I numeri primi: teoremi, congetture e applicazioni
Scuola Estiva di San Pellegrino Terme

Alessandro Zaccagnini
Dipartimento di Matematica e Informatica
Università di Parma

San Pellegrino Terme, 7 settembre 2016

Sommario

Utilizzando strumenti eterogenei della matematica di base, quali i coefficienti binomiali, la somma della serie geometrica, la divergenza della serie armonica e qualche limite notevole, otterremo delle informazioni qualitative e quantitative sulla distribuzione dei numeri primi. Dimostreremo in piú modi diversi che esistono infiniti numeri primi e in questo modo potremo "indovinare" il Teorema dei Numeri Primi, e anche parlare delle grandi congetture e dei numerosi problemi aperti. Concluderemo con qualche cenno alle applicazioni pratiche dei numeri primi, come la crittografia.

1 Introduzione

La distribuzione dei numeri primi è uno dei problemi matematici piú antichi, ma nonostante i secoli di studio presenta ancora aspetti molto misteriosi. In questo documento presenteremo in modo "elementare," e cioè facendo un uso molto limitato di tecniche proprie dell'analisi matematica, alcune idee al riguardo. Armati solo di strumenti relativamente modesti, riusciremo a scoprire informazioni non scontate sui numeri primi, che ci permetteranno di apprezzare alcuni dei piú importanti problemi ancora aperti.

Non intralceremo il discorso con continui riferimenti bibliografici: a questi dedichiamo un'apposita sezione in Appendice.

2 Il Teorema di Euclide: esistono infiniti numeri primi

Preferiamo enunciare il Teorema di Euclide (Elementi, IX, Proposizione 10) in una forma che, probabilmente, i matematici greci avrebbero trovato piú accettabile, perché non coinvolge il concetto di insieme infinito, ma solo quello di insieme (superiormente) illimitato.

Teorema 1 (Euclide)**.** *L'insieme dei numeri primi è illimitato superiormente.*

Esempio
Troviamo un numero primo > 1000. Facile! Un *qualsiasi* fattore primo di $M = 1000! + 1$.

Molto piú facile a dirsi che a farsi, naturalmente, dato che M ha 2568 cifre decimali: stiamo solo parlando in linea di principio. In ogni caso, sappiamo che ci sono infiniti numeri primi.

Dimostrazione
Sia n un qualsiasi intero positivo e sia p un qualsiasi fattore *primo* di $M = n! + 1$: evidentemente $p > n$ dato che $M \equiv 1 \bmod d$ per ogni intero $d \in [2, n]$. In altre parole, M dà resto 1 se diviso per un qualsiasi intero $d \in [2, n]$. Dunque l'insieme dei numeri primi è illimitato superiormente.

Esempio

n	1	2	3	4	5	6	7	8	9	10
p_n	2	3	7	5	11	7	71	61	19	11

In questa tabella, p_n è il piú piccolo fattore primo di $n! + 1$.

2.1 Quanti sono i numeri primi?

La domanda non deve sorprendere: ci chiediamo se sia possibile "prevedere" quanti numeri primi ci sono nell'intervallo $[1, n]$ quando n è grande. Tradizionalmente, questo numero si indica con $\pi(n)$: dunque $\pi(10) = 4$, $\pi(100) = 25$ e $\pi(1000) = 168$; si veda la Figura 1. Oggi è noto il valore esatto di $\pi\left(10^{25}\right)$, anche se non conosciamo individualmente tutti i numeri primi fino a questo numero. La domanda posta è di tipo qualitativo: sappiamo che esistono infiniti numeri primi, ma anche infiniti numeri pari, infiniti quadrati perfetti e infinite potenze di 2: per gli ultimi 3 insiemi, è chiaro che la "densità" dei rispettivi elementi è molto diversa. In un senso un po' vago, potremmo chiederci qual è la probabilità di scegliere un numero primo (pari, quadrato perfetto, potenza di 2) se prendiamo un numero "grande" a caso.

I numeri primi possono essere determinati con un procedimento meccanico scoperto da Eratostene di Alessandria, il cosiddetto *crivello*. A partire da questo, nel XVIII secolo il matematico francese Adrien-Marie Legendre scoprí un modo per determinare il numero dei numeri primi che non superano un certo intero dato. Una variante della formula di Legendre è stata usata per portare a termine il calcolo numerico esatto di $\pi(n)$ per $n = 10$, 10^2, 10^3 fino ad $n = 10^{25}$, come dicevamo sopra. A partire dai valori di $\pi(n)$ con n fino a qualche milione, lo stesso Legendre e Carl F. Gauss formularono una Congettura, di cui parleremo sotto nel §5.

