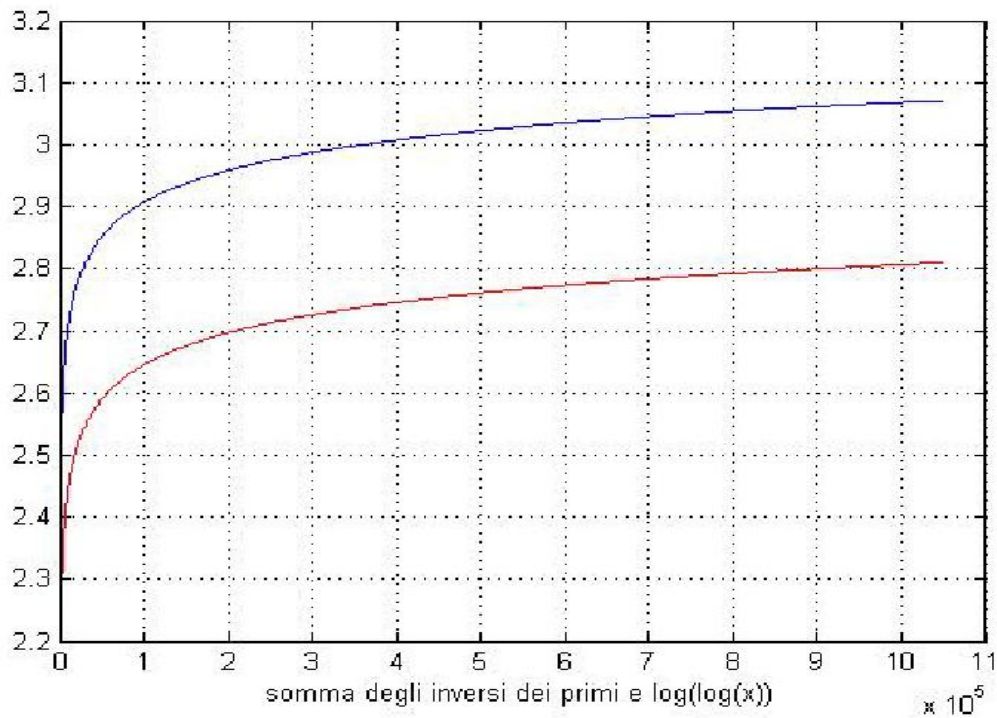
$$g(x) = \sum_{p \leq x} \frac{1}{p} \text{ si ha } g(x) \sim \log(\log(x)).$$

più esattamente Mertens dimostrò che

$$\lim_{x \rightarrow \infty} \left(\sum_{p \leq x} \frac{1}{p} - \log(\log(x)) \right) = M$$

dove M è la costante di Mertens: $M = 0.26149721284764278 \dots$

La costante di Mertens



Le due funzioni vanno all'infinito con grande lentezza e quasi parallele: la loro distanza tende alla costante M di Mertens.

Il Teorema dei Numeri Primi

È naturale chiedersi:

Come tende all'infinito $x/p(x)$?

Il Teorema dei Numeri Primi (TNP) asserisce che:

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

$$\pi(x) \sim \log(x)$$

ovvero:

$$\lim_{x \rightarrow \infty} \frac{\pi(x) \log(x)}{x} = 1$$

Il Logaritmo Integrale

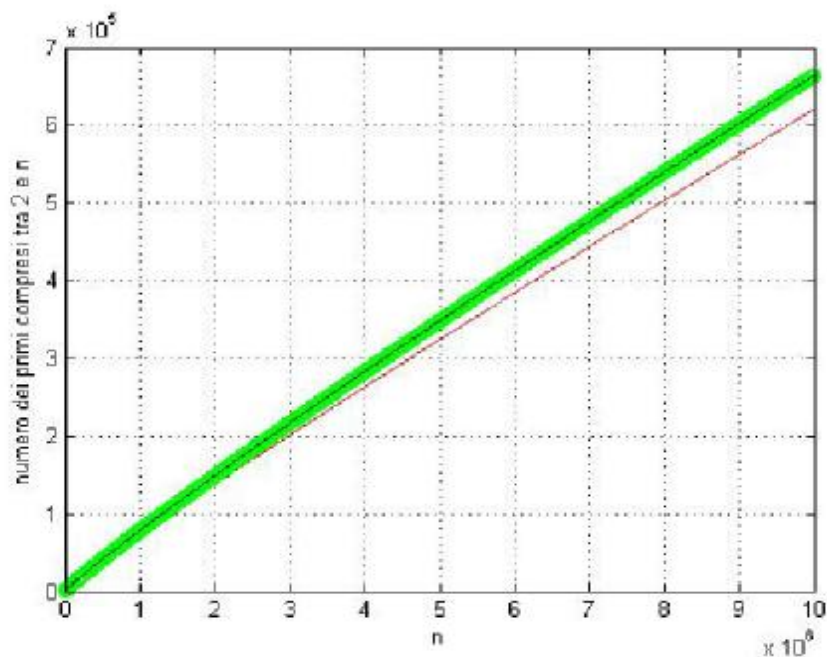
Ricordiamo la definizione del logaritmo integrale:

$$li(x) = \int_2^x \frac{dt}{\log(t)}$$

Il TNP è palesemente equivalente a:

$$\pi(x) \approx li(x)$$

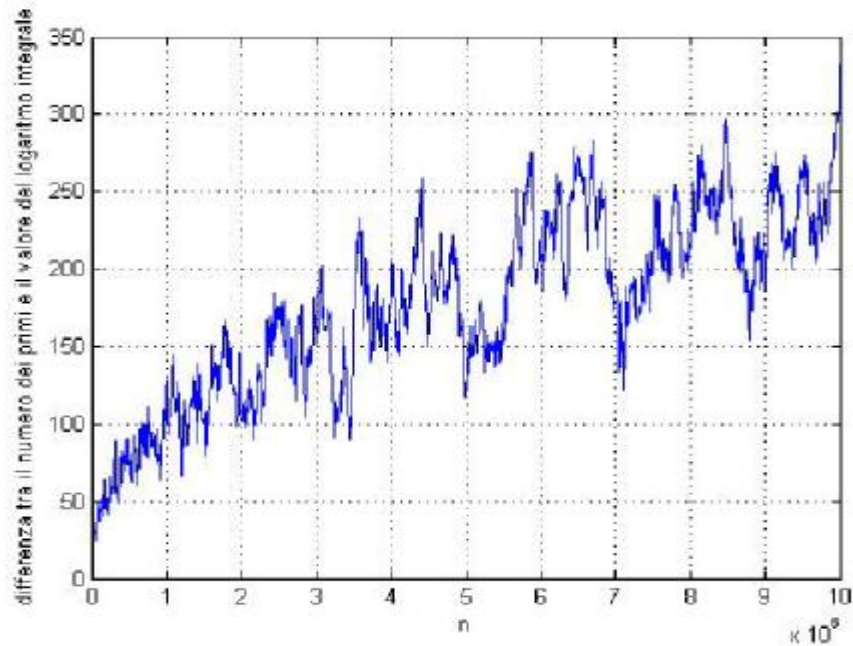
Però l'approssimazione che si ottiene con $li(x)$ è molto migliore di quella che si ha con $x/\log(x)$, è incredibilmente buona!



$x/\log(x)$, $\pi(x)$ e $li(x)$

La curva in basso è $x/\log(x)$, che sistematicamente sottovaluta $\pi(x)$. Le altre due curve sono indistinguibili sullo schermo del computer, in questa scala. Ho disegnato $li(x)$ con un tratto verde più spesso.

Nella figura seguente si vede che la differenza tra $\pi(x)$ e $li(x)$ è percentualmente assai piccola.



Differenza tra $p(x)$ e $li(x)$

La funzione Zeta

La funzione $\zeta(s)$

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

venne studiata dal maestro di tutti noi, Eulero, per s reale. Eulero dimostrò la famosa e splendida formula del prodotto:

$$\zeta(s) = \prod_p (1 - p^{-s})^{-1}$$

che lega indissolubilmente la $\zeta(s)$ ai numeri primi.

