
**Facoltà di Scienze Matematiche, Fisiche e Naturali**
**Corso di laurea in Matematica**

# Teoria dei Numeri Elementare

**Note tratte dal corso del**
**prof. Giuseppe Puglisi**

**A.A. 2017/2018**

**Ultimo aggiornamento: 10/12/2018**

**Mattia Puddu**

# Indice

# Introduzione

Questi appunti sono il risultato della rielaborazione delle lezioni del professor G. Puglisi per il corso di Teoria dei Numeri Elementare, tenutosi nel secondo semestre dell'anno accademico 2017/2018.

Il filo conduttore di questi appunti è lo stesso del corso, salvo alcune piccole variazioni che consistono principalmente in un riordinamento di quanto fatto a lezione.

**Prerequisiti**

Quanto fatto nei corsi di Aritmetica e Analisi Matematica 1 del primo anno è essenziale. In alcune (piccole) parti, saranno utili determinati argomenti studiati durante i corsi di Algebra 1 e Algebra 2.

Per distinguere i risultati che non saranno dimostrati dagli altri, i primi verranno evidenziati in rosso. La teoria dei numeri è un terreno molto fertile per le congetture: alcune di queste saranno enunciate nel corso degli appunti, ed evidenziate in blu.

Assumeremo che $0 \notin \mathbb{N}$. Inoltre, con $p, q$ denoteremo sempre numeri primi, con $m, n, k$ degli interi e con $x, y$ numeri reali qualunque. Quando parleremo dei divisori di un numero intero, intenderemo esclusivamente quelli positivi. Scriveremo quasi sempre la fattorizzazione di un intero positivo $n > 1$ nel seguente modo

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

o più semplicemente, se non ci sono ambiguità,

$$n = \prod_{p|n} p^{v_p},$$

dove

$$v_p(n) = v_p = \max\{k \in \mathbb{N} \mid n \equiv 0 \mod p^k\}.$$

Per evidenziare questa proprietà, scriveremo anche $p^{v_p(n)} \parallel n$.

**Contatti**

In caso di dubbi o errori vari (spero non troppi) contattatemi all'indirizzo e-mail

*mattiapuddu@icloud.com*

# CAPITOLO 1

## Richiami di teoria

**Introduzione**

In questo capitolo, richiamiamo alcuni risultati e alcuni strumenti che si presumono noti e che saranno utili in seguito.

## 1.1. Relazioni asintotiche

Siano $S \subseteq \mathbb{R}$, $f, g : S \to \mathbb{R}$, $s_0 \in \overline{S} \subset \overline{\mathbb{R}} = \mathbb{R} \cup \{\pm\infty\}$. Diremo che:

- $f$ è $\mathcal{O}$ **grande** di $g$ per $s \to s_0$, e scriveremo $f \in \mathcal{O}(g, s_0)$, (o anche $f <<_{s_0} g$, $g >>_{s_0} f$, secondo la notazione di Vinogradov) se esiste $c \in \mathbb{R}$ tale che

$$|f(s)| \leq c \cdot |g(s)|,$$

per ogni $s$ in un opportuno intorno di $s_0$;

- $f$ e $g$ hanno **uguale ordine di grandezza** per $s \to s_0$, e scriveremo $f \asymp_{s_0} g$, se allo stesso tempo $f <<_{s_0} g$ e $g <<_{s_0} f$, ovvero se esistono due costanti positive $c_1,\ c_2$ tali che

$$c_1 \cdot |g(s)| \leq |f(s)| \leq c_2 \cdot |g(s)|,$$

per ogni $s$ in un opportuno intorno di $s_0$;

- $f$ è $o$ **piccolo** di $g$ per $s \to s_0$, e scriveremo $f \in o(g, s_0)$, se

$$\lim_{s \to s_0} \frac{f(s)}{g(s)} = 0;$$

- $f$ e $g$ sono **asintotiche** per $s \to s_0$, e scriveremo $f \sim_{s_0} g$ se

$$\lim_{s \to s_0} \frac{f(s)}{g(s)} = 1.$$

Il simbolo di appartenenza $\in$ nelle definizioni delle relazioni di $\mathcal{O}$ grande e $o$ piccolo è giustificato dal fatto che $\mathcal{O}(g, s_0)$ indica una classe di funzioni. Tuttavia, per comodità di scrittura, ci capiterà di scrivere espressioni come $f = g + \mathcal{O}(h, s_0)$ al posto di $f - g \in \mathcal{O}(h, s_0)$.

Enunciamo alcune proprietà utili riguardanti le relazioni asintotiche introdotte:

✓ Se $f \in \mathcal{O}(g, s_0)$, allora per ogni costante positiva $C$ anche $f \in \mathcal{O}(Cg, s_0)$;

✓ Se $f \in \mathcal{O}(g, s_0)$, e $g \in \mathcal{O}(h, s_0)$, allora anche $f \in \mathcal{O}(h, s_0)$;

✓ Se $f_1 \in \mathcal{O}(g_1, s_0)$, e $f_2 \in \mathcal{O}(g_2, s_0)$, allora anche $f_1 f_2 \in \mathcal{O}(g_1 g_2, s_0)$;

- ✓ Se $f_1 \in \mathcal{O}(g_1, s_0)$, e $f_2 \in \mathcal{O}(g_2, s_0)$, allora anche $f_1 + f_2 \in \mathcal{O}(|g_1| + |g_2|, s_0)$;
- ✓ Se $f \in \mathcal{O}(gh, s_0)$, allora anche $f \in g \cdot \mathcal{O}(h, s_0)$;
- ✓ Se $f, g : (a, b) \to \mathbb{R}$ sono integrabili e $f \in \mathcal{O}(g, s_0)$, con $-\infty < a < s_0 < b < +\infty$, allora anche

$$\int_{s_0}^{s} f(x)dx \in \mathcal{O}\left(\int_{s_0}^{s} g(x)dx, s_0\right);$$

- ✓ Se $f \in o(g, s_0)$, allora anche $f \in \mathcal{O}(g, s_0)$;
- ✓ Se $f \in o(g, s_0)$, allora per ogni costante positiva $C$ anche $f \in o(Cg, s_0)$;
- ✓ Se $f \in o(g, s_0)$, e $g \in o(h, s_0)$, allora anche $f \in o(h, s_0)$;
- ✓ Se $f_1 \in o(g_1, s_0)$, e $f_2 \in o(g_2, s_0)$, allora anche $f_1 f_2 \in o(g_1 g_2, s_0)$;
- ✓ Se $f_1 \in o(g_1, s_0)$, e $f_2 \in o(g_2, s_0)$, allora anche $f_1 + f_2 \in o(|g_1| + |g_2|, s_0)$;
- ✓ Se $f \in o(gh, s_0)$, allora anche $f \in g \cdot o(h, s_0)$;
- ✓ Se $f \sim_{s_0} g$, e $g \sim_{s_0} h$, allora anche $f \sim_{s_0} h$;
- ✓ Se $f \sim_{s_0} g$, allora anche $g \sim_{s_0} f$;
- ✓ Se $f_1 \sim_{s_0} g_1$ e $f_2 \sim_{s_0} g_2$, allora anche $f_1 f_2 \sim_{s_0} g_1 g_2$.

## 1.2. Serie numeriche e serie di funzioni

Sia $\{a_n\}_{n\in\mathbb{N}} \subset \mathbb{R}$ una successione, e sia $\sum_{n\in\mathbb{N}} a_n$ la serie numerica associata. Diremo che la serie

- **converge** se esiste $L \in \mathbb{R}$ tale che

$$\lim_{N\to+\infty} \sum_{n=1}^{N} a_n = L.$$

  In tal caso, potremo anche scrivere $\left|\sum_{n\in\mathbb{N}} a_n\right| < +\infty$;

- **converge assolutamente** se esiste $L \in \mathbb{R}$ tale che

$$\lim_{N\to+\infty} \sum_{n=1}^{N} |a_n| = L.$$

- ✓ Se una serie numerica converge assolutamente, allora converge anche semplicemente.

Siano $I \subset \mathbb{R}$ un intervallo aperto, $\{f_n : I \to \mathbb{R}\}_{n\in\mathbb{N}}$ una successione di funzioni e sia $\sum_{i\in\mathbb{N}} f_n$ la serie di funzioni associata. Diremo che la serie

- **converge puntualmente** a una funzione $F$ in $I$ se

$$\lim_{N\to+\infty} \sum_{n\in\mathbb{N}} f_n(s) = F(s) \quad \forall s \in I;$$

- **converge uniformemente** a una funzione $F$ in $I$ se

$$\lim_{N\to+\infty} \sup \left| \sum_{n\in\mathbb{N}} f_n(s) - F(s) \right| = 0 \quad \forall s \in I;$$

- **converge totalmente** a una funzione $F$ in $I$ se esiste una successione di numeri reali positivi $\{M_n\}_{n\in\mathbb{N}}$ tale che

$$\begin{cases} \sum_{n\in\mathbb{N}} M_n < +\infty \\ \left|\sum_{n\in\mathbb{N}} f_n(s)\right| \leq M_n \quad \forall n \in \mathbb{N}, \forall s \in I \end{cases}$$

  o, equivalentemente, se converge la serie numerica

$$\sum_{n\in\mathbb{N}} \sup_{s\in I} |f_n(s)| < +\infty.$$

✓ Se una serie di funzioni converge totalmente, allora converge anche uniformemente;

✓ Se una serie di funzioni converge uniformemente, allora converge anche puntualmente;

✓ Sia $\{f_n : I \to \mathbb{R}\}_{n\in\mathbb{N}}$ una successione di funzioni derivabili in $I$. Se la serie di funzioni ad essa associata converge puntualmente in $I$ e se la serie derivata $\sum_{i\in\mathbb{N}} f_n'$ converge uniformemente in $I$, allora la serie $\sum_{i\in\mathbb{N}} f_n$ è derivabile in $I$, e

$$\left(\sum_{i\in\mathbb{N}} f_n\right)' = \sum_{i\in\mathbb{N}} f_n'.$$

## 1.3. Strutture algebriche

Sia $\mathbb{M}$ un insieme, e sia $\star : \mathbb{M} \times \mathbb{M} \to \mathbb{M}$ un'operazione su $\mathbb{M}$. Diremo che $\mathbb{M}$ è un **monoide** se $\star$ è associativa e ammette un elemento neutro.

Sia $\mathbb{K}$ un campo, e sia $\mathbb{A}$ un $\mathbb{K}-$spazio vettoriale. Se $\mathbb{A}$ è dotato di un'operazione $\star : \mathbb{A} \times \mathbb{A} \to \mathbb{A}$ tale che, per ogni $x, y, z \in \mathbb{A}$, e per ogni $a, b \in \mathbb{K}$,

- $(x + y) \star z = (x \star z) + (y \star z)$,
- $x \star (y + z) = (x \star y) + (y \star z)$,
- $(ax) \star y = a(x \star y)$,
- $x \star (by) = b(x \star y)$

diremo che $\mathbb{A}$ è un'**algebra sul campo** $\mathbb{K}$, o più semplicemente una $\mathbb{K}-$**algebra**. Se $\mathbb{A}_1, \mathbb{A}_2$ sono due $\mathbb{K}-$algebre, diremo che $f : \mathbb{A}_1 \to \mathbb{A}_2$ è un **omomorfismo di algebre** se, per ogni $x, y \in \mathbb{A}_1$ e per ogni $k \in \mathbb{K}$

- $f(kx) = kf(x)$;
- $f(x + y)$;
- $f(xy) = f(x)f(y)$.

Sia $\mathcal{R}$ un anello commutativo con unità. Diremo che un elemento $a$ di $\mathcal{R}$ è

- **Divisore di** $0$ se esiste $b \in \mathcal{R} - \{0\}$ tale che $ab = 0$;
- **Invertibile** se esiste $b \in \mathcal{R} - \{0\}$ tale che $ab = 1$.

Diremo infine che $a, b \in \mathcal{R}$ sono **associati** se esiste un elemento invertibile $\gamma \in \mathcal{R}$ tale che $a = \gamma b$. Denoteremo con $\mathcal{R}^\star$ l'insieme degli elementi invertibili di $\mathcal{R}$.

✓ $\mathcal{R}^\star$ è un gruppo moltiplicativo.

Siano $\mathcal{R}, \mathbb{S}$ due anelli commutativi con unità. Diremo che $f : \mathcal{R} \to \mathbb{S}$ è un **omomorfismo di anelli** se, per ogni $a, b \in \mathcal{R}$,

- $f(a + b) = f(a) + f(b)$;
- $f(ab) = f(a)f(b)$;
- $f(1_\mathcal{R}) = 1_\mathbb{S}$.

Diremo che $\mathcal{R}$ è un **anello locale** se ammette uno e un solo ideale massimale, e che è un **dominio di integrità**, o più semplicemente **dominio**, se il suo unico divisore di zero è $0$. Dato un dominio $\mathbb{D}$, diremo che un elemento $x \in \mathbb{D} - \{0\}$ è

- **Primo** se non è invertibile e per ogni $a, b \in \mathbb{D}$, se $p \mid ab$ allora anche $p \mid a$ oppure $p \mid b$;
- **Irriducibile** se non è invertibile e per ogni $a, b \in \mathbb{D}$, se $x = ab$, allora $a \in \mathbb{D}^\star$ oppure $b \in \mathbb{D}^\star$.