3 Stime numeriche dall'alto e dal basso per $\pi(n)$

3.1 Una maggiorazione per il numero di numeri primi

Vediamo ora come sia possibile ottenere informazioni, non molto precise ma al tempo stesso non ovvie, sul numero di numeri primi in un intervallo. Utilizziamo il coefficiente binomiale centrale(vedi §A.2): per esempio, per $n = 16$ abbiamo

$$\binom{32}{16} = \frac{17 \cdot 18 \cdot 19 \cdots 31 \cdot 32}{16!} = 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot m \leq 2^{32}.$$

Qui m è un certo intero positivo, poiché i numeri primi nell'intervallo $[17, 32]$ compaiono a numeratore ma non a denominatore del coefficiente binomiale a sinistra, e non possono essere "semplificati". Dunque

$$17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \leq 2^{32}.$$

n	$\pi(n)$	n	$\pi(n)$
10	4	10^{10}	455052511
10^2	25	10^{11}	4118054813
10^3	168	10^{12}	37607912018
10^4	1229	10^{13}	346065536839
10^5	9592	10^{14}	3204941750802
10^6	78498	10^{15}	29844570422669
10^7	664579	10^{16}	279238341033925
10^8	5761455	10^{17}	2623557157654233
10^9	50847534	10^{18}	24739954287740860

Figura 1: Alcuni valori di $\pi(n)$

Ma

$$17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \geq 16 \cdot 16 \cdot 16 \cdot 16 \cdot 16.$$

Fingiamo, per un momento, di non saper contare fino a 5. Posto $x = \pi(32) - \pi(16)$, abbiamo

$$16^x \leq 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \leq \binom{32}{16} \leq 2^{32}.$$

Riassumendo, abbiamo

$$16^x \leq 2^{32}.$$

Quindi

$$x \log(16) = \big(\pi(32) - \pi(16)\big) \log(16) \leq 32 \log(2),$$

cioè

$$x = 5 \leq \frac{32 \log(2)}{\log(16)} = 8.$$

A prima vista, questo non è un gran risultato, ma è solo un esempio di quanto è possibile ottenere per un *qualunque* intervallo. In generale, per $n \geq 2$ abbiamo

$$\pi(2n) - \pi(n) \leq \frac{2n \log(2)}{\log(n)}.$$

Questa formula conferma l'osservazione sperimentale, e intuitivamente ovvia, che i numeri primi tendono a diradarsi.

3.1.1 Un'applicazione concreta

Per semplificare i calcoli, prendiamo $n = 2^k$ ottenendo

$$\pi(2^{k+1}) - \pi(2^k) \leq \frac{2^{k+1} \log(2)}{\log(2^k)} = \frac{2^{k+1}}{k}.$$

Usiamo questa disuguaglianza con $k = 9, 8, 7, \ldots, 4$. Nella tabella in Figura 2 riportiamo i valori esatti di $\pi(2^{k+1}) - \pi(2^k)$ accanto alla maggiorazione trovata qui sopra. Come si vede, la stima trovata è piú grande del valore reale del 50% circa. Nell'ultima riga sommiamo tutti i valori trovati nelle righe precedenti: i primi membri sono scelti in modo da "semplificarsi" quando facciamo la loro somma.

$$\begin{aligned}
\pi(2^{10})-\pi(2^9) &= 75 \le 113\\
\pi(2^9)-\pi(2^8) &= 43 \le 64\\
\pi(2^8)-\pi(2^7) &= 23 \le 36\\
\pi(2^7)-\pi(2^6) &= 13 \le 21\\
\pi(2^6)-\pi(2^5) &= 7 \le 12\\
\pi(2^5)-\pi(2^4) &= 5 \le 8\\
\pi(2^4) &= 6 = 6\\
\text{Totale}\qquad \pi(2^{10}) &= 172 \le 260
\end{aligned}$$

Figura 2: Come utilizzare la disuguaglianza per $\pi(2n)-\pi(n)$

3.2 Stime dal basso per il numero di numeri primi

3.2.1 Con quante cifre 0 termina 1000! ?

Ci facciamo una domanda apparentemente scollegata con i numeri primi: con quante cifre 0 termina $M = 1000!$? In altre parole, qual è la massima potenza di 10 che divide 1000! ? Qual è la massima potenza di 5 che divide 1000! ? Dobbiamo scomporre M nei suoi fattori primi, anche se ci interessa solo l'esponente di 5. Nell'intervallo $[1,1000]$ ci sono 200 multipli di 5; ma poi ci sono 40 multipli di $25 = 5^2$; e poi ancora 8 multipli di $125 = 5^3$; e infine un multiplo di $625 = 5^4$. Complessivamente, $200+40+8+1 = 249$. Notiamo che

$$\begin{aligned}
249 &= \Big[\frac{1000}{5}\Big] + \Big[\frac{1000}{5^2}\Big] + \Big[\frac{1000}{5^3}\Big] + \Big[\frac{1000}{5^4}\Big]\\
&\sim \frac{1000}{5}\Big(1+\frac{1}{5}+\frac{1}{5^2}+\frac{1}{5^3}\Big)\\
&\sim \frac{1000}{5}\cdot\frac{1}{1-1/5} = \frac{1000}{4} = 250.
\end{aligned}$$

L'ultimo passaggio richiede saper sommare una serie geometrica (vedi §A.1). Osserviamo che, nonostante le approssimazioni, le due quantità estreme sono molto vicine fra loro.

