Itinerari nel Mondo dei Numeri Primi

Umberto Cerruti

Università di Torino

19 Aprile 2007, INFN Frascati

Itinerari nel Mondo dei Numeri Primi

Umberto Cerruti

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

Una visione ...

$$2$$

$$2, 3$$

$$3, 5, 7$$

$$5, 11, 17, 23$$

$$5, 11, 17, 23, 29$$

$$7, 37, 67, 97, 127, 157$$

$$7, 157, 307, 457, 607, 757$$

$$\ldots$$

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

La dimostrazione di Euclide

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

Consideriamo un insieme $\mathcal{P}$ di k numeri primi:
$\mathcal{P} = \{p_1, p_2, \ldots, p_k\}$
Definiamo $n = p_1 p_2 \cdots p_k + 1$
Per il teorema fondamentale dell'aritmetica esiste un fattore primo q di n.
Ovviamente q è diverso da tutti i p_i.

Dato un qualsiasi insieme finito $\mathcal{P}$ di primi, esiste sempre un primo al di fuori di $\mathcal{P}$

$$\{2, 3, 5, 7, 11, 13\} \rightarrow \{59, 509\}$$

$$\{2, 3, 5, 7, 11, 13, 59, 509\} \rightarrow \{901830931\}$$

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

La dimostrazione di Eulero

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

Consideriamo un insieme $\mathcal{P}$ di k numeri primi:
$\mathcal{P} = \{p_1, p_2, \ldots, p_k\}$

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

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

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

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:

E' proprio la infinità dei primi quella che garantisce la complessità dell'universo.

o, più modestamente, la complessità delle stringhe binarie

...

Comprimibilità delle stringhe

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

Se ci mostrassero queste tre stringhe di 30 bit:

$1,1,1,1,0,1,0,1,1,0,1,0,1,1,0,1,0,1,1,1,1,0,1,0,0,0,0,1,1,1$

$1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1$

$0,0,1,1,1,0,0,1,1,1,0,0,1,1,1,0,0,1,1,1,0,0,1,1,1,0,0,1,1,1$

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 $\frac{1}{2^{30}}$, 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).

Complessità delle stringhe

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

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

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

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 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!

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

Supponiamo che l'insieme dei primi $\mathcal{P}$ sia finito:
$\mathcal{P} = \{p_1, p_2, \ldots, p_k\}$
Allora ogni intero $n \in \mathbb{N}$ si potrebbe scrivere, in modo unico nella forma:

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

Sarebbe pertanto possibile *identificare* n con la sequenza dei k esponenti $(e_1, e_2, \cdots, e_k)$
La lunghezza di questa sequenza è dell'ordine di $klog(log(n))$, quindi:
le stringhe di lunghezza n potrebbero sempre essere espresse da stringhe di lunghezza circa $klog(log(n))$
L'infinità dei numeri primi è la causa della incomprimibilità della informazione

Tempo polinomiale deterministico

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

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 $O(|a|^k)$ rispondendo correttamente sì o no.

Con $|a|$ intendiamo il *peso* dei dati di ingresso.
Per esempio se si tratta di interi, 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

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

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 stiano in **P** questi problemi, tra infiniti altri:

(3) Il grafo F contiene una cricca con k vertici?

(4) Il grafo F è Hamiltoniano?

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

Tempo polinomiale non deterministico

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

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. ci dice sì, è Hamiltoniano. So che sei incredulo, eccoti la prova:
$V_1, V_2, ..., V_{1000}$
A noi rimane soltanto da verificare che la risposta è corretta.

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. Ogni problema ha 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:

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

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

Il primo problema del Millennio

$$\text{¿ } P = NP \text{ ?}$$

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

N è primo?

Consideriamo il problema decisionale chiamato **Primes**:

$$N \text{ è primo?}$$

Non deterministicamente il co-problema di **Primes** è **Composite**:

$$N \text{ è composto?}$$

Ovviamente **Composite** sta in **NP**. Per convincermi che N è composto, basta darmi un divisore d di N. La verifica consiste semplicemente nel dividere N per d.
Pertanto **Composite** $\in$ **NP**
Primes è il co-problema di **Composite** e dunque, per definizione:
Primes $\in$ **co-NP**
Soltanto nel 1974 Pratt riuscì a provare che:

$$\textbf{Primes} \in \textbf{NP}$$

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

Primes sta in P?

A questo punto, nel 1974, si sapeva che:

$$\textbf{Primes} \in \textbf{NP} \cap \textbf{co-NP}$$

Tutti gli esperti concordavano su questa ipotesi:

$$\textbf{Primes} \in \textbf{P}$$

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*.

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

Teorema di Pocklington

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

Supponiamo $N = RF + 1$.
Se $F > \sqrt{N}$, ed esiste un a tale che $\forall q$ primo che divide F si ha:

1. $a^{N-1} \equiv 1(modN)$
2. $a^{\frac{N-1}{q}} \not\equiv 1(modN)$

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 $\iff \exists a$ tale che $a^{(N-1)/2} \equiv -1(modN)$

Teorema di Pepin

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

Metodo semplice, efficace e diretto:
troveremo tanti primi della forma $N = 2^n + 1$.
Forse...

E' facile vedere, però, che se $N = 2^n + 1$ è primo, allora necessariamente:

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

$F_n = 2^{2^n} + 1$ si dice n-esimo *numero di Fermat*.

Teorema di Pepin:
F_n è primo $\iff 3^{\frac{F_n - 1}{2}} \equiv -1$

Primi di Fermat

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

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 $641 | F_5$.
Il giovane Gauss dimostrò che un poligono regolare con N lati è costruibile con riga e compasso se e solo se

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

dove i q_i sono primi di Fermat distinti.

