ALMA MATER STUDIORUM · UNIVERSITÀ DI BOLOGNA

Scuola di Scienze
Corso di Laurea in Matematica

Il Teorema dei Numeri Primi

Tesi di Laurea in Teoria dei Numeri

Relatore:
Chiar.mo Prof.
Fabrizio Caselli

Presentata da:
Davide Mauro Ferrario

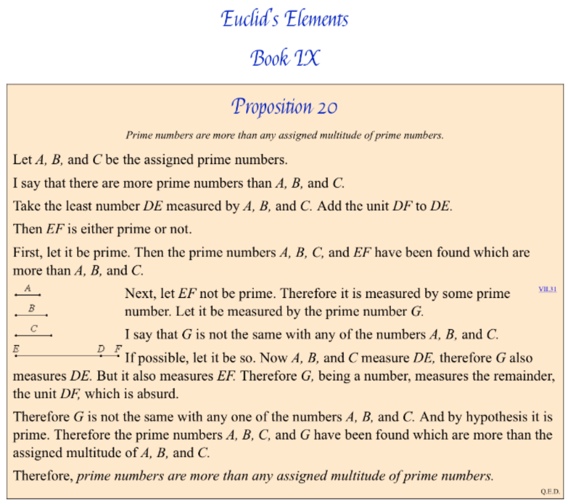
II Sessione
Anno Accademico 2013-2014

Indice

Introduzione

Introduzione

Un numero primo p è un intero, maggiore strettamente di 1, i cui divisori sono solo 1 e p. Si sa che la successione dei numeri primi è infinita già dai tempi di Euclide (III sec. a.C.). La dimostrazione è semplice: supponiamo per assurdo che il numero di primi sia finito e che $p_1 = 2 < \cdots < p_r$ siano tutti i primi; si consideri l'intero $P = p_1 p_2 \cdots p_r + 1$ e sia p un primo che divide P, allora p non può essere nessuno dei $p_1, \cdots, p_r$ altrimenti dividerebbe la differenza $P - p_1 p_2 \cdots p_r = 1$, che è impossibile.



Euclid's Elements

Book IX

Proposition 20

Prime numbers are more than any assigned multitude of prime numbers.

Let *A, B,* and *C* be the assigned prime numbers.

I say that there are more prime numbers than *A, B,* and *C.*

Take the least number *DE* measured by *A, B,* and *C.* Add the unit *DF* to *DE.*

Then *EF* is either prime or not.

First, let it be prime. Then the prime numbers *A, B, C,* and *EF* have been found which are more than *A, B,* and *C.*

Next, let *EF* not be prime. Therefore it is measured by some prime number. Let it be measured by the prime number *G.* VII.31

I say that *G* is not the same with any of the numbers *A, B,* and *C.*

If possible, let it be so. Now *A, B,* and *C* measure *DE,* therefore *G* also measures *DE.* But it also measures *EF.* Therefore *G,* being a number, measures the remainder, the unit *DF,* which is absurd.

Therefore *G* is not the same with any one of the numbers *A, B,* and *C.* And by hypothesis it is prime. Therefore the prime numbers *A, B, C,* and *G* have been found which are more than the assigned multitude of *A, B,* and *C.*

Therefore, *prime numbers are more than any assigned multitude of prime numbers.*

Q.E.D.

La dimostrazione originale di Euclide era piuttosto diversa: infatti per gli antichi greci i numeri non erano oggetti astratti, ma venivano rappresentati come lunghezze di segmenti (multipli di un segmento unità) e invece di divisibilità si parlava di misura, cioè una lunghezza a misurava un'altra lunghezza b, se con un numero intero di segmenti di lunghezza a si poteva ottenere un segmento di lunghezza uguale a b. Inoltre il concetto attuale di infinito non esisteva: Euclide scrisse che i numeri primi sono più di una qualsiasi moltitudine assegnata. [8]

Ci si può chiedere come sono distribuiti i numeri primi tra gli interi, in particolare quanti primi ci sono nell'intervallo $[1, x]$. Si definisce, per $x \geq 0$, la funzione $\pi(x)$ come

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

Come conseguenza del teorema di Euclide si ha che $\lim_{x \to \infty} \pi(x) = \infty$ e nei secoli successivi i matematici hanno cercato di trovare l'ordine di grandezza con cui questa funzione tende all'infinito inizialmente cercando di trovare una regola per trovare le posizioni dei primi, poi la loro distribuzione media, con l'aiuto di tavole dove erano riportati tutti i numeri primi trovati.

Queste tavole furono costruite inizialmente utilizzando il crivello di Eratostene (II sec a.C.) un procedimento con cui si riescono a trovare a tutti numeri primi minori di un fissato n. Consiste nello scrivere tutti i numeri naturali fino ad n in un elenco, poi nel cancellare tutti i multipli dei numeri primi minori o uguali di $\sqrt{n}$; ciò che resta sono i numeri primi minori di n. [9]
Fu Eulero [1737] il primo ad ottenere un risultato interessante dopo Euclide. Combinando il suo metodo per generare funzioni con un altro risultato di teoria dei numeri già conosciuto dai greci, l'unicità della fattorizzazione in primi di un intero, riuscì a dimostrare che la somma dei reciproci dei numeri primi $\sum_p \dfrac{1}{p}$ diverge. [4]
Nel 1798 Legendre nel suo libro *Essai sur la Théorie der Nombres* afferma che $\pi(x) = \frac{x}{\log(x)+A(x)}$ per $x \to \infty$, introducendo sulla base delle sue osservazioni limitate una costante ad hoc, detta di Legendre tale che $\lim_{x\to\infty} A(x) = B = 1.08366$. Già nel 1792 Gauss a soli 15 anni studiando le tavole dei numeri primi propone che

$$\pi(x) \sim \frac{x}{\log x} \tag{1}$$

poi perfeziona la sua stima con

$$\pi(x) = Li(x), \tag{2}$$

dove

$$Li(x) = \int_2^x \frac{dt}{\log t} \tag{3}$$

è il logaritmo integrale. Gauss non pubblica questi risultati, che vengono menzionati per la prima volta in una lettera ad Encke nel 1849, pubblicata postuma nel 1863.
Si ha:

$$Li(x) \sim \sum_{k=0}^{n} \frac{k!x}{(\log x)^{k+1}} + O_n\left(\frac{x}{\log(x)^{n+1}}\right) \tag{4}$$

$$= \frac{x}{\log x} + \frac{x}{(\log x)^2} + \frac{2x}{(\log x)^3} + \ldots + \frac{n!x}{(\log x)^{n+1}} + O_n\left(\frac{x}{\log(x)^{n+1}}\right)$$

e si è visto che i primi tre termini sono una migliore stima di $\pi(x)$ che $\dfrac{x}{\log x}$ solamente.

n	$\pi(n)$	$\dfrac{n}{\log n - 1.08366}$	$\dfrac{n}{\log n}$	$Li(n)$
1000	168	172	145	178
10000	1229	1231	1086	1246
100000	9592	9588	8686	9630
1000000	78498	78534	72382	78628
10000000	664579	665138	620420	664918
100000000	5761455	5769341	5428681	5762209

(5)

Studiando il rapporto tra queste due funzioni si era notato che per n piccoli $\pi(n) < Li(n)$. Matematici come Gauss e Riemann avevano ipotizzato che questa disuguaglianza fosse sempre vera, ma nel 1914 questa congettura fu rifiutata da Littlewood. Egli provò che per n sufficientemente grande la differenza $\pi(n) - Li(n)$ cambia segno infinite volte. Fu Skewes a mostrare che il cambiamento di segno avviene prima di $10^{10^{10^{34}}}$, noto come numero di Skewes, poi ridotto a 10^{371}. Nel 1966 infine Lehman provò che ci sono almeno 10^{500} inversioni per numeri con 1166 o 1167 cifre [12].

L'andamento delle funzioni $\pi(x)$, $Li(x)$, $\frac{x}{log(x)}$ è rappresentato graficamente in Figura 1 e in Figura 2, generate con lo script python riportato in appendice.

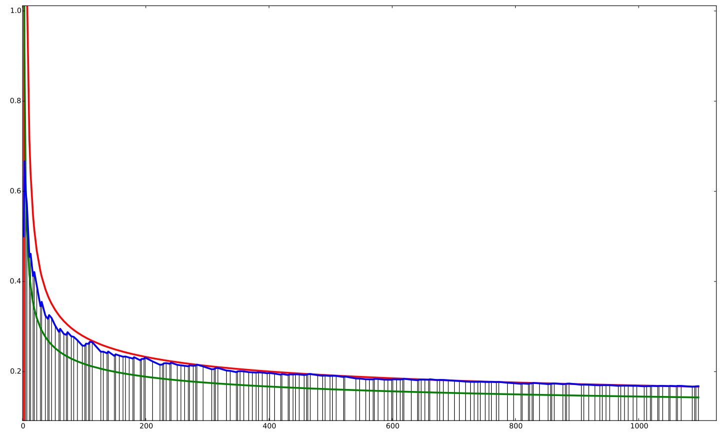


Figura 1. blu: $\frac{\pi(x)}{x}$ rosso: $\frac{1}{\log x - 1}$ verde: $\frac{1}{\log x}$

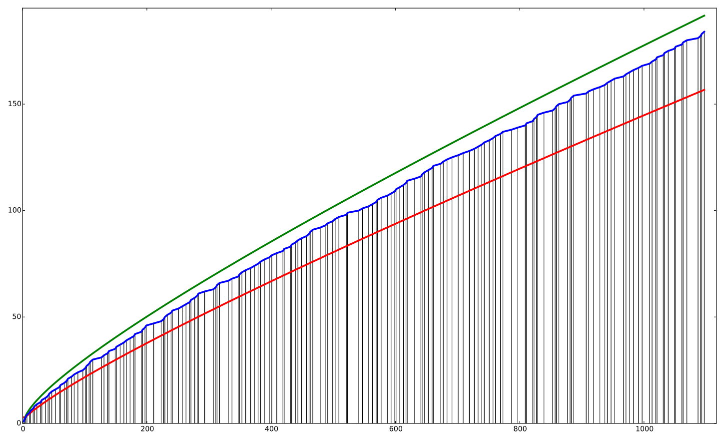


Figura 2. blu: $\pi(x)$ rosso: $\frac{x}{\log x}$ verde: $Li(x)$

Questo risultato $\pi(n) \sim Li(n)$, o nella sua forma più semplice $\pi(n) \sim \frac{\log(n)}{n}$, si chiama Teorema dei Numeri Primi ed è stato provato per la prima volta indipendentemente da Hadamard e de la Vallée Poussin nel 1896 utilizzando la funzione Zeta di Riemann, dopo più di cento anni di tentativi da parte di numerosi matematici ed ha fornito l'incentivo per lo sviluppo della teoria delle funzioni complesse.[2]
Un importante risultato nello studio di $\pi(x)$ è ottenuto da Tchebychev: nel 1849 mostra che se esiste $\lim_{x\to\infty} \pi(x)log(x)/x$, allora il suo valore deve essere 1, ma non riesce a provare che questo limite esiste. Stima però l'ordine di grandezza di $\pi(x)$ provando che esistono due numeri reali positivi A e B tali che per ogni $x \geq 2$ si ha

$$\frac{Ax}{\log(x)} < \pi(x) < \frac{Bx}{\log(x)}.$$

La prova pubblicata nel 1852 nelle sue *Mémoire sur les nombres premiers* si basa su una serie di incastri e sfrutta le seguenti funzioni:

$$\theta(x) := \sum_{p\leq x} \log(p), \quad \psi(x) := \sum_{p^\nu \leq x} \log(p), \quad T(x) := \sum_{n\leq x} \psi(x/n).$$

I teoremi di Tchebychev hanno rappresentato un notevole passo avanti ed erano motivati dal suo desiderio di provare il Postulato di Bertrand(1845), che afferma che per tutti gli interi $n \geq 2$ c'è almeno un primo nell'intervallo $[n,2n]$. La prova di questo postulato è data da Tchebychev nel 1850 e si basa sul trovare valori espliciti per A e B; nella prova originale si mostra che per ogni $x > 30$ si possono prendere

$$A = \log \frac{2^{1/2}3^{1/3}4^{1/4}}{30^{1/30}} = 0.921... \quad e \quad B = \frac{6}{5}A = 1.105...$$

Nel 1949 Paul Erdös e Atle Selberg(1917) pubblicano una dimostrazione "elementare" del teorema, cioè una dimostrazione che non usa né la funzione ζ di Riemann, né, più in generale, altre funzioni di variabile complessa. Questa dimostrazione è stata sorprendente perché si riteneva che fosse impossibile fornire una dimostrazione di questo tipo per il Teorema dei Numeri Primi: infatti fino a quel momento era abitudine dividere i teoremi sui numeri primi in due classi:

(a) *teoremi elementari* che potevano essere provati con manipolazioni algebriche e analisi di funzioni a variabile reale,

(b) *teoremi trascendenti* che si possono provare solo con metodi in variabile complessa.