✓ Dato un dominio $\mathbb{D}$, se $p \in \mathbb{D}$ è primo, allora è anche irriducibile.

Diremo che un dominio di integrità $\mathbb{D}$ è un **anello euclideo** se esiste una funzione **grado** $g : \mathbb{D} - \{0\} \to \mathbb{N}$ tale che

- $\forall a, b \in \mathbb{D} - \{0\}$, $g(a) \leq g(ab)$;
- $\forall a, b \in \mathbb{D}$, con $b \neq 0$, esistono $q, r \in \mathbb{D}$ tali che $a = qb + r$, dove $r = 0$, oppure $g(r) < g(b)$.

Diremo invece che un dominio di integrità $\mathbb{D}$ è un **dominio a ideali principali**, o più semplicemente **PID**, se ogni suo ideale è principale, e che è un **dominio a fattorizzazione unica**, o più semplicemente **UFD**, se ogni elemento di $\mathbb{D} - \{0\}$ non invertibile si scrive come prodotto di un numero finito di elementi irriducibili di $\mathbb{D}$, e tale decomposizione è unica, a meno dell'ordine e di elementi associati. In un UFD, ha senso parlare di massimo comun divisore e di minimo comune multiplo.

✓ Ogni anello euclideo è anche un PID. Ogni PID è anche un UFD.

✓ $\mathbb{Z}$ è un anello euclideo, PID, UFD.

✓ Se $\mathbb{D}$ è un UFD, $p \in \mathbb{D}$ è irriducibile se e solo se è primo.

Un anello commutativo con unità $\mathcal{R}$ si dice **noetheriano** se ogni suo ideale è finitamente generato.

✓ Un anello commutativo con unità $\mathcal{R}$ è noetheriano se e solo se ogni sua catena ascendente di ideali è stazionaria.

✓ Un anello commutativo con unità $\mathcal{R}$ è noetheriano se e solo se ogni famiglia di ideali di $\mathcal{R}$ non vuota ammette un elemento massimale (rispetto alla relazione di inclusione $\subseteq$).

Ricordiamo infine i teoremi di Fermat, di Eulero, e il teorema cinese del resto (o più semplicemente CRT):

**(Fermat)** Se $p$ è un numero primo, per ogni intero $a \in \mathbb{Z}$, $a^p \equiv a \mod p$;

**(Eulero)** Se $n \in \mathbb{N}$ e $m \in \mathbb{Z}$ sono coprimi, $m^{\phi(n)} \equiv 1 \mod n$;

**(CRT)** Se $n_1, \ldots, n_m$ sono interi positivi a due a due coprimi, comunque si scelgano $a_1, \ldots, a_m \in \mathbb{Z}$ il sistema di congruenze

$$\begin{cases} x \equiv a_1 \mod n_1 \\ \ldots \\ x \equiv a_m \mod n_m \end{cases}$$

ammette una e una sola soluzione.

# CAPITOLO 2

## Il problema della distribuzione dei numeri primi

**Introduzione**

In questo capitolo, introduciamo il problema della distribuzione dei numeri primi, dimostrando alcuni semplici risultati. Elencheremo inoltre alcune congetture, come la congettura di Goldbach, e anche alcuni teoremi avanzati, con l'intento di far capire quanto sia ricca e profonda la teoria dei numeri.

Diremo che $p \in \mathbb{N} - \{1\}$ è un **numero primo** se gli unici divisori di $p$ sono 1 e $p$. Denoteremo con $\mathbb{P}$ l'insieme dei numeri primi, e con $\mathbb{P}^\star = \mathbb{P} - \{2\}$ l'insieme dei numeri primi dispari. Poiché $\mathbb{N}$ è un insieme totalmente ordinato, possiamo ordinare gli elementi di $\mathbb{P}$ in una successione, che denoteremo con $\{p_n\}_{n\in\mathbb{N}}$ : purtroppo, non si conosce una formula chiusa per i numeri primi, ovvero un'applicazione

$$\begin{aligned} f: \quad N \quad &\to \quad \mathbb{N} \\ n &\mapsto p_n \end{aligned}$$

Iniziamo con un risultato classico:

**Teorema 2.1. (Euclide)** *I numeri primi sono infiniti.*

**Dimostrazione**

Supponiamo per assurdo che i numeri primi siano in numero finito, $n$, e sia $q_1, \ldots, q_n$ una loro elencazione. Il numero $P = q_1 \ldots q_n + 1$ non è divisibile per nessuno dei $q_k$ ed è maggiore di ciascuno di essi. Se $P$ è primo, abbiamo trovato un nuovo primo che non sta nell'elenco, se non lo è, è sicuramente divisibile per un primo che non sta nell'elenco. In ogni caso, l'elenco dei primi è incompleto, assurdo.

□

Seguendo l'idea alla base del teorema di Euclide sull'infinità dei primi, costruiamo la successione $\{z_n\}_{n\in\mathbb{N}} \subset \mathbb{N}$ definita da

$$\begin{cases} z_1 = p_1 = 2 \\ z_n = \prod_{k=1}^{n-1} p_k + 1 \quad \text{se } n > 1 \end{cases}$$

Tale successione non è fatta di soli primi (ad esempio, $z_6 = 30031 = 59 \cdot 509$) né li contiene tutti, dato che è chiaramente crescente, $z_2 = 3$, $z_3 = 7$, e quindi ad esempio il numero primo 5 non appartiene alla successione. Osserviamo che, per ogni $n > 1$ $p_n \leq z_n$, da cui

$$p_n \leq z_n = \prod_{k=1}^{n-1} p_k + 1 < \prod_{k=1}^{n-1} p_{n-1} + 1 = p_{n-1}^{n-1} + 1.$$

Miglioreremo in seguito questa disuguaglianza.

**Proposizione 2.1.** *Se $n \in \mathbb{N}$ non è primo, allora ammette almeno un fattore primo che è minore o uguale a $\sqrt{n}$.*

**Dimostrazione**

Supponiamo che $n$ sia prodotto di due primi, $n = pq$. Se fosse $\min\{p, q\} > \sqrt{n}$, si avrebbe $pq > n$, assurdo. A maggior ragione, la tesi è vera se $n$ è prodotto di più di due primi.

□

Questo semplicissimo risultato è alla base del famoso crivello di Eratostene, un modo per trovare i numeri primi in un intervallo: dato $n \in \mathbb{N}$, e supposti noti tutti i primi minori o uguali a $\sqrt{n}$, si ottengono tutti i primi $p$ compresi fra $\sqrt{n}$ e $n$ cancellando dall'elenco dei numeri da $\sqrt{n}$ a $n$ tutti i multipli di questi numeri primi. Accenneremo in seguito ai metodi di crivello.

## 2.1. I numeri di Fermat

Chiamiamo successione dei numeri di Fermat la successione

$$\{F_n\}_{n\in\mathbb{N}} = \{2^{2^{n-1}} + 1\}_{n\in\mathbb{N}}$$

Calcoliamone i primi termini:

| $n$ | $F_n$ |
|---|---|
| 1 | 3 |
| 2 | 5 |
| 3 | 17 |
| 4 | 257 |

Questi numeri sono tutti primi, tuttavia la speranza che questa successione sia fatta di soli primi è vana: $641 \nmid F_6$. Anzi, si congettura che

**Congettura 2.1.** *Il numero di primi di Fermat è finito.*

Questa successione ha comunque proprietà interessanti:

**Proposizione 2.2.** *Se $m, n \in \mathbb{N}$ e $m > n$, allora $F_n \mid F_m - 2$. In particolare, per ogni $m, n \in \mathbb{N}$, $m \neq n$, $(F_n, F_m) = 1$.*

**Dimostrazione**

Poniamo $m = n + k$, $k \in \mathbb{N}$. Osserviamo che

$$\frac{F_{n+k} - 2}{F_n} = \frac{2^{2^{n+k-1}} - 1}{2^{2^{n-1}} + 1} = \frac{(2^{2^{n-1}})^{2^k} - 1}{2^{2^{n-1}} + 1} \in \mathbb{N}$$

in quanto vale l'identità

$$x^{2N} - 1 = (x + 1) \sum_{k=0}^{2N-1} (-1)^{k+1} x^k,$$

per ogni $x \in \mathbb{R}$, $N \in \mathbb{N}$. Quindi, $F_n \mid F_m - 2$. In particolare, se $p$ divide sia $F_{n+k}$ sia $F_n$, deve dividere anche 2. Poiché i numeri di Fermat sono dispari, l'unica possibilità è che $F_m, F_n$ siano coprimi.

□

## 2.2. Il Teorema dei Numeri Primi

Anziché cercare di trovare una formula chiusa per i numeri primi, accontentiamoci di risolvere un problema più semplice, cercando delle funzioni $f : \mathbb{N} \to \mathbb{N}$ che siano **frequentemente prime**, cioè tali che $f(n)$ sia primo per infiniti valori di $n \in \mathbb{N}$.

Introduciamo la seguente importante funzione, detta anche **counting function**:

$$\begin{aligned} \pi : \quad [1,+\infty) &\to \mathbb{R} \\ x &\mapsto \sum_{p \le x} 1. \end{aligned}$$

É semplice notare che la counting function è non decrescente, costante a tratti, e che $\pi(p_n) = n$, per ogni $n \in \mathbb{N}$. Vogliamo studiare con quale ordine questa funzione cresca: osserviamo i valori del rapporto fra $n$ e $\pi(n)$ per certi valori di $n$ :

| $n$ | $\pi(n)$ | $\frac{n}{\pi(n)}$ |
|---|---|---|
| 10 | 4 | 2,5 |
| 100 | 25 | 4 |
| 1.000 | 168 | 5,95 |
| 10.000.000 | 664.579 | 15,05 |
| 100.000.000 | 5761455 | 17.36 |

La quantità $\frac{n}{\pi(n)}$ può essere interpretata come la distanza media tra due primi consecutivi. Gauss intuì che

$$\lim_{k\to+\infty} \frac{10^{k+1}}{\pi(10^{k+1})} - \frac{10^k}{\pi(10^k)} = \log 10,$$

e congetturò quello che è noto come il teorema dei numeri primi (PNT), che si può presentare nella forma seguente:

**Teorema 2.2. (PNT)** $\pi(x) \sim_{+\infty} \frac{x}{\log x}$.

Di questo teorema si conoscono sia una dimostrazione analitica (Hadamard, 1896), sia una dimostrazione elementare (Selberg, 1949). Un'altra versione del PNT è:

**Teorema 2.3. (PNT)**

$$\pi(x) \sim_{+\infty} Li(x),$$

dove

$$\begin{aligned} Li : \quad (2,+\infty) &\to \mathbb{R} \\ x &\mapsto \int_2^x \frac{dy}{\log y} \end{aligned}$$

è la funzione **logaritmo integrale**.[1]

[1] Potremmo definire la funzione logaritmo integrale, anziché su $(2,+\infty)$, su $(0,+\infty) - \{1\}$. In questo caso, per $z < 2$, il valore di

$$\int_2^z \frac{1}{\log x} dx = -\int_z^2 \frac{1}{\log x} dx$$

è inteso nel senso di valore principale di Cauchy, ovvero ponendo

$$\int_z^2 \frac{1}{\log x} dx = \lim_{\epsilon\to 0^+} \int_0^{1-\epsilon} \frac{1}{\log n} dx + \int_{1+\epsilon}^2 \frac{1}{\log n} dx.$$

Un risultato più semplice, che dimostreremo più avanti, è il seguente:

**Teorema 2.4. (Chebychev)** *Vale la seguente stima asintotica*

$$\pi(x) \asymp_{+\infty} \frac{x}{\log x}.$$

Vediamo una stima per la counting function. Premettiamo alcuni risultati:

**Lemma 2.1.** *Esiste un numero reale* $x^\star \in (2,3)$ *tale che, per ogni* $x > x^\star$,

$$x - 1 \geq \log\log 2 + x \log 2.$$

*In particolare, per ogni* $x > x\star$, $e^{x-1} \geq 2^x \log 2$.

**Dimostrazione**
La funzione

$$\begin{array}{rccc} f: & \mathbb{R} & \to & \mathbb{R} \\ & x & \mapsto & (1-\log 2)x - 1 - \log\log 2 \end{array}$$

è di classe $\mathcal{C}^1(\mathbb{R})$, e $f(2) < 0$, $f(3) > 0$, $f'(x) = 1 - \log 2 > 0$, per ogni $x \in \mathbb{R}$. La conclusione è immediata.

