Alma Mater Studiorum · Università di Bologna

**SCUOLA DI SCIENZE**
**Corso di Laurea in Matematica**

# LA DISTRIBUZIONE DEI NUMERI PRIMI

**Tesi di Laurea in Matematica**

**Relatore:**
**Chiar.mo Prof.**
**PIERO PLAZZI**

**Presentata da:**
**FRANCESCO DIOMEI**

**Sessione Unica**
**Anno Accademico 2018-2019**

# Indice

# Introduzione

<<La Matematica è la regina delle scienze e la Teoria dei Numeri è la regina della Matematica>>

Questa è l'ormai celebre frase che Gauss utilizzò per esplicare in maniera sintetica il ruolo della Teoria dei Numeri all'interno della Matematica.
La Teoria dei Numeri nasce intrinsecamente con la Matematica in quanto studia le proprietà e le caratteristiche dei primi numeri utilizzati, i numeri naturali, e delle prime operazioni ad essi collegate, come l'addizione e la moltiplicazione.
Nonostante parta da studi molto semplici ed elementari, la Teoria dei Numeri sconfina poi in studi molto avanzati coinvolgendo l'Algebra, l'Analisi Reale fino all'Analisi Complessa. Al suo interno contiene problemi apparentemente semplici ma che, dopo molto tempo e lavoro di illustri matematici, ancora risultano irrisolti.
La sua importanza non è legata solamente ad aspetti teorici ma anche ad aspetti molto pratici ed attuali in quanto, per esempio, si trova alla base dell'attuale sicurezza informatica, cioè la crittografia.

Qui, in particolar modo, andremo ad analizzare il problema dei numeri primi e della loro distribuzione $\pi(x)$.
Hardy e Wright strutturano il loro testo "An introduction to the theory of numbers", testo fondamentale per chi si voglia addentrare nella questione, sul ricercare la risposta alle seguenti domande:

- C'è una formula semplice e generale per l'$n$-esimo numero primo $p_n$?
- C'è una formula generale per il primo $p_{n+1}$ che segue un dato primo $p_n$?
- C'è una legge per cui, dato un primo $p$, noi possiamo trovare un primo più grande $q$?
- Quanti sono i primi minori di un dato numero $x$?

Si può dire che i numeri primi stiano alla teoria dei numeri come la teoria dei numeri sta alla matematica.

Da tempo i matematici si sono adoperati cercando di dare loro una struttura, una legge che possa comprendere, nella maniera più precisa, la loro comparsa. La difficoltà di base per lo studio dei numeri primi è che sembra che essi compaiano in maniera casuale o che comunque non abbiano un ordine preciso e stabilito, per questo motivo si è affrontata la questione sotto diversi aspetti ed utilizzando risultati di ogni branchia della matematica.

Qui partiremo,ovviamente, dalla definizione di numero primo e dalla fattorizzazione di tutti gli interi in numeri primi. Poi vedremo la celebre dimostrazione di Euclide sull'infinità dei numeri primi e alcuni teoremi sull'esistenza di infiniti numeri primi con forma definita. In seguito daremo delle prime stime di $\pi(x)$ e $p_n$ e alcuni algoritmi in grado di determinare quando un dato numero è primo o meno, cioè stabilirne la primalità.

Attraverso la relazione d'equivalenza della congruenza si avrà modo di avere altri test sulla verifica della primalità e di avere una formula per $\pi(x)$ e $p_n$ anche se purtroppo difficilmente utilizzabile visto il numero di calcoli da svolgere.

Poi vedremo dei particolari tipi di numeri, i numeri di Fermat e di Marsenne, su cui si è congetturato potessero avere un'infinita quantità di primi. Altre congetture sono quelle che riguardano la differenza tra numeri primi consecutivi, come quella sui primi gemelli, e che riguardano la somma di numeri primi, cioè la congettura di Goldbach.

Nel secondo capitolo si parlerà di un insieme di funzioni fondamentali per lo studio della distribuzione dei numeri primi: le funzioni aritmetiche e, tra queste, le funzioni moltiplicative. Ne daremo la definizione e ne vedremo le proprietà, sopratutto legate a come si comporta con il prodotto di Dirichlet. Poi vedremo le proprietà delle specifiche funzioni aritmetiche: la funzione di Möbius $\mu$ con le sue formule di inversione; la funzione $\phi$ di Eulero che conta i numeri minori di un numero primi con esso; la funzione sul numero di divisori $d$ e la funzione sulla somma dei divisori $\sigma$; la funzione $\Lambda$ di von Mangoldt.

Infine nell'ultimo capitolo si affronterà il problema da un punto di vista asintotico, cioè cercare di comprendere come si comportano i numeri primi, e le funzioni ad essi associate, per valori molto grandi di $n$ o $x$. Inizieremo vedendo alcune stime delle funzioni aritmetiche già viste, poi, parleremo di uno dei maggiori risultati sui numeri primi, cioè il teorema dei numeri primi. In riferimento a questo teorema vedremo i teoremi Tschebyscheff, risultati fondamentali per la dimostrazione del teorema dei numeri primi. Si osserveranno le conseguenze di questi teoremi e le stime su di essi. Inoltre vedremo come questi teoremi portarono alla dimostrazione del teorema dei numeri primi Poi introdurremo la funzione zeta di Riemann e come essa si collega alla distribuzione dei numeri primi e alle funzioni aritmetiche già incontrate. Infine vedremo la famosa ipotesi di Riemann e le conseguenze che essa ha sui numeri primi e sulle funzioni aritmetiche, osservando pure delle formulazioni equivalenti dell'ipotesi di Riemann, come per esempio il teorema di Robin.

Alcune dimostrazioni, data la lunghezza e la complessità, saranno omesse. Per un maggiore approfondimento si rimanda alla bibliografia.

# Capitolo 1

# Risultati preliminari

## 1.1 Definizione e fattorizzazione

*Notazione.* Indichiamo con il simbolo $(n, m)$ il Massimo Comune Divisore di $n$ e $m$, $(n, m)$ è considerato positivo.
Indichiamo con il simbolo $d|n$ quando $d$ divide $n$.
Indichiamo con il simbolo $\mathbb{N}$ l'insieme dei numeri interi, positivi e maggiori di 0.

**Teorema 1.1.1** (Euclide)**.** *Dati n,m* $\in \mathbb{Z}$ *non entrambi nulli, siano*
$\mathcal{A}(n, m) := \{an + bn : a, b \in \mathbb{Z}\}$ *e* $d := (n, m)$.
*Allora* $\mathcal{A} = d\mathbb{Z}$ *è l'insieme dei multipli di d, e dunque esistono* $\lambda, \mu \in \mathbb{Z}$ *tali che*

$$d = \lambda n + \mu m$$

*Dimostrazione.* É ovvio che $d$ divide ogni elemento di $\mathcal{A}$.
Sia $\delta = \lambda n + \mu m$ il minimo elemento positivo di $\mathcal{A}$ (che esiste perché almeno uno tra $n$ e $m$ non è nullo).
Poiché $d|\delta$ resta da dimostrare che $\delta|d$.
Consideriamo il resto $r$ della divisione euclidea di $n$ per $\delta$ (cioè l'intero $r$ tale che $0 \leq r < \delta$ ed inoltre esiste $q \in \mathbb{Z}$ tale che $n = q\delta + r$).
É chiaro che $r \in \mathcal{A}$, poiché $r = (1 - \lambda q)n - \mu q m$, e dunque $r = 0$ (poiché altrimenti esisterebbe un elemento positivo di $\mathcal{A}$ strettamente minore di $\delta$), cioè $\delta|d$.
Analogamente $\delta|m$, e quindi $\delta|d$. □

**Definizione 1.1.2** (Numero primo)**.** *Un numero intero* $n \geq 2$ *si dice primo se* $d|n$ *implica* $d = 1$ *oppure* $d = n$.
*Se invece n non è primo allora si dice composto.*

*Notazione.* D'ora in poi ogni qual volta useremo la lettera $p$ intenderemo un numero primo.

**Corollario 1.1.3** (Euclide)**.** *Se $p$ è un numero primo e $p|ab$, allora $p|a$ oppure $p|b$.*

*Dimostrazione.* Se $p \not| a$ allora $(a, p) = 1$, per il teorema di Euclide, esistono $\lambda$ e $\mu$ tali che $\lambda p + \mu a = 1$.
Moltiplichiamo questa uguaglianza per $b$ ed otteniamo $\lambda pb + \mu ab = b$.
Poiché $p$ ne divide il primo membro, deve dividere anche il secondo. □

**Definizione 1.1.4** (Fattorizzazione canonica)**.** *Dato $n \in \mathbb{N}$ chiamiamo fattorizzazione canonica di $n$ la decomposizione*

$$n = \prod_{i=1}^{k} p_i^{\alpha_i}$$

*dove $p_i < p_j$ se $i < j$, $\alpha_i \in \mathbb{N}$ per $i = 1, \ldots, k$.*

**Teorema 1.1.5** (Fattorizzazione unica: Teorema Fondamentale dell'Aritmetica)**.** *Ogni $n \in \mathbb{N}$ ha un'unica fattorizzazione canonica.*

*Dimostrazione.* Sia $n \geq 2$ il più piccolo numero naturale con due fattorizzazione canoniche diverse

$$n = \prod_{i=1}^{k} p_i^{\alpha_i} = \prod_{j=1}^{l} q_j^{\beta_j}$$

con le convenzioni della fattorizzazione canonica, in particolar modo con $p_i$ e $q_j$ primi.
Per il corollario di Euclide se $p_1|n$ allora $p_1$ è uno dei primi $q_j$, ed analogamente $q_1$ è uno dei primi $q_j$ e dunque $p_1 = q_1$ (poiché entrambi sono uguali al più piccolo fattore primo di $n$).
Quindi anche il numero $n/p_1 = n/q_1 < n$ ha due fattorizzazione canoniche distinte, contro la minimalità di $n$. □

**Corollario 1.1.6.** *Il minimo divisore positivo $d > 1$ di un intero $n > 1$ è primo.*

**Corollario 1.1.7.** *Se $n > 2$ è un numero composto, allora $n$ ha un divisore $p$ primo tale che $p \leq \sqrt{n}$.*

**Teorema 1.1.8** (Euclide)**.** *Esistono infiniti numeri primi.*

*Dimostrazione.* Sia $\mathcal{P} = \{p_1, \ldots, p_n\}$ un'insieme finito non vuoto di numeri primi.
Il numero $N := p_1 \cdots p_n + 1 > 1$ non è divisibile per alcuno dei primi $p \in \mathcal{P}$ quindi o è primo o è divisibile per qualche altro primo. □

Il metodo dimostrativo utilizzato è chiamato argomento di Euclide.

### 1.1.1 Forme particolari di primi

In questa sezione faremo riferimento ai risultati trovati in [10](Cap. 2; §2.3-2.7).

Lucas usando delle varianti dell'argomento di Euclide riuscì a dimostrare diversi teoremi che mostrano come ci siano infiniti primi di particolari forme:

**Teorema 1.1.9.** *Ci sono infiniti primi $p$ nella forma $p = 4n + 3$, con $n \in \mathbb{N}$.*

*Dimostrazione.* Siano $2, 3, \ldots, p$ i numeri primi fino a $p$ e sia $N = 2^2 \cdot 3 \cdots p - 1$, allora $N$ è della forma $4n + 3$ e non è divisibile per nessun primo minore di $p$.
Non può essere un prodotto solo di numeri primi della forma $4n + 1$ quindi è divisibile per un primo $4n + 3$ più grande di $p$. □

In maniera simile si dimostrano i seguenti teoremi: [10](Theorem 12-14)

**Teorema 1.1.10.** *Ci sono infiniti primi $p$ nella forma $p = 6n + 5$, con $n \in \mathbb{N}$.*

**Teorema 1.1.11.** *Siano $a, b$ tali che $(a, b) = 1$, allora esiste un primo dispari $p$ tale che $p|a^2 + b^2$ ed è nella forma $p = 4n + 1$, con $n \in \mathbb{N}$.*

**Teorema 1.1.12.** *Ci sono infiniti primi $p$ nella forma $p = 8n + 5$, con $n \in \mathbb{N}$.*

Questi sono tutti casi particolari del teorema: [10](Theorem 15)

**Teorema 1.1.13** (Teorema di Dirichlet)**.** *Siano $a, b$ tali che $(a, b) = 1$, allora esistono infiniti numeri primi $p$ nella forma $p = an + b$, per qualche $n \in \mathbb{N}$.*

In questa maniera si è dimostrata l'esistenza di infiniti primi di una particolare forma ma questo risultato non è sufficiente per trovare una formula che ci generi infiniti numeri primi, infatti Goldbach, nel 1752, dimostrò che:

**Teorema 1.1.14.** *Non esiste alcun polinomio $f(n)$, non costante ed a coefficienti in $\mathbb{Z}$, tale che assuma come valore un numero primo $p$ per ogni $n \in \mathbb{N}$, o per $n$ sufficientemente grande.*

*Dimostrazione.* Prendiamo $f(n) = a_k n^k + \ldots + a_0$ con $a_k > 0$, così $\lim_{n\to+\infty} f(n) = +\infty$, e $f(n) > 1$ per $n > N$. Se $x > N$ e

$$f(x) = a_k x^k + \ldots + a_0 = y > 1$$

allora

$$f(ry + x) = a_k(ry + x)^k + \ldots + a_0$$

è divisibile per $y$ per ogni $r \in \mathbb{Z}$, e $\lim_{r\to+\infty} f(ry + x) = +\infty$. Quindi ci sono infiniti valori composti di $f(n)$. □

I primi di Fermat e di Marsenne saranno esposti nella sottosezione 1.4.1.

## 1.2 Primi risultati su $\pi(x)$ e $p_n$

In questa sezione faremo riferimento ai risultati trovati in [10](Cap. 1; §1.5; Cap. 2; §2.1, §2.2, §2.6).

**Definizione 1.2.1** (Ennesimo numero primo)**.** *Sia $n \in \mathbb{N}$ definisco $p_n$ come l'n-esimo numero primo.*
*Si considerano i primi numeri primi: $p_1 = 2, p_2 = 3, \ldots$.*

**Definizione 1.2.2** (Funzione $\pi(x)$)**.** *Sia $x \geq 1$*

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

*Osservazione.* Questa funzione è ovviamente crescente, tendente a $+\infty$ e, localmente, risulta costante fino a che, al crescere di $x$, si incontri un nuovo numero primo.
Se consideriamo la grandezza $\frac{\pi(n)}{n}$, questa misura la probabilità di estrarre un numero primo tra i primi $n$ numeri.
Ovviamente si ha che $\pi(p_n) = n$.

*Osservazione.* Il teorema sull'infinità dei numeri primi è equivalente a dire che $\lim_{x \to +\infty} \pi(x) = +\infty$.

**Corollario 1.2.3.** *Sia $p_n$ l'n-esimo numero primo. Si ha $p_n < 2^{2^n}$.*

*Dimostrazione.* Dimostriamo per induzione.
Per $n = 1$ è ovvio.
Supponiamo $p_n < 2^{2^n}$ per $n = 1, 2, \ldots, N$. Allora per l'argomento di Euclide

$$p_{N+1} \leq p_1 p_2 \ldots p_N < 2^{2+4+\ldots+2^N} + 1 < 2^{2^{N+1}}$$

□

**Corollario 1.2.4.** *Per $x \geq 2$*

$$\pi(x) \geq \log\log x$$

*Dimostrazione.* Dimostriamo per casi.
Per $x > e^{e^3}$ e $n \geq 4$ prendiamo $x$ tale che $e^{e^{n-1}} < x \leq e^{e^n}$ e quindi $\log\log x \geq n$.
Da $e^{e^{n-1}} > 2^{2^n}$ e dal corollario precedente

$$\pi(x) \geq \pi(e^{e^{n-1}}) > \pi(2^{2^n}) \geq n$$

Quindi $\pi(x) \geq \log\log x$ per $x > e^{e^3}$.
É semplice mostrare che vale pure per $2 \leq x \leq e^{e^3}$. □

**Definizione 1.2.5.** *Dato un $j \in \mathbb{N}$ e siano $\{2, 3, \ldots, p_j\}$ i primi $j$ numeri primi. Allora definisco la funzione $N_j(x)$ con $x$ appartenente ai numeri naturali, come la funzione che ad $x$ restituisce il numero di numeri naturali minori o uguali di $x$ non divisibili per qualche primo $p_k$ con $k > j$, cioè*

$$N_j(x) = |\{n \in \mathbb{N}; n \leq x, p \not| n \quad \forall p > p_j\}|$$

*Osservazione.* Sia $p_j$ il $j$-esimo numero primo, allora $N_j(x) = x$ per ogni $x$ minore di $p_{j+1}$ in quanto, ovviamente, tutti i numeri naturali minori di $p_{j+1}$ non possono essere divisibili per qualche primo maggiore o uguale di $p_{j+1}$.
Invece $N_j(p_{j+1}) = p_{j+1} - 1$.