3.2.2 Scomponiamo in fattori $n!$

La scomposizione in fattori primi di $n!$ contiene informazioni sui numeri primi fino ad n. Per esempio

$$20! = 2^{10+5+2+1}\cdot 3^{6+2}\cdot 5^4\cdot 7^2\cdot 11\cdot 13\cdot 17\cdot 19.$$

Il punto essenziale è che c'è un modo alternativo per calcolare (approssimativamente) quanto vale $n!$. Si tratta della formula di Stirling, presentata nel §A.4. In generale, se $p \le n$ è un numero primo, la massima potenza di p che divide $n!$ ha esponente

$$\Big[\frac{n}{p}\Big] + \Big[\frac{n}{p^2}\Big] + \Big[\frac{n}{p^3}\Big] + \Big[\frac{n}{p^4}\Big] + \cdots \sim \frac{n}{p-1},$$

con qualche calcolo basato, come sopra, sulla somma della serie geometrica. Quindi,

$$\log(n!) \sim \sum_{p \le n} \frac{n \log(p)}{p-1},$$

dove la somma è fatta sui numeri primi che non superano n. Confrontando con il valore approssimato per $\log(n!)$ fornito dalla Formula di Stirling (vedi §A.4) si ricava che

$$\sum_{p \le n} \frac{\log(p)}{p-1} \sim \log(n).$$

Con un po' di pazienza, ragionando ancora sui coefficienti binomiali, è possibile ottenere stime dal basso per $\pi(n)$ del giusto ordine di grandezza. Con qualche calcolo ulteriore si dimostra che per n grande si ha $\pi(n) \ge (n\log(2))/\log(n)$. La dimostrazione di quest'ultimo fatto può essere ottenuta in modo piuttosto semplice utilizzando il calcolo integrale di base, ma qui la omettiamo per la sua lunghezza.

4 Il Teorema di Eulero

4.1 Versione qualitativa

Abbiamo bisogno della formula per la somma della serie geometrica, che ricordiamo nel §A.1. Consideriamo le somme delle serie geometriche di ragione $1/2$, $1/3$, $1/5$ ed $1/7$, che chiameremo A, B, C, D rispettivamente.

$$\begin{aligned}
A &= 2 = \left(1-\frac{1}{2}\right)^{-1} = 1+\frac{1}{2}+\frac{1}{4}+\frac{1}{8}+\frac{1}{16}+\ldots \ge 1+\frac{1}{2}+\frac{1}{4}+\frac{1}{8} \\
B &= \frac{3}{2} = \left(1-\frac{1}{3}\right)^{-1} = 1+\frac{1}{3}+\frac{1}{9}+\frac{1}{27}+\ldots \ge 1+\frac{1}{3}+\frac{1}{9} \\
C &= \frac{5}{4} = \left(1-\frac{1}{5}\right)^{-1} = 1+\frac{1}{5}+\frac{1}{25}+\ldots \ge 1+\frac{1}{5} \\
D &= \frac{7}{6} = \left(1-\frac{1}{7}\right)^{-1} = 1+\frac{1}{7}+\frac{1}{49}+\ldots \ge 1+\frac{1}{7}
\end{aligned}$$

Le disuguaglianze numeriche qui sopra sono del tutto banali: le diamo in una forma che può apparire curiosa perché ci permetterà di introdurre in modo naturale l'identità di Eulero. Se moltiplichiamo fra loro i 4 numeri A, B, C e D (come se fossero polinomi costituiti da monomi non simili, in un certo senso, e quindi eseguendo solo le moltiplicazioni e non le addizioni) e i lati destri delle disuguaglianze qui sopra, troviamo *tutti* i reciproci degli interi fra 1 e 10, oltre ad altre frazioni che possiamo trascurare, poiché che ci interessa dare una stima dal basso. In definitiva, abbiamo

$$\begin{aligned}
A \cdot B \cdot C \cdot D &\ge \left(1+\frac{1}{2}+\frac{1}{4}+\frac{1}{8}\right)\left(1+\frac{1}{3}+\frac{1}{9}\right)\left(1+\frac{1}{5}\right)\left(1+\frac{1}{7}\right) \\
&\ge 1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{5}+\frac{1}{6}+\frac{1}{7}+\frac{1}{8}+\frac{1}{9}+\frac{1}{10} \\
&\ge \log(10).
\end{aligned}$$

Come si vede, a stretto rigore non abbiamo veramente bisogno della formula per la somma della serie geometrica, dato che possiamo dimostrare direttamente le disuguaglianze richieste per A, B, C e D. Abbiamo preferito lasciare la dimostrazione in questa forma, anche se leggermente piú sofisticata, perché è piú chiara e, soprattutto, spiega le idee successive.

In generale, possiamo ripetere lo stesso ragionamento considerando tutti i numeri primi fino ad un certo intero n e le relative serie geometriche: moltiplicando fra loro le disuguaglianze corrispondenti, come abbiamo fatto sopra, troviamo i reciproci di *tutti* gli interi che non superano n e molti altri addendi piú piccoli che possiamo trascurare ancora una volta. Notiamo che stiamo implicitamente usando il Teorema di Unicità della Fattorizzazione. Utilizzando poi la serie armonica (vedi §A.5), si ottiene la dimostrazione del Teorema di Eulero: la sua importanza sta nel fatto che per la prima volta nella storia sono stati collegati un fatto "aritmetico" ed un fatto "analitico." Questa idea si è rivelata molto fruttuosa nei secoli successivi, ed è ancora alla base di tutti gli studi piú seri sui numeri primi, nonché di tutte le piú importanti generalizzazioni.