□

**Lemma 2.2.** $p_n < 2^{2^n}$, *per ogni* $n \in \mathbb{N}$.

**Dimostrazione**
Procediamo per induzione su $n$ :

- (passo base, $n = 1$) Basta osservare che $p_1 = 2 < 4 < 2^2$;
- (passo induttivo $1, \ldots, n \Rightarrow n+1$) Usando l'ipotesi induttiva, otteniamo

$$p_{n+1} \leq \prod_{k=1}^{n} p_k + 1 \overset{\text{Ip.Ind}}{<} \prod_{k=1}^{n} 2^{2^k} + 1 = 2^{\sum_{k=1}^{n} 2^k} + 1 = 2^{2(2^n-1)} + 1 < 2^{2^{n+1}}.$$

□

Possiamo ora dimostrare il seguente risultato:

**Proposizione 2.3.** *Per ogni* $x \in [2, +\infty)$, $\pi(x) \geq \log\log x$.

**Dimostrazione**
Sia $n \geq 4$ un numero naturale, e sia $e^{e^{n-1}} < x \leq e^{e^n}$. Per monotonia,

$$\pi(x) \geq \pi(e^{e^{n-1}}) \overset{Lem\ 2.1}{\geq} \pi(2^{2^n}) \overset{Lem\ 2.2}{\geq} \pi(p_n) = n \geq \log\log x.$$

Quindi la tesi per $x > e^{e^3}$. Se invece $5 \leq x \leq e^{e^3}$ $\log\log x \leq 3$, e quindi per $x \geq 5$, dato che $\pi(x) \geq 3$, la proposizione è dimostrata. Infine, se $2 \leq x < 5$, $\pi(x) \geq 1$, e poiché per $x < e^e$ $\log\log x < 1$, abbiamo la tesi.

□

A proposito della distribuzione dei numeri primi è interessante il seguente:

**Proposizione 2.4.** *Esistono sequenze di numeri naturali consecutivi di lunghezza arbitraria che non contengono nessun primo.*

**Dimostrazione**
Sia $n$ un numero naturale qualsiasi, e sia $p$ il più piccolo primo maggiore di $n$. Consideriamo la sequenza di numeri naturali consecutivi

$$p! + 2,\ p! + 3,\ \ldots,\ p! + p.$$

Essa ha lunghezza $p - 1$, ed è interamente costituita da numeri naturali composti. In particolare, essendo $n \leq p - 1$, abbiamo la tesi.

□

Enunciamo, senza darne la dimostrazione alcuni teoremi noti. Sia $A \subset \mathbb{N}$, chiamiamo densità asintotica di $A$, se esiste, il limite

$$d_A = \lim_{n\to+\infty} \frac{|A \cap \{1, 2, 3, \ldots, n\}|}{n} = \lim_{x\to+\infty} \frac{1}{x} \sum_{\substack{n\leq x \\ n\in A}} 1,$$

mentre chiamiamo densità superiore e densità inferiore di $A$, rispettivamente, i limiti

$$\overline{d_A} = \limsup_{n\to+\infty} \frac{|A \cap \{1, 2, 3, \ldots, n\}|}{n} = \limsup_{x\to+\infty} \frac{1}{x} \sum_{\substack{n\leq x \\ n\in A}} 1,$$

$$\underline{d_A} = \liminf_{n\to+\infty} \frac{|A \cap \{1, 2, 3, \ldots, n\}|}{n} = \liminf_{x\to+\infty} \frac{1}{x} \sum_{\substack{n\leq x \\ n\in A}} 1.$$

**Teorema 2.5.** *Esiste una costante positiva $K$ ed esistono infiniti numeri naturali $n$ tali che $p_{n+1} - p_n \leq K$.*

**Teorema 2.6.** *La successione*

$$\left\{ \frac{p_n - p_{n-1}}{\log p_n} \right\}_{n\in\mathbb{N}}$$

*è tale che l'insieme dei suoi punti di accumulazione ha misura di Lebesgue positiva. In particolare, per il teorema 2.5, tale successione ha $0$ fra i suoi punti di accumulazione.*

**Teorema 2.7. (Szmeredy, 1975)** *Se $A \subset \mathbb{N}$ ha densità superiore positiva, allora $A$ contiene infinite progressioni aritmetiche di lunghezza $k$, per ogni $k \in \mathbb{N}$.*

**Teorema 2.8. (Green-Tao, 2004)** *Se $A \subset \mathbb{P}$ è tale che*

$$\limsup_{N\to+\infty} \frac{|A \cap \{1, 2, 3, \ldots, n\}|}{\pi(N)} > 0,$$

*allora $A$ contiene infinite progressioni aritmetiche di lunghezza $k$, per ogni $k \in \mathbb{N}$. In particolare, esistono progressioni aritmetiche di numeri primi di lunghezza arbitraria.*

## 2.3. Numeri primi di una determinata forma

**Proposizione 2.5.** *Siano $n, k \in \mathbb{N}$, con $n, m > 1$. Se $n^k + 1$ è primo, allora $n$ è pari e $k$ è una potenza di 2.*

**Dimostrazione**

Se $n^k + 1$ è primo, ovviamente $n$ è pari, altrimenti $n^k + 1$ è pari e maggiore di 2. Poniamo $k = 2^h d$, con $d \in \mathbb{N}$ dispari. Allora esiste $m \in \mathbb{N}$ tale che

$$n^k + 1 = (n^{2^h})^d + 1 = (n^{2^h} + 1)m.$$

Poiché $n^k + 1$ è primo, necessariamente $m = 1$, e $n^k + 1 = n^{2^h} + 1$, cioè $n$ è una potenza di 2.

□

**Proposizione 2.6.** *Siano $n, k \in \mathbb{N}$, con $n, m > 1$. Se $n^k - 1$ è primo, allora $n = 2$ e $k \in \mathbb{P}$.*

**Dimostrazione**

Osserviamo che se $n > 2$, $n - 1 \mid n^k - 1$, e la divisibilità sarebbe propria, quindi necessariamente $n = 2$. Inoltre, se $k$ non fosse primo, potremmo scrivere $k = q_1 q_2$, con $q_1, q_2 > 1$ e si avrebbe la relazione di divisibilità propria $2^{q_1} - 1 \mid 2^k - 1$.

□

La successione $\{M_n\}_{n\in\mathbb{N}} = \{2^{p_n} - 1\}_{n\in\mathbb{N}}$ è la successione dei **numeri di Mersenne.** La ritroveremo in seguito, quando parleremo dei numeri perfetti.

**Proposizione 2.7.** *Non esiste un polinomio $p(x) \in \mathbb{Z}[x]$ di grado positivo tale che $p(m)$ sia primo per ogni $m \in \mathbb{N}$.*

**Dimostrazione**

Poniamo

$$p(x) = \sum_{k=0}^{N} a_k x^k,$$

con $a_N > 0$. Poiché $\lim_{n\to+\infty} p(n) = +\infty$, esiste $M \in \mathbb{N}$ tale che, per ogni numero naturale $n > M$ valga $p(n) > 1$. Poiché $p(n) \mid p(n + rp(n))$, comunque si scelga $r \in \mathbb{N}$, e dato che

$$\lim_{r\to+\infty} p(n + rp(n)) = +\infty,$$

esistono infiniti numeri naturali $m$ tali che $p(m)$ non è primo.

□

## 2.4. Congetture sui numeri primi

Elenchiamo alcune congetture sui numeri primi:

**Congettura 2.2.** *Siano $a, b, c \in \mathbb{N}$ primi tra loro e tali che $a$ sia positivo, $a + b$ e $c$ non siano entrambi pari, e $b^2 - 4ac$ non sia un quadrato perfetto. Allora esistono infiniti $n \in \mathbb{N}$ tali che $an^2 + bn + c$ sia primo.*

**Congettura 2.3. (Goldbach)** *Sia $n > 2$. Allora esistono $p_1, p_2 \in \mathbb{P}^\star$ tali che $2n = p_1 + p_2$.*

Vinogradov ha dimostrato nel 1930 la versione "dispari" della congettura:

**Teorema 2.9. (Vinogradov)** *Per ogni $n \in \mathbb{N}$, $n \geq 3$, esistono $p_1, p_2, p_3 \in \mathbb{P}$ tali che*

$$2n + 1 = p_1 + p_2 + p_3.$$

**Congettura 2.4.** *Esiste una costante positiva $c$ tale che, per ogni $x > 1$, se $y \geq c\sqrt{x}\log x$ allora esiste un primo compreso fra $x$ e $x + y$.*

Diremo che $(p, p + 2)$ è una coppia di numeri **primi gemelli** se $p, p + 2 \in \mathbb{P}$. Denoteremo con $\mathbb{P}_2$ l'insieme dei numeri primi che appartengono a una coppia di primi gemelli. Definiamo una **counting function per i primi gemelli**

$$\begin{aligned} \pi_2 : \quad [1, +\infty) &\to \mathbb{R} \\ x &\mapsto \sum_{\substack{p \leq x \\ p \in \mathbb{P}_2}} 1. \end{aligned}$$

**Congettura 2.5.** *Esistono infinite coppie di primi gemelli.*

## 2.5. Numeri primi e progressioni

Vale il seguente teorema, che dimostreremo alla fine del corso:

**Teorema 2.10. (Dirichlet)** *Se $m, n$ sono tali che $1 \leq m \leq n$ e $(m, n) = 1$, allora esistono infiniti numeri primi congrui ad $m$ modulo $n$.*

Al momento, possiamo riadattare la dimostrazione del teorema di Euclide sull'infinità dei numeri primi per dimostrare che in alcune progressioni aritmetiche questi ultimi compaiono frequentemente:

**Proposizione 2.8.** *Esistono infiniti numeri primi congrui a 3 modulo 4.*

**Dimostrazione**

Supponiamo che i primi di tale forma siano finiti, e sia $q_1, \ldots, q_n$ una loro elencazione. Il numero $P = 4 \cdot q_1 \ldots q_n - 1$ è congruo a 3 modulo 4 e nessuno dei $q_i$ lo divide. Se $P$ è primo, abbiamo trovato un nuovo primo che non sta nell'elenco, se non lo è, è sicuramente divisibile per un primo che non sta nell'elenco: infatti, se tutti i primi che lo dividono fossero congrui a 1 modulo 4 anche $P$ sarebbe congruo a 1 modulo 4. In ogni caso, l'elenco dei primi è incompleto, assurdo.

□

**Proposizione 2.9.** *Esistono infiniti numeri primi congrui a 5 modulo 6.*

**Dimostrazione**

Come prima, supponiamo che i primi di tale forma siano finiti, e sia $q_1, \ldots, q_n$ una loro elencazione. Il numero $P = 6 \cdot q_1 \ldots q_n - 1$ è congruo a 5 modulo 6 e nessuno dei $q_i$ lo divide. Se $P$ è primo, abbiamo trovato un nuovo primo che non sta nell'elenco, se non lo è, è sicuramente divisibile per un primo che non sta nell'elenco: infatti, se tutti i primi che lo dividono fossero congrui a 1 modulo 6 anche $\alpha$ sarebbe congruo a 1 modulo 6. In ogni caso, l'elenco dei primi è incompleto, assurdo.

□

Dando per buono il seguente risultato, che dimostreremo in seguito, possiamo dimostrare anche qualcosa di più:

**Proposizione 2.10.** *Se $p \in \mathbb{P}$ e $m, n \in \mathbb{N}$ sono tali che $p \mid m^2 + n^2$ e $(m, n) = 1$, allora o $p = 2$ o $p \equiv 1 \mod 4$.*

**Proposizione 2.11.** *Esistono infiniti numeri primi congrui a $1$ modulo $4$.*

**Dimostrazione**
Come prima, supponiamo che i primi di tale forma siano finiti, e sia $q_1, \ldots, q_n$ una loro elencazione. Il numero $P = 4q_1^2 \ldots q_n^2 + 1$ è congruo a $1$ modulo $4$ e nessuno dei $q_i$ lo divide. Se $P$ è primo, abbiamo trovato un nuovo primo che non sta nell'elenco, se non lo è, è sicuramente divisibile per un primo che non sta nell'elenco: infatti, per la proposizione 2.10, i primi che lo dividono sono congrui a $1$ modulo $4$. In ogni caso, l'elenco dei primi è incompleto, assurdo.

□

## 2.6. I numeri perfetti

Diremo che $n \in \mathbb{N}$ è un **numero perfetto** se $\sigma(n) = 2n$, mentre diremo che è un **numero abbondante** se $\sigma(n) > 2n$. Ad esempio, $6$ è un numero perfetto, mentre $120$ è un numero abbondante:

$$\sigma(6) = 1 + 2 + 3 + 6 = 12,$$

$$\sigma(120) = 1 + 2 + 3 + 4 + 5 + 6 + 8 + 10 + 12 + 15 + 20 + 24 + 30 + 40 + 60 + 120 = 360.$$

Valgono i seguenti teoremi:

**Teorema 2.11. (Euclide)** *Per ogni $n \in \mathbb{N}$, $2^{n-1}(2^n - 1)$ è un numero perfetto se e solo se $2^n - 1$ è un numero primo, cioè un primo di Mersenne.*

**Dimostrazione**

($\Leftarrow$) Se $2^n - 1$ è primo, allora $\sigma(2^{n-1}(2^n - 1)) = (1 + 2^n - 1)(2^n - 1) = 2^n(2^n - 1)$.

($\Rightarrow$) Se $2^n - 1$ non è primo, $2^{n-1}(2^n - 1)$ è chiaramente sovrabbondante.