**Lemma 1.2.6.** *Sia $x \in \mathbb{N}$, allora*

$$N_j(x) \leq 2^j \sqrt{x}$$

*Dimostrazione.* Scriviamo $n$ nella forma $n = n_1^2 m$ dove $m$ non è divisibile per nessun quadrato di un primo, quindi $m = 2^{b_1} 3^{b_2} \ldots p_j^{b_j}$ con ogni $b$ uguale a 0 o 1.
Ci sono solo $2^j$ possibili scelte per gli esponenti e non più di $2^j$ diversi possibili valori di $m$, poi $n_1 \leq \sqrt{n} \leq \sqrt{x}$. □

Eulero nel 1737 provò, in una maniera diversa da Euclide, l'infinità dei numeri primi, dimostrando che:

**Teorema 1.2.7** (Eulero)**.** *La serie*

$$\sum \frac{1}{p} = \frac{1}{2} + \frac{1}{3} + \cdots$$

*è divergente.*

*Dimostrazione.* Per assurdo supponiamo la serie convergente, quindi

$$\frac{1}{p_{j+1}} + \frac{1}{p_{j+2}} + \cdots < \frac{1}{2}$$

Il numero di $n \leq x$ divisibili per $p$ è al massimo $x/p$.
Allora per $x - N_j(x)$, il numero di $n \leq x$ divisibile per almeno un $p_{j+1}, p_{j+2}, \ldots$, vale

$$\frac{x}{p_{j+1}} + \frac{x}{p_{j+2}} + \cdots < \frac{1}{2}x$$

Quindi, dal lemma precedente,

$$\frac{1}{2} < N_j(x) \leq 2^j \sqrt{x}$$

per $x < 2^{2j+2}$ ma quindi falsa per $x \geq 2^{2j+2}$. □

**Teorema 1.2.8.** *Per* $x \geq 1$

$$\pi(x) \geq \frac{\log x}{2 \log 2}$$

*e che* $p_n \leq 4^n$.

*Dimostrazione.* Prendiamo $j = \pi(x)$ tale che $p_{j+1} > x$ e $N_j(x) = x$. Abbiamo

$$x = N_j(x) \leq 2^{\pi(x)} \sqrt{x}$$

per $2^{\pi(x)} \geq \sqrt{x}$.
La seconda parte segue da

$$\pi(p_n) = n \geq \frac{\log p_n}{2 \log 2}$$

quindi

$$\log p_n \leq 2n \log 2$$

e perciò $p_n \leq (e^{\log 2})^{2n}$. □

## 1.3 Alcuni algoritmi per la primalità

In questa sezione faremo riferimento ai risultati trovati in [16](Cap. 2; §I).

### 1.3.1 Crivello di Eratostene

Nel terzo secolo a.C. Eratostene creò una procedura per stabilire la primalità di un numero $n$ e allo stesso tempo per stabilire il valore di $\pi(n)$.

La procedura (anche chiamata crivello) si sviluppa nella seguente maniera:

- Il primo passo è elencare tutti i numeri naturali dal 2 al numero $n$ in questione.
- Successivamente eliminare dall'elenco tutti i multipli del primo numero dell'elenco, quindi il 2.
- Ora, con il successivo numero cioè il 3, eliminare nuovamente dall'elenco tutti i multipli di questo.
- Continuare fino ad dover eliminare tutti i multipli del più grande primo minore o uguale di $\sqrt{n}$. Se alla fine $n$ è ancora presente nella lista vuol dire che è primo, se non è presente vuol dire che è composto.
  Tra l'altro se conto tutti i numeri rimasti nella lista ottengo il valore di $\pi(n)$.

### 1.3.2 Algoritmo elementare

L'algoritmo più intuitivo per stabilire la primalità di un numero $n$ si sviluppa nel seguente modo:

- Si divide $n$ per 2. Se la divisione non ha resto allora $n$ è composto. Altrimenti si continua.
- Si divide $n$ per 3. Se la divisione non ha resto allora $n$ è composto. Altrimenti si continua.
- Iterando si continua ogni volta dividendo per il primo successivo a quello utilizzato fino a che non si ha resto nullo o non si raggiunge $\sqrt{n}$.
- Se $n$ non è divisibile per nessun $p \leq \sqrt{n}$ allora è primo, altrimenti è composto.

Purtroppo questi metodi risultano troppo lenti per testare la primalità di numeri con centinaia di cifre come richiede il metodo della crittografia RSA, cioè il metodo utilizzata nella crittografia attuale.

## 1.4 Congruenza

In questa sezione faremo riferimento ai risultati trovati in [16](Cap. 2; §IIA, §IIB, §III; Cap. 3; §I).

Andiamo ora a definire la relazione di congruenza, un concetto fondamentale nello sviluppo della teoria dei numeri.

**Definizione 1.4.1** (Congruenza modulo)**.** *Fissati $a, b \in \mathbb{Z}$ e un numero naturale $m > 1$ tale che $m|(a-b)$.*
*Allora diciamo che $a$ è congruo $a$ $b$ modulo $m$ e scriviamo $a \equiv b \bmod m$.*

*Osservazione.* La relazione di congruenza è una relazione di equivalenza.

Un importante teorema che fornisce una condizione necessaria per la primalità di un numero è:

**Teorema 1.4.2** (Piccolo teorema di Fermat)**.** *Se $p$ è un numero primo, qualunque sia $a \in \mathbb{Z}$ si ha*

$$a^p \equiv a \bmod p$$

*Dimostrazione.* Dimostriamolo per induzione.
Per $a = 1$ è ovvio.
Supponiamo vero per $a$, allora

$$(a+1)^p \equiv a^p + 1 \equiv a + 1 \bmod p$$

□

Da questo teorema Lucas, nel 1876 e nel 1891, sviluppò due test per verificare la primalità di numero:

**Teorema 1.4.3** (Test Lucas 1)**.** *Sia $n > 1$. Se esiste un intero $a > 1$ tale che*

- $a^{n-1} \equiv 1 \bmod n$
- $a^m \not\equiv 1 \bmod n$ *per* $m = 1, 2, \ldots, n-2$

*Allora $n$ è primo.*

*Dimostrazione.* É sufficiente mostrare che per ogni intero $m$, tale che $1 \leq m \leq n$, è primo con $n$, cioè $\phi(n) = n - 1$ dove $\phi(n)$ è la funzione di Eulero, definita nella sezione 2.1, che conta i naturali positivi minori di $n$ e primi con $n$. Per questo scopo è sufficiente mostrare che esiste $a$, $1 \leq a < n$ e primo con $n$, tale che $a \equiv n - 1 \bmod n$. Questo viene dichiarato esattamente nelle ipotesi. □

**Teorema 1.4.4** (Test Lucas 2)**.** *Sia $n > 1$. Se esiste un intero $a > 1$ tale che*

- $a^{n-1} \equiv 1 \bmod n$
- $a^m \not\equiv 1 \bmod n$ *per ogni* $m < n$ *tale che* $m$ *divida* $n - 1$

*Allora $n$ è primo.*

La dimostrazione è la stessa del test di Lucas 1.

*Osservazione.* Difetto di questi test è il fatto che viene richiesta la conoscenza di tutti i fattori di $n - 1$, quindi è facilmente applicabile solo quando $n$ è in qualche forma particolare, per esempio $n = 2^n + 1$ oppure $n = 3 \cdot 2^n + 1$.

Osserviamo ora un altro importante teorema che lega i numeri primi alle congruenze:

**Teorema 1.4.5** (Wilson)**.** *Se $p$ è un numero primo allora si ha*

$$(p-1)! \equiv -1 \bmod p$$

*Dimostrazione.* Per il piccolo teorema di Fermat abbiamo che $x^{p-1} \equiv -1 \bmod p$ per ogni $x \neq 0$.
Ma una congruenza modulo $p$ non può avere più radici del suo grado, quindi

$$x^{p-1} - 1 \equiv (x-1)(x-2)\dots(x-(p-1)) \bmod p$$

Confrontando i termini noti a destra e sinistra $-1 \equiv (-1)^{p-1}(p-1)! = (p-1)! \bmod p$. □

**Corollario 1.4.6.** *Sia $m > 1$, una condizione necessaria e sufficiente affinché $m$ sia primo è*

$$m|(m-1)! + 1$$

Purtroppo questo risultato è di difficile applicazione per la verifica della primalità di un numero, in quanto richiede di calcolare $(m-1)!$, quindi di effettuare $(m-2)$ moltiplicazioni.

**Definizione 1.4.7** (Parte intera e parte decimale)**.** *Sia $x \in \mathbb{R}$, la parte intera di $x$ si definisce come il più grande numero intero minore o uguale di $x$, cioè*

$$[x] := \max\{k \in \mathbb{Z} : k \leq x\}$$

*La parte decimale di $x$ si definisce invece come*

$$\{x\} := x - [x]$$

Nel 1964 Willans, grazie al teorema di Wilson, diede formule per $\pi(x)$ e $p_n$ attraverso le funzioni cos e sin: [16](Cap. 3; §I)

**Teorema 1.4.8.** *Sia $j \in \mathbb{N}$ si definisca*

$$F(j) := \left[\cos^2\left(\pi\frac{(j-1)!+1}{j}\right)\right]$$

*Allora per ogni intero $j > 1$, $F(j) = 1$ quando $j$ è primo, mentre $F(j) = 0$ altrimenti. Anche $F(j) = 1$.*
*Perciò*

$$\pi(n) = -1 + \sum_{j=1}^{n} F(j)$$

**Teorema 1.4.9.** *Sia $j \in \mathbb{N}$ si definisca*

$$H(j) := \frac{\sin^2\left(\frac{((j-1)!)^2}{j}\right)}{\sin^2(\pi/j)}$$

*Allora*

$$\pi(n) = \sum_{j=2}^{n} H(j)$$

*Osservazione.* Dalle formule precedenti si può ricavare che

$$p_n = 1 + \sum_{m=1}^{2^n} \left[ \left( \frac{n}{\sum_{j=1}^{m} F(j)} \right)^{1/n} \right]$$

oppure

$$p_n = 1 + \sum_{m=1}^{2^n} \left[ \left( \frac{n}{1 + \pi(m)} \right)^{1/n} \right]$$

Successivamente Mináč ne diede, anche se mai pubblicata, un'espressione alternativa senza il seno e il coseno. La dimostrazione in seguito è quella data da Ribenboim nel [16](Cap. 3; §I).

**Teorema 1.4.10.** *Sia $n \geq 2$, allora*

$$\pi(n) = \sum_{j=2}^{n} \left[ \frac{(j-1)! + 1}{j} - \left[ \frac{(j-1)!}{j} \right] \right]$$

*Dimostrazione.* Sia $n \neq 4$ composto, allora $n$ divide $(n-1)!$.
Quindi $n$ è uguale al prodotto $n = ab$, con $2 \leq a, b \leq n-1$ e $a \neq b$, oppure a $n = p^2 \neq 4$.
Nel primo caso $n|(n-1)!$, nel secondo $2 < p \leq n-1 = p^2 - 1$, ma $2p \leq p^2 - 1$, quindi $n|2p^2 = p \cdot 2p$ ma a sua volta $2p^2|(n-1)!$.
Per ogni primo $j$, dal teorema di Wilson, $(j-1)! + 1 = kj$, con $k \in \mathbb{N}$. Quindi

$$\left[ \frac{(j-1)! + 1}{j} - \left[ \frac{(j-1)!}{j} \right] \right] = \left[ k - \left[ k - \frac{1}{j} \right] \right] = 1$$

Se $j$ è composto e $j \geq 6$, allora $(j-1)! = kj$. Perciò

$$\left[ \frac{(j-1)! + 1}{j} - \left[ \frac{(j-1)!}{j} \right] \right] = \left[ k + \frac{1}{j} - k \right] = 0$$

Infine, se $j = 4$,

$$\left[ \frac{3! + 1}{4} - \left[ \frac{3!}{4} \right] \right] = 0$$

□

Purtroppo, dato l'elevato numero di calcoli, queste formule risultano di difficile attuazione.

### 1.4.1 Numeri di Fermat e numeri di Marsenne

In questa sezione faremo riferimento ai risultati trovati in [16](Cap. 2; §VI, §VII).

**Teorema 1.4.11.** *Sia $m \in \mathbb{N}$ e $2^m + 1$ un numero primo, allora $m = 2^n$ per qualche $n \in \mathbb{N}$.*

Per la dimostrazione si fa riferimento alla dimostrazione del teorema 1.4.17.

Quindi se un numero $2^m + 1$ è primo allora è un numero di Fermat, infatti i numeri di Fermat sono:

**Definizione 1.4.12** (Numeri di Fermat)**.** *Sia $n \in \mathbb{N}$, definiamo l'n-esimo numero di Fermat come*

$$F_n := 2^{2^n} + 1$$

**Teorema 1.4.13.** *Siano $F_n, F_m$ due numeri di Fermat distinti, allora $(F_n, F_m) = 1$*

*Dimostrazione.* Prendiamo $F_n, F_{n+k}$, con $k > 0$, e m tale che $m|F_n, m|F_{n+k}$.
Se $x = 2^{2^n}$, abbiamo

$$\frac{F_{n+k} - 2}{F_n} = \frac{2^{2^{n+k}} - 1}{2^{2^n} + 1} = \frac{x^{2^k} - 1}{x + 1} = x^{2^k - 1} - x^{2^k - 2} + \ldots - 1$$

e quindi $F_n | F_{n+k} - 2$.
Allora $m|F_{n+k}, m|F_{n+k} - 2$, perciò $m|2$
Ma $F_n$ è dispari, quindi $m = 1$. □

*Osservazione.* Dall'ultimo teorema si nota che ogni numero $F_1, F_2, \ldots, F_n$ è divisibile per un primo dispari che non divide gli altri, quindi ci sono almeno $n$ primi dispari minori di $F_n$ e ciò da un'altra dimostrazione sull'infinità dei numeri primi.
Si noti anche che $p_{n+1} \leq F_n = 2^{2^n} + 1$, che è una stima migliore della precedente trovata.

Fermat riuscì a calcolare fino a $F_4$ ed ognuno di questi valori risultò essere primo per questo ipotizzò che ognuno dei numeri $F_n$ fosse primo.
Questa ipotesi fu smentita da Eulero nel 1732, che calcolò $F_5$ e trovò che esso non era primo.
Da questo risultato Eulero dimostrò, trovando una formula per i divisori, quali numeri di Fermat non fossero primi.

**Teorema 1.4.14** (Eulero)**.** *Ogni numero di Fermat $F_n$ non primo ha un divisore del tipo $k \cdot 2^{n+1} + 1$*

Per la dimostrazione si fa riferimento a quella contenuta in [16](Cap. 2; §VI) dove viene utilizzato il simbolo di Legendre.

Dimostrato che non tutti i numeri di Fermat sono primi, rimane da verificare se esistano o meno infiniti numeri primi tra quelli Fermat e, analogamente, se ne esiste un numero infinito di numeri di Fermat composti.
Al momento gli unici numeri primi di Fermat verificati sono appunto quelli trovati da Fermat, cioè fino a $F_4$.

**Congettura 1.4.15.** *Esistono infiniti numeri di Fermat primi.*

**Congettura 1.4.16.** *Esistono infiniti numeri di Fermat composti.*

Una generalizzazione dei numeri dei Fermat primi è contenuta nel seguente teorema:

**Teorema 1.4.17.** *Se $a \geq 2$ e $a^n + 1$ è primo allora $a$ è pari e $n = 2^m$.*

*Dimostrazione.* Se a è dispari allora $a^n + 1$ è pari; se n ha un fattore dispari k e $n = kl$, allora $a^n + 1$ è divisibile per $a^l + 1$

$$\frac{a^{kl} + 1}{a^l + 1} = a^{(k-1)l} - a^{(k-2)l} + \ldots + 1$$

□

**Teorema 1.4.18.** *Sia $n > 1$ e $a^n - 1$ un numero primo, allora $a = 2$ e $n$ è primo.*

*Dimostrazione.* Se $a > 2$ allora $a - 1 | a^n - 1$; se $a = 2$ e $n = kl$ allora $2^k - 1 | 2^n - 1$ □

Quindi se $a^n - 1$ è un numero primo allora è un numero di Marsenne, i numeri di Marsenne sono:

**Definizione 1.4.19** (Numeri di Marsenne)**.** *Sia $n > 1$, definiamo l'n-esimo numero di Marsenne come*

$$M_n := 2^n - 1$$

Ovviamente se $n$ è un numero composto si verifica facilmente che $M_n$ anch'esso composto.

La particolarità di questi numeri è che, per $n$ primo, spesso assumono valori primi. Spesso ma non sempre quindi, come per i numeri di Fermat, resta da verificare per quali valori di $n$ assumano valori primi e se assumono o meno valori primi infinite volte.

**Congettura 1.4.20.** *Esistono infiniti numeri di Marsenne primi.*

**Congettura 1.4.21.** *Esistono infiniti numeri di Marsenne composti.*

Ora un risultato sui divisori dei numeri di Marsenne, prima congetturato da Eulero nel 1750, poi dimostrato da Lagrange nel 1775 e poi nuovamente da Lucas nel 1878:

**Teorema 1.4.22.** *Sai $q$ un primo tale che $q \equiv 3 \bmod 4$, allora $2q+1 | M_q$ se e solo se $2q+1$ è primo.*

La dimostrazione di questo teorema e dei due successivi sono contenute in [Rib](Cap. 2; Sez. VII) e utilizzano il simbolo di Legendre.