Guardando l'uguaglianza formale, dove $\mu(n)$ è la funzione di Möbius che vedremo più avanti,

$$\prod_p \left(1 - \frac{1}{p}\right) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n}$$

si era notato che dal termine sinistro si poteva ricavare un teorema elementare (utilizzando i prodotti di Eulero si può scrivere il suo inverso come la serie $\sum_1^\infty \frac{1}{n}$ che diverge), mentre provare che il termine destro converge a zero per n che tende all'infinito é un teorema trascendente, equivalente al Teorema dei Numeri Primi. Questo aveva portato ad elaborare una nozione di equivalenza o profondità tra teoremi trascendenti: due teoremi erano equivalenti se potevano essere ricavati l'uno dall'altro con metodi elementari. Ad esempio Landau aveva dimostrato che il Teorema dei numeri Primi era "equivalente" a:

$$M(x) = \sum_{n \leq x} \mu(n) = o(x) \quad per \quad x \to \infty$$

ed anche a:

$$\sum_{n=1}^{\infty} \frac{\mu(n)}{n} = 0.$$

Poiché i teoremi trascendenti avevano una tendenza a diventare elementari con il passare del tempo non si era mai arrivati ad avere una classificazione fissa e, quando nel 1949 anche il Teorema dei Numeri Primi è diventato elementare, questa classificazione non ha più avuto senso. [5]

Eulero

Analizziamo un po' meglio i risultati e le tecniche ottenute da Eulero: inizialmente aveva fornito un'altra dimostrazione dell'infinità dei numeri primi utilizzando la serie armonica (divergente):

$$S = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} + \cdots .$$

Si può scrivere questa serie come prodotto delle serie geometriche S_p per ogni primo p.

$$S_2 = 1 + \frac{1}{2} + \frac{1}{2^2} + \cdots + \frac{1}{2^n} + \cdots = 2$$

$$S_3 = 1 + \frac{1}{3} + \frac{1}{3^2} + \cdots + \frac{1}{3^n} + \cdots = \frac{3}{2}$$

$$S_5 = 1 + \frac{1}{5} + \frac{1}{5^2} + \cdots + \frac{1}{5^n} + \cdots = \frac{5}{4}$$

Per il teorema fondamentale dell'aritmetica secondo cui ogni numero naturale si può scrivere come prodotto di primi, allora ogni termine di S si può vedere come prodotto di termini delle S_p. Poiché le S_p sono tutte finite, allora se i numeri primi fossero finiti anche la serie armonica sarebbe convergente.

A questo punto aveva studiato l'identità (che noi sappiamo valere solo per valori di s tali che la serie converge assolutamente)

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \frac{1}{1 - p^{-s}}$$

Poiché possiamo esprimere ogni intero in maniera unica come $n = \prod_p p^{c_p}$ con ogni c_p intero non negativo, nullo a meno di un numero finito di primi, allora l'espansione formale del prodotto infinito

$$\prod_p \left(\sum_{c_p=0}^{\infty} p^{-c_p s} \right)$$

contiene ogni termine

$$n^{-s} = \left(\prod_p p^{c_p} \right)^{-s} = \prod_p p^{-c_p s} \tag{6}$$

esattamente una volta sola. Se la somma degli n^{-s} converge assolutamente, possiamo riordinare i termini arbitrariamente e concludere che equivale al prodotto 6. D'altra parte ogni fattore di questo prodotto è una serie geometrica la cui somma è uguale a $1/(1 - p^s)$.
Eulero non aveva imposto la condizione di convergenza delle serie, poiché in quel tempo limiti e convergenza non erano ancora trattati in maniera rigorosa, ma aveva considerato il caso $s = 1$ (oggi dovremmo guardare il limite per $s \to 1^+$) e aveva preso i logaritmi dei termini visti sopra per dedurre un andamento asintotico della somma dei reciproci dei primi minori di n. Infatti

$$\log\left(\sum_{n=1}^{\infty} \frac{1}{n} \right) = \log\left(\prod_p \frac{1}{1 - p^{-1}} \right) = \log\left(\prod_p \left(1 - \frac{1}{p}\right) \right) = -\sum_p \log\left(1 - \frac{1}{p}\right)$$

Sviluppando in serie di Taylor

$$\begin{aligned}
&= \sum_p \left(\frac{1}{p} + \frac{1}{2p^2} + \frac{1}{3p^3} + \cdots \right) \\
&= \left(\sum_p \frac{1}{p} \right) + \sum_p \frac{1}{p^2} \left(\frac{1}{2} + \frac{1}{3p} + \frac{1}{4p^2} + \cdots \right) \\
&< \left(\sum_p \frac{1}{p} \right) + \sum \frac{1}{p^2} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \cdots \right) \\
&= \left(\sum_p \frac{1}{p} \right) + \sum \frac{1}{p(p-1)} \\
&= \left(\sum_p \frac{1}{p} \right) + C \qquad \text{con C costante<1}
\end{aligned}$$

Poiché la somma dei primi n interi positivi è asintoticamente equivalente a $\log(n)$ Eulero concluse intuitivamente che

$$\sum_{p \leq n} \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \cdots \sim \log(\log(n))$$

Capitolo 1

Risultati preliminari

1.1 Funzioni aritmetiche

Definizione 1. Una funzione aritmetica è un'applicazione $\mathbb{N}_+ \to \mathbb{C}$

Definizione 2. Una funzione aritmetica f si dice moltiplicativa se $f(1) = 1$ e se n ed m sono coprimi, $f(mn) = f(n)f(m)$. Si dice invece completamente moltiplicativa se $f(mn) = f(n)f(m)$ per ogni $n, m \in \mathbb{N}$

Osservazione 1. Se f è una funzione moltiplicativa possiamo scrivere che

$$f(n) = \prod_{p^\alpha || n} f(p^\alpha) \text{ (Il simbolo } p^\alpha || n \text{ significa che } p^\alpha | n \text{ e } p^{\alpha+1} \nmid n)$$

e ciò mostra che è determinata dai valori che assume sulle potenze dei primi.
Se è completamente moltiplicativa

$$f(n) = \prod_{p^\alpha || n} (f(p))^\alpha$$

cioé è determinata dai valori che assume sui primi.

Un esempio di funzione moltiplicativa è la φ di Eulero: $\varphi(n) = |\mathbb{Z}_n^*|$, cioé conta gli interi $m \leq n$ e m primi con n.
Sono esempi di funzioni completamente moltiplicative invece

Definizione 3. $\mathbb{1}(n) = 1$ per ogni $n \in \mathbb{N}_+$

Definizione 4. $\varepsilon(n) = \delta_{1,n}$

Sull'insieme delle funzioni aritmetiche $\mathcal{F}$ possiamo definire

1. $(f + g)(n) = f(n) + g(n)$;

2. $(fg)(n) = f(n)g(n)$;

3. $(f * g)(n) = \sum_{d|n} f(d)g(n/d) = \sum_{d_1 d_2 = n} f(d_1)g(d_2)$ detto convoluzione

Osservazione 2. La somma ed il prodotto di convoluzione definiscono una struttura di un anello commutativo su $\mathcal{F}$: la convoluzione è commutativa ed associativa, distributiva rispetto alla somma ed ammette la funzione $\varepsilon(n)$ come elemento neutro; inoltre una funzione $f \in \mathcal{F}$ è invertibile rispetto alla convoluzione $*$ se e solo se $f(1) \neq 0$.
In questo caso definendo $g = f^{-1}$ abbiamo che:

$$\begin{array}{ll} n = 1 & g(n) = 1/f(n) \\ n > 1 & g(n) = -\dfrac{\sum_{d|n, d>1} f(d)g(\frac{n}{d})}{f(1)} \end{array}$$

Funzione di Möbius

Un'importante funzione moltiplicativa è la funzione di Möbius, definita come l'inversa della funzione costante $\mathbb{1}(n)$ rispetto alla convoluzione

$$\mu * \mathbb{1}(n) = \varepsilon(n) \tag{1.1}$$

esplicitamente può essere descritta così:

Osservazione 3. Sia $n \in \mathbb{N}_+$ e sia

$$n = \prod_{i=1}^{r} p_i^{m_i}$$

la sua fattorizzazione in primi, con $p_i \neq p_j$ per $i \neq j$ e $m_i \geq 1$ per ogni i. Allora

$$\mu(n) = \begin{cases} 0 & \textit{se esiste i tale che } m_i \geq 2 \\ (-1)^r & \textit{altrimenti} \end{cases}$$

Osservazione 4. Le funzioni di Eulero e di Möbius sono legate da questa relazione

$$\varphi(n) = \mu * Id(n).$$

Funzione di Von Mangoldt

Si può pensare la funzione $\log(n)$ come una funzione aritmetica non moltiplicativa, e definire la funzione di Von Mangoldt come:

$$\Lambda(n) = \log * \mu(n) \tag{1.2}$$

Anche se non è moltiplicativa può essere calcolata facilmente conoscendo la fattorizzazione in numeri primi.

Osservazione 5. Si ha $\Lambda(1) = 0$ e se $n \geq 2$ abbiamo

$$\Lambda(n) = \begin{cases} \log(p) & se\ n\ \ potenza\ di\ un\ primo\ p \\ 0 & altrimenti \end{cases}$$

Ecco una tabella con i primi valori di $\mu(n)$ e $\Lambda(n)$

n	1	2	3	4	5	6	7	8	9	10	11
$\mu(n)$	$+1$	-1	-1	0	-1	1	-1	0	0	1	-1
$\Lambda(n)$	0	log(2)	log(3)	log(2)	log(5)	0	log(7)	log(2)	log(3)	0	log(11)

[3]

1.2 Identità di Eulero

Teorema 1. *Sia $f(n)$ una funzione moltiplicativa che soddisfa una delle condizioni seguenti:*

(i) $\sum_{n=1}^{\infty} |f(n)| < \infty$,

(ii) $\prod_p (1 + \sum_{v=1}^{\infty} |f(p^v)|) < \infty$.