**Teorema 2.12. (Eulero)** *Un numero perfetto $n$ pari è della forma $(2^{\rho+1} - 1)2^\rho$, con $\rho + 1, 2^{\rho+1} - 1 \in \mathbb{P}$.*

**Dimostrazione**
Poniamo $n = 2^\rho \delta$, e supponiamo che $\sigma(n) = 2n$. Poiché $\sigma$ è una funzione aritmetica moltiplicativa, si deve avere

$$\sigma(\delta)\sigma(2^\rho) = 2^{\rho+1}\delta \Rightarrow \sigma(\delta)(2^{\rho+1} - 1) = 2^{\rho+1}\delta.$$

Gli interi $2^{\rho+1} - 1$ e $2^{\rho+1}$ sono coprimi, quindi

$$\frac{2^{\rho+1}}{2^{\rho+1} - 1}$$

è una frazione ridotta ai minimi termini: deve esistere un intero positivo $m$ tale che

$$\sigma(\delta) = 2^{\rho+1}m$$

$$\delta = \left(2^{\rho+1} - 1\right) m.$$

Supponiamo per assurdo che $m$ sia maggiore di $1$ : allora

$$1, m, \delta$$

sono divisori distinti di $\delta$, e

$$2^{\rho+1}m = \sigma(\delta) \geq 1 + m + \left(2^{\rho+1} - 1\right) m = 2^{\rho+1}m + 1,$$

assurdo. Quindi $m = 1$, e

$$\delta = 2^{\rho+1} - 1$$
$$\sigma(\delta) = 2^{\rho+1}.$$

Ma solo i numeri primi hanno come somma dei divisori il loro successivo, quindi $2^{\rho+1} - 1$ è un primo. Per la proposizione 2.6, anche $\rho + 1$ è un primo.

□

Attualmente, non si conoscono numeri perfetti dispari, anzi si congettura che

**Congettura 2.6.** *Non esistono numeri interi perfetti dispari.*

Questi risultati sui numeri perfetti sono poco sopra al livello delle curiosità matematiche, nel senso che non hanno dato impulso alla ricerca matematica, come ad esempio ha fatto l'ultimo teorema di Fermat, dimostrato da Wiles alla fine del ventesimo secolo, che ha dato vita alla teoria algebrica dei numeri:

**Teorema 2.13. (Fermat-Wiles)** *Sia $n$ un intero positivo maggiore di 2. Non esistono terne di numeri interi positivi $(a, b, c)$ tale che*

$$a^n + b^n = c^n.$$

Un altro risultato, molto bello ma che non ha prodotto nessun nuovo sviluppo è la congettura di Catalan, oggi anche nota come **teorema di Mihailescu**, dal nome di Preda Mihailescu, matematico rumeno che l'ha dimostrata nel 2002 :

**Teorema 2.14. (Catalan-Mihailescu)***L'unica soluzione dell'equazione diofantea*

$$x^a - y^b = 1$$

*sui numeri naturali maggiori di 1 è $(x, y, a, b) = (3, 2, 2, 3)$. In altre parole, le uniche due potenze consecutive con esponente maggiore di 1 sono 8 e 9.*

# CAPITOLO 3

## Il teorema dei quattro quadrati

**Introduzione**

In questo capitolo, enunceremo e dimostreremo alcuni risultati di approssimazione, dovuti a Dirichlet. In seguito, definiremo i residui quadratici modulo un primo e ne studieremo le principali proprietà. Affronteremo infine il problema della rappresentazione di un intero come somma di due, tre e quattro quadrati, dimostrando il teorema di Lagrange che afferma che ogni numero naturale è esprimibile come somma di al più quattro quadrati.

## 3.1. Gli anelli $\mathbb{Z}[i\sqrt{n}]$, $n \in \mathbb{N}$

Sia $n$ un numero naturale libero da quadrati: ci chiediamo per quali $n$ l'anello $\mathbb{Z}[i\sqrt{n}]$ sia euclideo. Definiamo l'applicazione **norma**

$$\begin{array}{rccc} N: & \mathbb{C} & \to & \mathbb{R} \\ & z & \mapsto & z\overline{z} \end{array}$$

**Lemma 3.1.** $N(\alpha\beta) = N(\alpha)N(\beta)$, *per ogni* $\alpha, \beta \in \mathbb{C}$.

**Dimostrazione**
Basta osservare che

$$N(\alpha\beta) = \alpha\beta\overline{\alpha\beta} = \alpha\overline{\alpha}\beta\overline{\beta} = N(\alpha)N(\beta).$$

□

**Lemma 3.2.** $\alpha \in \mathbb{Z}[i\sqrt{n}]^\star$ *se e solo se* $N(\alpha) = 1$. *In particolare,* $\mathbb{Z}[i]^\star = \{1, -1, i, -i\}$.

**Dimostrazione**
Se $\alpha$ è un'unità,

$$1 = \alpha\alpha^{-1} \Rightarrow 1 = N(1) \overset{Lem\ 3.1}{=} N(\alpha)N(\alpha^{-1}).$$

Ma essendo $N(\alpha), N(\alpha^{-1})$ due numeri naturali, necessariamente $N(\alpha) = N(\alpha^{-1}) = 1$. Se invece $\alpha$ è tale che $N(\alpha) = 1$, posto $\alpha = x + iy\sqrt{n}$, si deve avere $x^2 + ny^2 = 1$. Se $n > 1$, le unica possibilità sono $x = 1, y = 0$ e $x = -1, y = 0$, che corrispondono a $\alpha = 1$ e $\alpha = -1$, che sono unità in $\mathbb{Z}[i\sqrt{n}]$. Invece, se se $n = 1$, è semplice osservare che le uniche possibilità per $\alpha$ sono $1, -1, i, -i$, che sono unità in $\mathbb{Z}[i]$.

□

**Lemma 3.3.** 2 *è irriducibile in* $\mathbb{Z}[i\sqrt{n}]$, *per ogni* $n \in \mathbb{N}$, $n \geq 3$.

**Dimostrazione**
Se $2 = (a + ib\sqrt{n})(c + id\sqrt{n})$ in $\mathbb{Z}[i\sqrt{n}]$, passando alle norme, se nessuno dei due fattori fosse un'unità,

$$4 = (a^2 + nb^2)(c^2 + nd^2) \Rightarrow \begin{cases} a^2 + nb^2 = 2 \\ c^2 + nd^2 = 2 \end{cases}.$$

Poiché le ultime due equazioni, per $n \geq 3$, non hanno soluzione in $\mathbb{Z}$, abbiamo un assurdo. Quindi uno dei due fattori è un'unità, e 2 è irriducibile in $\mathbb{Z}[i\sqrt{n}]$.

□

Invece

**Lemma 3.4.** *2 non è primo in $\mathbb{Z}[i\sqrt{n}]$, per ogni $n \in \mathbb{N}$.*

**Dimostrazione**
*Se $n = 1$, oppure se $n = 2$, nno le fattorizzazioni*

$$2 = (1+i)(1-i)$$
$$2 = (i\sqrt{2})(-i\sqrt{2}.$$

*Quindi 2 non è irriducibile e nemmeno primo. Supponiamo $n > 2$ : se $n$ è pari, allora $2 \mid n = (i\sqrt{n})(-i\sqrt{n})$, ma non divide nessuno dei due fattori (osserviamo che se dividesse uno dei due fattori, allora dividerebbe anche l'altro, poiché sono associati): se dividesse $i\sqrt{n}$, esisterebbe $a + ib\sqrt{n} \in \mathbb{Z}[i\sqrt{n}]$ tale che*

$$2(a + ib\sqrt{n}) = i\sqrt{n}.$$

*Ma allora si dovrebbe avere $2b = 1$, assurdo. Quindi 2 non è primo in $\mathbb{Z}[i\sqrt{n}]$ per ogni $n \in \mathbb{N}$.*

□

Questo lavoro ci permette di dimostrare il seguente

**Teorema 3.1.** *$\mathbb{Z}[i\sqrt{n}]$ è euclideo se e solo se $n = 1, 2$. In particolare, $\mathbb{Z}[i]$ e $\mathbb{Z}[i\sqrt{2}]$ sono PID, UFD.*

**Dimostrazione**
Prendiamo $\alpha, \beta \in \mathbb{Z}[i\sqrt{n}]$, $\alpha \neq 0$, e consideriamo $\lambda = \frac{\beta}{\alpha}$ : osserviamo che possiamo scrivere $\lambda = u + iv\sqrt{n}$, con $u, v \in \mathbb{Q}$. Siano inoltre $a, b \in \mathbb{Z}$ tali che

$$|u - a| = d(u, \mathbb{Z})$$
$$|v - b| = d(v, \mathbb{Z}),$$

e poniamo $\gamma = a + ib\sqrt{n}$ : osserviamo che

$$|u - a|, |v - b| \leq \frac{1}{2} \tag{3.1}$$

e inoltre

$$\beta = \alpha\lambda = \alpha\gamma + \alpha(\lambda - \gamma).$$

Vediamo che l'applicazione $N$ ristretta ad $\mathbb{Z}[i\sqrt{n}]$, è una funzione grado per $n = 1, 2$ :

- Per ogni $\alpha, \beta \in \mathbb{Z}[i\sqrt{n}] - \{0\}$,

$$N(\alpha\beta) \overset{Lem\ 3.1}{=} N(\alpha)N(\beta) \geq N(\alpha).$$

- Poiché $\lambda - \gamma = (u - a) + i(v - n)\sqrt{n}$,

$$N(\lambda - \gamma) = (u-a)^2 + n(v-b)^2 \overset{Eq.(3.1)}{\leq} \frac{n+1}{4} \quad \Rightarrow$$
$$N(\alpha(\lambda - \gamma)) \leq N(\alpha)\frac{n+1}{4},$$

Poiché per $n < 3$, $\frac{n+1}{4} < 1$, per $n = 1, 2$ l'anello $\mathbb{Z}[i\sqrt{n}]$ è euclideo. Invece, per i lemmi 3.3 e 3.4, se $n \geq 3$ esiste in $\mathbb{Z}[i\sqrt{n}]$ un elemento irriducibile, ma non primo. Quindi, per $n \geq 3$, $\mathbb{Z}[i\sqrt{n}]$ non è un UFD, e quindi non è né un PID, né euclideo.

□

Dato un campo $\mathbb{K} \supset \mathbb{Q}$, poniamo

$$\mathbb{O}_K = \{\alpha \in K \mid \exists p(x) \in \mathbb{Z}[x], p(x) \text{ monico}, p(\alpha) = 0\},$$

e chiameremo **interi algebrici di** $K$ **su** $\mathbb{Q}$ i suoi elementi. Si può dimostrare che

**Teorema 3.2.** *$\mathbb{O}_K$ è un anello.*

Quindi, è legittimo chiamare $\mathbb{O}_K$ l'**anello degli interi di** $K$.
Vogliamo calcolare $\mathbb{O}_{\mathbb{Z}[i\sqrt{n}]}$ : osserviamo che sicuramente $\mathbb{Z}[i\sqrt{n}] \subset \mathbb{O}_{\mathbb{Z}[i\sqrt{n}]}$.

**Teorema 3.3.** *Per ogni* $n \in \mathbb{N}$,

$$\mathbb{O}_{\mathbb{A}_n} = \begin{cases} \mathbb{Z}[i\sqrt{n}] & \text{se } n \equiv 1, 2 \mod 4 \\ \mathbb{Z}[\frac{1+i\sqrt{n}}{2}] & \text{se } n \equiv 3 \mod 4 \end{cases}$$

**Dimostrazione**
Sia $a + ib\sqrt{n} \in \mathbb{O}_{\mathbb{Z}[i\sqrt{n}]} - \mathbb{Z}[i\sqrt{n}]$ : il suo polinomio minimo è

$$\mu(x) = x^2 - 2ax + a^2 + nb^2.$$

Affinché $\mu(x) \in \mathbb{Z}[x]$, dobbiamo imporre

$$\begin{cases} 2a \in \mathbb{Z} \\ a^2 + nb^2 \in \mathbb{Z} \end{cases}.$$

Affinché la prima condizione sia verificata, o $a \in \mathbb{Z}$ o $a$ si scrive nella forma $a = \frac{m}{2}$, con $m$ intero dispari:

- Se $a \in \mathbb{Z}$, affinché la seconda condizione sia soddisfatta si deve avere $nb^2 \in \mathbb{Z}$ :

  $$nb^2 \in \mathbb{Z} \overset{\substack{n \text{ è libero} \\ \text{da quadrati}}}{\Leftrightarrow} b^2 \in \mathbb{Z} \Leftrightarrow b \in \mathbb{Z}.$$

  Non si trovano quindi altri interi algebrici;

- Se $a$ si scrive nella forma $a = \frac{m}{2}$, con $m$ intero dispari,

  $$a^2 + nb^2 = \frac{m^2 + 4nb^2}{4} \in \mathbb{Z} \Leftrightarrow m^2 + 4nb^2 \equiv 0 \mod 4 \overset{m^2 \equiv 1}{\Leftrightarrow}{}^{\mod 4} 4nb^2 \equiv 3 \mod 4.$$

  Perché questo accada, chiaramente deve aversi $b \notin \mathbb{Z}$. Tuttavia, essendo $n$ libero da quadrati, deve valere $4b^2 \in \mathbb{Z}$ e ciò è possibile se e solo se $2b \in \mathbb{Z}$. Quindi $b$ si può scrivere nella forma $b = \frac{\beta}{2}$, con $\beta$ intero dispari. In questo caso è possibile che esistano interi algebrici che non stiano in $\mathbb{Z}[i\sqrt{n}]$, e effettivamente ciò accade quando

  $$4n\frac{\beta^2}{4} = \beta^2 n \overset{\beta^2 \in 1+4\mathbb{Z}}{\equiv} 3 \mod 4 \Leftrightarrow n \equiv 3 \mod 4.$$