L'idea straordinaria di Riemann fu quella di estendere ζ ai numeri complessi, considerando $\zeta(s)$ funzione della variabile *complessa* s . Se s è complesso si ha $s = a + b i$, dove $i^2 = -1$; $a = \text{Re}(s)$ viene detta *parte* reale di s , e $b = \text{Im}(s)$ viene detta parte immaginaria. Cominciamo a vedere alcuni risultati ottenuti da Eulero nel suo studio di $\zeta(s)$ come funzione di variabile reale. Eulero scoprì notevolissime relazioni con i numeri di Bernoulli.

I numeri di Bernoulli sono generati dalle somme di potenze.

$$S_m(n) = \sum_{a=0}^{n-1} a^m \text{ si ha:}$$

$$S_m(n) = \frac{1}{m+1} \sum_{k=0}^{m-1} \binom{m}{k} B_k n^{m-k+1}$$

In questa espressione i numeri di Bernoulli sono i B_k . Per esempio la somma dei primi n quadrati (partendo da 0) ha questa espressione:

$$S_2(n) = \sum_{k=0}^{n-1} k^2 = \frac{n^3}{3} - \frac{n^2}{2} + \frac{n}{6}$$

Eulero provò che:

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

Per $n = 1$ ritroviamo $\zeta(2) = \pi^2/6$. Per $n = 2$ si ha $\zeta(4) = \pi^4/90$, e così via.

p e i primi

Le espressioni di $\zeta(2n)$ che contengono π e i B_k , unite alla formula del prodotto, danno luogo ad una sorprendente relazione tra π e i numeri primi. Per esempio da

$$\frac{\pi^2}{6} = \zeta(2) = \prod_p \frac{p^2}{p^2 - 1}$$

si ottiene:

$$\pi^2 = 6 \frac{4 \times 9 \times 25 \times 49 \times 121 \dots}{3 \times 8 \times 24 \times 48 \times 120 \dots}$$

Al variare di n si ottengono infinite identità.

$\zeta(2n + 1)$

Poiché l'espressione di $\zeta(2n)$ contiene π , possiamo asserire con certezza che, per ogni intero $n \geq 1$ la funzione $\zeta(2n)$ è trascendente (un numero è trascendente se non è zero di alcun polinomio con coefficienti razionali).

Può sembrare impossibile ma di $\zeta(2n + 1)$ in generale non si sa nulla, nemmeno se sia razionale. Il matematico Roger Apéry (1916-1994) divenne famoso nel 1979 per avere dimostrato che $\zeta(3)$ è irrazionale! E' stato dimostrato recentemente (Rivoal 2000) che $\zeta(s)$ irrazionale per infiniti s interi dispari, ma non si conosce alcun altro valore certo all'infuori di $s = 3$.

Nel 2001 Wadim Zudilin ha provato che uno almeno tra i quattro numeri $\zeta(5)$, $\zeta(7)$, $\zeta(9)$, $\zeta(11)$ è irrazionale.

$\zeta(-m)$

La funzione $\zeta(s)$ ha un prolungamento analitico a tutto il piano complesso, con un solo polo (singolarità) in $s = 1$. Ha senso allora chiedersi quanto vale $\zeta(-m)$ con m intero non negativo.

$$\zeta(-m) = -\frac{B_{m+1}}{m+1}$$

Si noti che tutti gli $\zeta(-m)$ sono *razionali*. Poiché i numeri di Bernoulli con indice dispari > 1 sono nulli, segue inoltre che:

$$\forall m \geq 1 \quad \zeta(-2m) = 0$$

Gli interi $s = -2, -4, -6, \dots - 2m \dots$ sono detti zeri *banali* di $\zeta(s)$.

Gli zeri di ζ

Per $\text{Re}(s) \leq 0$ gli zeri di $\zeta(s)$ sono soltanto quelli banali. Si vede facilmente che $\zeta(s) \neq 0$ per $\text{Re}(s) > 1$. Provare che $\zeta(s) \neq 0$ quando $\text{Re}(s) = 1$ è difficile. Infatti il TNP è equivalente a:

la funzione $\zeta(s)$ non ha zeri per $\text{Re}(s) \geq 1$.