Allora vale la seguente uguaglianza:

$$\sum_{n=1}^{\infty} f(n) = \prod_p (1 + f(p) + f(p^2) + \ldots).$$

Dimostrazione. Definiamo le quantità S^* e P^* come

$$S^* = \sum_{n=1}^{\infty} |f(n)| \quad e \quad P^* = \prod_p \sum_{v=1}^{\infty} |f(p^v)|.$$

Si ha $1 \leq S^* \leq \infty$ e $1 \leq P^* \leq \infty$.
Supponiamo che sia vera (i), cioè $S^* \leq \infty$. La serie $\sum f(n)$ è assolutamente convergente e sia S la sua somma. Per ogni primo p la serie $\sum_{v=0}^{\infty} |f(p^v)|$ è convergente perché maggiorata da S^*. Quindi per ogni primo p la serie $\sum_v f(p^v)$ è assolutamente convergente. Possiamo quindi definire i due prodotti

$$P(x) = \prod_{p \leq x} \sum_{v=0}^{\infty} f(p^v), \quad P^*(x) = \prod_{p \leq x} \sum_{v=0}^{\infty} |f(p^v)|$$

Per l'assoluta convergenza possiamo riscrivere la serie

$$P(x) = \sum{}' f(n) = S - \sum{}'' f(n)$$

dove $\sum'$ denota una sommatoria su tutti gli interi n che non hanno fattori primi maggiori di x e $\sum''$ una sommatoria estesa a tutti gli interi con almeno un fattore primo più grande di x.

$$|P(x) - S| \leq \sum{}'' |f(n)| \leq \sum_{n \geq x} |f(n)|.$$

Quindi si può concludere che $P(x)$ tende a S per $x \to \infty$ e ugualmente che $P^*(x)$ tende a S^*.
Se la condizione (ii) è soddisfatta $P^* < \infty$ e quindi

$$\sum_{n \leq x} |f(n)| \leq \sum' |f(n)| = P^*(x) \leq P^* < \infty,$$

da cui si conclude che $S^* < \infty$, cioè (i) è soddisfatta e segue la tesi. □

Teorema 2. *Sia $f(p)$ una funzione completamente moltiplicativa tale che per tutti i primi p*

$$|f(p)| < 1 \quad e \quad \sum_p |f(p)| < \infty.$$

Allora

$$\sum_{n=1}^{\infty} f(n) = \prod_p (1 - f(p))^{-1}.$$

Dimostrazione. Poiché $|f(p)| < 1$ e f è completamente moltiplicativa

$$\sum_{v=0}^{\infty} f(p^v) = \sum_{v=0}^{\infty} f(p)^v = (1 - f(p))^{-1}.$$

La convergenza della serie $\sum_p |f(p)|$ implica la convergenza delle seguenti serie e prodotti:

$$\prod_p (1 - |f(p)|), \quad \prod_p (1 - |f(p)|)^{-1}, \quad \prod_p \left(\sum_{v=0}^{\infty} |f(p^v)| \right).$$

Così è soddisfatta la (ii) del Teorema 1 e segue la tesi □

Teorema 3. *Se f(n) è una funzione moltiplicativa reale, non negativa, allora*

$$\sum_{n=1}^{\infty} f(n) = \prod_p \left(\sum_{v=0}^{\infty} f(p^v) \right)$$

è sempre vera se ammettiamo che entrambi i termini possano essere infiniti.

Dimostrazione. Se uno dei due numeri

$$\sum_{n=1}^{\infty} f(n) \quad o \quad \prod_p \left(\sum_{v=0}^{\infty} f(p^v) \right)$$

è finito il risultato è conseguenza del Teorema 1, se uno dei due è infinito, lo è anche l'altro. □

1.3 La funzione Zeta di Riemann

C'è una stretta connessione tra la distribuzione dei numeri primi ed il comportamento delle serie $\sum_{n=1}^{\infty} n^{-s} = \zeta(s)$.
Sia $s = \sigma + it$ un numero complesso che soddisfa $Re(s) > 1$. La serie

$$\sum_{n=1}^{\infty} n^{-s} \tag{1.3}$$

è assolutamente convergente, rappresentiamo la sua somma come $\zeta(s)$. La funzione così definita nel semipiano $Re(s) > 1$ è chiamata *funzione zeta di Riemann*. Utilizzando il Teorema 2 possiamo scrivere:

$$\zeta(s) = \prod_p \left(1 - p^{-s}\right)^{-1}. \tag{1.4}$$

Se poniamo $s = 1$ ed usiamo il Teorema 3, allora

$$\prod_p \left(1 - \frac{1}{p}\right)^{-1} = \infty$$

Così abbiamo provato il teorema di Eulero

Teorema 4. *Il prodotto $\prod_p (1 - p^{-1})$ e la serie $\sum_p p^{-1}$ divergono.*

L'equazione 1.4 è il punto di partenza per lo sviluppo della teoria dei numeri analitica.

1.4 Le funzioni θ e ψ

La funzione $\theta(x)$ è definita come:

$$\theta(x) = \sum_{p \le x} \log(p)$$

mentre la funzione $\psi(x)$ è:

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

Osservazione 6. Si può verificare che

$$\begin{aligned} \psi(x) &= \sum_{p^v \le x} \log(p) \\ &= \sum_{p \le x} \left\lfloor \frac{\log(x)}{\log(p)} \right\rfloor \log(p) \\ &= \theta(x) + \theta(x^{1/2}) + \theta(x^{1/3}) + \dots \end{aligned}$$

$\theta(x)$ conta i primi minori o uguali ad x con peso $\log(p)$, mentre $\psi(x)$ conta tutte le potenze di un primo p minori o uguali ad x, sempre con peso $\log(p)$ Per dimostrare il teorema dei numeri primi si preferisce studiare il comportamento di $\theta(x)$ e $\psi(x)$, infatti vale:

Teorema 5. *Se uno dei quozienti $q_1(x) = \frac{\theta(x)}{x}$, $q_2(x) = \frac{\psi(x)}{x}$ o $q_3(x) = \frac{\pi(x)\log(x)}{x}$ converge ad un limite reale per $x \to \infty$, allora gli altri quozienti convergono allo stesso limite.*

Dimostrazione.

$$\theta(x) = \sum_{p \le x} \log(p) \le \sum_{p \le x} \left\lfloor \frac{\log(x)}{\log(p)} \right\rfloor \log(p) = \psi(x) \le \sum_{p \le x} \frac{\log(x)}{\log(p)} \log(p) = \pi(x)\log(x).$$

Si deduce quindi che $q_1(x) \leq q_2(x) \leq q_3(x)$. Per $x > e$, sia $\sigma_x = \dfrac{x}{\log^2(x)} \in]1, x[$.

Allora $u(x) = \dfrac{\log(\sigma_x)}{\log(x)} = \dfrac{\log(x) - 2\log(\log(x))}{\log(x)} \xrightarrow{n\to\infty} 1$

e $\varepsilon(x) = \dfrac{\sigma_x \log(\sigma_x)}{x} = \dfrac{\log(x) - 2\log(\log(x))}{\log^2(x)} \xrightarrow{n\to\infty} 0$. Da cui

$$\theta(x) \geq \sum_{\sigma_x < p \leq x} \log(p) \geq \sum_{\sigma_x < p \leq x} \log(\sigma_x) = (\pi(x) - \pi(\sigma_x))\log(\sigma_x) \geq \pi(x)u(x)\log(x) - x\varepsilon(x).$$

Quest'ultima maggiorazione vale perché $\pi(\sigma_x) < \sigma_x$

Si deduce quindi che $q_1(x) \geq q_3(x)u(x) - \varepsilon(x)$, cioè $q_3(x) \leq \dfrac{q_1(x) + \varepsilon(x)}{u(x)}$.

E finalmente

$$q_1(x) \leq q_2(x) \leq q_3(x) \leq \frac{q_1(x) + \varepsilon(x)}{u(x)} \leq \frac{q_2(x) + \varepsilon(x)}{u(x)} \leq \frac{q_3(x) + \varepsilon(x)}{u(x)}$$

e (con $x > e$) per il Teorema dei due carabinieri abbiamo la tesi. $\square$

1.5 Lemma di Abel

Questo è un teorema molto utilizzato in Teoria dei Numeri che permette di sostituire una somma finita con un integrale, che spesso è molto più semplice da maneggiare.

Teorema 6. *Sia φ una applicazione complessa derivabile con continuità nell'intervallo $]1, \infty[$.*

1. *Se $(a_k)_{k\geq 1}$ è una successione di numeri complessi e se si pone per ogni x reale ≥ 1*

$$A(x) = \sum_{k \leq x} a_k. \tag{1.5}$$

   Allora

$$\sum_{k\leq x} a_k \varphi(k) = A(x)\varphi(x) - \int_1^x A(t)\varphi'(t)dt.$$

2. *In particolare*

$$\sum_{k\leq x} \varphi(k) = \lfloor x \rfloor \varphi(x) - \int_1^x \lfloor t \rfloor \varphi'(t)dt.$$

Dimostrazione. Si pone $n = \lfloor x \rfloor$ Allora $A(x) = A(n)$ in quanto sommatoria su interi $n \leq x$ e

$$\begin{aligned}
\textstyle\int_1^x A(t)\varphi'(t)dt &= \sum_{k=1}^{n-1} \int_k^{k+1} A(k)\varphi'(t)dt + \int_n^x A(n)\varphi'(t)dt \\
&= \sum_{k=1}^{n-1} A(k)(\varphi(k+1) - \varphi(k)) + A(n)(\varphi(x) - \varphi(n)) \text{ (teorema fond. calcolo integrale)} \\
&= A(1)\varphi(2) + \cdots + A(n-1)\varphi(n) - (A(1)\varphi(1) + \cdots \\
&\quad + A(n-1)\varphi(n-1)) - A(n)\varphi(n) - A(x)\varphi(x) \\
&= \sum_{k=2}^{n} A(k-1)\varphi(k) - \sum_{k=1}^{n} A(k)\varphi(k) + A(x)\varphi(x) \\
&= \sum_{k=2}^{n} (A(k-1) - A(k))\varphi(k) - A(1)\varphi(1) + A(x)\varphi(x) \\
&= A(x)\varphi(x) - \sum_{k=1}^{n} a_k\varphi(k).
\end{aligned}$$

La parte 2. segue se si pone $a_k = 1$ □

Applicazioni

Notazioni:
Le seguenti funzioni sono applicazioni limitate da $[1, +\infty[$ in [0,1]

- $\{x\} = x - \lfloor x \rfloor$ (parte frazionaria di x)
- $\beta_1(x) = \frac{1}{\log(x)} \int_1^x \frac{\{t\}}{t} dt$, con $\beta_1(1) = 0$ per continuità
- $\beta_0(x) = \frac{\log(x)}{\sqrt{x}}$
- $\beta_2(x) = x \int_x^\infty \frac{\{t\}}{t^2} dt$
- $\beta_3(x) = x \int_x^\infty \frac{\beta_2(t)}{t^2} dt$

Inoltre definendo

$$\lim_{n\to\infty} \left(\sum_{k=1}^{\infty} \frac{1}{k} - \log(n) \right) = \gamma = 0.57721566\ldots \quad (\textit{costante di Eulero})$$

Si ha:

$$\int_1^n \frac{\{t\}}{t^2} dt = \int_1^n \frac{t - \lfloor t \rfloor}{t^2} dt = \log(n) - \sum_{k=1}^{n-1} \int_k^{k+1} \frac{k}{t^2} dt = \log(n) - \sum_{k=1}^{n-1} k \left(\frac{1}{k+1} - \frac{1}{k} \right)$$

$$= \log(n) - \sum_{k=1}^{n-1} \frac{1}{k+1} = \log(n) - \sum_{k=1}^{n} \frac{1}{k} + 1$$

$$\Rightarrow \beta_2(1) = \int_1^\infty \frac{\{t\}}{t^2} dt = \lim_{n\to\infty} \int_1^n \frac{\{t\}}{t^2} dt = 1 - \gamma$$

Possiamo usare il lemma di Abel per trovare gli sviluppi asintotici delle seguenti funzioni:

Teorema 7. *Esistono tre funzioni limitate $b_1(x)$, $b_2(x)$, $b_3(x)$ a valori in [-1,+1] che verificano*

1. $\log(\lfloor x \rfloor !) = \sum_{k \le x} \log(k) = x\log(x) - x + 2b_1(x)\sqrt{x}$

2. $U(x) = \sum_{k \le x} \frac{x}{k} = x\log(x) + \gamma x + b_2(x)$

3. $V(x) = \sum_{k \le x} \frac{x}{k} \log\left(\frac{x}{k}\right) = \frac{1}{2} x \log^2(x) + \gamma x \log(x) + (\beta_3(1) - \beta_2(1))x + b_3(x)$

4. $W_\alpha(x) = \sum_{k \le x} \left(\frac{x}{k}\right)^\alpha \le \frac{x}{1-\alpha}$ *per ogni* $\alpha \in$*[0,1[*

Dimostrazione. 1.Prendendo $a_k = 1$ e $\varphi(n) = \log(n)$ nel Teorema 6 (Abel) otteniamo:

$$\sum_{n \le x} \log(n) = \lfloor x \rfloor \log(x) - \int_1^x \frac{\lfloor u \rfloor}{u} du = (x - \{x\})\log(x) - \int_1^x \frac{u - \{u\}}{u} du$$

$$x\log(x) - \{x\}\log(x) - (x-1) + \beta_1(x)\log(x) = x\log(x) - x + 2b_1(x)\sqrt{x}$$

dove $b_1(x) = \frac{1}{2\sqrt{x}} + \frac{\beta_1(x) - \{x\}}{2} \frac{\log(x)}{\sqrt{x}}$

Verifichiamo la limitatezza di $b_1(x)$

$$|b_1(x)| \le \frac{1}{2\sqrt{x}} + \frac{|\beta_1(x) - \{x\}|}{2} \beta_0(x) \le \frac{1}{2} + \frac{1}{2} = 1$$

Perché $\beta_1(x)$, $\beta_0(x)$, $\{x\}$ sono applicazioni a valori in [0,1]

2. Applicando Abel (6) con $\varphi(k) = \frac{1}{k}$ e $a_k = 1$

$$\begin{aligned}
\sum_{k \le x} \frac{1}{k} &= \frac{\lfloor x \rfloor}{x} + \int_1^x \frac{\lfloor t \rfloor}{t^2} dt = \frac{x - \{x\}}{x} + \int_1^x \frac{t - \{t\}}{t^2} dt \\
&= 1 - \frac{\{x\}}{x} + \int_1^x \frac{1}{t} dt - \int_1^x \frac{\{t\}}{t^2} dt = 1 - \frac{\{x\}}{x} + \log(x) + \int_1^\infty \frac{\{t\}}{t^2} dt - \int_x^\infty \frac{\{t\}}{t^2} dt \\
&= 1 - \frac{\{x\}}{x} + \log(x) + \frac{\beta_2(x)}{x} - \beta_2(1) = \log(x) + \gamma + \frac{\beta_2(x) - \{x\}}{x}
\end{aligned}$$

Allora $U(x) = \sum_{k \le x} \frac{x}{k} = x\log(x) + \gamma x + b_2(x)$ con $b_2(x) = \beta_2(x) - \{x\} \in [-1, +1]$

3.Applichiamo Abel (6) con $\varphi(t) = \log\left(\frac{x}{t}\right)$ e $a_k = \frac{1}{k}$, allora

$$\varphi'(t) = -\frac{1}{t} \quad e \quad A(x) = \sum_{k \le x} \frac{1}{k} = \log(x) + \gamma + \frac{\beta_2(x) - \{x\}}{x} \text{ (per la parte 2)}$$

$$\begin{aligned}
\sum_{k \le x} \frac{1}{k} \log\left(\frac{x}{k}\right) &= A(x)\log\left(\frac{x}{x}\right) + \int_1^x \frac{A(t)}{t} dt \\
&= \int_1^x \left(\frac{\log(t)}{t} + \frac{\gamma}{t} + \frac{\beta_2}{t^2} - \frac{\{t\}}{t^2}\right) dt \\
&= \frac{1}{2}\log^2(x) + \gamma\log(x) + \beta_3(1) - \frac{\beta_3(x)}{x} - \beta_2(1) + \frac{\beta_2(x)}{x}
\end{aligned}$$

$$\text{Quindi } V(x) = \sum_{k \leq x} \frac{x}{k} \log\left(\frac{x}{k}\right) = \frac{1}{2} x \log^2(x) + \gamma x \log(x) + (\beta_3(1) - \beta_2(1))x + b_3(x)$$

$$\text{con } b_3(x) = \beta_2(x) - \beta_3(x) \in [-1, +1]$$

4.Applichiamo Abel (6) con $\varphi(k) = \dfrac{1}{k^\alpha}$ e $a_k = 1$ con $\alpha \in [0,1[$

$$\sum_{k \leq x} \frac{1}{k^\alpha} = \frac{\lfloor x \rfloor}{x^\alpha} + \alpha \int_1^x \frac{\lfloor t \rfloor}{t^{\alpha+1}} dt \leq x^{1-\alpha} + \alpha \int_1^x t^{-\alpha} dt = x^{1-\alpha} + \alpha \frac{x^{1-\alpha} - 1}{1-\alpha} \leq \frac{x^{1-\alpha}}{1-\alpha}$$

da cui $W_\alpha = \sum_{k \leq x} \left(\dfrac{x}{k}\right)^\alpha = x^\alpha \sum_{k \leq x} \dfrac{1}{k^\alpha} \leq \dfrac{x}{1-\alpha}$ □

1.6 Coppie di Möbius

In teoria dei numeri spesso nascono situazioni di questo tipo:
due funzioni reali $\tilde{f}(x)$ e $f(x)$ sono così in relazione:

$$\tilde{f}(x) = \sum_{n \leq x} f\left(\frac{x}{n}\right)$$

Ad esempio abbiamo già incontrato alcuni casi particolari:

(i) $f(x) = 1, \qquad \tilde{f}(x) = \lfloor x \rfloor$

(ii) $f(x) = x, \qquad \tilde{f}(x) = xU(x)$

(iii) $f(x) = x \log(x), \qquad \tilde{f}(x) = \sum_{n \leq x} \dfrac{x}{n} \log\left(\dfrac{x}{n}\right) = V(x)$

In queste situazioni spesso si hanno informazioni sul comportamento asintotico di $F(x)$ e si vorrebbero dedurre informazioni su quello di $f(x)$, ad esempio per (iii) si è visto che $F(x) = x\log(x) - x + O(\log(x))$ e si vorrebbe arrivare a $\psi(x) \sim x$ o almeno $\psi(x) = O(x)$. Per fare questo si utilizza la formula di inversione di Möbius:

Teorema 8. *Per tutti gli interi $n \leq 1$ abbiamo:*

$$\sum_{k|n} \mu(k) = \begin{cases} 1 & se\ n = 1 \\ 0 & altrimenti \end{cases} \tag{1.6}$$

E inoltre se le funzioni $f(x)$ e $\tilde{f}(x)$ sono così in relazione:

$$\tilde{f}(x) = \sum_{n \leq x} f\left(\frac{x}{n}\right)$$

allora

$$f(x) = \sum_{n\leq x} \mu(n)\tilde{f}\left(\frac{x}{n}\right).$$

Dimostrazione. La prima parte si può tradurre facilmente con la notazione convolutiva come $\mu * \mathbb{1}(n) = \epsilon(n)$ cioè $\mu(n)$ è l'inversa rispetto alla convoluzione di $\mathbb{1}$, che è vero per definizione. Ora abbiamo dunque che $\mathbb{1}(n) = \sum_{k|n}\mu(k)$ e che $\mathbb{1}(1) = 1$ e $\mathbb{1}(n) = 0$ se $n > 1$. Così:

$$\begin{aligned} f(x) = & \sum_{n\leq x} \varepsilon(n) f\left(\frac{x}{n}\right) = \sum_{n\leq x} f\left(\frac{x}{n}\right)\sum_{k|n}\mu(k) \\ &= \sum_{kl\leq x}\mu(k) f\left(\frac{x}{kl}\right) = \sum_{k\leq x}\mu(k)\sum_{l\leq x|k} f\left(\frac{x}{kl}\right) \\ &= \sum_{k\leq x}\mu(k)\tilde{f}\left(\frac{x}{k}\right). \end{aligned}$$

Quando $f(x) = 0$ per valori non interi di x allora possiamo formulare la seconda parte come:

$$\textit{Se}\quad \tilde{f}(n) = \sum_{m|n} f(m) \quad \textit{allora} \quad f(n) = \sum_{m|n}\mu(n)\tilde{f}\left(\frac{m}{n}\right)$$

o in notazione convolutiva

$$\textit{Se}\quad \tilde{f}(n) = f * \mathbb{1}(n) \quad \textit{allora} \quad f(n) = \mu * \tilde{f}(n)$$

E possiamo verificare più semplicemente, sfruttando la convoluzione, che

$$\mu * \tilde{f}(n) = \mu * (\mathbb{1} * f(m))(n) = (\mu * \mathbb{1}(m)) * f(n) = \epsilon * f(n) = f(n)$$

□

Definizione 5. Possiamo allora definire una coppia di funzioni $(f, \tilde{f})$ così in relazione:

$$\tilde{f}(x) = \sum_{k\leq x} f\left(\frac{x}{k}\right)$$

come *coppia di funzioni di Möbius o μ-coppia di funzioni*

Possiamo costruire una μ-coppia di funzioni a partire da $\psi(x) = \sum_{n\leq x}\Lambda(n)$

Teorema 9. *Se poniamo $\alpha_p(x) = \sum_\nu \left\lfloor \frac{x}{p^v} \right\rfloor$ per ogni primo $p \leq x$, si ha allora*

$$\lfloor x \rfloor ! = \prod_{p\leq x} p^{\alpha_p(x)}$$

E la coppia $(\psi, \tilde{\psi})$ è una μ-coppia di funzioni:

$$\psi(x) = \sum_{n\leq x}\Lambda(n) \qquad \tilde{\psi}(x) = \log(\lfloor x \rfloor !)$$

Dimostrazione. Per tutti i primi $p \leq x$, $\left\lfloor \frac{x}{p^v} \right\rfloor$ è il numero di multipli di p^v compresi tra 1 e x, e dunque $\alpha_p(x) = \sum_v \left\lfloor \frac{x}{p^v} \right\rfloor$ è l'esponente di p nella fattorizzazione in primi di $\lfloor x \rfloor !$.

$$\sum_{n \leq x} \psi\left(\frac{x}{n}\right) = \sum_{n \leq x} \sum_{m \leq x/n} \Lambda(m) = \sum_{m \leq x} \sum_{n \leq x/m} \Lambda(m) = \sum_{m \leq x} \left\lfloor \frac{x}{m} \right\rfloor \Lambda(m)$$

Poiché $\Lambda(m) = \log(p)$ se $m = p^v$ e 0 altrimenti

$$\sum_{n \leq x} \psi\left(\frac{x}{n}\right) = \sum_{p \leq x} \sum_{v} \left\lfloor \frac{x}{p^v} \right\rfloor \log(p) = \sum_{p \leq x} \alpha_p(x) \log(p) = \log\left(\prod_{p \leq x} p^{\alpha_p(x)}\right) = \log(\lfloor x \rfloor !) = \tilde{\psi}(x).$$

□

Cerchiamo ora come dedurre il comportamento asintotico di $f(x)$ da $\tilde{f}(x)$

Teorema 10. *Siano $(f, \tilde{f})$ una μ-coppia di Möbius, A,B,C tre numeri reali e $\alpha \in [0,1[$.*

1. *Se $\tilde{f}(x) = O(x^\alpha)$, allora $f(x) = O(x)$*
2. *se $\tilde{f}(x) = Ax\log^2(x) + Bx\log(x) + C + O(x^\alpha)$, allora $f(x) = 2Ax\log(x) + O(x)$.*

Dimostrazione.