□

Si può dimostrare che

**Teorema 3.4.** *$\mathbb{O}_{\mathbb{A}_n}$ è un UFD se e solo se $n \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$.*

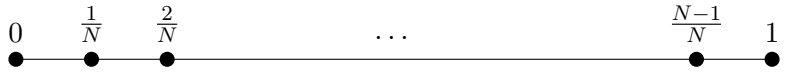
## 3.2. Alcuni risultati di approssimazione

Vogliamo dimostrare alcuni risultati che ci garantiscano di approssimare numeri razionali e irrazionali con numeri razionali che rispettino certe proprietà. Iniziamo con il seguente:

**Teorema 3.5. (Dirichlet)** *Sia $\alpha$ un numero irrazionale compreso fra $0$ e $1$, e sia $N \in \mathbb{N}$. Allora esistono $h, k \in \mathbb{N}$ coprimi tali che $1 \leq h < k \leq N$,*

$$\left|\alpha - \frac{h}{k}\right| < \frac{1}{kN} \leq \frac{1}{k^2}.$$

**Dimostrazione**
*Consideriamo l'insieme $A = \{n\alpha - \lfloor n\alpha \rfloor \mid 1 \leq n \leq N\}$. É immediato osservare che $A \subset (0, 1)$, e che $|A| = N$, ovvero $n\alpha - \lfloor n\alpha \rfloor \neq m\alpha - \lfloor m\alpha \rfloor$ per ogni $m \neq n$, $1 \leq m, n \leq N$. Dividiamo l'intervallo $(0, 1)$ in $N$ parti uguali:*




*Abbiamo due possibilità:*

- *Esiste $n_0 \in \mathbb{N},\ 1 \leq n_0 \leq N$ tale che $n_0\alpha - \lfloor n_0\alpha \rfloor < \frac{1}{N}$ : allora*

$$\left|\alpha - \frac{\lfloor n_0\alpha \rfloor}{n_0}\right| = \frac{|n_0\alpha - \lfloor n_0\alpha \rfloor|}{n_0} < \frac{1}{Nn_0}.$$

- *Non esiste $n_0 \in \mathbb{N},\ 1 \leq n_0 \leq N$ tale che $n_0\alpha - \lfloor n_0\alpha \rfloor < \frac{1}{N}$ : per il principio dei cassetti, in almeno uno degli altri intervalli ci sono almeno due elementi di $A$. La loro differenza è allora minore di $\frac{1}{N}$, cioè esistono $n_0, m_0 \in \mathbb{N}$, con $1 \leq n_0 < m_0 \leq N$ tali che*

$$|n_0\alpha - \lfloor n_0\alpha \rfloor - m_0\alpha + \lfloor m_0\alpha \rfloor| < \frac{1}{N} \Rightarrow \left|\alpha - \frac{\lfloor m_0\alpha \rfloor - \lfloor n_0\alpha \rfloor}{m_0 - n_0}\right| < \frac{1}{N(m_0 - n_0)}.$$

*In ogni caso, il teorema è dimostrato*

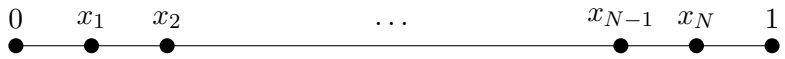
□

Raffinando il ragionamento, si può migliorare il teorema precedente:

**Teorema 3.6. (Dirichlet)** *Sia $\alpha$ un numero irrazionale compreso fra $0$ e $1$, e sia $N \in \mathbb{N}$. Allora esistono $h, k \in \mathbb{N}$ coprimi tali che $1 \leq h < k \leq N$,*

$$\left|\alpha - \frac{h}{k}\right| < \frac{1}{k(N+1)}$$

**Dimostrazione**
Sia $A$ come nel teorema precedente, e sia $x_1 < \cdots < x_N$ un riordinamento dei suoi elementi. Questa volta, dividiamo l'intervallo $(0, 1)$ in $N + 1$ parti, utilizzando questi punti:




Abbiamo tre possibilità:

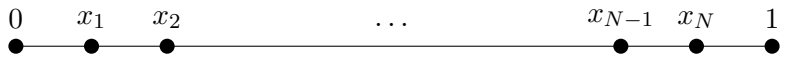
1. $x_1 < \frac{1}{N+1}$ : allora esiste $n_0 \in \mathbb{N}$, $1 \leq n_0 \leq N$, tale che $|n_0\alpha - \lfloor n_0\alpha \rfloor| < \frac{1}{N+1}$, e
$$\left|\alpha - \frac{\lfloor n_0\alpha \rfloor}{n_0}\right| < \frac{1}{n_0(N+1)}.$$
2. $1 - x_N < \frac{1}{N+1}$ : allora $n_0 \in \mathbb{N}$, $1 \leq n_0 \leq N$, tale che $|1 - n_0\alpha + \lfloor n_0\alpha \rfloor| < \frac{1}{N+1}$, e
$$\left|\alpha - \frac{1 + \lfloor n_0\alpha \rfloor}{n_0}\right| < \frac{1}{n_0(N+1)}.$$
3. Entrambi i due casi precedenti non sono verificati: per il principio dei cassetti, esiste almeno un $l \in \mathbb{N}$, $1 \leq l \leq N-1$, tale che
$$|x_{l+1} - x_l| < \frac{1}{N+1}.$$
Con passaggi analoghi ai precedenti, si dimostra il teorema anche in questo caso.

□

Possiamo riadattare l'idea usata nella dimostrazione di questi due teoremi per approssimare numeri razionali con altri razionali, imponendo un controllo sul denominatore:

**Proposizione 3.1.** *Sia $\frac{l}{q}$ un numero razionale, con $l, q \in \mathbb{N}$ coprimi, e sia $N < q$ un numero naturale. Allora esistono $h, k \in \mathbb{N}$ coprimi tali che $k \leq N$,*
$$\left|\frac{l}{q} - \frac{h}{k}\right| \leq \frac{1}{k(N+1)}.$$

**Dimostrazione**
Supponiamo inizialmente $l < q$, e consideriamo l'insieme
$$A = \left\{ \frac{nl}{q} - \left\lfloor \frac{nl}{q} \right\rfloor \Big| 1 \leq n \leq N \right\}.$$
Anche in questo caso, $|A| = N$ : infatti, se esistessero $n_1, n_2 \in \mathbb{N}$, $1 \leq n_1, n_2 \leq N$, $n_1 \neq n_2$ tali che $n_1\frac{l}{q} - \lfloor n_1\frac{l}{q} \rfloor = n_2\frac{l}{q} - \lfloor n_2\frac{l}{q} \rfloor$, si avrebbe
$$\frac{(n_1 - n_2)l}{q} = n_1\frac{l}{q} - n_2\frac{l}{q} = \left\lfloor n_1\frac{l}{q} \right\rfloor - \left\lfloor n_2\frac{l}{q} \right\rfloor \in \mathbb{Z},$$
e questo è assurdo, dato che $l, q$ sono coprimi e $n_1 - n_2 < q$. Sia $x_1 < \cdots < x_N$ un riordinamento degli elementi di $A$ : dividiamo l'intervallo $(0, 1)$ in $N+1$ parti, utilizzando questi punti:




Abbiamo tre possibilità:

- $x_1 \leq \frac{1}{N+1}$ : allora esiste $n_0 \in \mathbb{N}$, $1 \leq n_0 \leq N$, tale che $|n_0\alpha - \lfloor n_0\alpha \rfloor| \leq \frac{1}{N+1}$, e
$$\left|\alpha - \frac{\lfloor n_0\alpha \rfloor}{n_0}\right| \leq \frac{1}{n_0(N+1)}.$$

- $1 - x_N \leq \frac{1}{N+1}$ : allora esiste $n_0 \in \mathbb{N}$, $1 \leq n_0 \leq N$ tale che $|1 - n_0\alpha + \lfloor n_0\alpha \rfloor| \leq \frac{1}{N+1}$, e

$$\left|\alpha - \frac{1 + \lfloor n_0\alpha \rfloor}{n_0}\right| \leq \frac{1}{n_0(N+1)}.$$

- Entrambi i due casi precedenti non sono verificati: per il principio dei cassetti, esiste almeno un $l \in \mathbb{N}$, $1 \leq l \leq N-1$, tale che tale che

$$|x_{l+1} - x_l| \leq \frac{1}{N+1}.$$

  Con passaggi analoghi ai precedenti, si dimostra il teorema anche in questo caso.

(Osserviamo che, a differenza del teorema precedente, le disuguaglianze non sono necessariamente strette). Se invece $l \geq q$, possiamo scrivere

$$\frac{l}{q} = \left\lfloor \frac{l}{q} \right\rfloor + \left\{ \frac{l}{q} \right\}.$$

Chiaramente, $\left\{ \frac{l}{q} \right\} \in (0,1)$ : per il teorema 3.6, esistono $h, k \in \mathbb{N}$ coprimi tali che, $1 \leq h < k \leq N$,

$$\left| \left\{ \frac{l}{q} \right\} - \frac{h}{k} \right| < \frac{1}{k(N+1)}$$

Ma allora, aggiungendo e sottraendo la parte intera di $\frac{l}{q}$,

$$\left| \frac{l}{q} - \frac{h}{k} - \left\lfloor \frac{l}{q} \right\rfloor \right| = \left| \frac{l}{q} - \frac{h + k\lfloor \frac{l}{q} \rfloor}{k} \right| \leq \frac{1}{k(N+1)},$$

e quindi la tesi.

□

## 3.3. Rappresentazioni come somma di due quadrati

Diremo che $n \in \mathbb{N}$ ammette una **rappresentazione primitiva** se esistono due numeri naturali $s, t$ coprimi, tali che $n = s^2 + t^2$. La proposizione 3.1 ha il seguente corollario:

**Corollario 3.1.** *Se $m, n \in \mathbb{N}$ sono tali che $n \mid m^2 + 1$, allora $n$ ammette una rappresentazione primitiva.*

**Dimostrazione**

Chiaramente $m$ e $n$ sono coprimi: consideriamo il numero razionale $\frac{m}{n}$, e fissiamo $N = \lfloor \sqrt{n} \rfloor < n$ : per la proposizione 3.1, esistono $r, s \in \mathbb{N}$ tali che

$$\frac{1}{s(N+1)} \geq \left| \frac{m}{n} - \frac{r}{s} \right| \Rightarrow |ms - rn| \leq \frac{n}{N+1} < \sqrt{n}.$$

Poniamo $t = |ms - rn|$ :

$$t^2 + s^2 = s^2(1 + m^2) + n(r^2 n - 2msr).$$

Poiché $n \mid m^2 + 1$, $n \mid s^2 + t^2$. D'altra parte, $s^2 + t^2 < N^2 + n < 2n$. Quindi $s^2 + t^2$ è un multiplo di $n$ minore del suo doppio: allora non può che essere

$$n = s^2 + t^2 = s^2(1 + m^2) + n(r^2 n - 2msr). \tag{3.2}$$

Verifichiamo infine che $(s,t) = 1$ : poiché $(r,s) = 1$,

$$(s,t) = (s, ms - rn) = (s, rn) = (s,n).$$

Se $d \in \mathbb{N}$ è tale che $d \mid (s,n)$, per l'equazione (3.2),

$$1 = s^2 \frac{1+m^2}{n} + r^2 n - 2msr.$$

Quindi, si deve avere $d \mid 1$, e cioè $d = 1$. Ma allora $s, t$ sono coprimi e il corollario è dimostrato.

□

Denotiamo con $\mathcal{Q}_1$ l'insieme degli interi non negativi che sono un quadrato,

$$\mathcal{Q}_1 = \{n \in \mathbb{N} \cup \{0\} \mid \exists x \in \mathbb{N} \cup \{0\}, x^2 = n\}.$$

Similmente, denotiamo con $\mathcal{Q}_2$ l'insieme degli interi non negativi che sono esprimibili come somma di due quadrati:

$$\mathcal{Q}_2 = \{n \in \mathbb{N} \cup \{0\} \mid \exists x, y \in \mathbb{N} \cup \{0\}, x^2 + y^2 = n\},$$

e più in generale con $\mathcal{Q}_k$ l'insieme degli interi non negativi che sono esprimibili come somma di $k$ quadrati. Osserviamo che, se $m < n$, allora $\mathcal{Q}_m \subset \mathcal{Q}_n$. Proviamo che

**Lemma 3.5.** *$(\mathcal{Q}_2, \cdot)$ è un monoide.*

**Dimostrazione**

Per ogni $m, n, a, b \in \mathbb{N}$,

$$(m^2+n^2)(a^2+b^2) = N(m+in)N(a+bi) = N(am-bn+i(an+bm)) = (am-bn)^2+(an+bm)^2.$$

□

Il corollario 3.1 si può facilmente generalizzare:

**Proposizione 3.2.** *Se $a, b \in \mathbb{N}$ sono coprimi e $n \in \mathbb{N}$ è tale che $n \mid a^2 + b^2$, allora $n$ ammette una rappresentazione primitiva.*

**Dimostrazione**

Per il lemma di Bezout, essendo $a, b$ coprimi, esistono $a', b' \in \mathbb{Z}$ in modo tale che $aa' - bb' = 1$. Poiché $n \mid a^2 + b^2$ allora

$$n \mid (a^2 + b^2)(a'^2 + b'^2) = (aa' + bb')^2 + 1.$$

Per il corollario 3.1, la tesi.