Pertanto: **Tutti gli zeri di $\zeta(s)$ stanno nella fascia critica $0 < \text{Re}(s) < 1$.**

Fu Riemann ad accorgersi per primo che la distribuzione dei numeri primi è controllata dagli zeri di $\zeta(s)$. Riemann fece questa ipotesi (RH):

Tutti gli zeri non banali di $\zeta(s)$ hanno $\text{Re}(s) = \frac{1}{2}$.

Il secondo problema del Millennio

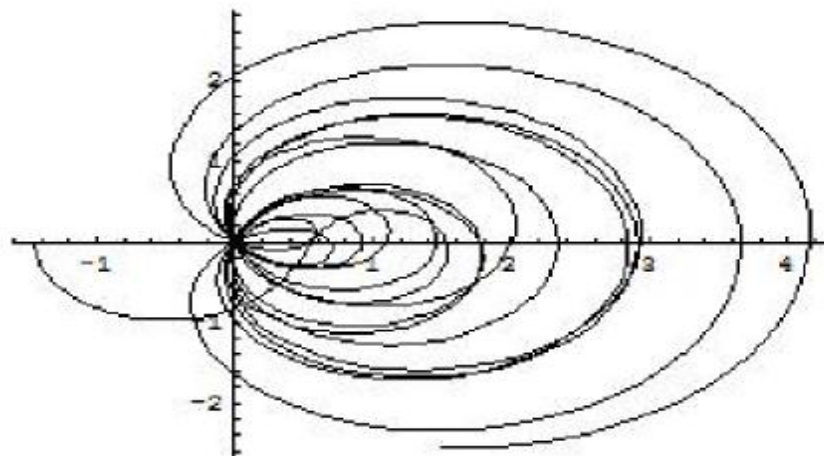
- ▶ $s = c + it$
- ▶ $t \neq 0$
- ▶ $\zeta(s) = 0$

$$\Rightarrow c = \frac{1}{2}$$

Anche per questo problema il Clay Institute offre un milione di dollari.

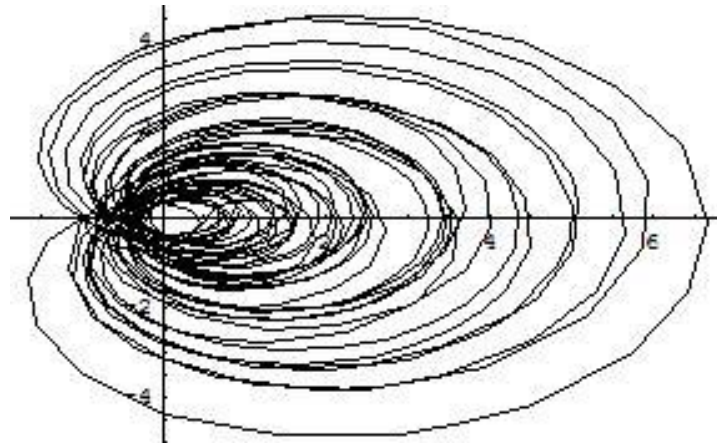
Si tratta di provare che se il numero complesso s è zero di ζ , ed è uno zero non banale in quanto la parte immaginaria $t = \text{Im}(s)$ non è nulla, allora s se ne sta allineato, con tutti gli altri zeri, sulla retta $\text{Re}(s) = \frac{1}{2}$, che, nel piano complesso, è la retta verticale che passa per il punto di coordinate $(\frac{1}{2}, 0)$. Sono stati calcolati più di 1000 miliardi di zeri! Se ne stanno tutti lì, in fila come soldatini. E' stato provato che infiniti zeri di ζ hanno $\text{Re}(s) = \frac{1}{2}$. Il sogno è che questo valga per tutti gli zeri!

L'eterno ritorno



$$\zeta\left(\frac{1}{2} + it\right) \text{ per } 0 \leq t \leq 64$$

$z(s)$ è un numero complesso, e si può rappresentare come un punto nel piano complesso. Se poniamo $s = \frac{1}{2} + i t$, cioè fissiamo $\text{Re}(s) = \frac{1}{2}$ e consideriamo $\text{Im}(s) = t$ come un parametro reale, possiamo disegnare la traiettoria nel piano compiuta dal punto $z(s) = z(\frac{1}{2} + i t)$, al variare del parametro t . Poiché sappiamo che esistono infiniti zeri con parte reale $\frac{1}{2}$ la traiettoria passerà infinite volte per zero, con infiniti ritorni all'origine! La congettura RH asserisce che se $u = \text{Re}(s)$ è diversa da $\frac{1}{2}$, allora il tracciato di $z(s) = z(u + i t)$, non passerà *mai* per l'origine! Si veda, nella figura seguente, il tracciato di $z(\frac{1}{3} + i t)$ per t compreso tra 0 e 128.