1. Sia K una costante che verifichi $\left|\tilde{f}(x)\right| \leq Kx^\alpha$. Allora per il Teorema 8,

$$|f(x)| = \left|\sum_{n \leq x} \mu(n)\tilde{f}\left(\frac{x}{n}\right)\right| \leq \sum_{n \leq x} \left|\tilde{f}\left(\frac{x}{n}\right)\right| \leq K \sum_{n \leq x} \left(\frac{x}{n}\right)^\alpha = KW_\alpha(x) \leq \frac{K}{1-\alpha} x \text{ (Teorema 7)}$$

2. Nel caso generale si definisce un'altra coppia di Möbius $(g, \tilde{g})$, ponendo

$$g(x) = f(x) - ax\log(x) - bx - c \quad e \quad \tilde{g}(x) = \tilde{f}(x) - -aV(x) - bU(x) - c\lfloor x \rfloor$$

Allora sempre per il Teorema 7

$$\tilde{g}(x) = \left(A - \frac{1}{2}a\right) x\log^2(x) + (B - a\gamma - b)x\log(x) + (C - a(\beta_3(1) - \beta_2(1)) - b\gamma - c)x + O(x^\alpha)$$

Scegliendo $a = 2A, b = B - a\gamma$ e $c = C - a(\beta_3(1) - \beta_2(1)) - b\gamma$ abbiamo $\tilde{g}(x) = O(x^\alpha)$, e per la parte 1 di questo teorema $g(x) = O(x)$.

$$\text{Quindi } f(x) = g(x) + ax\log(x) + bx + c = ax\log(x) + O(x) = 2Ax\log(x) + O(x).$$

□

Sia $(f, \tilde{f})$ una μ-coppia di funzioni, se $f(x) = 0$ per $x \notin \mathbb{N}$, lo stesso vale per $\tilde{f}(x)$ e viceversa. Allora si avrà

$$\tilde{f}(k) = \sum_{m|k} f\left(\frac{k}{m}\right) = \sum_{mn=k} f(n) \quad e \quad f(k) = \sum_{mn=k} \mu(m)\tilde{f}(n), \qquad n \in \mathbb{N}.$$

Date f e $\tilde{f}$ funzioni aritmetiche che soddisfano la relazione precedente, la coppia $(f, \tilde{f})$ costituisce una *μ-coppia aritmetica*, e utilizzando la proprietà di convoluzione vale:

$$\tilde{f} = f * \mathbb{1}, \qquad f = \mu * \tilde{f}$$

Teorema 11. *Le coppie seguenti sono μ-coppie aritmetiche:*

1. (μ, ε)

2. $(\Lambda, \log)$

3. $(\mu \log, -\Lambda)$

4. $(\mu \log^2, b)$, *con* $b = (\Lambda * \Lambda) - \Lambda \log$

5. $(c, \log^2)$, *con* $c = (\Lambda * \Lambda) + \Lambda \log$

Dimostrazione. 1. Vera perché $\mu * \mathbb{1} = \varepsilon$

2. Vera perché $\Lambda = \log * \mu$ e quindi $\sum_{mn=k} \Lambda(n) = \log(k)$, cioè $\log = \Lambda * \mathbb{1}$

3. Verifichiamo che $(\mu \log) * \mathbb{1} = -\Lambda$

$$(\mu \log) * \mathbb{1} = \textstyle\sum_{mn=k} \mu(n) \log(n) \mathbb{1}(m) = \sum_{mn=k} \mu(n) \log(n) = \sum_{mn=k} \mu(n) \log(\frac{k}{m}) =$$
$$\textstyle\sum_{mn=k} \mu(n)(\log(k) - \log(m)) = \log(k) \sum_{mn=k} \mu(n) - \sum_{mn=k} \mu(n) \log(m) =$$
$$\log(k)(\mu * \mathbb{1})(k) - \mu * \log(k) = 0 - \Lambda(k)$$

4. Studiamo $(\mu \log^2) * \mathbb{1}$

$$(\mu \log^2) * \mathbb{1}(k) = \textstyle\sum_{mn=k} \mu(m) \log^2(m) = \sum_{mn=k} \mu(m) \log(m)(\log(k) - \log(n)) =$$
$$\log(k)(\mu \log * \mathbb{1})(k) - \textstyle\sum_{mn=k, rs=n} \mu(m) \log(m) \Lambda(r) \mathbb{1}(s) = -\log(k)\Lambda(k) - \mu \log * \Lambda * \mathbb{1}(k) =$$
$$-\log(k)\Lambda(k) - (\mu \log * \mathbb{1}) * \Lambda(k) = -\log(k)\Lambda(k) + \Lambda * \Lambda(k)$$

5. Studiamo ugualmente $\mu * \log^2$:

$$\mu * \log^2 = \sum_{mn=k} \mu(m) \log(m)(\log(k) - \log(n)) = \Lambda(k) \log(k) - \sum_{mn=k} \mu(m) \log(m) \log(n) = c(k)$$

□

Vediamo come definire una nuova μ-coppia di funzioni da una μ-coppia aritmetica:

Osservazione 7. Se $(f(k), \tilde{f}(k))$ è una μ-coppia aritmetica, chiamiamo $g(x) = \sum_{k \leq x} f(k)$, allora

$$\tilde{g}(x) = \sum_{n \leq x} g\left(\frac{x}{n}\right) = \sum_{n \leq x} \sum_{k \leq \frac{x}{n}} f(k) = \sum_{kn \leq x} f(k) = \sum_{m \leq x} \sum_{kn=m} f(k) = \sum_{m \leq x} \tilde{f}(m)$$

E quindi $\left(\sum_{k \leq x} f(k), \sum_{k \leq x} \tilde{f}(k)\right)$ è una μ-coppia di funzioni.

Studiamo il comportamento della successione $\{c(k)\}$ definita nel teorema 11:

Teorema 12. *1.* $\sum_{k \leq x} \dfrac{c(k)}{k} = \log^2(x) - 2\gamma \log(x) + O(1)$ *dove* γ *è la costante di Eulero*

2. $\sum_{y<k\leq x} \frac{c(k)}{k} = \log\left(\frac{x}{y}\right)(\log(xy) - 2\gamma) + O(1)$.

Dimostrazione. 1. Sia $g(x) = \sum_{k\leq x} g\frac{x}{k}c(k)$ e $f(x) = g(x) - x\log^2(x)$

Allora $\tilde{g}(x) = \sum_{n\leq x}\left(\frac{x}{n}\right) = \sum_{n\leq x}\sum_{k\leq x/n}\frac{x}{nk}c(k) = \sum_{nk\leq x}\frac{x}{nk}c(k) = \sum_{m\leq x}\sum_{nk=m}\frac{x}{m}c(k) =$

$$= \sum_{m\leq x}\frac{x}{m}(c * \mathbb{1})(m) = \sum_{m\leq x}\log^2(m)$$

Quindi

$$\tilde{f}(x) = \sum_{m\leq x}\frac{x}{m}\log^2(m) - \sum_{m\leq x}\frac{x}{m}\log^2\left(\frac{x}{m}\right) = \sum_{m\leq x}\frac{x}{m}\left(\log^2(m) - \log^2\left(\frac{x}{m}\right)\right)$$

Poiché

$$\begin{aligned} & \log^2(m) - \log^2\left(\frac{x}{m}\right) = \log^2(m) - (\log(x) - \log(m))^2 \\ = \; & \log^2(m) - \log^2(x) - \log^2(m) + 2\log(x)\log(m) = -\log^2(x) + 2\log(x)\log(m) = A \end{aligned}$$

e

$$\begin{aligned} & \log^2(x) - 2\log(x)(\log(x) - \log(m)) = \log^2(x) - 2\log^2(x) + 2\log(x)\log(m) \\ = \; & -\log^2(x) + 2\log(x)\log(m) = A \end{aligned}$$

Allora

$$\tilde{f}(x) = \sum_{m\leq x}\frac{x}{m}\left(\log^2(x) - 2\log(x)\log\left(\frac{x}{m}\right)\right)$$

e per il Teorema 7

$$\begin{aligned} = \; & \log^2(x)U(x) - 2\log(x)V(x) \\ = \; & \log^2(x)(x\log(x) + \gamma x + b_2(x)) - 2\log(x)\left(\frac{1}{2}x\log^2(x) + \gamma x\log(x) + \delta x + b_3(x)\right) \\ \text{con} \; & \delta = \beta_3(1) - \beta_2(1) \text{ vedi Teorema 7} \\ = \; & \log^2(x)x\log(x) - \log(x)x\log^2(x) + \gamma x\log^2(x) - 2\gamma x\log^2(x) + \log^2(x)b_2(x) \\ & -2\log(x)x\delta - 2\log(x)b_3(x) \\ = \; & -\gamma x\log^2(x) - 2\delta x\log(x) + O(\sqrt{x}) \end{aligned}$$

Ponendo $A = -\gamma, B = -2\delta, C = D = 0$ nel Teorema 10 deduciamo che

$$f(x) = -2\gamma x\log(x) + O(x)$$

e quindi

$$\sum_{k\leq x}\frac{c(k)}{k} = \frac{g(x)}{x} = \log^2(x) + \frac{f(x)}{x} = \log^2(x) - 2\gamma\log(x) + O(1)$$

2.

$$
\begin{aligned}
\textstyle\sum_{y<k\leq x} \frac{c(k)}{k} &= \sum_{k\leq x} \frac{c(k)}{k} - \sum_{k\leq y} \frac{c(k)}{k} \\
&= \log^2(x) - 2\gamma \log(x) - \log^2(y) + 2\gamma \log(y) + O(1) \\
\text{Poiché} \quad & \log^2(x) - \log^2(y) = (\log(x) - \log(y))(\log(x) + \log(y)) \\
&= (\log(xy)) \left(\log\left(\frac{x}{y}\right) \right) \\
\textstyle\sum_{y\leq k\leq x} \frac{c(k)}{k} &= \log(x)\log(x) - \log(y)\log(y) - 2\gamma(\log(x) - \log(y)) \\
&= \log\left(\frac{x}{y}\right)(\log(xy) - 2\gamma) + O(1)
\end{aligned}
$$

$\square$

Capitolo 2

Una prova elementare del TNP

2.1 Comportamento asintotico di M(x)

La dimostrazione del teorema dei numeri primi che vedremo in questa tesi parte dallo studio della funzione di Mertens,

$$M(x) = \sum_{n \leq x} \mu(n)$$

Questa funzione è legata alla distribuzione dei numeri primi ed alla funzione $\psi(x)$. Studiamo il comportamento asintotico di $M(x)$, iniziando con qualche maggiorazione:

Teorema 13. *1.* $|M(x)| \leq x$

2. $|M(y) - M(x)| \leq |y - x| + 1$
3. $\left| \sum_{k \leq x} \frac{\mu(k)}{k} \right| \leq 1.$
4. *Se x<y, allora* $\left| \int_x^y \frac{M(t)}{t^2} dt \right| \leq 4$
5. $\varphi(x) = |M(x)| \log^2(x) - 2x \log(x) \leq \sum_{k \leq x} c(k) \left| M\left(\frac{x}{k}\right) \right|$

Dimostrazione. 1.

$$|M(x)| \leq \sum_{k \leq x} |\mu(k)| \leq \sum_{k \leq x} 1 = \lfloor x \rfloor \leq x$$

2.