Ora altri due teoremi sui numeri di Marsenne, il primo è sui divisori di questi mentre il secondo è una caratterizzazione dei numeri di Marsenne primi: [16](Cap. 2; §VII)

**Teorema 1.4.23.** *Sia $n \geq 1$ tale che $n | M_q$, allora $n \equiv \pm 1 \bmod 8$ e $n \equiv 1 \bmod q$.*

**Teorema 1.4.24.** *Sia $n \geq 1$, definiamo la successione $(S_n)_{n \geq 0}$ in maniera ricorsiva da $S_0 = 4$ e $S_{k+1} = S_k^2 - 2$, allora $M_n = 2^n - 1$ è primo se e solo se $M_n | S_{n-2}$.*

### 1.4.2 Numeri gemelli e congettura di Goldbach

In questa sezione faremo riferimento ai risultati trovati in [16](Cap. 4; §III, §VI).

**Definizione 1.4.25** (Primi gemelli)**.** *Due numeri $p, p+2$ vengono definiti primi gemelli se entrambi sono primi.*

Nel 1949 Clement ne diede una caratterizzazione:

**Teorema 1.4.26.** *Sia $n \geq 2$. Allora $(n, n+2)$ sono primi gemelli se e solo se*

$$4((n-1)! + 1) + n \equiv 0 \bmod (n(n+2))$$

*Dimostrazione.* Se la congruenza è soddisfatta, con $n \neq 2, 4$ e $(n-1)! + 1 \equiv 0 \bmod n$, dal teorema di Wilson $n$ è primo.
Anche

$$4(n-1)! + 2 \equiv 0 \bmod (n+2)$$

poi moltiplicando per $n(n+1)$

$$4((n+1)! + 1) + 2n^2 + 2n - 4 \equiv 0 \bmod (n+2)$$

$$4((n+1)! + 1) + (n+2)(2n-2) \equiv 0 \bmod (n+2)$$

e per il teorema di Wilson anche $n+2$ è primo.
Viceversa, se $n, n+2$ sono primi, allora $n \neq 2$ e

$$(n-1)! + 1 \equiv 0 \bmod n$$

$$(n+1)! + 1 \equiv 0 \bmod (n+2)$$

Ma $n(n+1) = (n+2)(n-1) + 2$ e $2(n-1)! + 1 = k(n+2)$ con $k$ intero. Da $(n-1) \equiv -1 \bmod n$, poi $2k+1 \equiv 0 \bmod n$ e sostituendo $4(n-1)! + 2 \equiv -(n+2) \bmod (n(n+2))$ si ha $4((n-1)! + 1) + n \equiv 0 \bmod (n(n+2))$. □

Congetture legate a questo tipo di primi sono:

**Congettura 1.4.27.** *Ci sono infinite coppie di numeri primi del tipo* $(p, p+2)$.

**Congettura 1.4.28.** *Ci sono infinite triplette di numeri primi del tipo* $(p, p+2, p+6)$.

**Congettura 1.4.29.** *Ci sono infinite triplette di numeri primi del tipo* $(p, p+4, p+6)$.

Finora nessuna di queste congetture è stata smentita o provata.

Invece è banale dimostrare che:

**Teorema 1.4.30.** *Non esistono triplette di numeri primi del tipo* $(p, p+2, p+4)$ *e del tipo* $(p, p+4, p+8)$.

*Dimostrazione.* Se $p$ è primo allora può essere soltanto $p \equiv 1 \bmod 3$ oppure $p \equiv 2 \bmod 3$, quindi procediamo per casi:
Se $p \equiv 1 \bmod 3$ allora $3|p+2$ e $3|p+8$.
Se invece $p \equiv 2 \bmod 3$ allora $3|p+4$. □

Una generalizzazione della congettura sui numeri primi gemelli è la congettura di Polignac del 1849:

**Congettura 1.4.31.** *Per ogni numero primo* $2k$ *esistono infinite coppie di numeri primi consecutivi* $(p_n, p_{n+1})$ *tali che* $p_{n+1} - p_n = 2k$.

Lucas nel 1891 mostrò che:

**Teorema 1.4.32.** *Per ogni* $N \in \mathbb{N}$ *esiste* $n$ *tale che* $p_{n+1} - p_n > N$, *cioè la differenza fra due numeri primi consecutivi non ha massimo.*

*Dimostrazione.* Sia $N > 1$, esiste sempre una stringa di almeno $N$ numeri composti consecutivi, per esempio

$$(N+1)! + 2, (N+1)! + 3, \ldots, (N+1)! + (N+1)$$

□

In una lettera ad Eulero, nel 1742, Goldbach congetturò che:

**Congettura 1.4.33** (Congettura di Goldbach)**.** *Ogni intero $n > 5$ è somma di tre primi.*

Eulero gli rispose che questo è equivalente a dire che:

**Congettura 1.4.34.** *Ogni intero pari $2n \geq 4$ è somma di due primi.*

*Dimostrazione.* Sia vera la formulazione di Eulero, allora, per $2n \geq 6$, $2n - 2 = p + p'$ e $2n = 2 + p + p'$, poi $2n + 1 = 3 + p + p'$ e quindi si avrebbe vera anche la prima formulazione.
Viceversa, con $2n \geq 4$, $2n+2 = p+p'+p''$ quindi uno dei primi è necessariamente uguale a 2, perciò $2n = p + p'$. □

La congettura è ancora tuttora irrisolta. Tuttavia, nel 1973, Chen provò che: [16](Cap. 4; §VI)

**Teorema 1.4.35** (Chen)**.** *Ogni numero pari $2n$ sufficientemente grande può essere scritto come $2n = p + m$, con $m$ nella forma $m = qr$ con $q$ ed $r$ primi.*

# Capitolo 2

# Funzioni aritmetiche

## 2.1 Definizione e funzioni moltiplicative

In questa sezione faremo riferimento ai risultati trovati in [1](Cap. 5; §5.1, §5.2).

**Definizione 2.1.1** (Funzioni aritmetiche)**.** *Si dice funzione aritmetica una qualsiasi applicazione* $f : \mathbb{N} \to \mathbb{R}$

**Definizione 2.1.2** (Funzione potenza)**.** *Siano* $n \in \mathbb{N}, \beta \in \mathbb{R}$ *definiamo*

$$N_\beta(n) := n^\beta$$

*la funzione potenza di esponente* $\beta$*.*

Ovviamente $N_0$ è la funzione che restituisce 1 per ogni n e $N_1$ è la funzione che restituisce n per ogni n.

**Definizione 2.1.3** (Funzione di Eulero)**.** *Sia* $n \in \mathbb{N}$ *definiamo*

$$\phi(n) := \sum_m 1 \qquad\qquad 1 \leq m < n, (m, n) = 1$$

*la funzione di Eulero che conta gli interi positivi* $m$ *minori di* $n$ *e primi con* $n$*.*

**Definizione 2.1.4** (Funzione potenze $\beta$-esime dei divisori di n)**.** *Siano* $n \in \mathbb{N}, \beta \in \mathbb{R}$ *definiamo*

$$\sigma_\beta(n) := \sum_{d|n} d^\beta$$

$\sigma_\beta$ *è la funzione somma delle potenze di esponente* $\beta$ *dei divisori di* $n$*, compresi 1 ed* $n$*.*

**Definizione 2.1.5** (Funzione numero di divisori)**.** *Sia $n \in \mathbb{N}$ definiamo*

$$d(n) := \sigma_0(n) = \sum_{d|n} 1 = |\{d \in \mathbb{N} : d|n\}| :$$

*è la funzione che conta il numero di divisori di n.*

**Definizione 2.1.6** (Funzione somma dei divisori)**.** *Sia $n \in \mathbb{N}$ definiamo*

$$\sigma(n) := \sigma_1(n) = \sum_{d|n} d$$

**Definizione 2.1.7** (Funzione logaritmo)**.** *Sia $n \in \mathbb{N}$ definiamo*

$$L(n) := \log n$$

*il logaritmo naturale di n.*

**Definizione 2.1.8** (Funzione di von Mangoldt)**.** *Sia $n \in \mathbb{N}$ definiamo*

$$\Lambda(n) := \begin{cases} \log p & \text{se } \exists p, \exists m \in \mathbb{N} : n = p^m \\ 0 & \text{altrimenti} \end{cases}$$

**Definizione 2.1.9** (Funzione I)**.**

$$I(n) := \left[\frac{1}{n}\right] = \begin{cases} 1 & n = 1 \\ 0 & n > 1 \end{cases}$$

*è la funzione caratteristica $\chi\{1\}$.*

**Definizione 2.1.10** (Prodotto di Dirichlet)**.** *Date due funzioni aritmetiche $f, g$ chiamiamo prodotto di Dirichlet di $f$ e $g$ la funzione aritmetica $h$ definita dalla relazione*

$$h(n) := (f * g)(n) := \sum_{d|n} f(d) g\left(\frac{n}{d}\right) = \sum_{d_1 d_2 = n} f(d_1) g(d_2)$$

**Definizione 2.1.11** (Funzioni moltiplicative)**.** *Una funzione aritmetica $f$ si dice moltiplicativa se $f(1) = 1$ e per ogni $n, m \in \mathbb{N}$ con $(n, m) = 1$ si ha $f(nm) = f(n)f(m)$.*
*Se questo vale per ogni $n, m \in \mathbb{N}$, $f$ si dice completamente moltiplicativa.*
*Indicheremo con $\mathcal{M}$ ed $\mathcal{M}^*$ rispettivamente l'insieme delle funzioni moltiplicative e quello delle funzioni completamente moltiplicative.*

*Osservazione.* Per esempio $\phi, d, \sigma_\beta \in \mathcal{M}$, mentre $I, N_\beta \in \mathcal{M}^*$, infine $\Lambda, L$ non sono moltiplicative.

**Teorema 2.1.12.** *Se $f, g \in \mathcal{M}$ allora anche $f * g \in \mathcal{M}$*

*Dimostrazione.* Sia $h = f * g$ e siano $n, m \in \mathbb{N}$ tali che $(n, m) = 1$. Osserviamo che se $d|mn$, sono univocamente determinati $d_1, d_2 \in \mathbb{N}$ tali che $d_1|n, d_2|m$ e $d_1 d_2 = d$.
Inoltre $(d_1, d_2) = 1$. Quindi

$$\begin{aligned} h(nm) &= \sum_{d|mn} f(d) g\left(\frac{nm}{d}\right) = \sum_{d_1|n, d_2|m} f(d_1 d_2) g\left(\frac{n}{d_1} \cdot \frac{m}{d_2}\right) \\ &= \sum_{d_1|n} \sum_{d_2|m} f(d_1) f(d_2) g\left(\frac{n}{d_1}\right) g\left(\frac{m}{d_2}\right) \\ &= \sum_{d_1|n} f(d_1) g\left(\frac{n}{d_1}\right) \sum_{d_2|m} f(d_2) g\left(\frac{m}{d_2}\right) \\ &= h(n) h(m) \end{aligned}$$

□

**Lemma 2.1.13.** *Siano $f \in \mathcal{M}$ e $n \in \mathbb{N}$. Sia $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ la fattorizzazione canonica di $n$ definita in 1.1.4, allora le seguenti relazioni:*

$$f(n) = \prod_{i=1}^{k} f(p_i^{\alpha_i}) \quad e \quad \sum_{d|n} f(d) = \prod_{i=1}^{k} \sum_{j=0}^{\alpha_j} f(p_i^j)$$

*Dimostrazione.* La prima segue immediatamente dalla definizione di molteplicità: nella seconda entrambi i membri sono uguali ad $(f * N_0)(n)$ per il teorema precedente. □

**Teorema 2.1.14.** *L'insieme delle funzioni aritmetiche con l'operazione $*$ è un anello commutativo con identità I. Gli elementi invertibili sono le funzioni aritmetiche $f$ tali che $f(1) \neq 0$, e per queste la funzione inversa (che indicheremo con $f^{-1}$) soddisfa*

$$f^{-1}(1) = \frac{1}{f(1)} \quad f^{-1}(n) = \frac{1}{f(1)} \sum_{d|n, d<n} f\left(\frac{d}{n}\right) f^{-1}(d) \quad \text{per } n > 1$$

*Inoltre per tutte le funzioni $f \in \mathcal{M}$ l'inversa $f^{-1}$ esiste ed è in $\mathcal{M}$*

*Dimostrazione.* La proprietà commutativa ed il fatto che $I$ sia l'identità è immediato per definizione.
Per dimostrare la proprietà associativa, osserviamo che

$$((f * g) * h)(n) = \sum_{d_1 d_2 = n} (f * g)(d_1) h(d_2) = \sum_{d_1 d_2 = n} \left( \sum_{\delta_1 \delta_2 = d_1} f(\delta_1) g(\delta_2) \right) h(d_2) =$$

$$= \sum_{\delta_1 \cdot (n/\delta_1)} f(\delta_1) \left( \sum_{\delta_2 \delta_3 = (n/\delta_1)} g(\delta_2) h(\delta_3) \right) = \sum_{\delta_1 \delta_2 \delta_3 = n} f(\delta_1) g(\delta_2) h(\delta_3) = (f * (g * h))(n)$$

. Ora vogliamo dimostrare che se $f(1) \neq 0$ allora esiste una funzione aritmetica tale che $f * f^{-1} = I$. Quindi se $f$ è moltiplicativa, esiste $f^{-1}$, e per avere $(f * f^{-1})(1)$ deve necessariamente essere $f^{-1}(1) = 1/f(1)$. Supponiamo per induzione che $f^{-1}$ sia univocamente determinata per $1 \leq k < n$ dove $n > 1$: la relazione $(f * f^{-1})(n) = 0 = I(n)$ equivale a

$$\sum_{d|n} f\left(\frac{n}{d}\right) f^{-1}(d) = 0 \text{ cioè } f(1) f^{-1}(n) = - \sum_{d|n, d<n} f\left(\frac{n}{d}\right) f^{-1}(d) \tag{2.1}$$

come si voleva.
Dunque se $f \in \mathcal{M}$ allora $f(1) = f^{-1}(1) = 1$ e quindi $f^{-1}(n) = -\sum_{d|n,d<n} f\left(\frac{n}{d}\right) f^{-1}(d)$.
Dopo aver definito $f^{-1}$ dimostriamo che è moltiplicativa. Scegliamo ora due naturali $m, n$ primi fra loro tali che $nm > 1$, e supponiamo di aver dimostrato che $f^{-1}(ab) = f^{-1}(a) f^{-1}(b)$ per tutti i naturali $a, b$ tali che $(a, b) = 1$ ed $ab < mn$.
Per la (2.1)

$$f^{-1}(nm) = - \sum_{d|mn, d<mn} f\left(\frac{nm}{d}\right) f^{-1}(d) =$$

$$= - \sum_{d_1|n, d_1<n} \sum_{d_2|m, d2<m} f\left(\frac{n}{d_1}\right) f\left(\frac{m}{d_2}\right) f^{-1}(d_1) f^{-1}(d_2) + f^{-1}(n) f^{-1}(m) =$$

$$= - \sum_{d_1|n} f\left(\frac{n}{d_1}\right) f^{-1}(d_1) \sum_{d_2|m} f\left(\frac{m}{d_2}\right) f^{-1}(d_2) + f^{-1}(n) f^{-1}(m) =$$

$$= -I(n) I(m) + f^{-1}(n) f^{-1}(m) = f^{-1}(n) f^{-1}(m)$$

poiché almeno uno fra $n$ e $m$ è $> 1$ e quindi $I(n) I(m) = 0$.
Nella stessa maniera, nel secondo passaggio, dovevano comparire due sommatorie: una con $d_1 < n$ e $d_2 = m$; invece nell'altra $d_1 = 1$, $d_2 < m$. Entrambe risultano 0 per lo stesso motivo di prima. □

## 2.2 Principali proprietà di alcune funzioni aritmetiche

### 2.2.1 Funzione di Möbius

In questa sezione faremo riferimento ai risultati trovati in [10](Cap. 16; §16.3, §16.4).