Le successioni di Fibonacci

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

Poniamo $W_0(a,b,h,k) = a$, $W_1(a,b,h,k) = b$ e
$\forall n > 1 \quad W_n(a,b,h,k) =$
$hW_{n-1}(a,b,h,k) - kW_{n-2}(a,b,h,k)$
Diciamo successione generalizzata di Fibonacci la sequenza:
$U_n(h,k) = W_n(0,1,h,k)$
La classica successione dei coniglietti è:
$\{U_n(1,-1)\} =$
$\{0,1,1,2,3,5,8,13,21,34,55,89,144,\cdots\}$
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:
$\{V_n(1,-1)\} =$
$\{2,1,3,4,7,11,18,29,47,76,123,199\cdots\}$

Come calcolare i Fibonacci

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

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

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

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

dove

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

Per esempio

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

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

Proprietà di divisibilità

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

I numeri di Fibonacci possiedono notevolissime proprietà di divisibilità

1. $$m|n \Rightarrow U_m(h,k)|U_n(h,k)$$
2. $$p|U_{p-\left(\frac{\Delta}{p}\right)}(h,k)$$
3. $$p|U_p(h,k) - \left(\frac{\Delta}{p}\right)$$

dove $\Delta = h^2 - 4k$ e $\left(\frac{\Delta}{p}\right)$ è il simbolo di Legendre, che vale 1 se Δ è un quadrato modulo p e -1 altrimenti (supporremo sempre che $p \not| \Delta$).

Teorema di Morrison

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

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

1. $N | U_{N+1}(h, k)$
2. $MCD\left(N, U_{\frac{N+1}{q}}(h, k)\right) = 1$

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 di Mersenne

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

Si prova che per $n \geq 3$:
$M_n = 2^n - 1$ è primo se e solo se:

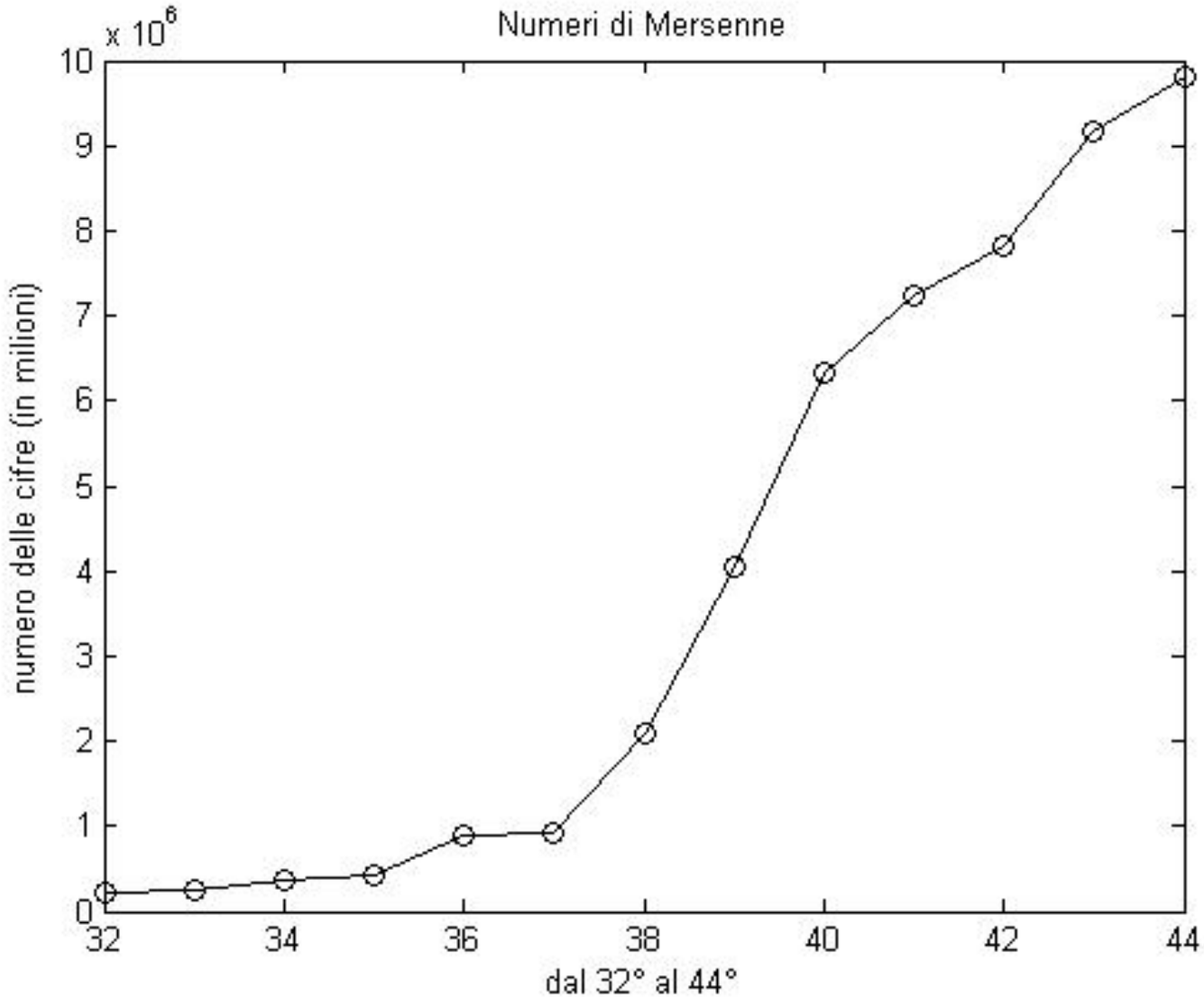
$$M_n \mid V_{2^{n-2}}(4, 1)$$

Per esempio $M_7 = 127$ è primo perché
$127 \quad | \quad 20059565468227461 14 = V_{32}$
$V_{2^{n-2}}(4, 1)(mod\ M_n)$ si calcola velocemente con successive quadrature modulo M_n, in quanto:
$V_{2^{n-2}}(4, 1) = L_{n-1}$, dove