$$|M(x) - M(y)| \leq \sum_{x < k \leq y} |\mu(k)| \leq \sum_{x < k \leq y} 1 = \lfloor y \rfloor - \lfloor x \rfloor \leq y - x + 1$$

3.

$$\mu(1) = 1, \quad \mu(2) = -1, \quad \mu(3) = -1, \quad \mu(4) = 0$$

La maggiorazione vale per $x \leq 4$. Supponiamo $x \geq 4$
$(1, \lfloor x \rfloor)$ è una μ-coppia di funzioni, quindi

$$1 = \sum_{k \leq x} \mu(k) \left\lfloor \frac{x}{k} \right\rfloor = \sum_{k \leq x} \mu(k) \frac{x}{k} - \sum_{k \leq x} \mu(k) \left\{ \frac{x}{k} \right\}$$

da cui

$$x \left| \sum_{k \leq x} \frac{\mu(k)}{k} \right| = \left| 1 + \sum_{k \leq x} \mu(k) \left\{ \frac{x}{k} \right\} \right| \leq 1 + \sum_{k \leq x} |\mu(k)| \leq 1 + \lfloor x \rfloor - 1 \leq x$$

4. Dal lemma di Abel, con $\varphi = \mu(k), \quad a_k = \dfrac{1}{k}$

$$\sum_{k \leq x} \frac{\mu(k)}{k} = \frac{M(x)}{x} + \int_1^x \frac{M(t)}{t^2} dt$$

Quindi

$$\left| \int_1^x \frac{M(t)}{t^2} dt \right| = \left| \sum_{k \leq x} \frac{\mu(k)}{k} - \frac{M(x)}{x} dt \right| \leq 1 + 1 = 2.$$

E infine:

$$\left| \int_x^y \frac{M(t)}{t^2} dt \right| = \left| \int_1^y \frac{M(t)}{t^2} dt - \int_1^x \frac{M(t)}{t^2} dt \right| \leq 2 + 2 = 4$$

5. Dal lemma di Abel abbiamo che

$$\sum_{k \leq x} \mu(k) \log^2(k) = M(x) \log^2(x) - 2 \int_1^x M(t) \frac{\log(t)}{t} dt$$

Quindi

$$|M(x)| \log^2(x) \leq \left| \sum_{k \leq x} \mu(k) \log^2(k) \right| + 2 \int_1^x |M(t)| \frac{\log(t)}{t} dt.$$

Ora da una parte $\displaystyle\int_1^x \frac{|M(t)|}{t} \log(t) dt \leq \int_1^x \log(t) dt = x \log(x) - x + 1 \leq x \log(x)$

Mentre per l'osservazione 7 $\left(\sum_{k \leq x} \mu(k) \log^2(k), \sum_{k \leq x} b(k) \right)$ è una μ-coppia di funzioni, quindi per la formula di inversione di Möbius

$$\sum_{k \leq x} \mu(k) \log^2(k) = (\mu * b)(x) = \sum_{k \leq x} \sum_{n \leq x/k} \mu(n) b(k) = \sum_{k \leq x} b(k) M\left(\frac{x}{k}\right)$$

Quindi

$$\left| \sum_{k \leq x} \mu(k) \log^2(k) \right| \leq \sum_{k \leq x} |b(k)| \left| M\left(\frac{x}{k}\right) \right| \leq \sum_{k \leq x} c(k) \left| M\left(\frac{x}{k}\right) \right|.$$

□

Ora dimostriamo l'esistenza di intervalli su cui $\left| \dfrac{M(x)}{x} \right|$ prende dei valori piccoli.

Teorema 14. *Sia $\Delta \le 3$ e sia $\delta = \Delta^{-1}$. Allora per tutti i numeri reali $A \ge \Delta$, l'intervallo $[A, Ae^{\Delta}[$ contiene un intervallo $[a, ae^{\delta}[$ é su cui* $\left|\frac{M(x)}{x}\right| \le 7\delta$.

Dimostrazione. Supponiamo per assurdo che

$$\forall x \in [A, Ae^{\Delta-\delta}[\quad |M(x)| \ge 5\delta x$$

$$\text{Si avrà allora} \quad \forall x \in [A, Ae^{\Delta-\delta}[\quad |M(x)| \ge 5\delta A \ge 5\delta\Delta = 5.$$

Dunque la funzione mantiene un segno costante nell'intervallo $[A, Ae^{\Delta-\delta}[$ e quindi si ha:

$$\left|\int_A^{Ae^{\Delta-\delta}} \frac{M(x)}{x^2}dx\right| = \int_A^{Ae^{\Delta-\delta}} \frac{|M(x)|}{x^2}dx \ge \int_A^{Ae^{\Delta-\delta}} \frac{5\delta x}{x^2}dx = 5\delta(\Delta-\delta) = 5 - 5\delta^2 \ge 5 - \frac{5}{9} > 4,$$

Ma questo è impossibile per il Teorema 13
Quindi esiste almeno un elemento a di $[A, Ae^{\Delta-\delta}[$ che verifica $|M(a)| < 5\delta a$.
Allora $[a, ae^{\delta}[$ è tale che $A < a < Ae^{\Delta-\delta} < Ae^{\Delta}$ e $ae^{\delta} < Ae^{\Delta-\delta}e^{\delta} = Ae^{\Delta}$
Cioè $[a, ae^{\delta}[\subset [A, Ae^{\Delta}[$ e $\forall x \in [a, ae^{\delta}[$ si ha:

$$|M(x)| \le |M(x) - M(a)| + |M(a)| \le (x - a + 1) + 5\delta a$$
$$x < ae^{\delta} \Rightarrow a > xe^{-\delta} \qquad e \qquad x\delta = \tfrac{x}{\Delta} \le \tfrac{x}{3}, \quad \text{ma} \quad A > \Delta \Rightarrow x > A \Rightarrow \tfrac{x}{\Delta} > 1$$
$$\text{Quindi} |M(x)| \le x - xe^{-\delta} + \delta x + 5\delta x \le \delta x\left(\frac{1-e^{-\delta}}{\delta} + 6\right) \le 7\delta x.$$

□

Si può quindi stabilire il seguente teorema fondamentale:

Teorema 15.

$$\sigma(x) = sup_{t \ge x}\left|\frac{M(t)}{t}\right| \to 0 \textit{ per } x \to \infty \textit{ e quindi } \frac{M(x)}{x} \to 0 \textit{ per } x \to \infty$$

Dimostrazione. La dimostrazione è lunga e tecnica, andremo per tappe
La funzione σ
Questa funzione è decrescente, e per il Teorema 13 prende valori in [0,1]. Dunque converge verso un limite $\lambda \in [0,1]$. Dobbiamo dimostrare che $\lambda = 0$.

$$\text{Si avrà che } \limsup\left|\frac{M(x)}{x}\right| = \lim_{x\to\infty}\sigma(x) = 0 \text{ e quindi } \lim_{x\to\infty}\frac{M(x)}{x} = 0$$

Gli intervalli I_m
Si fissa $\Delta > 3$ e si pone $\delta = \Delta^{-1}$

$$\text{Per tutti gli interi } m \ge 1, \text{ chiamiamo } I_m = \left[e^{\Delta m}, e^{\Delta(m+1)}\right[\text{ e } s_m = sup_{t\in I_m}\left|\frac{M(t)}{t}\right|.$$

$$\text{Allora } \limsup s_m = \lim_{n\to\infty} sup_{m\geq n} s_m = \lim_{n\to\infty} \sigma(e^{\Delta n}) = \lambda$$

D'altra parte per il Teorema 14, l'intervallo I_m contiene un intervallo $[a_m, a_m e^{\delta}[$ su cui $|M(x)| \leq 7\delta x$.

Scelta delle maggiorazioni di $\left|M\left(\frac{x}{k}\right)\right|$
Si fissa una intero $n \geq 2$ ed un numero reale $x \in I_n$. Poniamo $l = \lfloor\sqrt{n}\rfloor$.

$$\text{Per tutti gli interi } k \in K_m =]xa_m^{-1}e^{-\delta}, xa_m^{-1}],$$

$$\frac{x}{k} \in [a_m, a_m e^{\delta}[\quad e \quad \left|M\left(\frac{x}{k}\right)\right| \leq \frac{7\delta x}{k} \text{ per il Teorema 14}$$

$$\text{Per tutti gli interi } k \in I =]xe^{-\Delta l}, x], \quad \frac{x}{k} \in [1, e^{\Delta l}[\quad \text{e} \quad \left|M\left(\frac{x}{k}\right)\right| \leq \frac{x}{k} \text{ per il Teorema 13}$$

$$\text{Per ogni intero } k \in J = [1, xe^{-\Delta l}], \quad \frac{x}{k} \in [e^{\Delta l}, x] \text{ e } \left|M\left(\frac{x}{k}\right)\right| \leq \sigma(e^{\Delta l})\frac{x}{k} \text{ per definizione di } \sigma.$$

$$\text{In più } \cup_{m=l}^{n-1} [a_m, a_m e^{\delta}[\subset \cup_{m=l}^{n-1} I_m = [e^{\Delta l}, e^{\Delta n}[\subset [e^{\Delta l}, x]$$

$$\text{quindi abbiamo che } e^{\Delta l} \leq a_m \leq a_m e^{\delta} \leq x, \text{ da cui } \frac{x}{a_m e^{\delta}} > 1, \quad \frac{x}{e^{\Delta l}} > \frac{x}{a_m}$$

$$\text{Possiamo concludere che } K = \cup_{m=l}^{n-1} K_m \subset J$$

Maggiorazioni di $\varphi(x) = |M(x)|\log^2 x - 2x\log(x)$
Dall'ultima maggiorazione del Teorema 13 abbiamo che:

$$\begin{aligned}
\varphi(x) &\leq \sum_{k\leq x} c(k)\left|M\left(\frac{x}{k}\right)\right| \leq \sum_{k\in I} c(k)\left|M\left(\frac{x}{k}\right)\right| + \sum_{k\in J\setminus K} c(k)\left|M\left(\frac{x}{k}\right)\right| + \sum_{k\in K} c(k)\left|M\left(\frac{x}{k}\right)\right| \\
&\leq x\sum_{k\in I}\frac{c(k)}{k} + \sigma(e^{\Delta l})x\sum_{k\in J\setminus K}\frac{c(k)}{k} + 7\delta x\sum_{k\in K}\frac{c(k)}{k} \qquad \text{Quindi} \\
\frac{\varphi(x)}{x} &\leq \sum_{k\in I}\frac{c(k)}{k} + \sigma(e^{\Delta l})\sum_{k\in J}\frac{c(k)}{k} + (7\delta - \sigma(e^{\Delta l}))\sum_{k\in K}\frac{c(k)}{k} = \phi(x).
\end{aligned}$$

Comportamento asintotico del maggiorante ϕ(x)

$\Delta n \leq \log(x) \leq \Delta(n+1)$ Perché x $\in I_m$, quindi $\log(x) = \Delta n + O(1)$. Allo stesso modo $\log(a_m) = \Delta m + O(1)$.