Teorema 2 (Eulero)**.** *Per $n \geq 2$ si ha*

$$\prod_{p \leq n} \Big(1 - \frac{1}{p}\Big)^{-1} \geq 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} \geq \log(n),$$

dove il prodotto è fatto su tutti i numeri primi che non superano n.

4.2 L'identità di Eulero e la funzione zeta di Riemann

Teorema 3 (Identità di Eulero)**.** *Se $x > 1$ allora*

$$\begin{aligned} \zeta(x) &= 1 + \frac{1}{2^x} + \frac{1}{3^x} + \frac{1}{4^x} + \frac{1}{5^x} + \frac{1}{6^x} + \frac{1}{7^x} + \frac{1}{8^x} + \cdots \\ &= \Big(1 - \frac{1}{2^x}\Big)^{-1} \cdot \Big(1 - \frac{1}{3^x}\Big)^{-1} \cdot \Big(1 - \frac{1}{5^x}\Big)^{-1} \cdot \Big(1 - \frac{1}{7^x}\Big)^{-1} \cdots \end{aligned}$$

dove il prodotto è fatto su tutti i numeri primi.

In particolare,

$$\lim_{x \to 1+} \zeta(x) = +\infty$$

e quindi esistono infiniti numeri primi! Questo perché per $x = 1$ la funzione zeta "corrisponde" alla serie armonica, che sappiamo divergere.

La funzione ζ è stata studiata in casi particolari fin dal XVII secolo, ma ha preso il nome di Riemann da quando quest'ultimo ha pubblicato un articolo rivoluzionario nel 1859 nel quale sono descritte le proprietà piú importanti. Al proposito della funzione ζ, nel 1644 Pietro Mengoli chiese quanto vale $\zeta(2)$, cioè un'espressione esplicita per il suo valore. Il calcolo esatto, oggi, può essere considerato un esercizio sulle serie di Fourier, alla portata di studenti universitari del secondo anno. La risposta, piuttosto sorprendente, è $\zeta(2) = \pi^2/6$.

4.3 Teorema di Eulero: versione quantitativa

Utilizzando la serie geometrica, la serie armonica e il "limite notevole" per il logaritmo, è possibile dimostrare una versione piú forte del Teorema di Eulero

$$\sum_{p \leq n} \frac{1}{p} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \cdots + \frac{1}{p^*} \sim \log(\log(n)) \qquad \text{quando } n \to +\infty,$$

dove p^* indica il massimo numero primo che non supera n. Questo fatto suggerisce, senza dimostrare, che $\pi(n)$ sia dell'ordine di grandezza di $n/\log(n)$.

5 Il Teorema dei Numeri Primi

5.1 La Congettura di Gauss–Legendre

L'esame delle prime righe della nostra Figura 1 ha condotto Legendre e, indipendentemente, Gauss a congetturare un possibile andamento di $\pi(n)$ per n grande. Probabilmente Legendre aveva a disposizione solo il valore di $\pi(400\,000)$, mentre Gauss aveva calcolato anche altri dati.

Abbiamo dimostrato che, per n grande, si ha

$$\frac{n\log(2)}{\log(n)} \leq \pi(n) \leq \frac{2n\log(2)}{\log(n)}.$$

Questo ci dà l'*ordine di grandezza* della funzione $\pi(n)$: Gauss e Legendre hanno immaginato che fosse vero un risultato piú preciso.

Congettura 1 (Gauss–Legendre)**.**

$$\pi(n) \sim \frac{n}{\log(n)} \qquad \textit{quando } n \to +\infty.$$

È necessario ricordare che Gauss ha dato una versione piú precisa di questa congettura dal punto di vista numerico, ma per poterla enunciare nella forma originale dovremmo introdurre il calcolo integrale e una funzione trascendente "di ordine superiore." Per questo motivo, ne enunciamo una variante che non richiede ulteriori strumenti, al costo di una nuova definizione, dovuta al matematico russo P. Chebyshev. Poniamo

$$\begin{aligned}\theta(n) &= \sum_{p\leq n} \log(p) = \log(2)+\log(3)+\log(5)+\cdots+\log(p^*)\\ &= \log\bigl(2\cdot 3\cdot 5\cdots p^*\bigr),\end{aligned}$$

dove p^* indica il massimo numero primo che non supera n.