La funzione di Liouville

La congettura di Riemann RH possiede molte formulazioni diverse, alcune delle quali sono del tutto elementari. Una di queste utilizza la funzione di Liouville.

Poniamo $\omega(n)$ = numero dei fattori primi di n , contati con la loro molteplicità.

$$\omega(n) = \sum_{i=1}^{i=k} e_i$$

$$n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$$

La funzione $\lambda(n)$ di Liouville è definita da $\lambda(1n) = 1$ e:

$$\lambda(n) = (-1)^{\omega(n)}$$

Il TNP è equivalente a:

$$\lim_{n \rightarrow \infty} \frac{\lambda(1) + \lambda(2) + \lambda(3) + \dots + \lambda(n)}{n} = 0$$

e la RH è equivalente a:

$$\forall \epsilon > 0 \lim_{n \rightarrow \infty} \frac{\lambda(1) + \lambda(2) + \lambda(3) + \dots + \lambda(n)}{n^{\frac{1}{2} + \epsilon}} = 0$$

Queste espressioni sono del tutto elementari: non ci sono funzioni complesse, si deve soltanto contare il numero dei fattori primi di un intero. Da esse appare con straordinaria chiarezza come la RH sia un *rafforzamento* del teorema dei numeri primi, TPN.

La funzioni di Möebius e di Mertens

La funzione $\mu(n)$ di Möebius, per definizione vale 1 se $n = 1$, vale 0 se n è divisibile per un quadrato, e

$$\mu(n) = (-1)^k$$

quando n è prodotto di k primi distinti.
La funzione di Mertens $M(n)$ è:

$$M(n) = \sum_{k=1}^{k=n} \mu(k)$$

Mertens congetturò nel 1897 che:

$$|M(n)| < n^{\frac{1}{2}}$$

La RH è vera se e solo se:

$$M(n) = O(n^{\frac{1}{2} - \epsilon})$$

La congettura di Mertens è stata provata falsa nel 1985, ma *non è noto alcun controesempio*.

Non fidarsi mai delle apparenze

Agli inizi del 1900 Von Sterneck, basandosi sui dati sperimentali in suo possesso (il calcolo di $M(n)$ fino a $n = 5000000$), congetturò che:

$$(VS) \quad \forall n > 200 \quad |M(n)| < \frac{1}{2} n^{\frac{1}{2}}$$

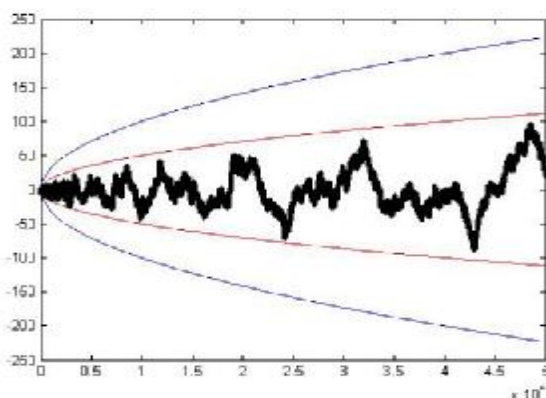
Questa congettura rimase in piedi fino al 1979, quando venne trovato un controesempio.

Il più piccolo intero per cui non vale (VS) è $n = 7725038629$

Precisamente si ha $M(7725038629) = 43947$ e $\frac{1}{2} \times 7725038629^{1/2} = 43946.09$.

Questo fatto invita essere molto cauti in questo campo!

Passeggiare con Möebius



curva rossa: $\frac{1}{2} n^{\frac{1}{2}}$, curva blu: $n^{\frac{1}{2}}$

Il tracciato nella figura qui sopra è stato costruito così: per ogni n si segna nel piano il punto (n, y_n) dove y_n è definito ricorsivamente, $y_1 = 1$, e $y_{n+1} = y_n + \mu(n)$.