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

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

Come aumenta il numero delle cifre dei numeri primi di Mersenne



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

Pseudoprimi di Fermat

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

Il piccolo teorema di Fermat (PTF) asserisce che se N è primo:

1. $$N \nmid a \Rightarrow a^{N-1} \equiv 1 \, (mod \, N)$$

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 diciamo $P(x)$ la probabilità che un numero random $N \leq x$ sia $ppf(a)$ su random $a < N$, si prova che:
$P(10^{100}) < 2.77 \times 10^{-8}$
$P(x) < (\log x)^{-197}$ se $x > 10^{10^5}$

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:

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

Sono numeri molto originali:
$a^{N-1} \equiv 1 (mod\ N) \quad \forall a \quad \Longleftrightarrow$
(1) $N = p_1 p_2 \cdots p_k$
(2) $\forall i, p_i - 1 \mid N - 1$
E' stato dimostrato che esitono infiniti numeri di Carmichael.

$$U_k(m) = (6m+1)(12m+1)\prod_{i=1}^{k-2}(9 \times 2^i m + 1)$$

è un numero di Carmichael se tutti i fattori sono primi.

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

Pseudoprimi di Miller

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

Dato N dispari:
$N-1=2^s T$ con $s \geq 1$ e T dispari.

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

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

Diciamo che N composto è uno *pseudoprimo di Miller sulla base a* ($ppm(a)$) se:
$a^T \equiv 1\,(mod\ N)$, oppure
$\exists k\ 0 \leq k \leq s-1 \qquad a^{2^k T} \equiv -1\,(mod\ N)$

Per ogni base a ci sono infiniti ppm(a). Però ...
Non esistono interi N che siano ppm(a) su tutte le basi.

Primi probabili

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

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 $\frac{1}{4}$ delle possibili $\phi(N)$ basi.

La probabilità che un intero N composto passi il test di Miller su k basi random è

$$< \quad \frac{1}{4^k}$$

Pseudoprimi di Fibonacci

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

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

1. $$N | U_{N-\left(\frac{\Delta}{N}\right)}(h,k)$$
2. $$N | U_N(h,k) - \left(\frac{\Delta}{N}\right)$$

dove $\Delta = h^2 - 4k$, e $\left(\frac{\Delta}{N}\right)$ 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 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

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

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

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

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

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 ...

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

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

Se N è composto:

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

Questo fornisce un criterio di primalità deterministico e polinomiale. Però questo criterio ha il difetto di essere *condizionato*.

Quanti sono i primi?

La funzione $\pi(x)$ conta il numero dei primi $\leq x$.
Sappiamo che $\lim_{x\to\infty} \pi(x) = \infty$
Sappiamo che i numeri primi sono più frequenti dei quadrati, infatti $\sum_p \frac{1}{p} = \infty$, mentre $\sum_n \frac{1}{n^2} = \frac{\pi^2}{6}$.
Però, poiché $\lim_{x\to\infty} \frac{\pi(x)}{x} = 0$, la sequenza dei primi ha *densità* nulla.
Come tende all'infinito la somma dei reciproci dei primi?
Posto $g(x) = \sum_{p<x} \frac{1}{p}$ si ha $g(x) \sim log(log(x))$.
Più esattamente Mertens dimostrò che