Congettura 2 (Variante della Congettura di Gauss–Legendre)**.**

$$\theta(n) \sim n \qquad \textit{quando } n \to +\infty.$$

La funzione θ, per quanto un po' piú artificiosa della funzione π, è piuttosto naturale, dato che è il logaritmo del prodotto dei numeri primi che non superano n. Per esempio, per $n = 100$ il prodotto dei numeri primi che non superano n ha 37 cifre decimali, mentre per $N = 1000$ ha 416 cifre decimali. Si usa il logaritmo naturale del prodotto dei numeri primi fino ad un certo valore per evitare di dover prendere in considerazione numeri troppo grandi: in questo modo troviamo $\theta(100) \approx 83.7$ e $\theta(1000) \approx 956.2$. Nella Figura 4 vediamo i valori di $\theta(x)$ per $x \in [0,20]$; in particolare, $\theta(20) = \log(2\cdot 3\cdot 5\cdot 7\cdot 11\cdot 13\cdot 17\cdot 19) = \log(9699690) \approx 16.088$.

Diamo due versioni equivalenti del Teorema dei Numeri Primi; in sostanza si tratta della conferma che Gauss e Legendre avevano visto giusto, sulla base, ricordiamolo, di dati del tutto insufficienti.

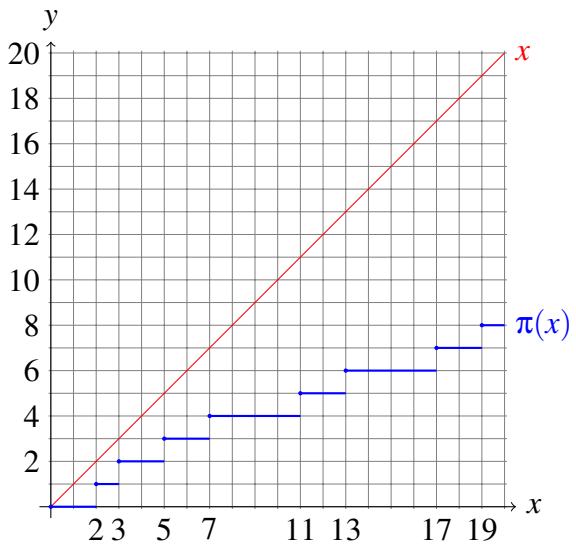

Figura 3: Il grafico della funzione $\pi(x)$ per $x \in [0,20]$.

Teorema 4 (Hadamard, de la Vallée Poussin (1896))**.**

$$\pi(n) \sim \frac{n}{\log(n)} \qquad \textit{e anche} \qquad \theta(n) \sim n.$$

È necessaria qualche parola di spiegazione: chiamiamo *scarto* il valore assoluto della differenza fra n e il logaritmo naturale del prodotto dei numeri primi che non superano n, cioè $|n - \theta(n)|$; nel primo esempio lo scarto vale circa 16.3 e nel secondo circa 43.8. Il Teorema dei Numeri Primi, nella seconda versione data qui sopra, afferma che, se n è sufficientemente grande, lo scarto risulta minore di $n/100$; se n è sufficientemente grande, lo scarto è minore di $n/1000$, e cosí via. Se introduciamo lo *scarto relativo*, e cioè lo scarto diviso per n, possiamo dire che, a patto di prendere n sufficientemente grande, lo scarto relativo è piú piccolo di qualunque numero positivo fissato a priori, cioè che lo scarto relativo tende a 0 quando n tende ad infinito. In realtà, grazie ai risultati trovati nel corso del XX secolo e quindi posteriori a Riemann, oggi è noto un risultato piú preciso, ma anche piú difficile da enunciare. Nelle applicazioni è essenziale avere una misura precisa dell'approssimazione, cioè della velocità con cui lo scarto relativo tende a 0 quando n tende ad infinito.

Le due versione del Teorema dei Numeri Primi date sopra sono equivalenti: per dimostrarlo, è necessario utilizzare una formula che è, in un certo senso, l'equivalente discreto della formula di integrazione per parti. La dimostrazione del Teorema dei Numeri Primi è stata data seguendo in dettaglio le idee nell'articolo di Riemann del 1859.

6 La Congettura di Riemann

L'enunciato del Teorema dei Numeri Primi dato qui sopra non è molto esplicito su un punto molto importante, e cioè quanto velocemente le frazioni $\pi(n)\log(n)/n$ e $\theta(n)/n$ tendono al loro limite 1. In molte applicazioni è cruciale avere questa informazione, se possibile in senso quantitativo forte. Qui discutiamo solo un caso, che è quello "ottimale."

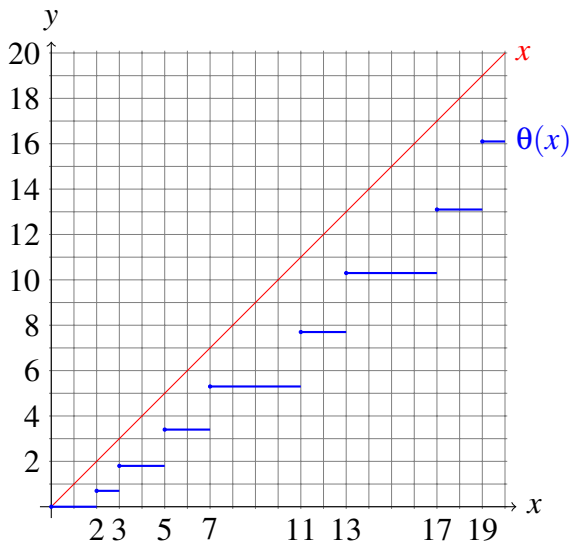

Figura 4: Il grafico della funzione $\theta(x)$ per $x \in [0,20]$.