**Definizione 2.2.1** (Funzione di Möbius)**.** *Sia $n \in \mathbb{N}$, con la fattorizzazione canonica data da*

$$n = \prod_{i=1}^{k} p_i^{\alpha_i}$$

*dove $p_i < p_j$ se $i < j, \alpha_i \in \mathbb{N}$ per $i = 1, \ldots, k$ ed i $p_i$ sono numeri primi.*
*Si dice funzione $\mu$ di Möbius la funzione moltiplicativa $\mu$ definita da*

$$\mu(n) := \begin{cases} 1 & n = 1 \\ (-1)^k & \alpha_i = 1 \ \forall i \in 1, \ldots, k \\ 0 & \textit{altrimenti} \end{cases}$$

**Lemma 2.2.2.** *$\mu(n)$ è moltiplicativa*

*Dimostrazione.* Siano $m, n$ naturali tali che $(m, n) = 1$. Andiamo per casi.
Se $n = 1$, allora

$$\mu(mn) = \mu(m) = \mu(m)\mu(1) = \mu(m)\mu(n)$$

Possiamo ora assumere $m > 1$ e $n > 1$. Poi supponiamo che c'è un primo $p$ tale che $p^2|n$. Allora $p^2|mn$ e quindi

$$\mu(mn) = 0\mu(m) \cdot 0 = \mu(m)\mu(n)$$

Ora assumiamo che entrambi $m$ e $n$ non siano divisibile per il quadrato di qualche primo. Possiamo quindi scrivere $m = p_1 \cdots p_r$ e $n = q_1 \cdots q_s$, dove $p_1, \ldots, p_r$ sono primi distinti e pure $q_1, \ldots, q_s$ lo sono. Da $(m, n)$ deduciamo che $p_i \neq q_j$ per ogni $i$ e $j$. Allora $mn = p_1 \cdots p_r q_1 \cdots q_s$ è un prodotto di primi tutti distinti tra loro, quindi

$$\mu(mn) = (-1)^{rs} = (-1)^r(-1)^s = \mu(m)\mu(n)$$

□

**Teorema 2.2.3.** *$I(n) = \sum_{d|n} \mu(d)$ cioè*
*$\sum_{d|n} \mu(d) = 1$ per $n = 1$ e $\sum_{d|n} \mu(d) = 0$ per $n > 1$*

*Dimostrazione.* Se $k \geq 1$ e $n = p_1^{a_1} \cdots p_k^{a_k}$ abbiamo

$$\sum_{d|n} \mu(d) = 1 + \sum_{i=1}^{k} \mu(p_i) + \sum_{i,j \in \{1,2,\ldots,k\}} \mu(p_i p_j) + \cdots =$$

$$= 1 - k + \binom{k}{2} - \binom{k}{3} + \cdots = (1-1)^k = 0$$

mentre se $n = 1$ allora $\mu(n) = 1$. □

Come conseguenza della dimostrazione precedente si ha anche:

**Corollario 2.2.4.** *Se $n > 1$ e $k$ il numero di fattori primi di $n$, allora*

$$\sum_{d|n} |\mu(d)| = 2^k$$

**Teorema 2.2.5.** *Si ha $N_0 * \mu = I$ cioè $\mu = N_0^{-1}$*

*Dimostrazione.* Per il Lemma 2.1.13. è sufficiente dimostrare che l'uguaglianza desiderata vale quando $n$ è potenza di un numero primo: se $\alpha \geq 1$

$$(N_0 * \mu)(p^\alpha) = \sum_{d|p^\alpha} \mu(d) = \sum_{\beta=0}^{\alpha} \mu(p^\beta) = 1 + \mu(p) = 0$$

poiché tutti gli addendi con $\beta \geq 2$ sono nulli. □

**Corollario 2.2.6.** *Se $f \in \mathcal{M}^*$ allora $f^{-1} = \mu f$*

*Dimostrazione.* Visto che è completamente moltiplicativa, per $\alpha \geq 1$, si ha

$$((\mu f) * f)(p^\alpha) = \sum_{\beta=0}^{\alpha} (\mu f)(p^\beta) f(p^{\alpha-\beta}) = f(1)f(p^\alpha) - f(p)f(p^{\alpha-1}) = 0$$

poiché $f(p)f(p^{\alpha-1}) = f(p^\alpha)$ □

**Teorema 2.2.7.** *Siano $f \in \mathcal{M}$ e $n < 1$, allora*

$$\sum_{d|n} \mu(d) f(d) = \prod_{p|n} (1 - f(p))$$

*Dimostrazione.* Siano $p_1, \ldots, p_r$ i numeri primi distinti che dividono $n$, allora si ha

$$\prod_{p|n} (1 - f(p)) = (1 - f(p_1)) \cdots (1 - f(p_r)) =$$

$$= 1 - f(p_1) - \ldots - f(p_r) + f(p_1)f(p_2) + \ldots + f(p_{r-1})f(p_r) + \ldots + (-1)^r f(p_1) \cdots f(p_r) =$$

$$= 1 - f(p_1) - \ldots - f(p_r) + f(p_1 p_2) + \ldots + f(p_{r-1} p_r) + \ldots + (-1)^r f(p_1 \cdots p_r)$$

che è proprio la sommatoria di sinistra in quanto gli unici divisori di $n$ tali che $\mu(d) \neq 0$, sono quelli che non sono divisibili per un quadrato dei primi $p_1, \ldots, p_r$. □

**Corollario 2.2.8** (Prima formula d'inversione di Möbius)**.** *Se $f$ e $g$ sono funzioni aritmetiche allora $f = g * \mu$ se e solo se $g = f * N_0$*

*Dimostrazione.* Se $f = g * \mu$, moltiplichiamo con * entrambi i membri per $N_0$, ottenendo $f * N_0 = (g * \mu) * N_0 = g * (\mu * N_0) = g * I = g$, e viceversa □

**Teorema 2.2.9** (Seconda formula di inversione di Möbius)**.** *Siano $f, g, h \in \mathcal{M}$, allora*

$$f(x) = \sum_{n|x} h(n) g\left(\frac{x}{n}\right) \qquad \textit{se e solo se} \qquad g(x) = \sum_{n|x} h^{-1}(n) f\left(\frac{x}{n}\right)$$

*Dimostrazione.* $\Rightarrow$)Infatti si ha

$$\sum_{n|x} h^{-1}(n) \sum_{d|(x/n)} h(d) g\left(\frac{x}{nd}\right) = \sum_{m|x} g\left(\frac{x}{m}\right) \sum_{nd|m} h^{-1}(n) h(d) =$$

$$= \sum_{m|x} g\left(\frac{x}{m}\right) I(m) = g(x)$$

L'implicazione inversa si dimostra scambiando $f$ e $g$ □

Attraverso la funzione di Möbius, nel 1971, Gandhi diede una formula per $p_n$: [16](Cap. 3; §I)

**Teorema 2.2.10** (Formula di Gandhi)**.** *Sia $p_n$ l'n-esimo numero primo. Poniamo $P_n := p_1 \cdots p_n$ per $n \geq 1$ e per $n = 0$ $P_0 = 1$, allora si ha*

$$p_{n+1} = \left[ 1 - \log_2 \left( -\frac{1}{2} + \sum_{d|P_n} \frac{\mu(d)}{2^d - 1} \right) \right]$$

*Dimostrazione.* Per $n = 0$ la formula dà $p_1 = 2$. Per $n1$ si ha

$$S_n := \sum_{d|P_n} \frac{\mu(d)}{2^d - 1} = \sum_{k \geq 1} \sum_{d|P_n} \frac{\mu(d)}{2^{kd}} = \sum_{m \geq 1} \frac{1}{2^m} \sum_{d|m, d|P_n} \mu(d) = \sum_{m \geq 1} I((m, P_n))$$

dove $I$ è la funzione Identità applicata al M.C.D. tra $m$ e $P_n$, mentre la prima uguaglianza si ha dal fatto che $\sum_{k \geq 1} \frac{1}{2(kd)} = \frac{1/2^d}{1-(1/2^d)} = \frac{1}{2^d - 1}$.
Ma $(m, P_n) = 1$ se e solo se $m = 1$ oppure tutti i fattori primi di $m$ superano $p_n$. Dunque

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

In particolare se $n \geq 1$

$$\frac{1}{2} + \frac{1}{2^{p_{n+1}}} < S_n < \frac{1}{2} + \frac{1}{2^{p_{n+1}}} (1 + \frac{1}{2} + \frac{1}{2^2} + \cdots = \frac{1}{2} + \frac{2}{2^{p_{n+1}}}$$

Da questo segue che

$$1 - \log_2 \left( S_n - \frac{1}{2} \right) \in (p_{n+1}, p_{n+1} + 1)$$

che implica la tesi. □

### 2.2.2 Funzione $\phi$ di Eulero

In questa sezione faremo riferimento ai risultati trovati in [10](Cap. 5; §5.5; Cap. 16; §16.1, §16.2).

Si è visto che la funzione di Eulero è moltiplicativa: è facile mostrare che $\phi(1) = 1$ e $\phi(p) = p - 1$.
Da questo si ha:

**Corollario 2.2.11.** *Sia* $n \in \mathbb{N}$

$$\limsup_{n\to+\infty} \phi(n) = +\infty \qquad\qquad \limsup_{n\to+\infty} \frac{\phi(n)}{n} = 1$$

**Lemma 2.2.12.** *Siano $N$ oggetti, $\alpha, \beta, \gamma \ldots$ proprietà.*
*Siano $N_\alpha$ gli oggetti con la proprietà $\alpha$, $N_{\alpha,\beta}$ gli oggetti con entrambe le proprietà $\alpha, \beta$, $N_{\alpha\beta\gamma}$ gli oggetti con le proprietà $\alpha, \beta, \gamma$ e così via.*
*Allora il numero di oggetti di $N$ che* **non** *ha le proprietà $\alpha, \beta, \gamma \ldots$ è*

$$N - N_\alpha - N_\beta - \ldots + N_{\alpha\gamma} + \ldots - N_{\alpha\beta\gamma} - \ldots$$

**Corollario 2.2.13.** *Sia $A = \{a, b, \ldots\}$ un insieme di numeri appartenenti a $\mathbb{N}$ e tali che $(a, b) = 1$ per ogni $a, b \in A$. Allora per ogni $n \in \mathbb{N}$*

$$|\{m : m \leq n, (m, a) = 1 \forall a \in A\}| = [n] - \sum_{a\in A} \left[\frac{n}{a}\right] + \sum_{a,b\in A} \left[\frac{n}{ab}\right] - \cdots$$

**Teorema 2.2.14.** *Per ogni $n \in \mathbb{N}$*

$$\frac{\phi(n)}{n} = \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

*Dimostrazione.* Indichiamo con $p, p', \ldots$ i primi che dividono $n$, si ha

$$\phi(n) = n - \sum_p \frac{n}{p} + \sum_{p,p'} \frac{n}{pp'} - \cdots = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

□

**Lemma 2.2.15.** *Per ogni $n \geq 1$ si ha*

$$\sum_{d|n} \phi(d) = n$$

*Dimostrazione.* Nella seguente uguaglianza gli insiemi a destra sono disgiunti e lo è anche quello di sinistra: le frazioni a destra si ottengono da quelle a sinistra riducendole ai minimi termini, e raggruppandole per valori comuni dei denominatori delle frazioni ridotte.

$$\left\{\frac{h}{n} : h \in \{1,\dots,n\}\right\} = \bigcup_{d|n} \left\{\frac{a}{d} : a \in \{1,\dots,d\}, (a,d) = 1\right\}$$

La cardinalità dell'insieme a sinistra è $n$, e quella di ciascun insieme a destra è, per definizione, $\phi(d)$. □

Attraverso la funzione di Eulero è possibile dare una forma più generale del teorema di Fermat:

**Teorema 2.2.16** (Eulero-Fermat)**.** *Siano $a$ e $m$ interi positivi tali che $(a,m) = 1$, allora*

$$a^{\phi(n)} \equiv 1 \bmod n$$

*Dimostrazione.* Siano $r = \phi(n)$ e $b_1,\dots,b_r$ gli interi primi tra loro e tali che $(b_i, n) = 1$ per ogni $i$.
Allora $ab_1,\dots,ab_r$ sono ancora primi tra loro e $(ab_i, n) = 1$ per ogni $i$. Quindi gli insiemi $\{b_1 \bmod n;\dots;b_r \bmod n\}$ e $\{ab_1 \bmod n;\dots;ab_r \bmod n\}$ sono uguali. Perciò

$$a^r \prod_{i=1}^{r} b_i \equiv \prod_{i=1}^{r} a^r b_i \equiv \prod_{i=1}^{r} b_i \bmod n$$

Quindi $(a^r - 1)\prod_{i=1}^{r} b_i \equiv 0 \bmod n$ e $a^r \equiv 1 \bmod n$, da cui la tesi. □

**Teorema 2.2.17.** *Per $n \geq 1$ si ha*

$$\phi(n) = \sum_{d|n} \mu(d)\frac{n}{d}$$

*Dimostrazione.*

$$\phi(n) = n\sum_{d|n} \frac{\mu(d)}{d} = \sum_{d|n} \frac{n}{d}\mu(d)$$

□

Diamo ora due teoremi sull'irregolarità della funzione $\phi$.

Il seguente fu dimostrato da Somayajulu nel 1950: [16](Cap. 2; §II)

**Teorema 2.2.18.** *Sia $n \in \mathbb{N}$*

$$\limsup_{n\to+\infty} \frac{\phi(n+1)}{\phi(n)} = +\infty \qquad \liminf_{n\to+\infty} \frac{\phi(n+1)}{\phi(n)} = 0$$

Poi Sierpinsky e Schinzel nel 1954 elaborarono un risultato più generale: [16](Cap. 2; §II)

**Teorema 2.2.19.** *L'insieme* $\{i : i = \frac{\phi(n+1)}{\phi(n)}, n \in \mathbb{N}\}$ *è denso in* $\mathbb{R}^+$*, dove* $\mathbb{R}^+$ *è l'insieme dei numeri reali positivi.*

### 2.2.3 Funzioni $d(n)$ e $\sigma_k(n)$

In questa sezione faremo riferimento ai risultati trovati in [10](Cap. 16; §16.7, §16.8).

**Teorema 2.2.20.** *Sia* $n \in \mathbb{N}$ *e* $n = p_1^{a_1} p_2^{a_2} \cdots p_l^{a_l}$ *la sua fattorizzazione canonica, allora*

$$d(n) = \prod_{i=1}^{l} (a_i + 1)$$

*Dimostrazione.* I divisori di $n = p_1^{a_1} \cdots p_l^{a_l}$ sono i numeri nella forma $p_1^{b_1} \cdots p_l^{b_l}$ con $0 \leq b_1 \leq a_1, \ldots, 0 \leq b_l \leq a_l$, che sono esattamente $(a_1 + 1) \cdots (a_l + 1)$. □

*Osservazione.* $d(n) = 2$ se e solo se $n$ è primo.

**Teorema 2.2.21.** *Sia* $n \in \mathbb{N}$ *e* $k > 0$*, allora*

$$\sigma_k(n) = \prod_{i=1}^{l} \frac{p_i^{k(\alpha+1)} - 1}{p_i^k - 1}$$

*Dimostrazione.* Se $k > 0$ si ha

$$\sigma_k(n) = \sum_{b_1=0}^{a_1} \sum_{b_2=0}^{a_2} \cdots \sum_{b_l=0}^{a_l} p_1^{b_1 k} p_2^{b_2 k} \cdots p_l^{b_l k} = \prod_{i=1}^{l} (1 + p_i^k + p_i^{2k} + \ldots + p_i^{a_i k})$$

da cui la tesi. □

*Osservazione.* Se $k = 1$ si ha

$$\sigma(n) = \prod_{i=1}^{l} \frac{p_i^{a_i+1} - 1}{p_i - 1}$$

**Definizione 2.2.22** (Numeri Perfetti)**.** *Si dice che* $n$ *è perfetto quando è uguale alla somma dei suoi divisori compreso se stesso, cioè se:*

$$2n = \sigma(n)$$

Al momento si conoscono solo numeri perfetti pari e non si sa se ne esistono o meno di dispari.

Si può dare una caratterizzazione dei numeri perfetti pari:

**Teorema 2.2.23.** *Ogni numero perfetto pari $N$ è nella forma $N = 2^n(2^{n+1} - 1)$, con $2^{n+1} - 1$ primo.*

*Dimostrazione.* $N$ è pari quindi è nella forma $N = 2^n b$ con $n > 0$ e $b$ dispari. Dal teorema 2.2.21. si ha che $\sigma(n)$ è moltiplicativa, e quindi

$$\sigma(n) = (2^n)\sigma(b) = (2^{n+1} - 1)\sigma(b)$$

Ma $N$ è perfetto, perciò $\sigma(N) = 2N = 2^{n+1}b$, e quindi

$$\frac{b}{\sigma(b)} = \frac{2^{n+1} - 1}{2^{n+1}}$$

La frazione a sinistra è ridotta ai minimi termini, allora $b = (2^{n+1} - 1)c$ e $\sigma(b) = 2^{n+1}c$ con $c$ numero intero positivo.
Se $c > 1$, allora $b$ ha come divisori almeno $b, c, 1$, quindi

$$\sigma(b) \geq b + c + 1 = 2^{n+1}c + 1 > 2^{n+1}c = \sigma(b)$$

e si ha una contraddizione. Perciò $c = 1$ e

$$N = 2^n(2^{n+1} - 1) \qquad \sigma(2^{n+1} - 1) = 2^{n+1}$$

Ma, se $2^{n+1} - 1$ non fosse primo, avrebbe più divisori di 1 e se stesso e quindi si avrebbe $\sigma(2^{n+1} - 1) > 2^{n+1}$. Quindi $2^{n+1} - 1$ è primo e si ha la tesi. □

Abbiamo già visto incontrato i numeri nella forma $2^{n+1} - 1$, cioè i numeri di Marsenne.
Allora si può far in modo che la verifica di primalità dei numeri di Marsenne sia equivalente allo studio dei perfetti pari:

**Teorema 2.2.24.** *Per ogni intero positivo $n$, $M_{n+1} = 2^{n+1} - 1$ è primo se e solo se $2^n \cdot M_{n+1}$ è un numero perfetto pari.*

*Dimostrazione.* $\Leftarrow$) L'implicazione da questo verso è il teorema precedente.
$\Rightarrow$) Scriviamo $2^{n+1} - 1 = p$, $N = 2^n p$, allora, dall'osservazione precedente

$$\sigma(N) = (2^{n+1} - 1)(p + 1) = 2^{n+1}(2^{n+1} - 1) = 2N$$

quindi $N$ è perfetto. □

### 2.2.4 Funzione di von Mangoldt $\Lambda$

In questa sezione faremo riferimento ai risultati trovati in [10](Cap. 17; §17.7).