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

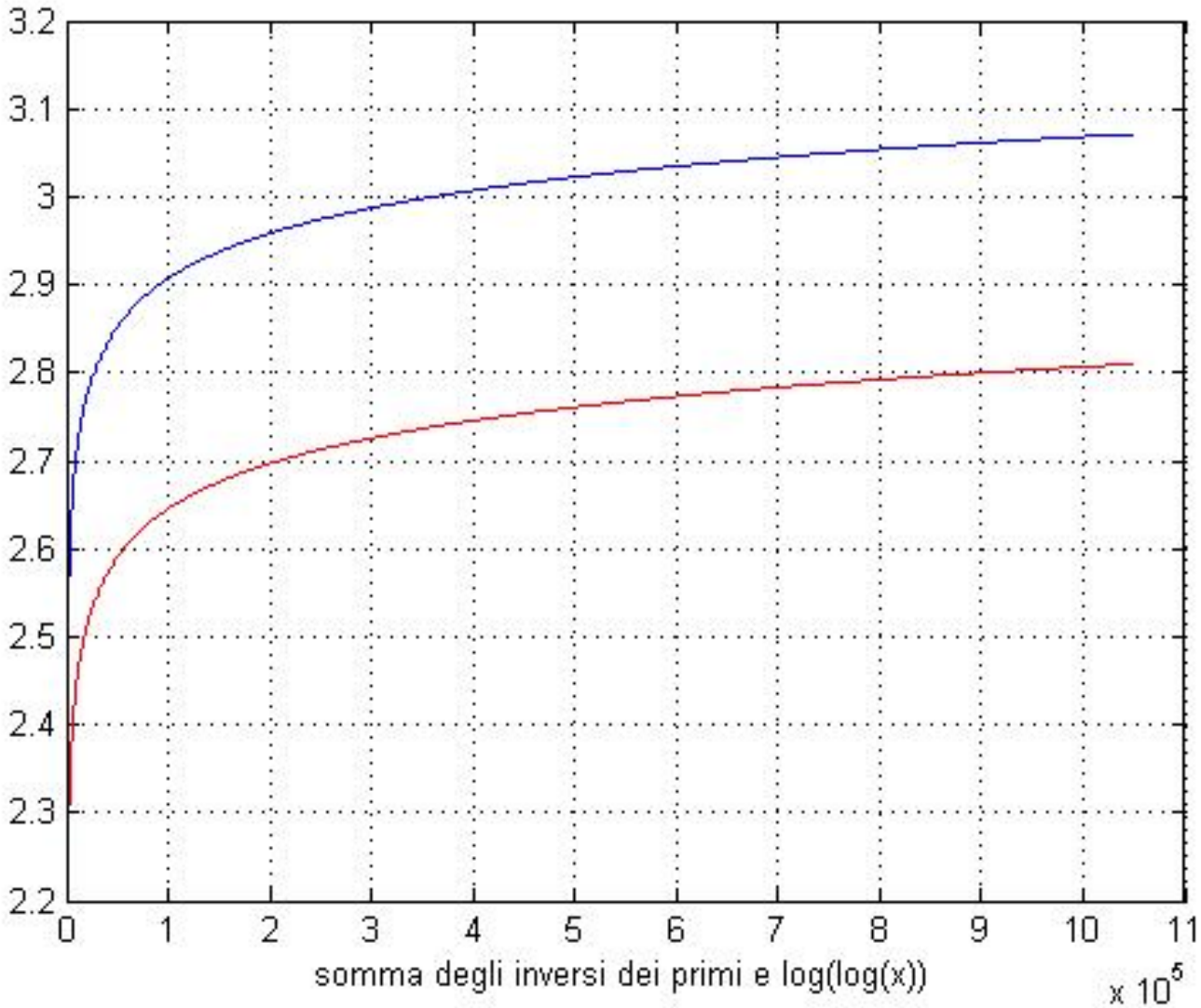
dove M è la *costante di Mertens*:

$$M = 0.2614972128476427 8\ldots$$

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

.

La costante di Mertens



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

Il Teorema dei Numeri Primi

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

E' naturale chiedersi:

$$\textit{Come tende all'infinito } \frac{x}{\pi(x)}?$$

Il Teorema dei Numeri Primi (TNP) asserisce che:

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

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

ovvero:

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

Il Logaritmo Integrale

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

Ricordiamo la definizione del logaritmo integrale:

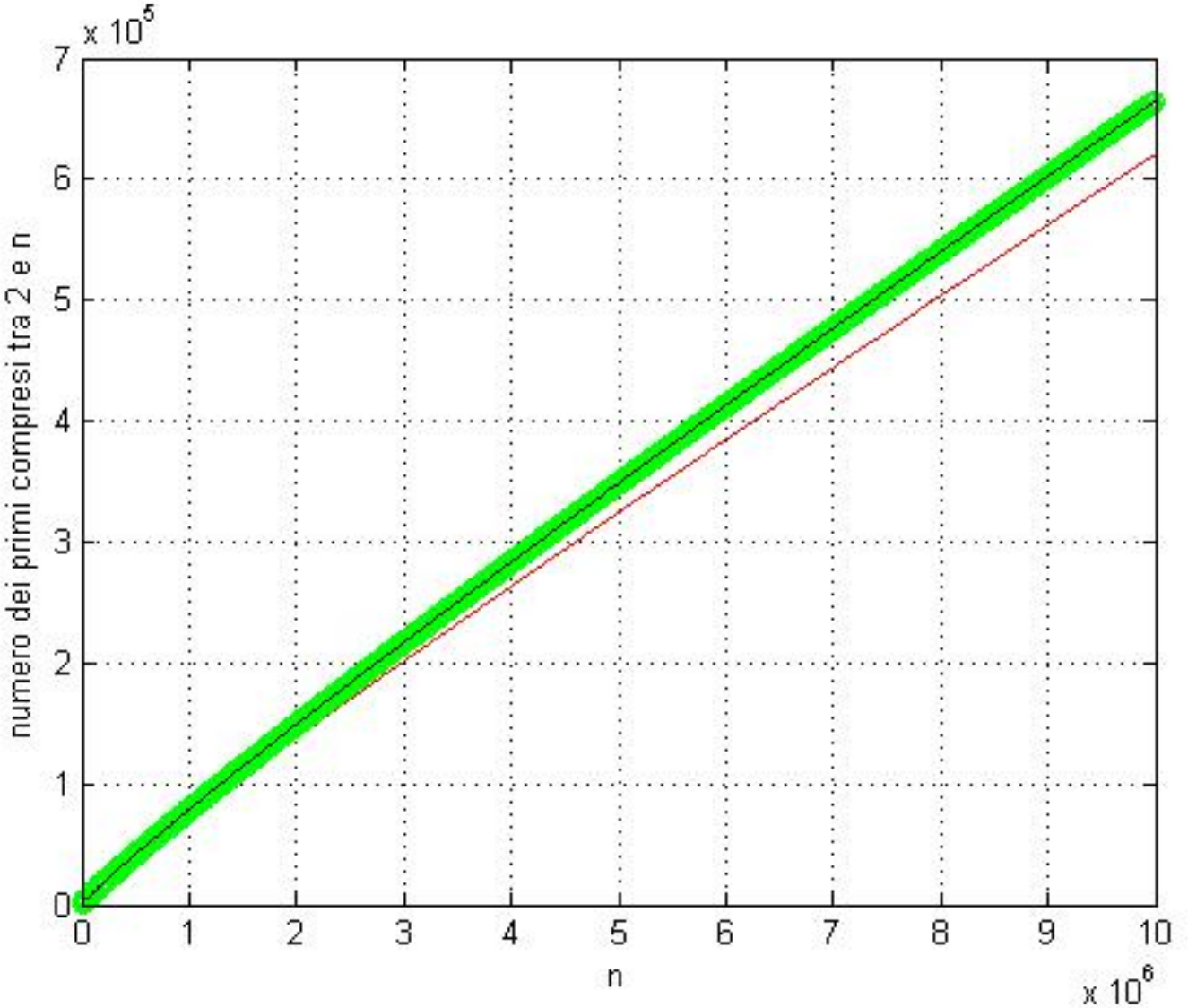
$$li(x) = \int_2^x \frac{dt}{log(t)}$$

Il TNP è palesemente equivalente a:

$$\pi(x) \sim li(x)$$

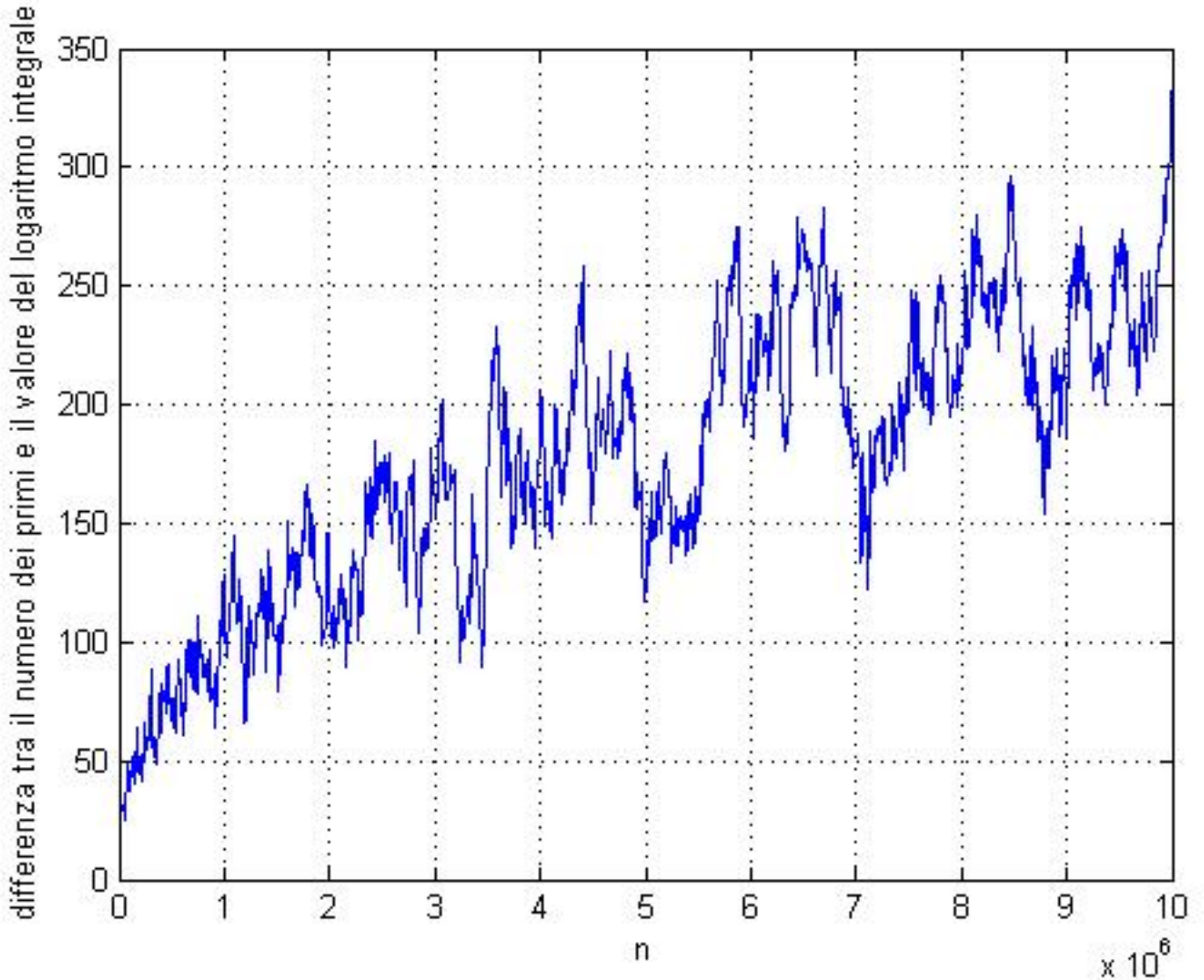
Però l'approssimazione che si ottiene con $li(x)$ è molto migliore di quella che si ha con $\frac{x}{log(x)}$, è incredibilmente buona!

$\frac{x}{log(x)}$, $\pi(x)$ e $li(x)$



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

Differenza tra $\pi(x)$ e $li(x)$



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

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 *formula del prodotto*:

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

che lega indissolubilmente la ζ ai numeri primi.

L'idea straordinaria di Riemann fu quella di estendere ζ ai *numeri complessi*

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

$\zeta(2n)$

I numeri di Bernoulli sono generati dalle somme di potenze.
Detta $S_m(n) = \sum_{a=0}^{a=n-1} a^m$ si ha:

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

In questa espressione i numeri di Bernoulli sono i B_k.