Congettura 3 (Riemann)**.** *Per ogni numero intero $n \geq 2$ si ha*

$$\left|\theta(n) - n\right| \leq 100\sqrt{n}\log^2(n).$$

La costante 100 qui sopra non ha un significato particolare. Per esempio

$$\theta(500\,000) \approx 499\,318.12.$$

Dunque la differenza vale ≈ 681.88. Per gli interi $n \leq 500\,000$ la massima differenza si ha per $n_0 = 463\,180$, per cui

$$\theta(463\,180) \approx 461\,975.38.$$

La differenza vale $\approx 1\,204.62$ e il rapporto

$$\frac{\left|\theta(n_0) - n_0\right|}{\sqrt{n_0}\log^2(n_0)} \approx 0.0104.$$

7 Problemi aperti

7.1 La forma ottimale del Teorema dei Numeri Primi

Oggi è noto che

$$|\theta(n) - n| \leq 100\frac{n}{\exp\left(\sqrt{\log(n)}\right)},$$

per tutti gli interi n da un certo punto in poi. La Congettura di Riemann afferma che

$$|\theta(n) - n| \leq 100\sqrt{n}\log^2(n).$$

Questa ultima stima è molto piú precisa di quella data qui sopra. Il matematico britannico John E. Littlewood ha dimostrato nel 1914 che (approssimativamente)

$$|\theta(n) - n| \geq \sqrt{n}$$

per infiniti interi n. Questo significa che la stima data dalla Congettura di Riemann è quasi "ottimale," cioè non può essere migliorata di molto. Accenniamo ad un problema connesso: qual è la massima distanza possibile tra numeri primi consecutivi?

7.2 I problemi di Landau (International Congress of Mathematicians; Cambridge, 1912)

1. Problema binario di Goldbach: se $n \geq 6$ è pari, allora esistono due numeri primi dispari p_1 e p_2 tali che $n = p_1 + p_2$ (parzialmente risolto: Helfgott 2013, problema ternario).

2. Primi gemelli: esistono infiniti numeri primi p per cui $p+2$ è primo (parzialmente risolto: Zhang, Maynard 2013).

3. Esistono infiniti numeri primi p per cui $p+2$ e $p+6$ sono simultaneamente primi (piú in generale, k-uple *ammissibili*).

4. Primi tra quadrati consecutivi: per $n \geq 2$, esiste un numero primo fra n^2 ed $(n+1)^2$ (quasi risolto se è vera la Congettura di Riemann).

5. Il polinomio n^2+1 assume valore primo per infiniti interi n ($n = 1$, 2, 4, 6, 10, 14, 16, 20, 26, ... ?).

8 Applicazioni dei numeri primi: la Crittografia

Nella trattazione precedente abbiamo parlato dei numeri primi, della loro distribuzione e dei relativi problemi aperti senza preoccuparci della loro utilità pratica. Negli ultimi decenni, i numeri primi si sono rivelati utilissimi ad un particolare scopo, quello di proteggere informazioni riservate. Per motivi di spazio, ci limitiamo ad elencare alcuni problemi legati ai numeri primi e pertinenti alla Crittografia: per i dettagli rimandiamo a trattazioni specializzate.

1. Riconoscere i numeri primi. Piccolo Teorema di Fermat, Miller-Rabin, AKS (Agrawal, Kayal, Saxena).

2. Determinare numeri primi grandi.

3. Crittografia a chiave pubblica (RSA, ElGamal, ...).

4. Protocolli crittografici: PEC, denaro elettronico, ...

5. Generazione di sequenze pseudo-casuali per le simulazioni.

A Appendice con elementi di base

In questa Appendice raccogliamo alcuni elementi utili a capire il testo, senza pretesa di completezza.

A.1 La serie geometrica

Ricordiamo, senza dimostrazione, un fatto elementare ma importantissimo, che è alla base della "regola" per trasformare numeri decimali periodici in frazioni con numeratore e denominatore interi. Se $q \in (-1,1)$ allora

$$1+q+q^2+q^3+q^4+\cdots = \frac{1}{1-q}.$$

Per esempio, per $q = 1/10$ abbiamo

$$\begin{aligned} 1.11111\ldots &= 1+\frac{1}{10}+\frac{1}{100}+\frac{1}{1\,000}+\frac{1}{10\,000}+\frac{1}{100\,000}+\ldots \\ &= \frac{1}{1-1/10} = \frac{10}{9}. \end{aligned}$$

A.2 I coefficienti binomiali

Ricordiamo che i numeri

$$\binom{m}{k} = \frac{m!}{k!(m-k)!} \qquad \text{per } k = 0,\, 1,\, \ldots,\, m$$

sono interi positivi. Ci interessa in particolare il coefficiente binomiale "centrale" per il quale valgono le disuguaglianze

$$\frac{2^{2n}}{2n+1} \leq \binom{2n}{n} \leq 2^{2n}$$

La seconda dipende dal fatto che la somma di tutti gli elementi sulla $2n$-esima riga del Triangolo di Tartaglia vale 2^{2n}. La prima dipende dal fatto che sulla stessa riga ci sono $2n+1$ elementi di cui quello centrale è il massimo.