**Lemma 2.2.25.**

$$\sum_{d|n} \Lambda(d) = \log n$$

*Dimostrazione.*

$$\sum_{d|n} \Lambda(d) = \sum_{p^a|n} \log p = \sum_{p|n} a \log p = \log \prod_{p|n} p^a = \log n$$

□

**Lemma 2.2.26.** *Si ha $\Lambda = L * \mu$ o, equivalentemente, $L = \Lambda * N_0$.*

*Dimostrazione.* Le due relazioni sono equivalenti per la prima formula di inversione di Möbius
Inoltre con la fattorizzazione canonica 1.1.4. di $n$ si ha

$$(\Lambda * N_0)(n) = \sum_{i=1}^{k} \sum_{r=1}^{\alpha_i} \log p_i = \sum_{i=1}^{k} \alpha_i \log p_i = \log n$$

poiché $\Lambda$ è diversa da 0 solo sulle potenze di primi. □

**Teorema 2.2.27.** *Si ha $\mu L = -\mu * \Lambda$ o, equivalentemente,*

$$\Lambda(n) = -\sum_{d|n} \mu(d) \log d$$

*Dimostrazione.* Dato che $I(n) \log n = 0$ per ogni $n \in \mathbb{N}$ e che $I(n) = \sum_{d|n} \mu(d)$ dal teorema 2.2.3, si ha

$$\Lambda(n) = \sum_{d|n} \mu(d) \log \frac{n}{d} = \sum_{d|n} \mu(d) \log n - \sum_{d|n} \mu(d) \log d$$

$$= I(n) \log n - \sum_{d|n} \mu(d) \log d$$

□

# Capitolo 3

# Teoria analitica dei numeri

### 3.0.1 Prime stime delle funzioni aritmetiche

In questa sezione si fa riferimento ai risultati trovati in [10](Cap. 18; §18.1-18.4).

*Notazione.* Sia $f(x)$ una funzione in $x$ e $g(x)$ una funzione positiva in $x$, allora, per ogni $x$, scriviamo

- $f(x) = O(g(x))$ se $|f(x)| < Ag(x)$ con $A$ indipendente da $x$.
- $f(x) = o(g(x))$ se $\lim_{x\to+\infty} f(x)/g(x) = 0$.
- $f(x) \sim g(x)$ se $\lim_{x\to+\infty} f(x)/g(x) = 1$.
- $f(x) \lesseqgtr g(x)$ se $C_1 g(x) < f(x) < C_2 g(x)$ con $C_1, C_2$ costanti e $x$ sufficientemente grande.

Notazione ripresa da [10](Cap. 1; §1.6).

**Teorema 3.0.1.** $\liminf_{n\to+\infty} d(n) = 2$

*Dimostrazione.* Basta prendere $n = p$ con $p$ primo e considerare il fatto che i primi sono infiniti. □

**Lemma 3.0.2.** *Sia $f(n) \in \mathcal{M}$ e $\lim_{p^m\to+\infty} f(p^m) = 0$ per ogni primo $p$, allora*

$$\lim_{n\to+\infty} f(n) = 0$$

*Dimostrazione.* Sia $n$ con la fattorizzazione canonica 1.1.4, allora

$$f(n) = f(p_1^{\alpha_1} \cdots p_m^{\alpha_m}) = f(p_1^{\alpha_1)\cdots f(p_m^{\alpha_m})=0}$$

□

**Teorema 3.0.3.** *Sia $n \geq 1$, allora per ogni $\delta > 0$*

$$\lim_{n \to +\infty} \frac{d(n)}{n^\delta} = 0$$

*Dimostrazione.* Sia $f(n) = \frac{d(n)}{n^\delta}$, allora $f(n)$ è moltiplicativa e, dal teorema 2.2.20, si ha

$$f(p^m) = \frac{m+1}{p^{m\delta}} \leq \frac{2m}{p^{m\delta}} = \frac{2 \log p^m}{p^{m\delta} \log p} \leq \frac{2}{\log 2} \frac{\log p^m}{(p^m)^\delta} \to 0$$

quando $p^m \to +\infty$. Quindi $f(n) \to 0$ quando $n \to +\infty$ e si ha la tesi □

**Teorema 3.0.4.** *Sia $n \geq 1$*

$$\sum_{i=1}^{n} d(i) \sim n \log n$$

**Teorema 3.0.5.** *Sia $n \geq 1$*

$$d(n) \sim \log n$$

*Dimostrazione.*

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

che tende a $\log n$ con $n$ che tende a $+\infty$. □

Questi teoremi sono casi particolari del seguente teorema dimostrato da Dirichlet nel 1849:

**Teorema 3.0.6** (Dirichlet)**.** *Sia $n \geq 1$*

$$\sum_{i=1}^{n} d(i) = n \log n + (2\gamma - 1)n + O(\sqrt{n})$$

*dove $\gamma$ è la costante di Eulero definita da:*

$$\gamma := 1 - \int_1^{+\infty} \frac{t - [t]}{t^2} dt = 0,577215665\ldots$$

La dimostrazione è contenuta in [10](Theorem 320).

Nella dimostrazione è utilizzato il teorema 3.0.8 che a sua volta utilizza il seguente lemma:

**Lemma 3.0.7.** *Sia $c_1, c_2, \ldots$ una successione di numeri, e siano $C(t) := \sum_{n \le t} c_n$ e $f(t)$ funzioni in $t$. Allora*

$$\sum_{n \le x} c_n f(n) = \sum_{n \le x-1} C(n)(f(n) - f(n+1)) + C(x)f([x]) \tag{3.1}$$

*Se, in aggiunta, si ha $c_j = 0$ per $j < n_1$ con $n_1$ numero naturale e $f(t)$ ha derivata continua per $t \ge n_1$, allora*

$$\sum_{n \le x} c_n f(n) = C(x)f(x) - \int_{n_1}^{x} C(t)f'(t)dt \tag{3.2}$$

*Dimostrazione.* Se scriviamo $N = [x]$, nella sommatoria di sinistra si ha

$$C(1)f(1) + (C(2) - C(1))f(2) + \ldots + (C(N) - C(N-1))f(N) =$$

$$= C(1)(f(1) - f(2)) + \ldots + C(N-1)(f(N-1) - f(N)) + C(N)f(N)$$

Così il fatto che $C(N) = C(x)$ prova la (3.1).
Per provare la (3.2) osserviamo che $C(t) = C(n)$ quando $n \le t < n+1$ e che

$$C(n)(f(n) - f(n+1)) = -\int_{n}^{n+1} C(t)f'(t)dt$$

Mentre invece $C(t) = 0$ quando $t < n_1$. □

**Teorema 3.0.8.** *Sia $x \ge 1$, allora*

$$\sum_{n \le x} \frac{1}{n} = \log x + \gamma + O\left(\frac{1}{x}\right)$$

*Dimostrazione.* Se poniamo $c_n = 1$ e $f(t) = 1/t$, si ha $C(x) = [x]$ e la (3.2) diventa

$$\sum_{n \le x} \frac{1}{n} = \frac{[x]}{x} + \int_{1}^{x} \frac{[t]}{t^2}dt = \log x + \gamma + E$$

con $\gamma$ come definito prima e

$$E = \int_{x}^{+\infty} \frac{(t - [t])}{t^2}dt - \frac{x - [x]}{x} = \int_{x}^{+\infty} \frac{O(1)}{t^2}dt + O\left(\frac{1}{x}\right) = O\left(\frac{1}{x}\right)$$

□

**Teorema 3.0.9.** *Sia $n \ge 1$, allora per ogni $\delta > 0$*

$$\sigma(n) = O(n^{1+\delta})$$

Più precisamente Gronwall, nel 1913, mostrò che:

**Teorema 3.0.10.** *Sia* $n \geq 1$

$$\limsup_{n\to+\infty} \frac{\sigma(n)}{n \log\log n} = e^{\gamma}$$

I due teoremi precedenti sono rispettivamente equivalenti ai due teoremi successivi su $\phi(n)$:[10](Cap. 18; §18.3)

**Teorema 3.0.11.** *Sia* $n \geq 1$*, allora per ogni* $\delta > 0$

$$\lim_{n\to+\infty} \frac{\phi(n)}{n^{1-\delta}} \to +\infty$$

Landau, nel 1903, dimostrò invece:

**Teorema 3.0.12.** *Sia* $n \geq 1$

$$\liminf_{n\to+\infty} \frac{\phi(n) \log\log n}{n} = e^{-\gamma}$$

La dimostrazione dei teoremi 3.0.10 e 3.0.12 si trova su [10](Cap. 22; §22.9) e utilizza il teorema di Mertens, anch'esso dimostrato nel [10](Theorem 429):

**Teorema 3.0.13** (Mertens)**.** *Per* $x \to +\infty$

$$\prod_{p\leq x} \left(1 - \frac{1}{p}\right) \sim \frac{e^{\gamma}}{\log x}$$

Per la dimostrazione dei teoremi 3.0.9 e 3.0.11 si utilizza il seguente risultato:

**Teorema 3.0.14.** *Per una costante positiva* $A < 1$

$$A < \frac{\sigma(n)\phi(n)}{n^2} < 1$$

*Dimostrazione.* Sia $n$ con la fattorizzazione canonica 1.1.4, allora

$$\sigma(n) = \prod_{i=1}^{k} \frac{p_i^{\alpha_i+1} - 1}{p - 1} = n \prod_{i=1}^{k} \frac{1 - p_i^{-\alpha_i-1}}{1 - p^{-1}}$$

e $\phi(n) = n \prod_{i=1}^{k}(1 - p_i^{-1})$, quindi

$$\frac{\sigma(n)\phi(n)}{n^2} = \prod_{i=1}^{k}(1 - p_i^{-\alpha_i-1})$$

che è minore di 1 e maggiore di $\prod_{i=1}^{k}(1 - p_i^{-2})$. □

*Dimostrazione teoremi 3.0.9 e 3.0.11.* Dal risultato precedente si ha che $\sigma(n)/n$ e $n/\phi(n)$ hanno lo stesso ordine di grandezza, quindi le due stime sono equivalenti.
Dimostriamo quindi soltanto il teorema 3.0.11: poniamo

$$f(n) := \frac{n^{1-\delta}}{\phi(n)}$$

$f(n)$ è moltiplicativa quindi, per il lemma 3.0.2, è sufficiente dimostrare che $\lim_{p^m \to +\infty} f(p^m) = 0$. Ma

$$\frac{1}{f(p^m)} = \frac{\phi(p^m)}{p^{m(1-\delta)}} = p^{m\delta}\left(1 - \frac{1}{p}\right) \geq \frac{1}{2}p^{m\delta} \to +\infty$$

□

## 3.1 Teorema dei numeri primi

Uno dei primi risultati importanti su $\pi(x)$ è dovuto a Legendre che nel 1808, attraverso il crivello di Eratostene, provò:(citato in [16](Cap. 4; §IA))

**Teorema 3.1.1.** *Sia* $n \geq 1$

$$\pi(n) = \pi(\sqrt{n}) - 1 + \sum_{d|n} \mu(d)\left[\frac{n}{d}\right]$$

Di conseguenza mostrò che:

**Corollario 3.1.2.** $\lim_{x\to+\infty}(\pi(x)/x) = 0$

Sempre Legendre, nel 1798, aveva congetturato che:

$$\pi(x) = \frac{x}{\log x - A(x)}$$

con $\lim_{x\to+\infty} A(x) = 1.08366\ldots$.
Questa congettura fu smentita grazie ai teoremi di Tschebycheff che vedremo tra poco.

A 15 anni, nel 1792, Gauss congetturò che:

$$\pi(x) \sim Li(x)$$

dove $Li(x)$ è il logaritmo integrale definito da:

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

Ma siccome $Li(x) \sim x/(\log x)$ ora, questo importante risultato, è conosciuto come:

**Teorema 3.1.3** (Teorema dei numeri primi)**.** *Sia* $x \geq 1$

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

La prima dimostrazione, nel 1896, è dovuta a Hadamard e de la Vallée Poussin attraverso lo studio dell'analisi complessa.
Invece, nel 1949, grazie ai risultati di Tschebycheff, Erdös e Selberg riuscirono contemporaneamente a darne una dimostrazione elementare, cioè solo attraverso lo studio delle funzioni aritmetiche, senza l'utilizzo dell'analisi complessa.

Il teorema dei numeri primi è equivalente ad affermare che:

**Corollario 3.1.4.** *Sia* $n \geq 1$

$$p_n \sim n \log n$$

### 3.1.1 Teorema di Tschebyscheff

In questa sezione si fa riferimento ai risultati trovati in [10](Cap. 22; §22.1, §22.2, §22.4, §22.6).

Andiamo ora a vedere i risultati di Tschebysheff che portarono alla dimostrazione del teorema dei numeri primi

**Definizione 3.1.5** (Funzioni di Tschebysheff)**.** *Sia* $x > 0$ *definiamo*

$$\theta(x) := \sum_{p \leq x} \log p = \log \prod_{p \leq x} p$$

$$\psi(x) := \sum_{p^m \leq x} \log p = \sum_{n \leq x} \Lambda(n)$$

*Osservazione.* Se $p^m \leq x$ e $m$ il massimo naturale tale che $p^m \leq x$, allora $m \log p \leq \log x$ e quindi si ha:

$$\psi(x) = \sum_{p \leq x} \left[ \frac{\log x}{\log p} \right] \log p$$

**Lemma 3.1.6.**

$$\psi(x) = \theta(x) + \theta(x^{1/2}) + \theta(x^{1/3}) + \ldots = \sum_{m \in \mathbb{N}} \theta(x^{1/m})$$

La serie è caso per caso una serie finita.