□

Possiamo adesso dimostrare la proposizione 2.10:

**Proposizione 3.3.** *Se $p \in \mathbb{P}$ e $m, n \in \mathbb{N}$ sono tali che $p \mid m^2 + n^2$ e $(m,n) = 1$, allora o $p = 2$ oppure $p \equiv 1 \mod 4$.*

**Dimostrazione**

Per la proposizione precedente, $p$ ammette una rappresentazione primitiva. Un numero primo $p \equiv 3 \mod 4$ non si può scrivere come somma di due quadrati: infatti il quadrato di un numero intero è congruo a $0$ modulo $4$ se è pari, mentre è congruo a $1$ modulo $4$ se è dispari. Quindi la somma dei quadrati di due numeri interi può essere congrua a $0$ (se entrambi i numeri sono pari), $1$ (se uno di essi è pari e l'altro è dispari), $2$ (se entrambi i numeri sono dispari) ma non a $3$ modulo $4$. Quindi $p = 2$, oppure $p \equiv 1 \mod 4$.

□

Più avanti, vedremo altri risultati sugli interi esprimibili come somma di due quadrati: ad esempio, nella prossima sezione daremo una completa caratterizzazione dell'insieme $\mathcal{Q}_2$.

## 3.4. Residui quadratici

Sia $a \in \mathbb{Z}$ e sia $p \in \mathbb{P}^\star$. Diremo che $a$ è un **residuo quadratico** modulo $p$ se esiste esiste $x \in \mathbb{Z}$ tale che $a \equiv x^2 \mod p$, e in tal caso scriveremo $a\mathcal{R}p$. Se $a$ non è un residuo quadratico modulo $p$, diremo che $a$ è un **non-residuo quadratico** modulo $p$, e scriveremo $a\mathcal{N}p$.

Ci chiediamo quanti siano i residui quadratici modulo $p$. Consideriamo il campo $\mathbb{Z}/p\mathbb{Z}$ : sappiamo che il suo sottogruppo moltiplicativo $(\mathbb{Z}/p\mathbb{Z})^\star$ è isomorfo al gruppo additivo $\mathbb{Z}/(p-1)\mathbb{Z}$, e quindi in particolare è ciclico. Sappiamo inoltre che esso ha un numero di generatori pari a $\phi(p-1)$. Tale campo non è algebricamente chiuso per ogni primo $p$, ma vale il seguente:

**Teorema 3.7. (Lagrange)** *Sia $p(x) \in (\mathbb{Z}/p\mathbb{Z})[x]$ un polinomio di grado $n$. Allora $p(x)$ ha al più $n$ soluzioni in $\mathbb{Z}/p\mathbb{Z}$.*

**Dimostrazione**
Procediamo per induzione su $n$ :

- (passo base, $n = 1$) Sia $q(x) = ax + b \in (\mathbb{Z}/p\mathbb{Z})[x]$ un polinomio di primo grado: in particolare assumiamo $a \neq 0$ in $\mathbb{Z}/p\mathbb{Z}$, e cioè $p \nmid a$. Poiché la congruenza $ax + b \equiv 0 \mod p$ ha una e una sola soluzione in $\mathbb{Z}/p\mathbb{Z}$, il passo base è verificato.
- (passo induttivo $1, \dots n-1 \Rightarrow n$) Sia $q(x) = a_n x^n + \cdots + a_1 x + a_0 \in (\mathbb{Z}/p\mathbb{Z})[x]$, con $a_n \neq 0$ in $\mathbb{Z}/p\mathbb{Z}$. Se $q(x)$ non ha radici abbiamo finito, se invece ne ha almeno una esiste $x_0 \in \mathbb{Z}/p\mathbb{Z}$ tale che $q(x_0) = 0$ in $\mathbb{Z}/p\mathbb{Z}$. Ma allora
$$q(x) = q(x) - q(x_0) = a_n(x^n - x_0^n) + \cdots + a_1(x - x_0) = (x - x_0)r(x),$$
dove $r(x) \in (\mathbb{Z}/p\mathbb{Z})[x]$ è un polinomio avente grado $n-1$. Poiché $\mathbb{Z}/p\mathbb{Z}$ è un campo,
$$p(x) = 0 \Leftrightarrow (x - x_0)r(x) = 0 \Leftrightarrow x - x_0 = 0 \ \vee \ r(x) = 0.$$
Per ipotesi induttiva, $r(x)$ ha al più $n-1$ radici in $\mathbb{Z}/p\mathbb{Z}$, quindi $p(x)$ ha al più $n$ radici in $\mathbb{Z}/p\mathbb{Z}$.

□

**Proposizione 3.4.** *Esistono esattamente $\frac{p-1}{2}$ residui quadratici modulo $p$ tra i numeri $1, \dots, p-1$, e i restanti $\frac{p-1}{2}$ sono non-residui quadratici. I residui quadratici modulo $p$ sono*
$$1^2, \dots, \left(\frac{p-1}{2}\right)^2 \mod p.$$

**Dimostrazione**
Proviamo che $x^2 \equiv a \mod p$ ha soluzione solo per $\frac{p-1}{2}$ valori di $a$ nell'insieme $\{1, \dots, p-1\}$. Siano $x, y \in \{1, \dots, \frac{p-1}{2}\}$ : se $x \neq y$, allora $x^2 \not\equiv y^2 \mod p$, in quanto
$$x^2 - y^2 \equiv 0 \mod p \Rightarrow x - y \equiv 0 \mod p \vee x + y \equiv 0 \mod p,$$
e queste ultime due congruenze non possono essere soddisfatte, dal momento che $1 \leq x, y \leq \frac{p-1}{2}$. Quindi, ci sono almeno $\frac{p-1}{2}$ residui quadratici modulo $p$. Inoltre, se $x \in \left\{\frac{p+1}{2}, \dots, p-1\right\}$, $x^2$ e $(p-x)^2 \in \left\{1, \dots, \frac{p-1}{2}\right\}$ sono tali che $x^2 \equiv (p-x)^2 \mod p$. Di conseguenza, ci sono esattamente $\frac{p-1}{2}$ residui quadratici modulo $p$.

□

Introduciamo un utile strumento per studiare la quadraticitá modulo un primo: per ogni $p \in \mathbb{P}^\star$, definiamo **simbolo di Legendre** modulo $p$ la funzione

$$\begin{aligned}\left(\frac{\cdot}{p}\right): \quad \mathbb{Z} &\to \{-1,0,1\} \\ m &\mapsto \left(\frac{m}{p}\right) = \begin{cases} 1 & \text{se } m\mathcal{R}p \\ 0 & \text{se } p \mid m \\ -1 & \text{se } m\mathcal{N}p \end{cases}.\end{aligned}$$

**Proposizione 3.5.** *Il simbolo di Legendre modulo $p$ gode delle seguenti proprietà:*

1. *Il simbolo di Legendre modulo $p$ è una funzione periodica di periodo $p$, cioè, per ogni $m \in \mathbb{Z}$,*
$$\left(\frac{m+p}{p}\right) = \left(\frac{m}{p}\right);$$
2. *Il simbolo di Legendre modulo $p$ è una funzione a media nulla, cioè*
$$\sum_{m=1}^{p-1} \left(\frac{m}{p}\right) = 0;$$
3. *Vale la seguente caratterizzazione*
$$m\mathcal{R}p \Leftrightarrow m^{\frac{p-1}{2}} \equiv 1 \mod p; \tag{3.3}$$
4. **(Criterio di Eulero)**
$$m^{\frac{p-1}{2}} \equiv \left(\frac{m}{p}\right) \mod p; \tag{3.4}$$
5. *Per ogni $m_1, m_2 \in \mathbb{Z}$,*
$$\left(\frac{m_1}{p}\right)\left(\frac{m_2}{p}\right) = \left(\frac{m_1 m_2}{p}\right).$$

**Dimostrazione.**

1. Completamente ovvio;
2. É una conseguenza immediata della proposizione 3.4;
3. ($\Rightarrow$) Per il piccolo teorema di Fermat, per ogni $x \in \mathbb{Z}$ non multiplo di $p$ $x^{p-1} \equiv 1 \mod p$. Poiché $m\mathcal{R}p$, esiste $x \in \mathbb{Z}$ tale che $x^2 \equiv m \mod p$, quindi
$$m^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \mod p.$$
($\Leftarrow$) Per il teorema 3.7, la congruenza
$$x^{\frac{p-1}{2}} \equiv 1 \mod p$$
ha al più $\frac{p-1}{2}$ soluzioni distinte in $\mathbb{Z}/p\mathbb{Z}$. Poiché i residui quadratici chiaramente verificano la congruenza, e poiché per la proposizione 3.4 i residui sono esattamente $\frac{p-1}{2}$, non ci sono altre soluzioni. In altri termini, se $m^{\frac{p-1}{2}} \equiv 1 \mod p$ allora $m\mathcal{R}p$.

4. Se $p \mid m$, non c'è nulla da dimostrare. Supponiamo dunque che $p \nmid m$ : per il piccolo teorema di Fermat,
$$(m^{\frac{p-1}{2}} - 1)(m^{\frac{p-1}{2}} + 1) \equiv m^{p-1} - 1 \equiv 0 \mod p.$$
Quindi, o $m^{\frac{p-1}{2}} - 1 \equiv 0 \mod p$ o $m^{\frac{p-1}{2}} + 1 \equiv 0 \mod p$. Per l'equazione (3.3), la prima congruenza è verificata da tutti e soli i residui quadratici, e quindi i non-residui quadratici, verificano la seconda congruenza.

5. Se $p$ divide uno fra $m_1, m_2$ la tesi è ovvia. Se $p$ non divide nessuno di essi, per il criterio di Eulero (3.4),
$$\left(\frac{m_1}{p}\right)\left(\frac{m_2}{p}\right) \equiv m_1^{\frac{p-1}{2}} m_2^{\frac{p-1}{2}} \equiv (m_1 m_2)^{\frac{p-1}{2}} \equiv \left(\frac{m_1 m_2}{p}\right) \mod p.$$
In più, sono anche uguali, poiché, se non lo fossero, la loro differenza, che in modulo è 2, dovrebbe dividere $p$.

□

Il criterio di Eulero ha conseguenze interessanti:

**Corollario 3.2.** *Sia $p \in \mathbb{P}^\star$ : $-1 \mathcal{R} p$ se e solo se $p \equiv 1 \mod 4$. In particolare, i primi $p \equiv 1 \mod 4$ ammettono una rappresentazione primitiva.*

**Dimostrazione**

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = 1 \Leftrightarrow \frac{p-1}{2} \equiv 0 \mod 2 \Leftrightarrow p \equiv 1 \mod 4.$$

Di conseguenza, dato un primo $p \equiv 1 \mod 4$, esiste $x \in \mathbb{Z}$ tale che $x^2 \equiv -1 \mod p$, e cioè $p \mid x^2 + 1$. Per il corollario 3.1, $p$ ammette una rappresentazione primitiva.

□

Come promesso, diamo ora una completa caratterizzazione del monoide $\mathcal{Q}_2$ :

**Teorema 3.8.** *Un numero naturale $n \geq 2$ si esprime come somma di due quadrati se e solo se ogni primo congruo a 3 modulo 4 che compare nella sua fattorizzazione ha esponente pari. In formule, se $n \in \mathbb{N}$, $n \geq 2$,*
$$n \in \mathcal{Q}_2 \Leftrightarrow (p^a \parallel n,\ p \equiv 3 \mod 4 \Rightarrow a \equiv 0 \mod 2).$$

**Dimostrazione**

($\Rightarrow$) Sia $n \in \mathcal{Q}_2$, e siano $x, y \in \mathbb{N} \cup \{0\}$ tali che $x^2 + y^2 = n$. Se $p \equiv 3 \mod 4$, e se $n$ ha solo rappresentazioni primitive, per la proposizione 2.10 che $p$ non divide $n$. Supponiamo che $n$ ammetta una rappresentazione che non è primitiva: sia allora $d = (x, y)$, con $d > 1$. Posti $X = \frac{x}{d}$, $Y = \frac{y}{d}$, $(X, Y) = 1$,
$$n = d^2(X^2 + Y^2).$$
Se $p \equiv 3 \mod 4$, e $p$ divide $n$ allora necessariamente $p$ divide $d^2$, e quindi $p$ divide $n$ con esponente pari.
($\Leftarrow$) Supponiamo che $n$ si possa scrivere nella forma
$$n = 2^{v_2} \prod_{\substack{p \mid n \\ p \equiv 1 \mod 4}} p^{v_p} \prod_{\substack{q \mid n \\ q \equiv 3 \mod 4}} q^{2v'_q(n)}.$$

Per il lemma 3.5, è sufficiente dimostrare che $n$ è prodotto di fattori che sono esprimibili come somma di due quadrati: ma questo è ovvio, poiché per il corollario 3.2 i primi congrui a 1 modulo 4 sono esprimibili come somma di due quadrati, e

$$2\prod_{j=1}^{s} q_j^{2v'_{q_j}(n)} = \left(\prod_{j=1}^{s} q_j^{2v'_{q_j}}\right)^2 + \left(\prod_{j=1}^{s} q_j^{2v'_{q_j}}\right)^2.$$