Secondo la congettura (VS) di Von Sterneck il cammino dovrebbe rimanere sempre compreso nella parabola rossa. Sappiamo invece che per $n = 7725038629$ esce fuori, seppure di pochissimo.

Nella dimostrazione della falsità della congettura di Mertens si dimostra che prima o poi la traccia uscirà anche dai limiti segnati dalla parabola blu, ma nessuno sa quando questo avverrà. Si ritiene che chi fa questa passeggiata si troverà in certi momenti lontano quanto si vuole dalla curva blu.

La congettura estesa di Riemann ERH

La RH è equivalente a:

$$\pi(x) = li(x) + O(x^{\frac{1}{2}+\epsilon})$$

questo significa che, per ogni $\epsilon > 0$ il valore assoluto $|\pi(x) - li(x)|$ resta, per x abbastanza grande, minore di $x^{1/2+\epsilon}$.

Definiamo

$$\pi(x, n, a) = |\{p \leq x : p \equiv a \pmod{n}\}|$$

Per un famoso teorema di Dirichlet in ogni successione aritmetica $a + kn$ (dove a è coprimo con n) ci sono infiniti primi, che si ripartiscono nelle relative $\phi(n)$ classi. Si ha:

$$\pi(x, n, a) \sim \frac{li(x)}{\phi(n)}$$

La seguente è una versione equivalente della ERH:

$$\pi(x, n, a) - \frac{li(x)}{\phi(n)} = O(x^{\frac{1}{2}+\epsilon})$$

Primi Gemelli

I primi p e q sono gemelli se $q = p + 2$. Definiamo:

$$\pi_2(x) = \text{numero delle coppie di gemelli } \leq x$$

Un ragionamento euristico porta a concludere che:

$$\pi_2(x) \sim 2C_2 li_2(x)$$

dove:

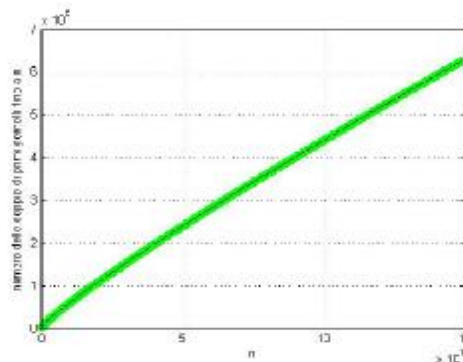


$$C_2 = \prod_{q>2} \frac{(q-2)/(q-1)}{(q-1)/q}$$



$$li_2(x) = \int_2^x \frac{dt}{\log^2(t)}$$

Evidenza sperimentale



curva verde: numero previsto, linea nera: numero effettivo di coppie di primi gemelli

Intervalli piccoli tra primi consecutivi

Malgrado l'evidenza sperimentale, non si sa se esistano davvero infinite coppie di primi gemelli. Tentare di provare la loro infinità mediante la divergenza della serie dei reciproci non funziona: la serie converge! (Brun)

$$\sum_{p>2} \frac{1}{p} = \left(\frac{1}{3} + \frac{1}{5}\right) + \left(\frac{1}{5} + \frac{1}{7}\right) + \left(\frac{1}{11} + \frac{1}{13}\right) + \dots = 1.902160582\dots$$

Poniamo:

$$E = \liminf_{n \rightarrow \infty} \frac{p_n - p_{n-1}}{\log p_n}$$

Evidentemente se la differenza tra due primi consecutivi $p_n - p_{n-1}$ scende infinite volte sotto un valore finito fissato (per esempio se esistono infiniti primi gemelli), $E = 0$. Questo limite è stato studiato da alcuni tra i più grandi matematici

1926 - $E \leq 2/3$ (Hardy e Littlewood, supponendo ERH)

1966 - $E \leq 0.46650\dots$ (Bombieri e Davenport)

1986 - $E \leq 0.2486\dots$ (Maier)

2005 - $E = 0$ (Goldston, Pintz, Yıldırım)

Il risultato del 2005 è veramente straordinario, e contiene idee e metodi nuovi che promettono nel prossimo futuro grandi applicazioni.