*Dimostrazione.* Dalla definizione di $\psi(x)$ si ha che

$$\psi(x) = \sum_{p \leq x} \log p + \sum_{p^2 \leq x} \log x + \ldots + \sum_{p^m \leq x} \log p$$

Considerando però che $p^i \leq x$ è equivalente a $p \leq x^{1/i}$, allora

$$\sum_{p^i \leq x} \log p = \sum_{p \leq x^{1/i}} \log p = \theta(x^{1/i})$$

da cui segue la tesi. □

**Teorema 3.1.7.**

$$\psi(x) = \theta(x) + O(x^{1/2}(\log x)^2)$$

*Dimostrazione.* La serie nella dimostrazione del lemma precedente finisce quando $x^{1/m} < 2$, cioè quando $m > \frac{\log x}{\log 2}$, quindi ci sono solo un $O(\log x)$ termini nella serie. Dalla definizione è ovvio che $\theta(x) < x \log x$ per $x \geq 2$, quindi, per $m \geq 2$, si ha

$$\theta(x^{1/m}) < x^{1/m} \log x \leq x^{1/2} \log x$$

Combinando le due osservazioni si ha:

$$\sum_{m \leq 2} \theta(x^{1/m}) = O(x^{1/2}(\log x)^2)$$

e quindi la tesi. □

**Teorema 3.1.8.** *Esistono due costanti $A, A' > 0$ tali che, per $x \geq 2$,*

$$Ax < \theta(x) < A'x \qquad\qquad Ax < \psi(x) < A'x$$

*Dimostrazione.* Per il teorema precedente ci basterà mostrare che, per $x \geq 2$,

$$\theta(x) < A'x \tag{3.3}$$

e

$$\psi(x) > Ax \tag{3.4}$$

Per provare (3.3) dimostriamo il seguente lemma dovuto ad Erdös e Kalmar:

**Lemma 3.1.9.** *Per ogni $n \geq 1$*

$$\theta(n) < 2n \log 2$$

Consideriamo $M := \binom{2m+1}{m} = \binom{2m+1}{m+1} = \dfrac{(2m+1)!}{m!(m+1)!} = \dfrac{(2m+1)(2m)\cdots(m+2)}{m!}$ che è un intero. Questo appare due volte nello sviluppo di $(1+1)^{2m+1}$, quindi $2M < 2^{2m+1}$ e $M < 2^{2m}$.
Se $m+1 < p \leq 2m+1$, allora $p$ divide il numeratore ma non il denominatore di $M$. Perciò $(\prod_{m+1<p\leq 2m+1} p)|M$ e

$$\theta(2m+1) - \theta(m+1) = \sum_{m+1<p\leq 2m+1} \log p \leq \log M < 2m \log 2$$

Il lemma è verificato per $n = 1$ e $n = 2$. Per induzione supponiamolo vero per tutti gli $n \leq n_0 - 1$.
Se $n_0$ è pari, allora

$$\theta(n_0) = \theta(n_0 - 1) < 2(n_0 - 1)\log 2 < 2n_0 \log 2$$

Se $n_0$ dispari, cioè $n_0 = 2m+1$, allora

$$\theta(n_0) = \theta(2m+1) = \theta(2m+1) - \theta(m+1) - \theta(m+1)$$

$$< 2m \log 2 + 2(m+1)\log 2 = 2(2m+1)\log 2 = 2n_0 \log 2$$

Così è dimostrata la (3.3).
Ora proviamo la (3.4):
I numeri $1, 2, \ldots, n$ hanno solo $[n/p]$ multipli di $p$, solo $[n/p^2]$ multipli di $p^2$, e così via. Quindi

$$n! = \prod_{p|n} p^{j(n,p)}$$

con

$$j(n,p) = \sum_{m\geq 1} \left[\frac{n}{p^m}\right]$$

Perciò si ha

$$N = \frac{(2n)!}{(n!)^2} = \prod_{p\leq 2n} p^{k_p}$$

con

$$k_p = \sum_{m\geq 1} \left( \left[\frac{2n}{p^m}\right] - 2\left[\frac{n}{p^m}\right] \right)$$

I termini dentro le parentesi tonde sono 1 o 0, asseconda che $[2n/p^m]$ sia dispari o pari. In particolare i termini sono 0 per $p^m > 2n$. Perciò

$$k_p \leq \left[\frac{\log 2n}{\log p}\right]$$

e

$$\log N = \sum_{p \le 2n} k_p \log p \le \sum_{p \le 2n} \left[ \frac{\log 2n}{\log p} \right] \log p = \psi(2n)$$

Ma

$$N = \frac{(2n)!}{(n!)^2} = \frac{n+1}{1} \cdot \frac{n+2}{2} \cdots \frac{2n}{n} \ge 2^n$$

quindi $\psi(2n) \ge n \log 2$.
Per $x \ge 2$, poniamo $n = [x/2] \ge 1$ e abbiamo

$$\psi(x) \ge \psi(2n) \ge n \log 2 \ge \frac{1}{4} x \log 2$$

da cui la (3.4) □

**Teorema 3.1.10** (Teorema di Tschebysheff)**.**

$$\pi(x) \lessgtr \frac{\theta(x)}{\log x} \lessgtr \frac{\psi(x)}{\log x}$$

Basta ragionare per $x$ sufficientemente grande.

D'ora in poi per le costanti useremo $C, C'$ che possono variare da un passaggio all'altro.

*Dimostrazione.* Dal teorema precedente basta dimostrare la prima parte del teorema. Innanzitutto

$$\theta(x) = \sum_{p \le x} \log p \le \log x \sum_{p \le x} 1 = \pi(x) \log x$$

e quindi

$$\pi(x) \ge \frac{\theta(x)}{\log x} > \frac{Cx}{\log x} \tag{3.5}$$

D'altra parte, per $0 < \delta < 1$,

$$\theta(x) \ge \sum_{x^{1-\delta} < p \le x} \log p \ge (1-\delta) \log x \sum_{x^{1-\delta} < p \le x} 1 =$$

$$= (1-\delta) \log x \cdot (\pi(x) - \pi(x^{1-\delta}) \ge (1-\delta) \log x (\pi(x) - x^{1-\delta})$$

e quindi

$$\pi(x) \le x^{1-\delta} + \frac{\theta(x)}{(1-\delta) \log x} \tag{3.6}$$

Dalla (3.5) e dalla (3.6) segue che

$$1 \leq \frac{\pi(x)\log x}{\theta(x)} \leq \frac{x^{1-\delta}\log x}{\theta(x)} + \frac{1}{1-\delta}$$

Per ogni $\varepsilon > 0$, possiamo scegliere $\delta = \delta(\varepsilon)$ tale che

$$\frac{1}{1-\delta} < 1 + \frac{1}{2}\varepsilon$$

e scegliamo $x_0 = x_0(\delta, \varepsilon) = x_0(\varepsilon)$ tale che

$$\frac{x^{1-\delta}\log x}{\theta(x)} < \frac{C'\log x}{x^{\delta}} < \frac{1}{2}\varepsilon$$

per ogni $x > x_0$. Così

$$1 \leq \frac{\pi(x)\log x}{\theta(x)} < 1 + \varepsilon$$

per ogni $x > x_0$. La tesi segue dal fatto che $\varepsilon$ è scelto arbitrario. □

Conseguenza del teorema di Tschebtcheff è :

**Corollario 3.1.11.** *Esistono due costanti $C, C' > 0$ tali che*

$$Cn\log n \leq p_n \leq C'n\log n$$

*Dimostrazione.* Innanzitutto

$$n = \pi(p_n) < \frac{Cp_n}{\log p_n} \qquad p_n > Cn\log p_n > Cn\log n$$

Poi $n = \pi(p_n) > \frac{C'p_n}{\log p_n}$, quindi

$$\sqrt{p_n} < \frac{C'p_n}{\log p_n} < C'n \qquad p_n < C'n^2$$

ed infine $p_n < C'n\log p_n < C'n\log n$. □

Per Tschebyscheff le due costanti venivano stimate $C = 0,92129\ldots$ e $C' = \frac{6}{5}A = 1,10555\ldots$.[16](Cap. 4; §I A)

Nel 1892 Sylvester migliorò la stima di Tschebyscheff con $C = 0,95695$ e $C' = 1.04423$, mentre nel 1932 Erdös pose $C = \log 2$ e $C' = 2\log 2$.[16](Cap. 4; §I E)

Di seguito esponiamo sempre da [10](Cap. 22; §22.6) il risultato di Tschebysheff (3.1.16)

**Lemma 3.1.12.** *Per $h > 0$ si ha*

$$\sum_{n \leq x} \log^h \left(\frac{x}{n}\right) = O(x)$$

*Dimostrazione.* Dal fatto che il logaritmo è una funzione crescente abbiamo che, per $n \geq 2$,

$$\log^h \left(\frac{x}{n}\right) \leq \int_{n-1}^{n} \log^h \left(\frac{x}{t}\right) dt$$

Quindi

$$\begin{aligned} \sum_{n=2}^{[x]} \log^h \left(\frac{x}{n}\right) &\leq \int_1^x \log^h \left(\frac{x}{t}\right) dt = x \int_1^x \frac{\log^h u}{u^2} du \\ &< x \int_1^{+\infty} \frac{\log^h u}{u^2} du = Ax \end{aligned}$$

dal fatto che l'integrale generalizzato è convergente. La tesi segue immediatamente. □

**Lemma 3.1.13.**

$$\sum_{n \leq x} \frac{\Lambda(n)}{n} = \log x + O(1)$$

*Dimostrazione.* Se nel lemma precedente poniamo $h = 1$ abbiamo

$$\sum_{n \leq x} \log n = [x] \log x + O(x) = x \log x + O(x)$$

Ma, dalla notazione all'interno della dimostrazione del teorema 3.1.8, si ha

$$\sum_{n \leq x} \log n = \sum_{p \leq x} j([x], p) \log p = \sum_{p^m \leq x} \left[\frac{x}{p^m}\right] \log p = \sum_{n \leq x} \left[\frac{x}{n}\right] \Lambda(n)$$

Se rimuoviamo la parte intera nell'ultima sommatoria, introduciamo un errore

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

e quindi

$$\sum_{n \leq x} \frac{x}{n} \Lambda(n) = x \log x + O(x)$$

Rimuovendo il fattore $x$ si ha la tesi □

**Lemma 3.1.14.**

$$\sum_{p \leq x} \frac{\log p}{p} = \log x + O(1)$$

*Dimostrazione.*

$$\sum_{n\le x}\frac{\Lambda(n)}{n}-\sum_{p\le x}\frac{\log p}{p}=\sum_{m\ge 2}\sum_{p^m\le x}\frac{\log p}{p^m}$$

$$<\sum_{p}\left(\frac{1}{p^2}+\frac{1}{p^3}+\dots\right)\log p=\sum_{p}\frac{\log p}{p(p-1)}$$

$$<\sum_{n=2}^{+\infty}\frac{\log n}{n(n-1)}=C$$

Se, nella notazione del lemma 3.0.8, poniamo $f(t)=1/t$ e $c_n=\Lambda(n)$, quindi $C(x)=\psi(x)$, abbiamo

$$\sum_{n\le x}\frac{\Lambda(n)}{n}=\frac{\psi(x)}{x}+\int_2^x\frac{\psi(t)}{t^2}dt$$

e, dal teorema 3.1.8 e dal lemma 3.1.13, si ha

$$\int_2^x\frac{\psi(t)}{t^2}dt=\log x+O(1) \tag{3.7}$$

□

Attraverso i due lemmi precedenti Tschebysheff arrivò a dire che:

**Teorema 3.1.15.** *Per $x\ge 2$*

$$\liminf_{x\to+\infty}\frac{\psi(x)}{x}\le 1 \qquad\qquad \limsup_{x\to+\infty}\frac{\psi(x)}{x}\ge 1$$

*Dimostrazione.* Dimostriamo per assurdo Se $\liminf_{x\to+\infty}(\psi(x)/x)=1+\delta$, con $\delta>0$, abbiamo $\psi(x)>(1+\frac{1}{2}\delta)x$ per ogni $x$ maggiore di qualche $x_0$. Quindi

$$\int_2^x\frac{\psi(t)}{t^2}dt>\int_2^{x_0}\frac{\psi(t)}{t^2}dt+\int_{x_0}^x\frac{(1+\frac{1}{2}\delta)}{t}dt>(1+\frac{1}{2}\delta)\log x-C$$

che entra in contraddizione con la (3.7).
Se supponiamo $\limsup_{x\to+\infty}(\psi(x)/x)=1-\delta$ si ha una contraddizione simile. □

E perciò si ha:

**Teorema 3.1.16.** *Se esiste*

$$m:=\lim_{x\to+\infty}\pi(x)/\frac{x}{\log x}$$

*allora $m=1$.*

Quindi l'unico passo che mancava per dimostrare il teorema dei numeri primi era dimostrare l'esistenza di quel limite.

Dal teorema di Tschebyscheff si può dedurre che:

**Teorema 3.1.17.** *Esiste una costante $B > 0$ tale che , per ogni $x > 1$,*

$$x < p \leq Bx$$

*per almeno un primo $p$.*

*Dimostrazione.* Dal teorema 3.1.8 si ha, per $x \geq 2$,

$$C_1 x < \theta(x) < C_2 x$$

per $C_1$ e $C_2$ fissati. Quindi

$$\theta(C_2 x/C_1) > C_1(C_2 x/C_1) = C_2 x > \theta(x)$$

e allora c'è almeno un primo $p$ tra $x$ e $C_2 x/C_1$. Ponendo $B = max(C_2/C_1, 2)$ si ha la tesi. □

Dell'ultimo teorema se ne può dare un risultato più preciso, cioè il postulato di Bertrand, congetturato nel 1845 e verificato dallo stesso Bertrand per $n < 3000000$, poi appunto dimostrato da Tschebyscheff nel 1850 per ogni $n > 3$:

**Teorema 3.1.18** (Postulato di Bertrand)**.** *Se $n > 3$ esiste almeno un primo $p$ tale che*

$$n < p \leq 2n$$

*o, equivalentemente, ponendo $n = p_r$*

$$p_{r+1} < 2p_r$$

*per ogni $r \in \mathbb{N}$*

La dimostrazione è contenuta in [10](Cap. 22; §22.3)

Conseguenze dei teoremi di Tschebyscheff furono pure i risultati ottenuti da Ishikawa (citati senza dimostrazione in [16](Cap. 4; §II B)) nel 1934:

**Teorema 3.1.19.** *Siano $n \geq 2$ e $m \geq 1$, allora*

$$p_n + p_{n+1} > p_{n+2}$$

*e*

$$p_n p_m > p_{m+n}$$

### 3.1.2 Dimostrazione teorema dei numeri primi

I risultati in seguito fanno riferimento agli scritti [22] e [6].

Andiamo ora a vedere come la collaborazione tra Selberg e Erdös portò al dimostrare il teorema dei numeri primi attraverso metodi elementari.

Risultato fondamentale fu il teorema di Selberg:

**Teorema 3.1.20** (Selberg)**.**

$$\theta(x)\log x + \sum_{p\leq x}\theta\left(\frac{x}{p}\right)\log p = 2x\log x + O(x) \tag{3.8}$$

*e*

$$\sum_{p\leq x}\log^2 p + \sum_{pp'\leq x}\log p\log p' = 2x\log x + O(x) \tag{3.9}$$

Così fu enunciato da Selberg, noi diamo la dimostrazione della forma equivalente contenuta in [10](Theorem 433):

$$\psi(x)\log x + \sum_{n\leq x}\Lambda(n)\psi\left(\frac{x}{n}\right) = 2x\log x + O(x) \tag{3.10}$$

e

$$\sum_{n\leq x}\Lambda(n)\log n + \sum_{mn\leq x}\Lambda(m)\Lambda(n) = 2x\log x + O(x) \tag{3.11}$$

*Dimostrazione.* Innanzitutto vediamo che le due affermazioni (3.10) e (3.11) sono equivalenti:

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

e, se poniamo $c_n = \Lambda(n)$ e $f(t) = \log t$ in (3.1),

$$\sum_{n\leq x}\Lambda(n)\log n = \psi(x)\log x - \int_2^x \frac{\psi(t)}{t}dt = \psi(x)\log x + O(x) \tag{3.12}$$

dal fatto che $\psi(x) = O(x)$ per il teorema 3.1.8.
Ora dimostriamo la (3.11).
Ricordiamo innanzitutto il teorema 2.2.3: $\sum_{d|1}\mu(d) = 1$ , $\sum_{d|n}\mu(d) = 0$ con $n > 1$.
Poi riprendiamo pure il teorema 2.2.27 e il lemma 2.2.25: $\Lambda(n) = -\sum_{d|n}\mu(d)\log d$ e $\sum_{d|n}\Lambda(d) = \log n$.
Quindi

$$\sum_{h|n}\Lambda(h)\Lambda\left(\frac{n}{h}\right) = -\sum_{h|n}\Lambda(h)\sum_{d|(n/h)}\mu(d)\log d =$$

$$= -\sum_{d|n} \mu(d) \log d \sum_{h|(n/d)} \Lambda(h) = -\sum_{d|n} \mu(d) \log d \log\left(\frac{n}{d}\right) =$$

$$= \Lambda(n) \log n + \sum_{d|n} \mu(d) \log^2 d \tag{3.13}$$

Poi, se $n = 1$,

$$\sum_{d|1} \mu(d) \log^2\left(\frac{x}{d}\right) = \log^2 x \tag{3.14}$$

ma, per $n > 1$, considerando che $\sum_{d|n} \mu(d) \log^2(x) = \log^2 x \sum_{d|n} \mu(d) = 0$

$$\sum_{d|n} \mu(d) \log^2\left(\frac{x}{d}\right) = \sum_{d|n} \mu(d)(\log^2 d - 2 \log x \log d) =$$

$$= -2 \sum_{d|n} \mu(d) \log d \log x + \sum_{d|n} \mu(d) \log^2 d =$$

$$= 2\Lambda(n) \log x - \Lambda(n) \log n + \sum_{hk=n} \Lambda(h)\Lambda(k) \tag{3.15}$$

per la (3.12).
Quindi, se scriviamo

$$S(x) := \sum_{n \le x} \left( \sum_{d|n} \mu(d) \log^2\left(\frac{x}{d}\right) \right)$$

abbiamo, per la (3.14) e la (3.15)

$$S(x) = \log^2 x + 2\psi(x) \log x - \sum_{n \le x} \Lambda(n) \log n + \sum_{hk \le x} \Lambda(h)\Lambda(k) =$$

$$= \sum_{n \le x} \Lambda(n) \log n + \sum_{mn \le x} \Lambda(m)\Lambda(n) + O(x)$$

per la (3.12).
Per completare la dimostrazione basta mostrare che $S(x) = 2x \log x + O(x)$.
Scriviamo

$$S(x) - \gamma^2 = \sum_{n \le x} \sum_{d|n} \mu(d)(\log^2\left(\frac{x}{d}\right) - \gamma^2) =$$

$$= \sum_{d \le n} \mu(d) \left[\frac{x}{d}\right] (\log^2\left(\frac{x}{d}\right) - \gamma^2)$$

dal fatto che il numero di $n \leq x$, tali che $d|n$, sono $[x/d]$.
Se rimuoviamo la parte intera, l'errore introdotto è meno di

$$\sum_{d\leq x}(\log^2\left(\frac{x}{d}\right)+\gamma^2) = O(x)$$

dal lemma 3.1.12.
Quindi

$$S(x) = x\sum_{d\leq x}\frac{\mu(d)}{d}(\log^2\left(\frac{x}{d}\right)-\gamma^2)+O(x) \tag{3.16}$$