D'altra parte $l = \lfloor \sqrt{n} \rfloor = \sqrt{n} + O(1) = o(n)$. Quindi per il Teorema 12 si ha:

$$\begin{aligned}
\sum_{k \in I} \frac{c(k)}{k} &= \log\left(\frac{x}{xe^{-\Delta l}}\right)\left(\log(x^2 e^{-\Delta l}) - 2\gamma\right) + O(1) \\
&= (\log(x) - \log(xe^{-\Delta l}))(\log(x) + \log(xe^{-\Delta l}) - 2\gamma) + O(1) \\
&= (\log(x) - \log(x) + \Delta l)(\log(x) + \log(x) - \Delta l - 2\gamma) + O(1) \\
&= \Delta l(2\log(x) - \Delta l - 2\gamma) + O(1) = o(n^2) \\
\sum_{k \in J} \frac{c(k)}{k} &= \log(xe^{-\Delta l})(\log(xe^{-\Delta l}) - 2\gamma) + O(1) \\
&= (\log(x) - \Delta l)(\log(x) - \Delta l - 2\gamma) + O(1) = \Delta^2 n^2 + o(n^2) \\
\sum_{k \in K_m} \frac{c(k)}{k} &= \log\left(\frac{xa_m^{-1}}{xa_m^{-1}e^{-\delta}}\right)(\log(x^2 a_m^{-2} e^{-\delta}) - 2\gamma)) + O(1) \\
&= \delta(2\log(x) - 2\log(a_m) - \delta - 2\gamma) + O(1) \\
&= \delta(2\Delta n - 2\Delta m) + O(1) = 2(n-m) + O(1) \\
\sum_{k \in K} \frac{c(k)}{k} &= \sum_{m=l}^{n-1} \sum_{k \in K_m} \frac{c(k)}{k} = \sum_{m=l}^{n-1} (2(n-m) + O(1)) \\
&= \sum_{m=l}^{n-1} 2n - \sum_{m=l}^{n-1} 2m + (n-l)O(1) \\
&= 2n(n-1-l) - 2(n-1)n/2 + 2l(l+1)/2 + (n-l)O(1) \\
&= -2nl + 2n^2 - 2n - n^2 + n + l^2 + l + (n-l)O(1) \\
&= -2nl + n^2 + l^2 - n + l + (n-l)O(1) \\
&= (n-l)(n-l-1) + (n-l)O(1) = n^2 + o(n^2).
\end{aligned}$$

Da cui

$$\begin{aligned}
\phi(x) &= o(n^2) + \sigma(e^{\Delta l})(\Delta^2 n^2 + o(n^2)) + (7\delta - \sigma(e^{\Delta l}))(n^2 + o(n^2)) \\
&= \sigma(e^{\Delta l})(\Delta^2 - 1)n^2 + 7\delta n^2 + o(n^2)
\end{aligned}$$

Conclusione

$$\begin{aligned}
\left|\frac{M(x)}{x}\right| &= \frac{\varphi(x)}{x\log^2(x)} + \frac{2}{\log(x)} \le \frac{\phi(x)}{\Delta^2 n^2} + \frac{2}{\Delta n} \\
&\le \frac{7\delta n^2}{\Delta n^2} + \frac{\sigma(e^{\Delta l})\Delta^2 n^2}{\Delta^2 n^2} + \frac{\sigma(e^{\Delta l})n^2}{\Delta^2 n^2} + o(1) \le \frac{7\delta}{\Delta^2} + \sigma(e^{\Delta l}\left(1 - \frac{1}{\Delta^2}\right) + o(1) \\
&= 7\delta^3 + \sigma(e^{\Delta l})(1-\delta^2) + o(1).
\end{aligned}$$

Questa maggiorazione vale per tutti gli $x \in I_n$ quindi si ha anche che $s_n \le 7\delta^3 + \sigma(e^{\Delta l})(1-\delta^2) + o(1)$,

Facendo tendere $n \to \infty$, $\quad \lambda = \limsup s_n \le 7\delta^3 + \lambda(1-\delta^2), \Rightarrow \lambda\delta^2 \le 7\delta^3 \Rightarrow \lambda \le 7\delta.$

Possiamo scegliere quindi δ piccolo a piacere ed avere $\lambda = 0$ □

2.2 Il teorema dei numeri primi

Teorema 16. *Sia a_n una successione decrescente di numeri reali positivi*
Per tutte le coppie di interi (m,n) che verificano $1 \leq m < n$, si ha

$$\left|\sum_{k=m+1}^{n} a_k\mu(k)\right| \leq 2n\sigma(m)a_{m+1}$$

Dimostrazione.

$$\begin{aligned}
\sum_{k=m+1}^{n} a_k\mu(k) &= \sum_{k=m+1}^{n} a_k(M(k)-M(k-1)) = \sum_{k=m+1}^{n} a_kM(k) - \sum_{k=m}^{n-1} a_{k+1}M(k) \\
&= -a_{m+1}M(m) + \sum_{k=m+1}^{n-1}(a_k - a_{k+1})M(k) + a_nM(n), \text{ Da cui} \\
\left|\sum_{k=m+1}^{n} a_k\mu(k)\right| &\leq a_{m+1}|M(m)| + \sum_{k=m+1}^{n-1}(a_k - a_{k+1})|M(k)| + a_n|M(n)| \\
&\leq a_{m+1}m\sigma(m) + \sum_{k=m+1}^{n-1}(a_k - a_{k+1})k\sigma(m) + a_nn\sigma(m) \\
&\leq n\sigma(m)\left(a_{m+1} + \sum_{k=m+1}^{n-1}(a_k - a_{k+1}) + a_n\right) = 2n\sigma(m)a_{m+1}.
\end{aligned}$$

□

Possiamo finalmente completare la dimostrazione del teorema dei numeri primi

Teorema 17.

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

Dimostrazione. Dal Teorema 5 sappiamo che è sufficiente mostrare che

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

Consideriamo le tre μ-coppie di funzioni $(g_1,\tilde{g}_1), (g_2,\tilde{g}_2), (g,\tilde{g})$ seguenti:

$$\begin{array}{cc}
g_1(x) = \psi(x) + 1 + \gamma & \tilde{g}_1(x) = \log(\lfloor x\rfloor)! + (1+\gamma)\lfloor x\rfloor \\
g_2(x) = x & \tilde{g}_2(x) = \sum_{n\leq x}\frac{x}{n} = U(x) \\
g(x) = g_1(x) - g_2(x) & \tilde{g}(x) = \tilde{g}_1(x) - \tilde{g}_2(x)
\end{array}$$

Si nota che le applicazioni $\tilde{g}_1$ e $\tilde{g}_2$ sono positive e crescenti. Per la proposizione 3

$$\begin{aligned}
\tilde{g}(x) &= x\log(x) - x + 2b_1(x)\sqrt{x} + (1+\gamma)(x - \{x\}) - (x\log(x) + \gamma x + b_2(x)) \\
&= 2b_1(x)\sqrt{x} - (1+\gamma)\{x\} - b_2(x)
\end{aligned}$$

Ricordando che $b_1(x), b_2(x), \{x\}$ prendono valori in $[-1,1]$

$$\text{Si ha } |\tilde{g}(x)| \leq (2|b_1(x)| + (1+\gamma)\{x\} + |b_2(x)|\sqrt{x} \leq (4+\gamma)\sqrt{x} \leq 5\sqrt{x}$$

Allora per η fissato in $]0,1[$ si ha per ogni $x > \eta^{-1}$

$$g(x) = (\tilde{g} * \mu)(x) = (\tilde{g} * \mu)(\eta x) + ((\tilde{g}_1 - \tilde{g}_2) * \mu)(x) - ((\tilde{g}_1 - \tilde{g}_2) * \mu)(\eta x)$$

$$\text{Cioè } g(x) = \sum_{n \leq \eta x} \mu(n)\tilde{g}\left(\frac{x}{n}\right) + \sum_{\eta x < n \leq x} \mu(n)\tilde{g}_1\left(\frac{x}{n}\right) - \sum_{\eta x < n \leq x} \mu(n)\tilde{g}_2\left(\frac{x}{n}\right)$$

$$\text{Ora } \left|\sum_{n \leq \eta x} \mu(n)\tilde{g}\left(\frac{x}{n}\right)\right| \leq \sum_{n \leq \eta x} \left|\tilde{g}\left(\frac{x}{n}\right)\right| \leq 5 \sum_{n \leq \eta x} \sqrt{\frac{x}{n}} = 5W_{1/2}(\eta x) \leq 10\eta x \text{ (per il Teorema 7)}$$

D'altra parte per il Teorema 16 e la crescenza di $\tilde{g}_1$

$$\left|\sum_{\eta x \leq n \leq x} \mu(n)\tilde{g}_1\left(\frac{x}{n}\right)\right| = \left|\sum_{n=\lfloor \eta x \rfloor+1}^{\lfloor x \rfloor} \mu(n)\tilde{g}_1\left(\frac{x}{n}\right)\right| \leq 2\lfloor x \rfloor \sigma(\lfloor \eta x \rfloor)\tilde{g}_1\left(\frac{x}{\lfloor \eta x \rfloor + 1}\right) \leq 2x\sigma(\lfloor \eta x \rfloor)\tilde{g}_1\left(\frac{1}{\eta}\right)$$

$$\text{Ed allo stesso modo } \left|\sum_{\eta x \leq n \leq x} \mu(n)\tilde{g}_2\left(\frac{x}{n}\right)\right| \leq 2x\sigma(\lfloor \eta x \rfloor)\tilde{g}_2\left(\frac{1}{\eta}\right)$$

$$\text{Quindi } |g(x)| \leq 10\eta x + 2x\sigma(\lfloor \eta x \rfloor)\left(\tilde{g}_1\left(\frac{1}{\eta}\right) + \tilde{g}_2\left(\frac{1}{\eta}\right)\right)$$

$$\text{Ora } \lim_{x\to\infty} \sigma(\lfloor \eta x \rfloor) = 0 \text{ (Teorema 15) ,} \qquad \text{Dunque } \limsup \left|\frac{g(x)}{x}\right| \leq 10\eta$$

Poiché la scelta di η è arbitraria in $]0,1[$ si ha che $\limsup \left|\frac{g(x)}{x}\right| = 0$, e quindi che $\lim_{x\to\infty} \frac{g(x)}{x} = 0$.

Infine

$$\psi(x) = g(x) + x - (1+\gamma) \Rightarrow \lim_{x\to\infty} \frac{\psi(x)}{x} = 1$$

$\square$

Capitolo 3

Cenni storici di altre dimostrazioni

3.1 Legami tra ζ di Riemann e Teoria dei Numeri

Presentiamo alcuni esempi di come la funzione ζ di Riemann è legata alla Teoria dei Numeri

Proposizione 18.

$$\text{Sia } \alpha > 1 \text{ e sia } \zeta(\alpha) = \sum_{n=1}^{\infty} \frac{1}{n^{\alpha}} \text{ allora } \sum_{n=1}^{\infty} \frac{\mu(n)}{n^{\alpha}} = \frac{1}{\zeta(\alpha)}$$

Dimostrazione.

$$\left(\sum_{n=1}^{\infty} \frac{\mu(n)}{n^{\alpha}}\right) \zeta(\alpha) = \left(\sum_{n=1}^{\infty} \frac{\mu(n)}{n^{\alpha}}\right) \left(\sum_{n=1}^{\infty} \frac{1}{n^{\alpha}}\right) = \sum_{n=1}^{\infty} \frac{\varepsilon(n)}{n^{\alpha}} = 1$$

$$\text{Perché } \varepsilon(n) = \mu * \mathbb{1}(n) = \begin{cases} 1 & se\ n = 1 \\ 0 & altrimenti \end{cases}$$

□

Ricordando che $\mathbb{P}'$ è l'insieme degli interi che non hanno divisori quadrati maggiori di 1, detti numeri di Möbius possiamo dimostrare questo interessante risultato:

Proposizione 19. *Il numero $\pi'(x)$ di elementi di $\mathbb{P}'$ inferiori o uguale ad x verifica*

$$\pi'(x) = \sum_{k \leq x} |\mu(k)| \sim \frac{x}{\zeta(2)} = \frac{6x}{\pi^2}$$

Dimostrazione.