A.3 Le funzioni esponenziale e logaritmo

Si veda la Figura 5. Il fatto che la retta tangente al grafico della funzione $y = \log(x)$ nel punto di coordinate $(1,0)$ è la retta di equazione $y = x-1$ è equivalente al "limite notevole"

$$\lim_{t\to 0} \frac{\log(1+t)}{t} = 1.$$

A.4 La formula di Stirling

Per N grande si ha

$$\log(N!) = \log(1)+\log(2)+\log(3)+\cdots+\log(N) \sim N\log(N)-N.$$

Questo perché $\log(N!)$ è l'area della regione colorata nella Figura 6, che vale sostanzialmente

$$\int_1^N \log(t)\,\mathrm{d}t = N\log(N)-N+1.$$

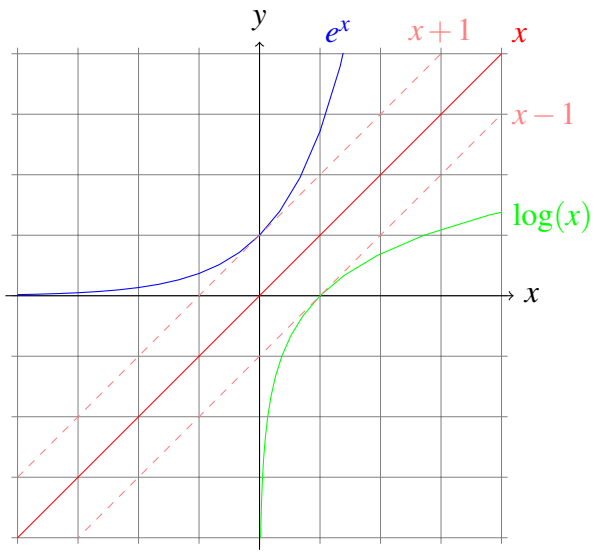

Figura 5: Il grafico della funzione e^x e della sua inversa $\log(x)$.

A.5 La serie armonica

Per N grande si ha

$$1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{N}\sim\log(N)$$

Analogamente a quanto detto sopra, la somma a sinistra è l'area della regione colorata nella Figura 7, che vale sostanzialmente

$$\int_1^N\frac{\mathrm{d}t}{t}=\log(N).$$

Diamo una dimostrazione elementare, cioè senza usare il calcolo integrale, del fatto qualitativo interessante, che la serie armonica diverge. Consideriamo la somma dei suoi primi 16 addendi, che raggruppiamo opportunamente per poterne dare una semplice stima dal basso. Ciascun termine racchiuso in parentesi vale almeno quanto il minimo addendo moltiplicato per il numero degli addendi. Dunque

$$\begin{aligned}&1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{5}+\frac{1}{6}+\frac{1}{7}+\frac{1}{8}+\frac{1}{9}+\frac{1}{10}+\frac{1}{11}+\frac{1}{12}+\frac{1}{13}+\frac{1}{14}+\frac{1}{15}+\frac{1}{16}\\ =&1+\frac{1}{2}+\left(\frac{1}{3}+\frac{1}{4}\right)+\left(\frac{1}{5}+\frac{1}{6}+\frac{1}{7}+\frac{1}{8}\right)\\ &+\left(\frac{1}{9}+\frac{1}{10}+\frac{1}{11}+\frac{1}{12}+\frac{1}{13}+\frac{1}{14}+\frac{1}{15}+\frac{1}{16}\right)\\ \geq&1+\frac{1}{2}+\frac{1}{2}+\frac{1}{2}+\frac{1}{2}=1+\frac{1}{2}\log_2(16)\end{aligned}$$

In generale

$$1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\cdots+\frac{1}{2^k}\geq 1+\frac{1}{2}\cdot k,$$

che può essere reso arbitrariamente grande. Il risultato ottenuto mediante il calcolo integrale è piú preciso ma meno elementare.

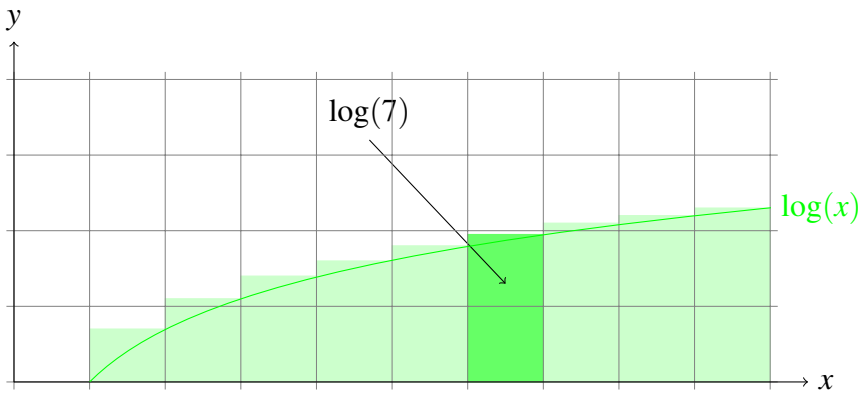

Figura 6: L'area colorata in figura è approssimativamente uguale all'area compresa fra l'asse delle ascisse e il grafico della funzione $\log(x)$ nell'intervallo $[1,10]$.