□

I numeri naturali esprimibili come somma di due quadrati "non sono tanti", nel senso della densità asintotica: vale infatti

**Teorema 3.9.** $d_{\mathcal{Q}_2} = 0$.

## 3.5. Da due a tre e quattro quadrati

L'insieme $\mathcal{Q}_3$ è più complicato da studiare: infatti, $\mathcal{Q}_3$ non è un monoide, dato che, ad esempio, $3, 5 \in \mathcal{Q}_3$, ma $15 \notin \mathcal{Q}_3$. Ci limitiamo a dimostrare che

**Proposizione 3.6.** *Sia $n \in \mathbb{N}$, $n \equiv 7 \mod 8$ : allora $n$ non si può scrivere come somma di 3 quadrati. Più in generale, se esistono $a, b \in \mathbb{N} \cup \{0\}$ tali che $n = (8b+7)4^a$, allora $n$ non si può scrivere come somma di tre quadrati.*

**Dimostrazione**

I residui quadratici modulo 8 sono $0, 1, 4$, quindi non è possibile, sommando tre quadrati, ottenere un numero congruo a 7 modulo 8. Proviamo il caso generale, usando la tecnica della discesa infinita: abbiamo appena provato il caso $a = 0$, supponiamo $a \geq 1$. Se $n$ si potesse scrivere come somma di tre quadrati, esisterebbero $x_1, x_2, x_3 \in \mathbb{N} \cup \{0\}$ tali che

$$(8b+7)4^a = n = x_1^2 + x_2^2 + x_3^2.$$

Osserviamo che $x_1, x_2, x_3$ sono tutti pari, essendo $n$ multiplo di 4. Poniamo

$$x_1 = 2x_{1,1}, x_2 = 2x_2^{1,2}, x_3 = 2x_{1,3}.$$

Sostituendo,

$$4x_{1,1}^2 + 4x_{1,2}^2 + 4x_{1,3}^2 = (8b+7)4^a \Rightarrow x_{1,1}^2 + x_{1,2}^2 + x_{1,3}^2 = (8b+7)4^{a-1}.$$

Iterando lo stesso ragionamento, dopo un numero finito di passi (esattamente $a$) ci si trova a dover risolvere l'equazione

$$x_{a,1}^2 + x_{a,2}^2 + x_{a,3}^2 = 8b+7.$$

Ma poiché questa equazione non ha soluzioni intere, non ne ha nemmeno l'equazione di partenza.

□

I numeri naturali che si possono scrivere come somma di tre quadrati sono "di più" rispetto a quelli che si possono scrivere come somma di due quadrati, sempre nel senso della densità asintotica. Si può infatti provare che

**Teorema 3.10.** $d_{\mathcal{Q}_3} = \frac{1}{6}$. Passiamo adesso al caso dei numeri naturali che si possono scrivere come somma di quattro quadrati. Premettiamo alcuni risultati preliminari:

**Lemma 3.6.** *$(\mathcal{Q}_4, \cdot)$ è un monoide.*

**Dimostrazione**

Per ogni $x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4 \in \mathbb{N}$,

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = z_1^2 + z_2^2 + z_3^2 + z_4^2,$$

dove

$$\begin{cases} z_1 = x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4 \\ z_2 = x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3 \\ z_3 = x_1y_3 - x_3y_1 - x_2y_4 + x_4y_2 \\ z_4 = x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2. \end{cases}$$

□

**Lemma 3.7.** *Se $p \in \mathbb{P}^\star$, allora esistono $x, y, m \in \mathbb{N}$ tali che $1 + x^2 + y^2 = mp$, con $1 \leq m < p$. In particolare, l'insieme*

$$\mathcal{Q}_4(p) = \{m \in \mathbb{N},\ m < p \mid \exists x, y, z, t \in \mathbb{N} \cup \{0\},\ mp = x^2 + y^2 + z^2 + t^2\} \tag{3.5}$$

*è non vuoto.*

**Dimostrazione**

Gli insiemi

$$A = \left\{ x^2 \middle| x = 0, \cdots, \frac{p-1}{2} \right\},$$
$$B = \left\{ -1 - y^2 \middle| y = 0, \cdots, \frac{p-1}{2} \right\},$$

sono chiaramente disgiunti. Poiché $|A| = |B| = \frac{p+1}{2}$, per il principio dei cassetti esistono $x^2 \in A$, $-1 - y^2 \in B$, tali che $x^2 \equiv -1 - y^2 \mod p$, cioè esiste $m \in \mathbb{N}$ tale che $x^2 + y^2 + 1 = mp$. Infine, poiché $x^2 + y^2 + 1 \leq 2\frac{(p-1)^2}{4} + 1 < \frac{p^2}{2} + 1 < p^2$, anche $m < p$.

□

Possiamo adesso dimostrare il famoso teorema dei quattro quadrati, dovuto a Lagrange (1770):

**Teorema 3.11. (Lagrange)** $\mathcal{Q}_4 = \mathbb{N}$.

**Dimostrazione**

Per il lemma 3.6, e poiché chiaramente $2 \in \mathcal{Q}_4$, basta provare che $\mathbb{P}^\star \subset \mathcal{Q}_4$. Sia $p \in \mathbb{P}^\star$ : per il lemma 3.7 l'insieme $\mathcal{Q}_4(p)$ definito nell'equazione (3.5) ammette minimo, $m_0$, con $m_0 < p$. Siano poi $x_1, x_2, x_3, x_4 \in \mathbb{N} \cup \{0\}$ tali che

$$m_0 p = x_1^2 + x_2^2 + x_3^2 + x_4^2 \tag{3.6}$$

Bisogna provare che $m_0 = 1$. Dividiamo la dimostrazione in due passi:

- $m_0$ non può essere pari: se $m_0$ fosse pari allora anche $m_0 p = x_1^2 + x_2^2 + x_3^2 + x_4^2$ sarebbe pari. In particolare, i numeri $x_1, x_2, x_3, x_4$ o sono tutti pari, o sono tutti dispari, o due sono pari e due sono dispari. In ogni caso, possiamo assumere senza perdere in generalità che $x_1, x_2$ e $x_3, x_4$ siano coppie di numeri naturali aventi la stessa parità. In particolare,

  $$a_1 = \frac{x_1 + x_2}{2}, \quad a_2 = \frac{x_1 - x_2}{2}, \quad a_3 = \frac{x_3 + x_4}{2}, \quad a_4 = \frac{x_3 - x_4}{2} \in \mathbb{N},$$

  e sommandone i quadrati,

  $$a_1^2 + a_2^2 + a_3^2 + a_4^2 = \frac{x_1^2 + x_2^2 + x_3^2 + x_4^2}{2} = \frac{m_0 p}{2},$$

  da cui si avrebbe che $\frac{m_0}{2} \in \mathcal{Q}_4(p)$, assurdo per la minimalitá di $m_0$. Quindi $m_0$ è dispari.

- $m_0 = 1$ : supponiamo per assurdo che $m_0 \geq 3$ : Per ogni $j = 1, 2, 3, 4$ possiamo scrivere

$$x_j = m_0 b_j + y_j, \tag{3.7}$$

dove $b_j$ e $y_j$ sono opportuni numeri interi e $|y_j| < \frac{m_0}{2}$. Almeno uno degli $y_j$ è non nullo: se per ogni $j$ si avesse $x_j = m_0 b_j$, si avrebbe

$$\sum_{j=1}^{4} b_j^2 m_0^2 = m_0 p \Rightarrow p = m_0 \sum_{j=1}^{4} b_j^2 \overset{m_0 \geq 3,}{\Rightarrow}{}^{p \in \mathbb{P}} \sum_{j=1}^{4} b_j^2 = 1 \Rightarrow p = m_0,$$

assurdo, in quanto $m_0 < p$. Dunque

$$\sum_{j=1}^{4} y_j^2 \neq 0$$

e in particolare, per il lemma 3.6,

$$0 \neq \sum_{j=1}^{4} x_j^2 \sum_{h=1}^{4} y_h^2 = \sum_{t=1}^{4} z_t^2, \tag{3.8}$$

dove $z_1, z_2, z_3, z_4$ sono come nel lemma 3.6. Usando l'espressione per $x_j$ nell'equazione (3.7) e l'equazione (3.6),

$$\sum_{h=1}^{4} y_h^2 = m_0 p + m_0 \sum_{h=1}^{4} (b_h^2 m_0 - 2 b_h x_h) \Rightarrow m_0 \mid \sum_{h=1}^{4} y_h^2.$$

Ma $|y_h| < \frac{m_0}{2}$ per ogni $j = 1, 2, 3, 4$, dunque

$$\sum_{h=1}^{4} y_h^2 < m_0^2 \Rightarrow \sum_{h=1}^{4} y_h^2 = m_1 m_0,$$

con $m_1 \in \mathbb{N}$, $1 \leq m_1 < m_0$. Usando l'espressione per $z_1$ nel lemma 3.6,

$$z_1 = \sum_{h=1}^{4} x_h y_h \overset{Eq.\ (3.7)}{=} \sum_{h=1}^{4} x_h (x_h - b_h m_0) = m_0 p - m_0 \sum_{h=1}^{4} x_h b_h \Rightarrow m_0 \mid z_1.$$

In modo analogo, si dimostra che anche $z_2, z_3, z_4$ sono multipli di $m_0$ : poniamo $z_h = m_0 T_h$ per ogni $h = 1, 2, 3, 4$. Per l'equazione (3.8),

$$m_1 m_0^2 p = m_0^2 (T_1^2 + T_2^2 + T_3^2 + T_4^2) \Rightarrow m_1 p = T_1^2 + T_2^2 + T_3^2 + T_4^2 \Rightarrow m_1 \in \mathcal{Q}_4(p),$$

assurdo, poiché $m_1 < m_0$, e questo contraddice la minimalitá di $m_0$. Quindi $m_0 = 1$.

□

# CAPITOLO 4

## La legge di reciprocità quadratica

**Introduzione**

In questo capitolo, completeremo lo studio del problema della quadraticità modulo un primo, enunciando e dimostrando la legge di reciprocità quadratica, e definendo il simbolo di Jacobi, una generalizzazione del simbolo di Legendre, che perde alcune delle proprietà aritmetiche di quest'ultimo ma che è molto utile per il calcolo diretto della quadraticità modulo un primo.

## 4.1. La legge di reciprocità quadratica

**Lemma 4.1. (Gauss)** *Sia $p$ un primo dispari e $n$ un numero naturale, $(n,p)=1$, e sia*

$$\mathbb{G} = \left\{ [kn]_p > \frac{p}{2} \,\middle|\, 1 \leq k \leq \frac{p-1}{2} \right\},$$

*dove con $[kn]_p$ denotiamo il resto nella divisione euclidea di $kn$ con $p$, con $m = |\mathbb{G}|$. Si ha*

$$\left(\frac{n}{p}\right) = (-1)^m.$$

*Inoltre, se $n = q$ è un primo dispari diverso da $p$,*

$$m \equiv \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor \mod 2.$$

**Dimostrazione**

Sia $b_1, \ldots, b_m$ un'elencazione degli elementi di $\mathbb{G}$, e sia invece $a_1, \ldots, a_l$ un'elencazione degli elementi nell'insieme

$$\left( \{[kn]_p < \frac{p}{2} \,\middle|\, 1 \leq k \leq \frac{p-1}{2}\} \right).$$

Chiaramente, $m + l = \frac{p-1}{2}$. Comunque si prendano $i, j \in \mathbb{N}$, $1 \leq i \leq l$, $1 \leq j \leq m$, non si può avere $p - b_j = a_i$ : se per assurdo esistessero $i_0, j_0$ tali che $p = b_{j_0} + a_{i_0}$, allora esisterebbero $k_1, k_2 \in \{1, \ldots, \frac{p-1}{2}\}$ tali che $k_1 n + k_2 n = (k_1 + k_2)n = p$, e poiché $(p,n) = 1$, si dovrebbe avere $p \mid k_1 + k_2$, e questo è assurdo, dato che $k_1 + k_2 \leq p - 1$. Quindi, e, ponendo $P = \frac{p-1}{2}$,

$$\{a_1, \ldots, a_l, p - b_1, \ldots, p - b_m\} = \left\{1, \ldots, \frac{p-1}{2}\right\}, \tag{4.1}$$

e (ponendo $P = \frac{p-1}{2}$)

$$\begin{aligned} P! = \prod_{i=1}^{l} a_i \prod_{j=1}^{m} (p - b_j) &\equiv (-1)^m \prod_{i=1}^{l} a_i \prod_{j=1}^{m} b_j \mod p \\ &\equiv (-1)^m \prod_{k=1}^{\frac{p-1}{2}} kn \mod p \\ &\equiv (-1)^m n^{\frac{p-1}{2}} P! \mod p \\ &\overset{Eq.\ (3.4)}{\equiv} (-1)^m \left(\frac{n}{p}\right) P! \mod p. \end{aligned}$$

Quindi $(-1)^m \left(\frac{n}{p}\right) \equiv 1 \mod p$, e di conseguenza

$$(-1)^m \left(\frac{n}{p}\right) = 1 \Rightarrow \left(\frac{n}{p}\right) = (-1)^m.$$