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

Eulero provò che:

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

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

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

π 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:

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

Al variare di n si ottengono infinite identità.

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

$\zeta(2n+1)$

Poiché l'espressione di $\zeta(2n)$ contiene π, possiamo asserire con certezza che, per ogni intero $n \geq 1$ $\zeta(2n)$ è trascendente.
Può sembrare impossibile ma di $\zeta(2n+1)$ 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 z(5), z(7), z(9), z(11) è irrazionale.

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

$\zeta(-m)$

La funzione $\zeta(s)$ ha un prolungamento analitico a tutto il piano complesso, con un solo polo 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 che:

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

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

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

Gli zeri di ζ

Per $Re(s) \leq 0$ gli zeri di $\zeta(s)$ sono soltanto quelli banali.
Si vede facilmente che $\zeta(s) \neq 0$ per $Re(s) > 1$.
Provare che $\zeta(s) \neq 0$ quando $Re(s) = 1$ è difficile. Infatti il TNP è equivalente a:
La funzione $\zeta(s)$ non ha zeri per $Re(s) \geq 1$.
Pertanto:
Tutti gli zeri di $\zeta(s)$ stanno nella fascia critica
$0 < Re(s) < 1$.
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 $Re(s) = \frac{1}{2}$

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

Il secondo problema del Millennio

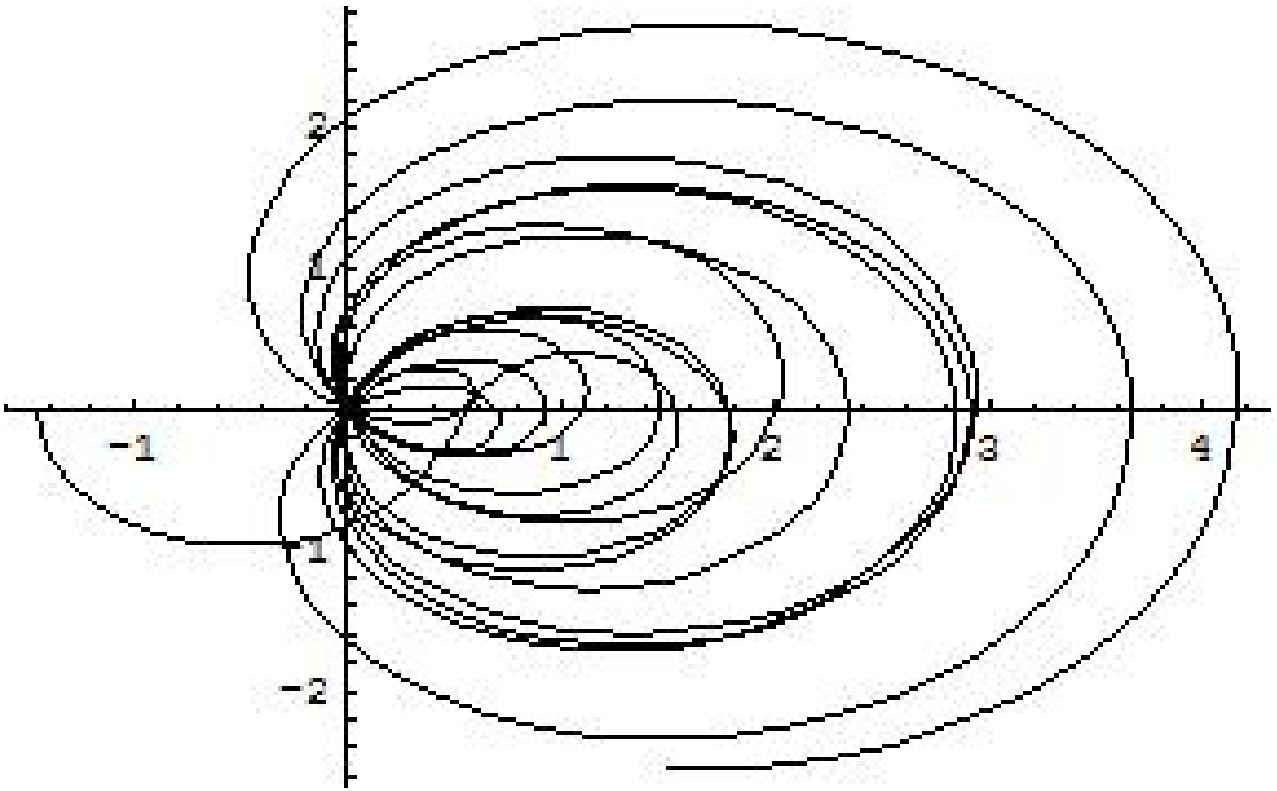
Ci sono infiniti numeri primi
Euclide
Eulero
Chaitin
Complessità
La classe P
La classe NP
Complessità dei primi
Test di primalità
Il mondo del +1
Successioni lineari ricorrenti
Il mondo del -1
Test probabilistici
Il Piccolo Teorema di Fermat
Miller e Fibonacci
Un criterio condizionato
Distribuzione dei numeri primi
Il Teorema dei Numeri Primi
La Congettura di Riemann
Gap tra i Primi
Conclusioni

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

$$\Rightarrow$$

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

L'eterno ritorno



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

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

La funzione di Liouville

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

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

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

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

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

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

Il TNP è equivalente a:

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

e la RH è equivalente a:

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

La funzioni di Möebius e di Mertens

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

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:

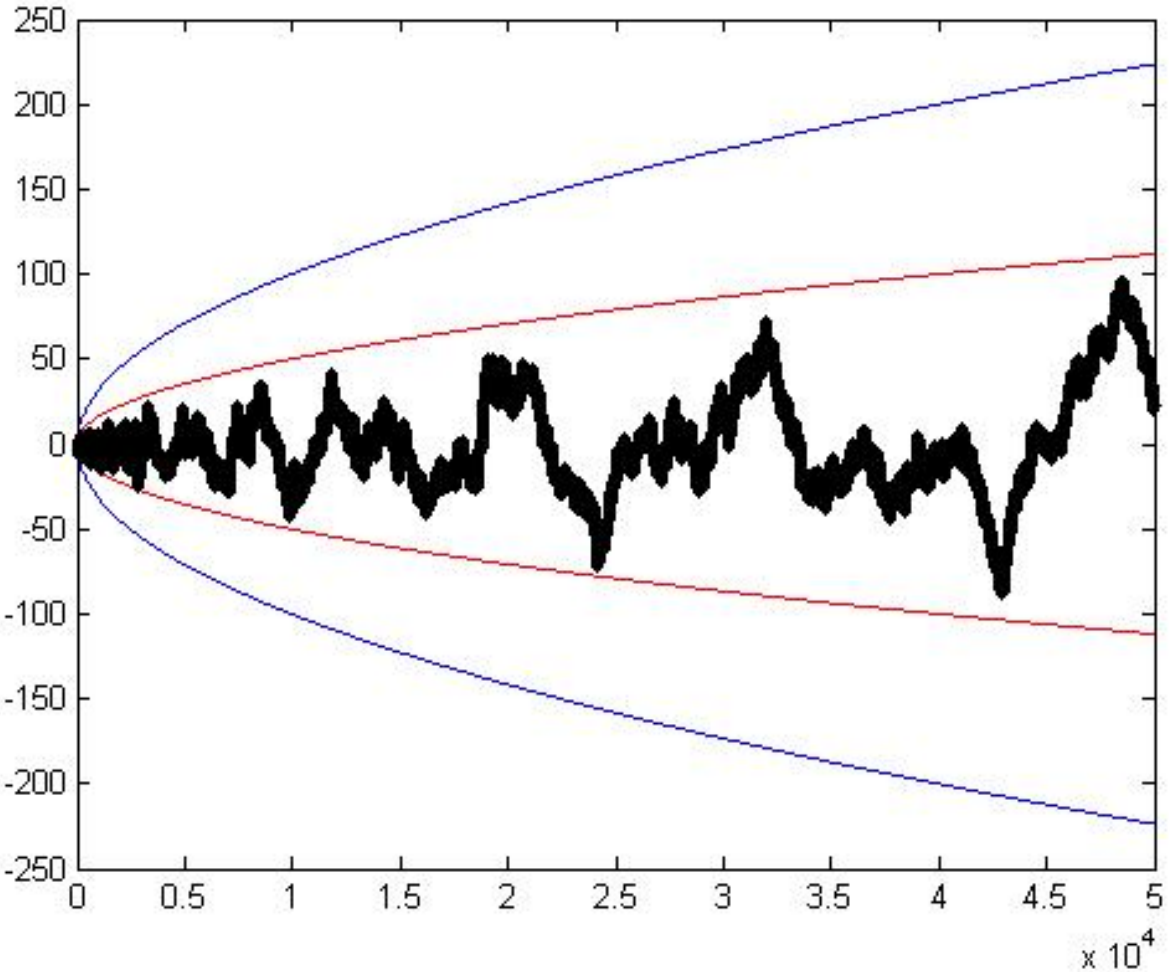
$$|M(n)| < n^{\frac{1}{2}}$$

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*.

Passeggiare con Möebius



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

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

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:

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

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 $\frac{1}{2} 7725038629^{\frac{1}{2}} = 43946.09$

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

La congettura estesa di Riemann ERH

La RH è equivalente a:

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

Definiamo

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

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

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

La seguente è una versione equivalente della ERH:

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

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

Primi Gemelli

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

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

Un ragionamento euristico porta a concludere che:

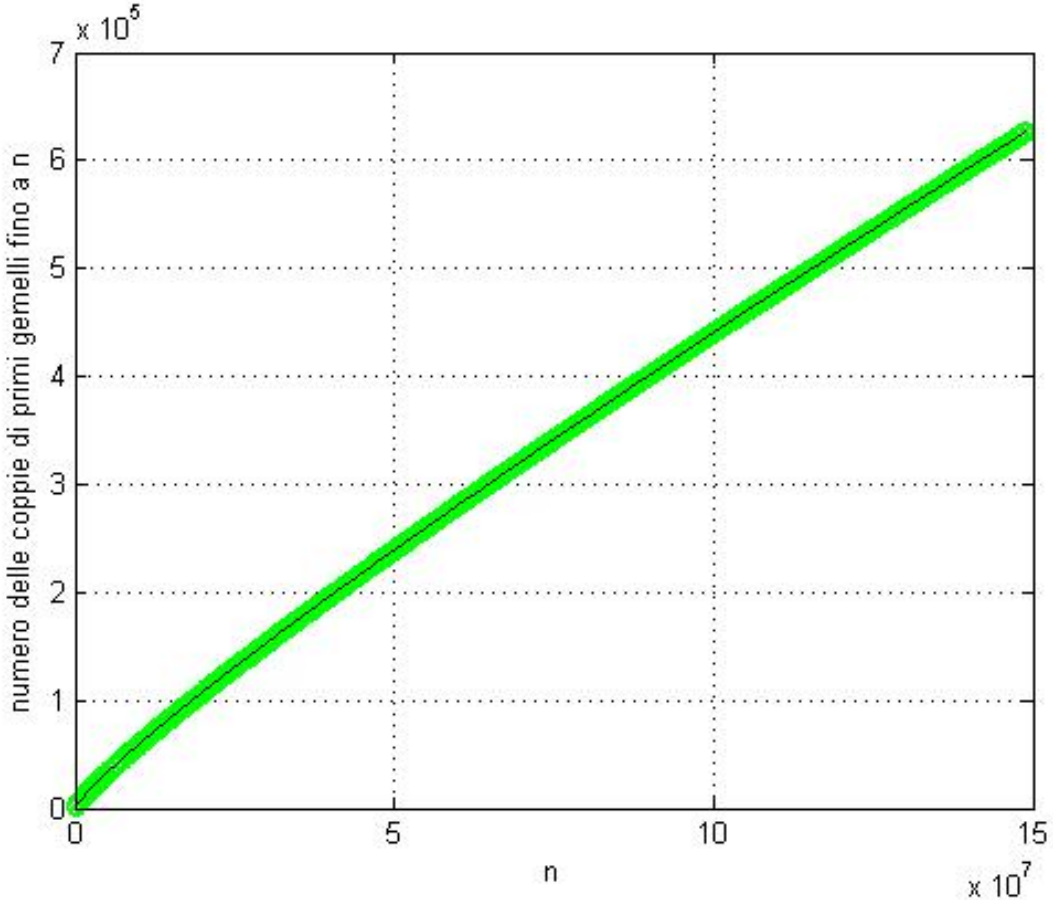
$$\pi_2(x) \sim 2C_2 li_2(x)$$

dove:

- $$C_2 = \prod_{q>2} \frac{(q-2)/(q-1)}{(q-1)/q}$$
- $$li_2(x) = \int_2^x \frac{dt}{log^2(t)}$$

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

Evidenza sperimentale



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

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

Intervalli piccoli tra primi consecutivi

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

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)

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

Poniamo $E = \liminf_{n\to\infty} \frac{p_n - p_{n-1}}{\log p_n}$.

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

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

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

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

Progressioni aritmetiche di primi

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

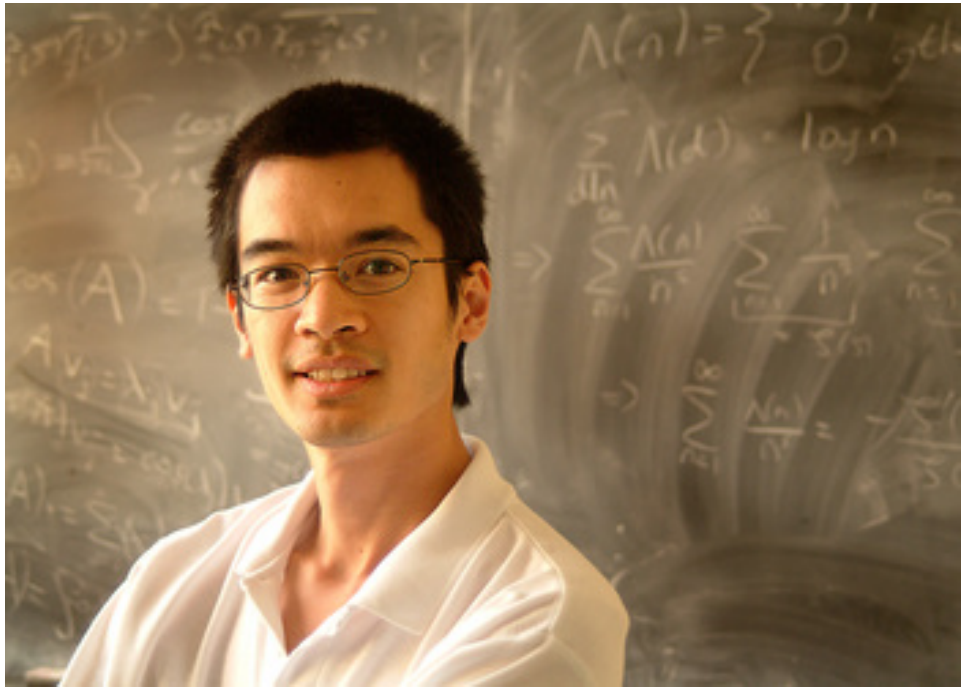
Problema : esistono progressioni aritmetiche di primi di qualsiasi lunghezza?
Ovvero, data una lunghezza $k \geq 1$, esistono $d \in \mathbb{N}$ e q primo tali che:

$$q, q+d, q+2d, \cdots q+h\,d, \cdots, q+(k-1)d$$

sono tutti primi?

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 ha 23 elementi ($k = 23$), $q = 56211383760397$ e $d = 44546738095860$.

Terence Tao



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

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

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.

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

Rivest, Shamir e Adleman

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

Il metodo RSA è un sistema crittografico a *chiave pubblica*.
L'utente A trova due primi grandi p e q, e calcola $n = p \times q$.
Prende e random coprimo con $\phi(n) = (p-1)(q-1)$, e calcola $d : ed \equiv 1 \, (mod \, n)$.
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 $c = m^e \, (mod \, n)$ e lo manda ad A.
A riceve c e calcola $c^d \, (mod \, n)$, recuperando così m.
Il tutto funziona per il teorema di Eulero:
$m^{\phi(n)} \equiv 1 \, (mod \, n)$.

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 trovare i componenti fondamentali della materia numerica! 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!

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