Ora, dal teorema 3.0.8,

$$\sum_{d\leq x}\frac{\mu(d)}{d}(\log^2\left(\frac{x}{d}\right)-\gamma^2) =$$

$$= \sum_{d\leq x}\frac{\mu(d)}{d}(\log\left(\frac{x}{d}\right)-\gamma)\left(\sum_{k\leq x/d}\frac{1}{k}+O\left(\frac{d}{x}\right)\right) \tag{3.17}$$

La somma dei vari termini in (3.17) è, nel caso della moltiplicazione con $O\left(\frac{d}{x}\right)$, al massimo

$$\sum_{d\leq x}\frac{1}{d}(\log\left(\frac{x}{d}\right)+\gamma)O\left(\frac{d}{x}\right) = O\left(\frac{1}{x}\right)\sum_{d\leq x}\log\left(\frac{x}{d}\right)+O(1) = O(1)$$

dal lemma 3.1.12. Poi, nel caso della moltiplicazione per $\sum_{k\leq x/d}\frac{1}{k}$

$$\sum_{d\leq x}\frac{\mu(d)}{d}(\log\left(\frac{x}{d}\right)-\gamma)\sum_{k\leq x/d}\frac{1}{k} =$$

$$= \sum_{dk\leq x}\frac{\mu(d)}{dk}(\log\left(\frac{x}{d}\right)-\gamma) = \sum_{n\leq x}\frac{1}{n}\sum_{d|n}\mu(d)(\log\left(\frac{x}{d}\right)-\gamma) =$$

$$= \log x-\gamma+\sum_{2\leq n\leq x}\frac{\Lambda(n)}{n} = 2\log x+O(1) \qquad (x\geq 2)$$

dal lemma 3.1.13. La tesi segue combinando l'ultimo risultato con la (3.16). □

**Definizione 3.1.21.** *Poniamo*

$$a := \liminf_{x\to+\infty}\frac{\theta(x)}{x} \qquad A := \limsup_{x\to+\infty}\frac{\theta(x)}{x}$$

Erdös, attraverso il risultato di Selberg(3.8), riuscì a dimostrare i seguenti lemmi:[6](Lemma 3; Lemma 4)

**Lemma 3.1.22.** $a + A = 2$

*Dimostrazione.* Si prenda $x \to +\infty$ così che $\theta(x) = Ax + o(x)$ per il teorema 3.1.8. Allora si ha che

$$\sum_{p \leq x} \log^2 p = Ax \log x + o(x \log x)$$

Quindi, dal teorema di Selberg, si ha

$$\sum_{p \leq x} \theta\left(\frac{x}{p}\right) \log p = (2 - A)x \log x + o(x \log x) \tag{3.18}$$

Poi dalla definizione di $a$

$$\sum_{p \leq x} \theta\left(\frac{x}{p}\right) \log p \geq ax \sum_{p \leq x} \frac{\log p}{p} + o(x \log x) = ax \log x + o(x \log x)$$

Combinando il risultato con la (3.18) troviamo $2 \geq a + A$.
Otteniamo $a + A \geq 2$ in maniera simile, scegliendo $\theta(x) = ax + o(x)$. □

**Lemma 3.1.23.** *Sia $\delta > 0$, allora si ha*

$$\theta\left(\frac{x}{p}\right) > (A - \delta)\frac{x}{p} \tag{3.19}$$

*tranne per un insieme $P_k$ di primi minori di $x$ per cui vale*

$$\sum_{p \in P_k} \frac{\log p}{p} = o(\log x)$$

*Inoltre si ha*

$$\theta\left(\frac{x}{p}\right) < (a + \delta)\frac{x}{p} \tag{3.20}$$

*tranne per un insieme $P_h$ di primi minori di $x$ per cui vale*

$$\sum_{p \in P_h} \frac{\log p}{p} = o(\log x)$$

*Infine, scelto $p \leq x$ tale che non appartenga ne a $P_k$ ne a $P_h$, si ha*

$$\frac{x}{p} < (1 + \delta)\frac{x}{p} \tag{3.21}$$

*Dimostrazione teorema numeri primi (Teorema 3.1.3).* Dai risultati di Tschebyscheff basta mostrare che $\lim_{x\to+\infty} \frac{\theta(x)}{x} = 1$.
Ripartendo dalle ipotesi e dalle notazioni dei due lemmi di Erdös precedenti si ha, per la (3.19), la (3.20) e la (3.21),

$$(A-\delta)\frac{x}{p} < \theta\left(\frac{x}{p}\right) < (a+\delta)\frac{x}{p} < (a+\delta)(1+\delta)\frac{x}{p}$$

quindi

$$A - \delta < (a+\delta)(1+\delta)$$

poi, facendo tendere $\delta$ a 0, si ha

$$A \leq a$$

Dalle definizione 3.1.21 si ha che $A \geq a$, che, combinato con $A + a = 2$, ci da $a = A = 1$. □

Diamo ora invece qualche risultato sul termine d'errore del teorema dei numeri primi. I risultati qui in seguito sono presi da [16](Cap. 4; §I A, §I E, §I G, §I B).

Nella propria dimostrazione del teorema dei numeri primi Hadamard e de la Vallée Poussin stimarono l'errore con:

**Teorema 3.1.24.**

$$\pi(x) = Li(x) + O(x\exp(-A\sqrt{\log x})$$

*per qualche costante positiva A.*

Invece Littlewood dimostrò:

**Teorema 3.1.25.**

$$\pi(x) = Li(x) + O(x\exp(-C(\log x \log\log x^{1/2}))$$

e successivamente Tschudakoff ottenne:

**Teorema 3.1.26.**

$$\pi(x) = Li(x) + O(x\exp(-C(\log x)^{\alpha}))$$

*con $\alpha < 4/7$ e $C > 0$.*

Nel 1962 Rosser e Schoenfeld dimostrarono, sulla differenza tra $\pi(x)$ e $\frac{x}{\log x}$, che:

**Teorema 3.1.27.** *Sia $x \geq 17$*

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

Invece Gauss e Riemann credevano che, per ogni $x > 1$, $Li(x) > \pi(x)$.
Ma Littlewood, nel 1914, dimostrò che la differenza $Li(x) - \pi(x)$ cambia segno infinite volte, quindi:

**Teorema 3.1.28.** *Esistono infiniti $x_i$ tali che $Li(x_i) - \pi(x_i) = 0$.*

Sulla stima di $p_n$, Rosser, nel 1938, provò che:

**Teorema 3.1.29.**

$$\log n + n(\log\log n - 10) < p_n < n\log n + n(\log\log n + 8)$$

e Robin, nel 1983, migliorò la stima con:

**Teorema 3.1.30.**

- *Se $n \geq 2$ allora $p_n \geq n\log n + n(\log\log n - 1,0072629)$;*
- *Se $n \geq 2$ e $p_n \leq 10^{11}$, allora $p_n \geq n\log n + n(\log\log n - 1)$;*
- *Se $n \geq 7022$ allora $p_n \leq n\log n + n(\log\log n - 0,9385)$;*

## 3.2 Zeta di Riemann

I risultati per questa sezione sono presi da [10](Cap. 17; §17.1-17.4).

**Definizione 3.2.1** (Serie di Dirichlet)**.** *Sia $(a_n)_{n\in\mathbb{N}}$ una successione a valori in $\mathbb{C}$ e $s \in \mathbb{C}$, allora la serie di Dirichlet è definita da*

$$F(s) := \sum_{n\geq 1} \frac{a_n}{n^s}$$

Per il momento consideriamo solo il caso con $s \in \mathbb{R}$, successivamente vedremo il caso con $s \in \mathbb{C}$.

**Teorema 3.2.2.** *Sia $F(s)$ una serie di Dirichlet assolutamente convergente per $s > s_0$, allora*

$$F'(s) = -\sum_{n\geq 1} \frac{a_n \log n}{n^s}$$

*per $s > s_0$.*

La serie di Dirichlet infinita più semplice è:

**Definizione 3.2.3** (Zeta di Riemann)**.**

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

E' convergente per $s > 1$.

Dal teorema precedente:

**Corollario 3.2.4.**

$$\zeta'(s) = -\sum_{n\geq 1} \frac{\log n}{n^s}$$

*per* $s > 1$.

Nel 1737 Eulero dimostrò che:

**Teorema 3.2.5** (Prodotto di Eulero)**.** *Se* $s > 1$*, allora*

$$\zeta(s) = \sum_{n\geq 1} \frac{1}{n^s} = \prod_p \frac{1}{1 - p^{-s}}$$

*Dimostrazione.*

$$\zeta(s) = \sum_{n\geq 1} \frac{1}{n^s} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \cdots$$

$$\frac{1}{2^s}\zeta(s) = \frac{1}{2^s} + \frac{1}{4^s} + \frac{1}{6^s} + \frac{1}{8^s} + \cdots$$

$$\left(1 - \frac{1}{2^s}\right)\zeta(s) = \frac{1}{3^s} + \frac{1}{5^s} + \frac{1}{7^s} + \cdots$$

$$\left(1 - \frac{1}{3^s}\right)\left(1 - \frac{1}{2^s}\right)\zeta(s) = \frac{1}{5^s} + \frac{1}{7^s} \cdots$$

$$\prod_p \left(1 - \frac{1}{p}\right)\zeta(s) = 1$$

I passaggi precedenti sono leciti per convergenza uniforme sui compatti □

**Teorema 3.2.6.** *Sia* $s > 1$

$$\zeta(s) = \frac{1}{s-1} + O(1)$$

*Dimostrazione.* Scriviamo $\zeta(s)$ nella forma

$$\zeta(s) = \sum_{n=1}^{+\infty} n^{-s} = \int_1^{+\infty} x^{-s}dx + \sum_{n=1}^{+\infty} \int_n^{n+1} (n^{-s} - x^{-s})dx \tag{3.22}$$

Però

$$\int_1^{+\infty} x^{-s}dx = \frac{1}{s-1}$$

per $s > 1$. Si ha anche

$$0 < n^{-s} - x^{-s} = \int_n^x st^{-s-1}dt < \frac{s}{n^2}$$

se $n < x < n + 1$, e quindi

$$0 < \int_n^{n+1} (n^{-s} - x^{-s})dx < \frac{s}{n^2}$$

e l'ultimo termine nella (3.22) è positivo e minore di $s\sum_n n^{-2}$. □

**Corollario 3.2.7.** *Sia* $s > 1$

$$\log \zeta(s) = \log \frac{1}{s-1} + O(s-1)$$

*Dimostrazione.*

$$\log \zeta(s) = \log \frac{1}{s-1} + \log(1 + O(s-1))$$

□

**Teorema 3.2.8.** *Sia* $s > 1$*, dal teorema 3.2.6 segue [10](Theorem 283)*

$$\zeta'(s) = -\frac{1}{(s-1)^2} + O(1)$$

**Teorema 3.2.9** (Prodotto di serie di Dirichlet)**.** *Siano le serie*

$$F(s) = \sum_{u\in\mathbb{N}} a_u u^{-s}, \qquad G(s) \sum_{v\in\mathbb{N}} b_v v^{-s}$$

*assolutamente convergenti, allora*

$$F(s)G(s) = \sum_{n\in\mathbb{N}} c_n n^{-s}$$

*con* $c_n = \sum_{uv=n} a_u b_v$.

**Corollario 3.2.10.** *Se* $f(1) = 1$ *e* $f(n)$ *è moltiplicativa, allora [10](Theorem 286)*

$$\sum_{n\in\mathbb{N}} f(n)n^{-s} = 1 + f(p)p^{-s} + f(p^2)p^{-2s} + \ldots + f(p^a)p^{-as} + \ldots$$

### 3.2.1 Zeta di Riemann e funzioni aritmetiche

Vediamo come si lega la zeta di Riemann alle funzioni aritmetiche. [10](Cap. 17; §17.5, §17.7)

**Teorema 3.2.11.**

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

*per* $s > 1$

*Dimostrazione.* Dal teorema 3.2.5, dal lemma 2.2.2 e dal corollario 3.2.10 si ha

$$\frac{1}{\zeta(s)} = \prod_p (1 - p^{-s}) = \prod_p (1 + \mu(p)p^{-s} + \mu(p^2)p^{-2s} + \ldots) = \sum_{n\geq 1} \mu_(n)n^{-s}$$

□

**Teorema 3.2.12.**

$$\frac{\zeta(s-1)}{\zeta(s)} = \sum_{n\geq 1} \frac{\phi(n)}{n^s}$$

*per* $s > 2$.

*Dimostrazione.* Dai teoremi 3.2.9 e 3.2.11 si ha

$$\frac{\zeta(s-1)}{\zeta(s)} = \sum_{n\geq 1} \frac{n}{n^s} \sum_{n\geq 1} \frac{\mu(n)}{n^s} = \sum_{n\geq 1} \frac{1}{n^s} \sum_{d|n} d\mu\left(\frac{n}{d}\right) = \sum_{n\geq 1} \frac{\phi(n)}{n^s}$$

□

**Teorema 3.2.13.** *Se* $k \geq 0$

$$\zeta(s)\zeta(s-k) = \sum_{n>1} \frac{\sigma_k(n)}{n^s}$$

*per* $s > k + 1$.

*10.* (Theorem 291)

$$\zeta(s)\zeta(s-k) = \sum_{n\geq 1} \frac{1}{n^s} \sum_{n\geq 1} \frac{n^k}{n^s} = \sum_{n\geq 1} \frac{1}{n^s} \sum_{d|n} d^k = \sum_{n\geq 1} \frac{\sigma_k(n)}{n^s}$$

□

Dal teorema precedente, per $k = 0$ oppure per $k = 1$, si ha:

**Corollario 3.2.14.** *Sia* $s > 1$

$$\zeta^2(s) = \sum_{n\geq 1} \frac{d(n)}{n^s}$$

*e per* $s > 2$

$$\zeta(s)\zeta(s-1) = \frac{\sigma(n)}{n^s}$$

**Teorema 3.2.15.** *Per* $s > 1$

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{n\geq 1} \Lambda(n) n^{-s}$$

*Dimostrazione.* Dal teorema 3.2.5 si ha

$$\log \zeta(s) = \sum_{p} \log\left(\frac{1}{1-p^{-s}}\right)$$

Derivando rispetto ad $s$, e osservando che

$$\frac{d}{ds} \log \frac{1}{1-p^{-s}} = -\frac{\log p}{p^s - 1}$$

si ottiene

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{p} \frac{\log p}{p^s - 1} \tag{3.23}$$

La derivazione è legittima in quanto le serie derivate sono uniformemente convergenti per $s \geq 1 + \delta > 1$.
Riscrivendo la (3.23) nella forma

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{p} \log p \sum_{m\geq 1} p^{-ms}$$

e la doppia serie $\sum_p \sum_{m\geq 1} p^{-ms} \log p$ è convergente uniformemente per $s \geq 1+\delta$. Quindi si può riscrivere come

$$\sum_{p,m\geq 1} p^{-ms} \log p = \sum_{n\geq 1} \Lambda(n) n^{-s}$$

dalla definizione di $\Lambda(n)$. □

## 3.3 Ipotesi di Riemann e conseguenze

La zeta viene chiamata di Riemann in quanto fu proprio lui, nel suo scritto *Über die Anzahl der Primzahlen unter einer gegebenen Grösse* pubblicato nel 1859, a dare il contributo maggiore nello studio di questa funzione.
Fu il primo a pensare all'estensione della funzione come funzione olomorfa in $\mathbb{C}$.

In questo modo $\zeta(s) = \sum_{n\geq 1} \frac{1}{n^s}$ è una serie convergente per ogni $s$ appartenente a $\mathbb{C}$ e con parte reale $Re(s) > 1$.
Inoltre $\zeta$ si estende analiticamente come funzione olomorfa in tutto $\mathbb{C}$, ad eccezione del punto $s = 1$ dove ha un polo semplice.

Dal prodotto di Eulero si trova che la zeta non ha zeri per $Re(s) > 1$, invece per $Re(s) < 0$ si ha che la zeta si annulla nei così detti zeri semplici $s = -2, -4, -6, \ldots$.
Riemann dimostrò che in $0 < Re(s) < 1$, detta la striscia critica, gli zeri si dispongono in maniera simmetrica rispetto alla retta $Re(s) = \frac{1}{2}$, detta retta critica.

Proprio sulla posizione di quest'ultimi zeri Riemann congetturò la sua famosa ipotesi:

**Congettura 3.3.1** (Ipotesi di Riemann (RH))**.** *Gli zeri non banali della $\zeta$ si trovano tutti nella retta $s = \frac{1}{2} + it$ con $t \in \mathbb{R}$, cioè si trovano tutti nella retta critica.*

Questa congettura è considerata il più grande problema aperto della matematica, tanto da essere inserita: sia nella lista dei 23 problemi da risolvere fornita da Hilbert nel 1900, sia nei 7 problemi per il millennio posti nel 2000. (Si veda [4])

Attraverso lo studio sugli zeri della zeta di Riemann si ha la miglior stima attualmente conosciuta per $\pi(x)$: [16](Cap. 4; §I G)

**Teorema 3.3.2.**

$$\pi(x) = Li(x) + O\left(x \exp\left(-C\frac{(\log x)^{3/5}}{(\log\log x)^{1/5}}\right)\right)$$

Nonostante ancora non sia stata provata, molti matematici hanno studiato che conseguenze avrebbe la verifica dell'ipotesi di Riemann.