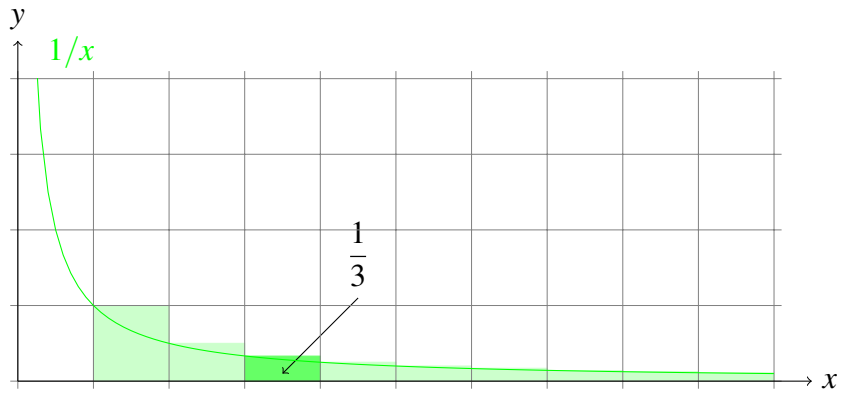

Figura 7: L'area colorata in figura è approssimativamente uguale all'area compresa fra l'asse delle ascisse e il grafico della funzione $1/x$ nell'intervallo $[1,10]$.

B Bibliografia essenziale

La bibliografia su questi argomenti, specie in lingua inglese, è sterminata e non tutta di livello accettabile, perché spesso libri e articoli divulgativi semplificano eccessivamente la materia e in definitiva la tradiscono. Indichiamo una decina di testi in italiano facilmente reperibili e di vari livelli che possono utilmente integrare quanto detto qui.

1. Esistenza di infiniti numeri primi: [5], [6].
2. Crivello di Eratostene–Legendre e sua forma quantitativa: [7].
3. Congettura di Riemann: [9].
4. Congettura di Goldbach: [2].
5. Congettura dei primi gemelli: [4].
6. Curiosità sui numeri primi: [3], [8].

7. Algoritmi sui numeri primi, crittografia, protocolli: [1].

8. Approfondimenti (per i quali sono necessarie conoscenze avanzate): [5], [6].

Riferimenti bibliografici

[1] A. Languasco & A. Zaccagnini, *Manuale di crittografia*, Ulrico Hoepli Editore, Milano, 2015.

[2] A. Zaccagnini, *Variazioni Goldbach: problemi con numeri primi*, L'Educazione Matematica, Anno XXI, Serie VI **2** (2000), 47–57, http://people.math.unipr.it/alessandro.zaccagnini/psfiles/papers/Goldbach_I.pdf.

[3] ———, *L'importanza di essere primo*, Ricordando Franco Conti (a cura di A. Abbondandolo, M. Giaquinta, F. Ricci), Scuola Normale Superiore, Pisa, 2004, http://people.math.unipr.it/alessandro.zaccagnini/psfiles/papers/importanza.pdf, pp. 343–354.

[4] ———, *Il cerchio si stringe intorno ai primi "gemelli"*, Sito web MaddMaths! (2013), http://maddmaths.simai.eu/divulgazione/il-cerchio-si-stringe-intorno-ai-primi-gemelli/.

[5] ———, *Breve storia dei numeri primi*, Ithaca: Viaggio nella Scienza **III** (2014), 67–83, http://ithaca.unisalento.it/nr-03_04_14/index.html.

[6] ———, *Introduzione alla Teoria Analitica dei Numeri*, 2015, Dispense del Corso di *Teoria dei Numeri*, A. A. 2014–2015. Disponibili all'indirizzo http://people.math.unipr.it/alessandro.zaccagnini/psfiles/lezioni/tdn2015.pdf.

[7] ———, *Macchine che producono numeri primi*, Matematica, Cultura e Società **1** (2016), no. 1, 5–19.

[8] ———, *Un giorno alle corse (dei numeri primi)*, Sito web MaddMaths! (2016), http://maddmaths.simai.eu/divulgazione/focus/un-giorno-alle-corse-dei-numeri-primi/.

[9] ———, *Una versione elementare della Congettura di Riemann*, Sito web MaddMaths! (2016), http://maddmaths.simai.eu/divulgazione/una-versione-elementare-della-congettura-di-riemann/.

Prof. Alessandro Zaccagnini
Dipartimento di Matematica e Informatica
Università degli Studi di Parma
Parco Area delle Scienze, 53/a
43124 Parma, ITALIA
Tel. 0521 906902 – Telefax 0521 906950
e-mail: alessandro.zaccagnini@unipr.it
pagina web: http://people.math.unipr.it/alessandro.zaccagnini/