Progressioni aritmetiche di primi

Problema: *esistono progressioni aritmetiche di primi di qualsiasi lunghezza?* (vedi la iniziale Visione...)

Ovvero, data una lunghezza $k \geq 1$, esistono $d \in \mathbb{N}$ e q primo tali che:

$$q, q + d, q + 2d, \dots, q + kd, \dots, q + (k-1)d$$

sono tutti primi?

Per esempio per $k=8$ abbiamo la sequenza 7, 157, 307, 457, 607, 757, 907 formata da 8 primi a distanza 150, con $q=7$.

Ben Green e Terence Tao hanno dimostrato nel 2005 che, per ogni k , esistono infinite progressioni aritmetiche di lunghezza k costituite da numeri primi! La più lunga che si conosce attualmente ha 23 elementi ($k = 23$), $q = 56211383760397$ e $d = 44546738095860$.

Terence Tao

Terence Tao (nato nel 1975) ha vinto il Premio Fields nel 2006



Fame di primi

Abbiamo visto che c'è abbondanza di primi grandi e che è facile trovarli, nel senso che esistono algoritmi veloci e sicuri per testare la primalità di interi di centinaia di cifre in frazioni di secondo. Il teorema AKS, deterministico polinomiale e incondizionato, molto importante per la tecnica innovativa, non viene ancora utilizzato praticamente perché è piuttosto lento e si preferisce utilizzare metodi

probabilistici assai rapidi e quasi certi. Ci sono poi tecniche che si basano sulle curve ellittiche, assai efficaci. Danno risposta certa, ma in una frazione di casi non terminano in tempo polinomiale. I numeri primi sono importanti in gran parte delle tecniche crittografiche. Il caso più noto è l'RSA.

Rivest, Shamir e Adleman

Il metodo RSA è un sistema crittografico a *chiave pubblica*. L'utente A trova due primi grandi p e q , e calcola $n = p \times q$. Cerca un intero e random, coprimo con $\phi(n) = (p - 1)(q - 1)$, e calcola d in modo tale che si abbia $e \times d \equiv 1 \pmod{\phi(n)}$ (d è l'inverso di e modulo $\phi(n)$).

A pubblica n ed e . Se B vuole inviare un messaggio m ad A (m è rappresentato da un intero coprimo con n e $< n$), calcola $c = m^e \pmod{n}$ e lo manda ad A. A riceve c e calcola $c^d \pmod{n}$, recuperando così m . Il tutto funziona per il teorema di Eulero:

$$m^{\phi(n)} \equiv 1 \pmod{n}.$$

Un problema millenario

Metodi del tipo RSA si possono rompere fattorizzando n . Ritengo personalmente che il problema della fattorizzazione degli interi sia uno dei più importanti in assoluto. Certamente non è blasonato come la RH, o la congettura di Goldbach. Non è profondo nelle sue implicazioni come $P = NP$. Rappresenta però una grandissima sfida. Dopo migliaia di anni di matematica non siamo in gradi di scovare i componenti fondamentali della materia numerica, quando sono nascosti dentro un numero composto! Un generico intero di appena 1000 cifre è un ostacolo insormontabile, anche per milioni di computer in parallelo! Anche per le tecniche più sofisticate, curve ellittiche o crivelli dei campi di numeri!

NOTIZIARIO

Roma – 16 maggio 2007 – Protocollo d'intesa Ministero Università e Ricerca – Ministero Difesa per la collaborazione nel campo delle attività di ricerca e sviluppo spaziali

Oggi il Ministero dell'Università e della Ricerca e il Ministero della Difesa annunciano la nascita di un rapporto di collaborazione nel campo delle attività di ricerca e sviluppo spaziali col quale intendono così consolidare e rafforzare mutue relazioni di consultazione, coordinamento e collaborazione nelle attività di ricerca scientifica e tecnologica applicata al campo spaziale e aerospaziale di interesse comune, al fine di perseguire obiettivi di eccellenza nazionale nel settore dello spazio mediante l'uso continuo e sinergico di programmi, risorse e competenze professionali. Un accordo che definisce una strategia d'azione comune e parametro di interpretazione per ogni ulteriore accordo, anche a carattere esecutivo, tra i Ministeri o soggetti ad essi facenti capo.