Innanzitutto, nel 1901, von Koch mostrò che l'ipotesi di Riemann è equivalente a dire che l'errore nei teorema dei numeri primi è della forma: [16](Cap. 4; §I G)

**Teorema 3.3.3.** *Assumendo vera (RH)*

$$\pi(x) = Li(x) = O(x^{1/2}\log x)$$

*e viceversa.*

Poi, nel 1933, Skewes mostrò che: [16](Cap. 4; §I E)

**Teorema 3.3.4.** *Assumendo vera (RH), se $x_0$ è il primo numero positivo tale che $Li(x_0) - \pi(x_0) = 0$, allora*

$$x_0 < 10^{10^{10^{34}}}$$

Anche se poi, senza supporre vera l'ipotesi di Riemann, lo stesso Skewes migliorò la sua stima trovando:

$$x_0 < e^{e^{e^{e^{7,7}}}}$$

### 3.3.1 Teorema di Robin

In questa sezione si farà particolarmente riferimento ai risultati ottenuti da Robin e Lagaris.

Arriviamo infine al teorema di Robin, provato dallo stesso Robin nel 1983, che ci da una formulazione equivalente dell'ipotesi di Riemann: [18](Theoreme 1)

**Teorema 3.3.5** (Robin)**.** *L'ipotesi di Riemann (RH) è equivalente a*

$$\forall n \geq 5041 \qquad \sigma(n) \leq e^{\gamma} n \log\log n \tag{3.24}$$

Abbiamo già visto che il risultato di Gronwall (teorema 3.0.10) afferma che $\limsup_{n\to+\infty} \frac{\sigma(n)}{n\log\log n} = e^{\gamma}$; andiamo ora a vedere invece come si è arrivati al teorema di Robin.

Fondamentale fu lo studio di particolari numeri:

**Definizione 3.3.6.** *Definiamo come numeri altamente compositi i numeri naturali $n$ tali che*

$$d(n) > d(k) \qquad 1 \leq k \leq n-1$$

*Definiamo i numeri altamente compositi superiori come i naturali $n$ per cui esiste $\epsilon > 0$ tale che*

$$\frac{d(n)}{n^{\epsilon}} \geq \frac{d(k)}{k^{\epsilon}} \qquad \forall k > 1$$

*Definiamo i numeri sovrabbondanti come i naturali $n$ tali che*

$$\frac{\sigma(n)}{n} > \frac{\sigma(k)}{k} \qquad 1 \leq k \leq n-1$$

*Definiamo i numeri colossalmente abbondanti come i numeri naturali $n$ per cui esiste $\epsilon > 0$ tale che*

$$\frac{\sigma(n)}{n^{1+\epsilon}} \geq \frac{\sigma(k)}{k^{1+\epsilon}} \qquad \forall k > 1$$

L'insieme dei numeri altamente compositi superiori forma un sottoinsieme dell'insieme dei numeri altamente compositi.

Ramunujan derivò l'estremo superiore ed inferiore dei numeri altamente compositi superiori assumendo vera l'ipotesi di Riemann. I suoi estremi implicano che, sempre assumendo vera l'ipotesi di Riemann, la disuguaglianza $\sigma(n) < e^{\gamma} n \log\log n$ risulta vera per ogni $n \geq 5041$.
I numeri colossalmente abbondanti furono definiti da Alaouglu e Erdös nel 1944 L'insieme dei numeri colossalmente abbondanti è infinito e forma un sottoinsieme dell'insieme dei numeri sovrabbondanti.
Alaoglu e Erdös mostrarono che, per un generico $\epsilon > 0$, esiste esattamente un unico numero colossalmente abbondante $n$ che massimizza $\sigma(k)/k^{1+\epsilon}$, e l'esponente $a_p(\epsilon)$ di ogni primo $p$ nella scomposizione di $n$ è

$$a_p(\epsilon) = \left[\frac{\log(p^{1+\epsilon} - 1) - \log(p^{\epsilon} - 1)}{\log p}\right] - 1$$

Inoltre, per ogni $\epsilon > 0$, il valore di $n$ definito dalla precedente formula è un numero colossalmente abbondante.
Erdös e Nicolas mostrarono che, per un dato valore di $\epsilon$, ci sono esattamente 1, 2 o 4 interi $n$ che raggiungono il massimo valore di $\sigma(k)/k^{1+\epsilon}$.
Robin mostrò che, se l'ipotesi di Riemann fosse falsa, all'ora si avrebbe un controesempio della disuguaglianza $\sigma(n) < e^{\gamma} n \log\log n$, e questo sarebbe proprio un numero colossalmente abbondante. (Vedi [11](§2))

Nella propria dimostrazione Robin utilizzò i due seguenti lemmi sui numeri colossalmente abbondanti:

**Lemma 3.3.7.** *Siano $3 \leq N \leq n \leq N'$ dei numeri naturali di cui $N$ e $N'$ sono 2 numeri colossalmente abbondanti, sia*

$$f(n) := \frac{\sigma(n)}{n \log\log n}$$

*allora si ha*

$$f(n) \leq Max(f(N), f(N'))$$

*Dimostrazione.* Se $N$ e $N'$ sono numeri colossalmente abbondanti allora esiste un solo valore $\epsilon$ per la quale si ha

$$\frac{\sigma(n)}{n^{\epsilon+1}} \leq \frac{\sigma(N)}{N^{1+\epsilon}} = \frac{\sigma(N')}{(N')^{\epsilon+1}} \qquad \forall n \geq 1$$

Perciò

$$f(n) \leq f(N) \left(\frac{n}{N}\right)^{\epsilon} \frac{\log\log N}{\log\log n}$$

da cui

$$f(n) \leq f(N) \qquad \text{se} \quad \frac{n^\epsilon}{\log\log n} \leq \frac{N^\epsilon}{\log\log N}$$

Il lemma è dimostrato se

$$\epsilon \log n - \log\log\log n \leq Max(\epsilon \log N - \log\log\log N, \epsilon \log N' - \log\log\log N')$$

che è una conseguenza della convessità della funzione

$$x \to \epsilon x - \log\log x \qquad\qquad x > 1$$

□

**Lemma 3.3.8.** *Se l'ipotesi di Riemann è vera, allora esiste un naturale* $n_0$ *tale che* $f(n) < e^\gamma$ *per* $n \geq n_0$.

La dimostrazione si trova in [18](Preposition 2)

Il teorema 3.3.5 è dedotto dai due seguenti teoremi di Robin, di questi daremo soltanto un'idea della dimostrazione:

**Teorema 3.3.9** (RH⇒(3.24))**.** *Se l'ipotesi di Riemann è vera, allora per ogni* $n \geq 5041$

$$\sigma(n) \leq e^\gamma n \log\log n$$

Il vantaggio principale del teorema è l'aver stabilito il limite esplicito oltre il quale vale la diseguaglianza. La dimostrazione contiene precise diseguaglianze usando formule per la funzione $\pi(x)$ in termini di zeri della funzione zeta di Riemann. Fa anche uso di errori stimati per la funzione $\pi(x)$ dovuti a Rosser e Schoenfeld [19],[20],[21].

**Teorema 3.3.10** ((3.24)⇒RH)**.** *Se l'ipotesi di Riemann è falsa, allora esistono due costanti* $0 < \beta < 1/2$ *e* $C > 0$ *tali che*

$$\sigma(n) \geq e^\gamma n \log\log n + \frac{Cn \log\log n}{(\log n)^\beta}$$

*per ogni* $n \geq 1$

La costante $\beta$ può essere scelta tale che $1 - b < \beta < 1/2$, dove $b = Re(\rho)$ per qualche zero $\rho$ di $\zeta(s)$ con $Re(\rho) > 1/2$, e $C > 0$ deve essere scelto sufficientemente piccolo, dipende da $\rho$. La dimostrazione usa idee dovute a un risultato di Nicolas [13],[14].

Vediamo ora un'altra condizione equivalente a RH.

**Definizione 3.3.11** (N-esimo numero armonico)**.** *Sia $n \in \mathbb{N}$, definiamo l'n-esimo numero armonico $H_n$ come*

$$H_n := \sum_{k=1}^{n} \frac{1}{k}$$

Diamo ora altri due lemmi:

**Lemma 3.3.12.** *Per $n \geq 3$*

$$e^{H_n} \log(H_n) \geq e^{\gamma} n \log\log n$$

*Dimostrazione.* Prendendo $[t]$ la parte intera di $t$ e $\{t\}$ la parte frazionaria di $t$, abbiamo

$$\int_1^n \frac{[t]}{t^2} dt = \int_1^n \frac{1}{t^2} \left( \sum_{1 \leq r \leq t} 1 \right) dt = \sum_{1 \leq r \leq n} \int_r^n \frac{1}{t^2} dt = \sum_{r=1}^{n} \left( \frac{1}{r} - \frac{1}{n} \right) = H_n - 1$$

Allora

$$H_n = 1 + \int_1^n \frac{t - \{t\}}{t^2} dt = \log n + 1 - \int_1^n \frac{\{t\}}{t^2} dt \tag{3.25}$$

Così otteniamo che

$$H_n = \log n + \gamma + \int_n^{+\infty} \frac{\{t\}}{t^2} dt \tag{3.26}$$

dal fatto che $\gamma = 1 - \int_1^{+\infty} \frac{\{t\}}{t^2} dt$ per definizione.
Dal teorema 3.0.8 abbiamo che $\gamma = \lim_{n \to +\infty} (H_n - \log n)$, che così, nella (3.26), ci da

$$H_n > \log n + \gamma$$

che applicando l'esponenziale diventa

$$e^{H_n} \geq e^{\gamma} n \tag{3.27}$$

Infine $H_n \geq \log n$, quindi $\log(H_n) \geq \log\log n > 0$ per $n \geq 3$. Combinando questo con la (3.27) si ha la tesi. □

**Lemma 3.3.13.** *Per $n \geq 3$*

$$H_n + e^{H_n} \log H_n \leq e^{\gamma} n \log\log n + \frac{4n}{\log n}$$

*Dimostrazione.* Per $n \geq 1$ definisco $R_n$ come

$$R_n := H_n - \log(n+1) = \int_1^{n+1} \left( \frac{1}{[t]} - \frac{1}{t} \right) dt$$

Si noti che $R_n$ è positivo e crescente con $n$. Da $\lim_{n\to+\infty}(H_n - \log(n+1)) = \gamma$ otteniamo

$$H_n - \log(n-1) \leq \gamma$$

Applicando l'esponenziale abbiamo

$$e^{H_n} \leq e^{\gamma}(n+1) \tag{3.28}$$

La (3.25) implica che, per $n \geq 3$,

$$\log H_n \leq \log(\log n + 1) = \log(\log n) \cdot (1 + \frac{1}{\log n}) \Big) \leq \log\log n + \frac{1}{\log n} \tag{3.29}$$

usando il fatto che $\log(1+x) \leq x$ per $x \geq 0$. Moltiplicando la (3.28) con la (3.29) si ottiene, per $n \geq 3$,

$$e^{H_n}\log(H_n) \leq e^{\gamma} n \log\log n + \frac{e^{\gamma n}}{\log n} + e^{\gamma}(\log\log n + \frac{1}{\log n})$$

(3.30)

Ora osserviamo che, per $n \geq 3$,

$$\log\left((\log n)\frac{1}{\log n}\right) \leq \frac{n}{2\log n}$$

Sostituendo in (3.30) si ha

$$e^{H_n}\log(H_n) \leq e^{\gamma} n \log\log n + \frac{3e^{\gamma} n}{2\log n}$$

Ora la (3.25) da, per $n \geq 3$,

$$H_n \leq \log n + 1 \leq \frac{n}{\log n}$$

Sommando le ultime due diseguaglianze, per $n \geq 3$,

$$H_n + e^{H_n}\log(H_n) \leq e^{\gamma} n \log\log n + \frac{4n}{\log n}$$

da $1 + 3e^{\gamma}/2 < 4$. □

Infine, grazie al teorema di Robin e ai due lemmi precedenti Lagaris trovò, nel 2001, un'ulteriore formulazione equivalente dell'ipotesi di Riemann: [11](Theorem 1)

**Teorema 3.3.14.** *L'ipotesi di Riemann è equivalente a*

$$\sigma(n) \leq H_n + e^{H_n} \log(H_n) \tag{3.31}$$

*per* $n \geq 1$ *e si ha l'uguaglianza per* $n = 1$.

*Dimostrazione.* $\Leftarrow$) Supponiamo l'ipotesi di Riemann vera. Allora per il teorema 3.3.9 e 3.3.12 abbiamo, per $n \geq 5041$,

$$\sigma(n) \leq e^{\gamma} n \log\log n < H_n + e^{H_n} \log(H_n)$$

Per $1 \leq n \leq 5040$ la (3.31) si verifica direttamente con il calcolo; l'unico caso di uguaglianza si ha con $n = 1$.
$\Rightarrow$) Supponiamo verificata la diseguaglianza. Andiamo per assurdo supponendo falsa l'ipotesi di Riemann, quindi applichiamo il teorema 3.3.10: però la stima contraddice il lemma 3.3.13. Così concludiamo che l'ipotesi di Riemann deve essere vera. □

# Bibliografia


[1] *W.W.Adams e L.J.Goldestein, Introduction to number theory, Maryland,1976.*

[2] *L.Alaoglu and P.Erdös, On Highly Composite and Similar Numbers, Trans. Amer. Math. Soc. 56 (1944), 448–469.*

[3] *M.Barnabei e F.Bonetti, Elementi di aritmetica modulare, Esculapio, Bologna, 2014.*

[4] *E.Bombieri, Problems of the millennium: The Riemann Hypothesis, CLAY, 2000*

[5] *H.E.Edwards, Riemann's Zeta Function, Academic Press: New York 1974.*

[6] *P.Erdös, On a New Method in Elementary Number Theory Which Leads to An Elementary Proof of the Prime Number Theorem, Proc. Nati. Acad. Sci. U.S.A. 1949 Jul; 35(7): 374-384.*

[7] *P.Erdös, On highly composite numbers, J. London Math. Soc., t.19 (1944) 130-133.*

[8] *P.Erdös e J.L.Nicolas, Repartition des nombres superabondants, Bull. Math. Soc. France 103 (1975) 65-90.*

[9] *L.J.Goldestein, A History of the Prime Number Theorem, The American Mathematical Monthly, Vol. 80, No. 6 (Jun. - Jul., 1973), pp. 599-615.*

[10] *G.H.Hardy e E.M.Wright, An introduction to the Theory of Number, Forth Edition. Oxford Univ. Press: Oxford 1960.*

[11] *J.C.Lagarias, An elementary problem equivalent to the Riemann hypothesis, Amer. Math. Monthly 109 (2002), 534–543.*

[12] *J.L.Nicolas e G.Robin, Majorations explicites pour le nombre de diviseurs de N, Cand. Math. Bull. Vol. 26 (4), 1983.*

[13] *J.L.Nicolas, Petites valeurs de la fonction d'Euler et hypothese de Riemann, Seminar on number theory, Paris 1981-82 (Paris 1981/1982), Birkhäuser, Boston 1983, pp. 207-218.*

[14] *J.L.Nicolas, Petites valeurs de la fonction d'Euler, J. Number Theory 17 (1983) 375-388.*

[15] *S.Ramanujan, Highly composite numbers, Proc. London Math. Soc. 14 (1915), 347-407.*

[16] *P.Ribenboim, The Book of Prime Number Records, Second Edition, Kingston, 1989.*

[17] *G.F.B.Riemann, Ueber die Anzahl der Primzalhem unter einer gegenenen Grösse, Monatsber. Akad. Berlin (1859), 671-680.*

[18] *G.Robin, Grandes valeurs de la fonction somme des diviseurs et hypothese de Riemann, J. Math. Pures Appl. 63 (1984), 187–213.*

[19] *J.B.Rosser and L.Schoenfeld, Approximate Formulas for Functions of Prime Numbers, Illinois J. Math. 6 (1962) 64-94*

[20] *J.B.Rosser and L.Schoenfeld, Sharper Bounds for the Chebyshev Functions $\theta(x)$ and $psi(x)$, Math Comp. 29 (1975) 243-269.*

[21] *J.B.Rosser and L.Schoenfeld, Sharper Bounds for the Chebyshev Functions $\theta(x)$ and $psi(x)$, Math Comp. 30 (1976) 337-360.*

[22] *A.Selberg ,An Elementary Proof of the Prime-Number Theorem (Annals of Mathematics, Second Series, Vol. 50, No. 2 (Apr., 1949), pp. 305-313.*