$$\text{Per tutti gli interi } k \geq 1 \text{ denotiamo con } \eta(k) = \max\{n | n^2 \text{ divide } k\} \leq \sqrt{k}$$

$$\text{Allora } \lfloor x \rfloor = \text{card}\{k | k \leq x\} = \sum_{n \leq \sqrt{x}} \text{card}\{k | k \leq x \quad e \quad \eta(k) = n\}$$

$$\sum_{n\le\sqrt{x}} \mathsf{card}\{p'n^2 | p'n^2 \le x \quad e \quad p' \in \mathbb{P}'\} = \sum_{n\le\sqrt{x}} \pi'\left(\frac{x}{n^2}\right) \tag{3.1}$$

Definiamo una nuova μ coppia di funzioni $(f, \tilde{f})$ ponendo $f(x) = \pi'(x^2)$

$$\text{Allora } \tilde{f}(\sqrt{x}) = \sum_{n\le\sqrt{x}} f\left(\frac{\sqrt{x}}{n}\right) = \sum_{n\le\sqrt{x}} \pi'\left(\frac{x}{n^2}\right) = \lfloor x \rfloor, \text{ Quindi } \tilde{f}(x) = \lfloor x^2 \rfloor$$

$$\text{Allora } \pi'(x^2) = f(x) = \mu * \tilde{f}(x) = \sum_{k\le x} \mu(k) \left\lfloor \frac{x^2}{k^2} \right\rfloor = \sum_{k\le x} \mu(k) \frac{x^2}{k^2} - \sum_{k\le x} \mu(k) \left\{ \frac{x^2}{k^2} \right\}$$

$$= \sum_{k=1}^{\infty} \mu(k) \frac{x^2}{k^2} - \sum_{k\le x} \mu(k) \frac{x^2}{k^2} - \sum_{k\le x} \mu(k) \left\{ \frac{x^2}{k^2} \right\} \sim x^2 \sum_{k=1}^{\infty} \frac{\mu(k)}{k^2} = \frac{x^2}{\zeta(2)}$$

$$\text{Perché } \left| \sum_{k>x} \frac{\mu(k)}{k^2} \right| \le \sum_{k>x} \frac{1}{k^2} \le \sum_{k>x} \int_{k-1}^{k} \frac{dt}{t^2} = \int_{\lfloor x \rfloor}^{\infty} \frac{dt}{t^2} = \frac{1}{\lfloor x \rfloor}$$

$$\text{e } \left| \sum_{k\le x} \mu(k) \left\{ \frac{x^2}{k^2} \right\} \right| \le \sum_{k\le x} 1 = \lfloor x \rfloor.$$

Allora si deduce che $\pi'(x) \sim \frac{x}{\zeta(2)}$ e si ritrova la tesi perché $\zeta(2) = \frac{\pi^2}{6}$ $\square$

3.2 La dimostrazione di Hadamard e de La Vallée Poussin

Nel 1896 Hadamard e De la Vallée Poussin, indipendentemente l'uno dall'altro, furono i primi a fornire la dimostrazione del Teorema dei Numeri Primi. Entrambi utilizzarono metodi dalla teoria delle funzioni complesse e più specificamente legati alle proprietà della funzione ζ di Riemann. Anche le successive dimostrazioni (Landau), più semplici rispetto a quella di Hadamard, erano comunque basate sul comportamento della funzione di Riemann $\zeta(s)$ sul piano complesso. I numerosi tentativi di dimostrarlo non basandosi sull'analisi complessa erano andati a vuoto, tanto che nel 1930 si era diffusa la convinzione che il Teorema dei Numeri Primi fosse equivalente al teorema "$\zeta(s)$ è una funzione olomorfa e non si annulla sulla retta $Re(s) = 1$", perché era possibile dimostrare l'uno come conseguenza dell'altro e viceversa. Soltanto nel 1949 questa conclusione euristica fu smentita dalle dimostrazioni elementari di Erdös e Selberg.
Le dimostrazioni del Teorema dei Numeri Primi basate sull'analisi complessa si basano tutte sulla possibilità di esprimere l'andamento delle funzioni definite nel paragrafo (1.4) utilizzando integrali sul piano complesso che coinvolgono la funzione ζ di Riemann.
Ad esempio volendo dimostrare il Teorema dei Numeri Primi nella forma

$$\psi(x) \sim x \text{ per } x \to \infty$$

si può passare alla funzione $\psi_1(x) \sim \frac{1}{2}x^2 \quad x \to \infty$

$$\psi_1(x) = \int_1^x \psi(t)dt$$

che in qualche modo regolarizza le discontinuità di $\psi(x)$ e permette di scambiare operazioni di limite in modo più agevole. La funzione $\psi_1(x)$ può essere messa in relazione con la funzione ζ di Riemann utilizzando il lemma di Abel per $Re(s) > 1$ e integrando ulteriormente per parti:

$$Z(s) = -\frac{\zeta'(s)}{\zeta(s)} = s\int_1^\infty \frac{\psi(t)}{t^{s+1}}dt = s(s+1)\int_1^\infty \frac{\psi_1(t)}{t^{s+2}}dt \tag{3.2}$$

Invertendo la relazione 3.2 si ottiene

$$\frac{\psi_1(x)}{x^2} = \frac{1}{2\imath\pi}\int_{c-\imath\infty}^{c+\imath\infty} \frac{Z(s)x^{s-1}}{s(s+1)}ds \tag{3.3}$$

con c un qualsiasi numero reale maggiore di 1 fissato. Per dimostrare il Teorema dei Numeri Primi quindi occorre mostrare che per x che tende ad infinito l'integrale nel piano complesso che compare nell'equazione 3.3 tende a $\pi\imath$. Quindi l'andamento asintotico della funzione $\psi_1(x)$ può essere trattato con tecniche di analisi complessa, in particolare utilizzando il teorema dei residui di Cauchy con una opportuna curva semplice chiusa. La difficoltà di queste dimostrazioni risiede nella complessità della funzione ζ di Riemann, in particolare sulla presenza di zeri della funzione $\zeta(s)$ sul percorso di integrazione. Sfortunatamente a tutt'oggi l'ipotesi di Riemann che $\zeta(s)$ non si annulla nel semipiano $Re(s) > \frac{1}{2}$ è uno dei più famosi problemi non ancora risolti in matematica. Di conseguenza è stato necessario scegliere percorsi di integrazione non semplici e la dimostrazione diventa tecnicamente complessa.

3.3 La dimostrazione di Erdös e Selberg

Nel 1949 Erdös e Selberg indipendentemente pubblicano una prova elementare del Teorema dei numeri primi. A differenza della dimostrazione descritta nel capitolo precedente il punto di partenza per entrambi era la relazione:

$$\sum_{p \le x}(\log^2(p) + \sum_{p_1 p_2 \le x} \log(p_1)\log(p_2) = 2x\log(x) + O(x) \tag{3.4}$$

nota come diseguaglianza di Selberg, da cui arrivano a dedurre, usando diverse tecniche elementari (ma con una derivazione tecnicamente molto complessa), l'andamento asintotico della funzione

$$\theta(x) = \sum_{p \le x} \log(p) \sim x$$

che è equivalente al Teorema dei Numeri Primi, come dimostrato nel Teorema 5

Capitolo 4

Conclusioni

Lo studio dei numeri primi ha sempre affascinato i matematici: tra i problemi più celebri il Teorema dei Numeri Primi è tra i pochissimi ad avere un enunciato relativamente semplice, tuttavia si è rivelato estremamente difficile da risolvere. Grandi difficoltà sono riscontrate nel risolvere in maniera elementare questo problema, che dal '700 in poi è stato affrontato dai migliori matematici dell'epoca come Eulero, Legendre e Gauss. Per superare questi ostacoli Riemann ha introdotto la sua funzione $\zeta(s)$, considerando per la prima volta la variabile s nel piano complesso. Il tentativo di risolvere questo teorema è stato dunque il catalizzatore per lo sviluppo di teorie di analisi complessa, come anche le serie di Dirichlet, utilizzate in seguito da Hadamard e De la Vallée Poussin nelle loro dimostrazioni del 1896. Infine quando ormai si credeva impossibile Erdös e Selberg hanno trovato una strada elementare per la risoluzione del problema e questo ha riaperto l'interesse sul teorema dei numeri primi e ha dato nuovo stimolo alla ricerca di nuovi metodi elementari per affrontare congetture ancora aperte in Teoria dei Numeri. In questo lavoro di tesi ho presentato una dimostrazione elementare del Teorema dei Numeri Primi, adattando l'approccio iniziale di William Ellison, riformulato da Ghislain Dupont cercando di utilizzare in maniera più esplicita la proprietà di convoluzione delle funzione aritmetiche per semplificare i calcoli.

Bibliografia

[1] Michèle Audin. *Jacques Hadamard et le théorème des nombres premiers*. 2013. URL: http://images.math.cnrs.fr/Jacques-Hadamard-et-le-theoreme.html.

[2] Chris K. Caldwell. *How Many Primes Are There?* URL: https://primes.utm.edu/howmany.html.

[3] Fabrizio Caselli. *Lezioni di aritmetica, dispense*. 2013.

[4] Ghislain Dupont. *Le théorème des nombres premiers*. 2008. URL: http://perso.univ-lemans.fr/~dupont/Maths/TNP.pdf.

[5] William Ellison e Fern Ellison. *Prime Numbers*. Hermann, Paris, 1985.

[6] P Erdős. «Démonstration élémentaire du théorème sur la distribution des nombres premiers». In: *Scriptum 1, Centre Mathématique, Amsterdam* (1949).

[7] Jack Hadamard. «Sur la distribution des zéros de la fonction $\zeta(s)$ et ses conséquences arithmétiques». In: *Bull. Soc. math. France* 24 (1896), pp. 199–220.

[8] David E. Joyce. *Euclid's Elements. Book IX, Proposition 20*. URL: http://aleph0.clarku.edu/~djoyce/java/elements/bookIX/propIX20.html.

[9] Melvyn B. Nathanson. *Elementary Methods in Number Theory*. Springer, New York, 2000.

[10] A Selberg. «An Elementary Proof of the Prime Number Theorem». In: *Ann. Math.* 50 (1949), pp. 305–313.

[11] C.-J de la Vallée Poussin. «Recherches analytiques la théorie des nombres premiers». In: *Ann. Soc. scient. Bruxelles* 20 (1896), pp. 183–256.

[12] Eric W. Weisstein. *Prime Number Theorem*. From MathWorld–A Wolfram Web Resource. URL: http://mathworld.wolfram.com/PrimeNumberTheorem.html.

Appendice A

```
def primos(n):
    k=0
    for i in range(2,int(n**(0.5))+1):
        r=n%i
        if(r==0):
            k=1
    return(k==0)


def primes(n):
    x=[]
    k=0
    for i in range(2,n):
        if primos(i):
            x.append(i)
            k=k+1
    return(k,x)

def plotta(m):
    import matplotlib.pyplot as plt
    import mpmath as mp
    (k,x)=primes(m)
    j=[]
    y=[]
    z=[]
    w=[]
    plt.hist(x,bins=100)
    plt.grid(True)
```

```
plt.show()
for i in range(0,k):
    j.append(i+1)
    y.append((i+1)/x[i])
    z.append(1./mp.log(x[i]))
    w.append(1./(mp.log(x[i])-1))
plt.vlines(x,[0],y)
plt.plot(x,w,'r', linewidth=3)
plt.plot(x,z,'g', linewidth=3)
plt.plot(x,y,'b', linewidth=3)
plt.show()
y1=[]
z1=[]
w1=[]
for i in range(0,k):
    y1.append(i+1)
    z1.append(mp.li(x[i]))
    w1.append(x[i]/mp.log(x[i]))
plt.vlines(x,[0],y1)
plt.plot(x,w1,'r', linewidth=3)
plt.plot(x,z1,'g', linewidth=3)
plt.plot(x,y1,'b', linewidth=3)
plt.show()
```