Siano ora $p, q \in \mathbb{P}^\star$, con $p \neq q$, e poniamo $a = \sum_{i=1}^{l} a_i$, $b = \sum_{j=1}^{m} b_j$. Si ha

$$\frac{p^2-1}{8} = \sum_{k=1}^{\frac{p-1}{2}} k \overset{Eq.\ (4.1)}{=} \sum_{i=1}^{l} a_i + \sum_{j=1}^{m} p - b_j = mp - b + a, \tag{4.2}$$

e inoltre

$$q\frac{p^2-1}{8} = \sum_{k=1}^{\frac{p-1}{2}} kq \overset{\substack{Divisione \\ euclidea}}{=} \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor p + r_k = p \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor + a + b. \tag{4.3}$$

Sottraendo all'equazione (4.3) l'equazione (4.2), otteniamo

$$(q-1)\frac{p^2-1}{8} = p\left(\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor - m\right) + 2b,$$

e, riducendo modulo 2,

$$\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor \equiv m \mod 2.$$

□

Il lemma 4.1 permette di dimostrare il seguente:

**Corollario 4.1.** *Se $p$ è un primo dispari,*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{se } p \equiv 1, 7 \mod 8 \\ -1 & \text{se } p \equiv 3, 5 \mod 8 \end{cases}$$

**Dimostrazione**

Per ogni $k \in \mathbb{N}$, con $1 \leq k \leq \frac{p-1}{2}$, $[2k]_p = 2k$ : usiamo il lemma 4.1 e calcoliamo

$$m = \left| \left\{ 2k > \frac{p}{2} \middle| 1 \leq k \leq \frac{p-1}{2} \right\} \right|.$$

Osserviamo che

$$m = \sum_{\frac{p}{2}<2k<p} 1 = \sum_{\frac{p}{4}<k<\frac{p}{2}} 1 = \left\lfloor \frac{p}{2} \right\rfloor - \left\lfloor \frac{p}{4} \right\rfloor .$$

Posto $p = 8q + r$, con $q, r \in \mathbb{N}$, $r \in \{1, 3, 5, 7\}$,

$$m = \left\lfloor \frac{8q+r}{2} \right\rfloor - \left\lfloor \frac{8q+r}{4} \right\rfloor = 2q + \left\lfloor \frac{r}{2} \right\rfloor - \left\lfloor \frac{r}{4} \right\rfloor .$$

Poiché di $m$ ci interessa la parità, possiamo trascurare il fattore $2q$ :

$$\left\lfloor \frac{r}{2} \right\rfloor - \left\lfloor \frac{r}{4} \right\rfloor \equiv \begin{cases} 0 \mod 2 & \text{se } r = 1, 7 \\ 1 \mod 2 & \text{se } r = 3, 5 \end{cases},$$

da cui la tesi.

□

La tecnica utilizzata per dimostrare questo risultato può essere riadattata anche in altri casi: lo vedremo nelle applicazioni alla fine del capitolo. In generale, però, si possono ottenere gli stessi risultati con minore fatica applicando il prossimo teorema: la legge di reciprocità quadratica:

**Teorema 4.1. (Legge di reciprocità quadratica)** *Siano $p, q \in \mathbb{P}^\star$, $p \neq q$. Allora*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

**Dimostrazione**

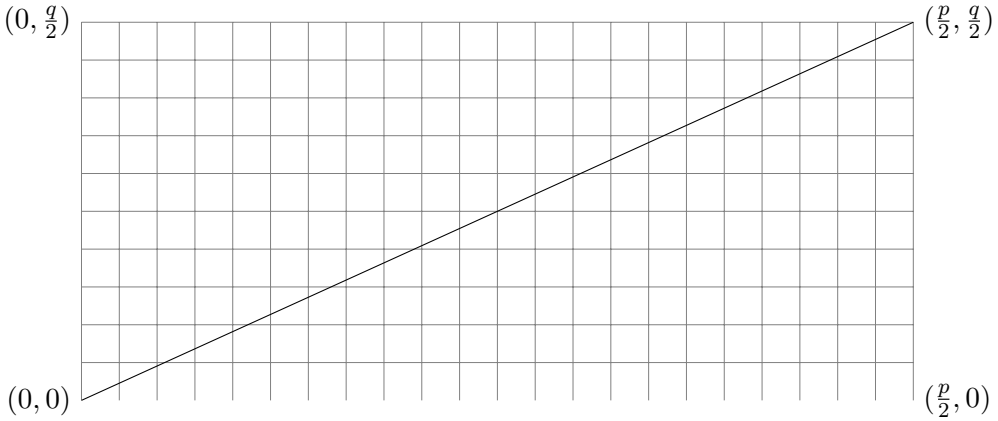
Per il lemma di Gauss 4.1,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^S,$$

con

$$S = \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{jq}{p} \right\rfloor + \sum_{k=1}^{\frac{q-1}{2}} \left\lfloor \frac{kp}{q} \right\rfloor.$$

Possiamo supporre, senza perdere in generalità, che $p < q$ : proviamo che $S$ è pari al numero di punti a coordinate intere nel rettangolo $(0, \frac{p}{2}) \times (0, \frac{q}{2})$ :




Chiaramente, ci sono $\frac{p-1}{2}\frac{q-1}{2}$ punti a coordinate intere nel rettangolo, dei quali nessuno è sulla diagonale: infatti quest'ultima si trova sulla retta $y = \frac{q}{p}x$, e per avere un punto a coordinate intere (positive) si dovrebbe avere $x > p$. Contiamo i punti a coordinate intere sotto la diagonale. Fissato $j \in \mathbb{N}$, $1 \leq j \leq$

$\frac{p-1}{2}$, i punti a coordinate intere aventi ascissa $j$ al di sotto della diagonale sono esattamente $\left\lfloor \frac{jq}{p} \right\rfloor$, quindi, al variare di $j$, abbiamo

$$\sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{jq}{p} \right\rfloor$$

punti a coordinate intere al di sotto della diagonale. Allo stesso modo si prova che i punti a coordinate intere al di sopra della diagonale sono

$$\sum_{k=1}^{\frac{q-1}{2}} \left\lfloor \frac{kp}{q} \right\rfloor.$$

Quindi

$$S = \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{jq}{p} \right\rfloor + \sum_{k=1}^{\frac{q-1}{2}} \left\lfloor \frac{kp}{q} \right\rfloor,$$

e così la legge di reciprocità quadratica è dimostrata.

□

La legge di reciprocità quadratica è molto importante per lo studio della quadraticità modulo un primo, fatto ancora più evidente se la si esprime nel modo seguente:

**Corollario 4.2.** *Siano $p, q$ due numeri primi dispari distinti. Allora*

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right).$$

In particolare, l'unico caso in cui $p$ è un quadrato modulo $q$ ma $q$ non è un quadrato modulo $p$ quando $p \equiv q \equiv 3 \mod 4$.

**Dimostrazione**
Basta osservare che

$$\left(\frac{q}{p}\right)^{-1} = \left(\frac{q}{p}\right),$$

e usare la legge di reciprocità quadratica.

□

## 4.2. Il simbolo di Jacobi

Introduciamo uno strumento per calcolare in modo agevole se un intero è un quadrato modulo un primo. Sia $m$ un numero intero dispari: chiamiamo **simbolo di Jacobi modulo** $m$ la funzione

$$\begin{aligned} \left(\frac{\cdot}{m}\right): \quad \mathbb{Z} &\to \{-1, 0, 1\} \\ n &\mapsto \prod_{p^{v_p} \| m} \left(\frac{n}{p}\right)^{v_p}. \end{aligned}$$

Il simbolo di Jacobi modulo $m$, che è chiaramente un'estensione del simbolo di Legendre modulo un primo, purtroppo perde il significato aritmetico di quest'ultimo (ad esempio, $\left(\frac{2}{15}\right) = 1$, ma 2 non è un quadrato modulo 15), ma continuano a valere tante proprietà del simbolo di Legendre, come la legge di reciprocità quadratica, che lo rendono uno strumento prezioso per il calcolo della quadraticitá modulo un primo di un numero intero: in particolare,

**Proposizione 4.1.** *Per ogni $m, m', n, n' \in \mathbb{N}$, con $m, m'$ dispari,*

1. *Il simbolo di Jacobi modulo $m$ è una funzione periodica di periodo $m$, cioè, per ogni $n \in \mathbb{Z}$,*
$$\left(\frac{n+m}{m}\right) = \left(\frac{n}{m}\right);$$
2. $$\left(\frac{nn'}{m}\right) = \left(\frac{n}{m}\right)\left(\frac{n'}{m}\right);$$
3. $$\left(\frac{n}{mm'}\right) = \left(\frac{n}{m}\right)\left(\frac{n}{m'}\right);$$
4. $$\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}};$$
5. $$\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}};$$
6. $$\left(\frac{m}{m'}\right)\left(\frac{m'}{m}\right) = (-1)^{\frac{m-1}{2}\frac{m'-1}{2}}.$$

**Dimostrazione.**

1. Segue immediatamente dalla definizione del simbolo di Jacobi e dalle proprietà del simbolo di Legendre elencate nella proposizione 3.5;
2. Segue immediatamente dalle proprietà del simbolo di Legendre elencate nella proposizione 3.5;
3. Segue immediatamente dalla definizione del simbolo di Jacobi;
4. Si ha
$$\left(\frac{-1}{m}\right) = \prod_{p^{v_p}|m}\left(\frac{-1}{p}\right)^{v_p} = \prod_{p^{v_p}|m}(-1)^{\frac{p-1}{2}v_p} = (-1)^S,$$
con
$$S = \sum_{p|m} v_p \frac{p-1}{2}.$$
Per concludere, basta dimostrare che
$$S \equiv \frac{m-1}{2} \mod 2.$$
Scriviamo
$$m = \prod_{j=1}^{M} p_j,$$

dove i primi $p_j$ possono essere anche ripetuti. In questo modo, bisogna provare che

$$\sum_{j=1}^{M} \frac{p_j - 1}{2} \equiv \frac{\prod_{j=1}^{M} p_j - 1}{2} = \frac{m-1}{2} \mod 2.$$

Procediamo per induzione su $M$ :

- (passo base, $M = 1$) Ovvio.
- (passo induttivo $M \Rightarrow M + 1$) Si ha

$$\sum_{j=1}^{M+1} \frac{p_j - 1}{2} = \sum_{j=1}^{M} \frac{p_j - 1}{2} + \frac{p_{M+1} - 1}{2} \overset{Ip.Ind.}{\equiv} \frac{\prod_{j=1}^{M} p_j - 1}{2} + \frac{p_{M+1} - 1}{2} \mod 2.$$

Poiché, se $u, v$ sono numeri interi dispari, vale

$$\frac{u-1}{2} + \frac{v-1}{2} \equiv \frac{uv-1}{2} \mod 2, \tag{4.4}$$

il passo induttivo è verificato.

5. É analogo al precedente.
6. Manteniamo la stessa notazione per $m$ dei due punti precedenti, e allo stesso modo scriviamo

$$n = \prod_{h=1}^{N} q_j.$$

Allora

$$\begin{aligned}
\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) &= \prod_{j=1}^{M} \left(\frac{n}{p_j}\right) \prod_{h=1}^{N} \left(\frac{m}{q_h}\right) \\
&= \prod_{j=1}^{M} \prod_{h=1}^{N} \left(\frac{q_h}{p_j}\right) \prod_{j=1}^{M} \prod_{h=1}^{N} \left(\frac{p_j}{q_h}\right) \\
&= \prod_{j=1}^{M} \prod_{h=1}^{N} \left(\frac{p_j}{q_h}\right)\left(\frac{q_j}{p_j}\right) \\
&\overset{Teo\ 4.1}{=} \prod_{j=1}^{M} \prod_{h=1}^{N} (-1)^{\frac{p_j-1}{2}\frac{q_h-1}{2}} \\
&= (-1)^S,
\end{aligned}$$

con

$$S = \sum_{j=1}^{M} \sum_{h=1}^{N} \frac{p_j - 1}{2} \frac{q_h - 1}{2}.$$

Poiché

$$\begin{aligned}
S &= \sum_{j=1}^{M} \frac{p_j - 1}{2} \sum_{h=1}^{N} \frac{q_h - 1}{2} \\
&\overset{Eq.\ (4.4)}{\equiv} \frac{\prod_{j=1}^{M} p_j - 1}{2} \frac{\prod_{h=1}^{N} q_h - 1}{2} \mod 2 \\
&\equiv \frac{m-1}{2} \frac{n-1}{2} \mod 2,
\end{aligned}$$

il risultato è dimostrato.

□

## 4.3. Applicazioni

**Esercizio 4.1.** *É risolubile la congruenza* $x^2 \equiv 30 \mod 79$?

**Risoluzione** Per rispondere, possiamo usare il simbolo di Legendre, poiché 79 è un numero primo: usando le proprietà elencate nelle proposizioni 3.5,4.1 e nel corollario 4.2

$$\begin{aligned}\left(\frac{30}{79}\right) &= \left(\frac{2}{79}\right)\left(\frac{3}{79}\right)\left(\frac{5}{79}\right)\\ &= -\left(\frac{79}{3}\right)\left(\frac{79}{5}\right)\\ &= -\left(\frac{79}{15}\right) = -\left(\frac{4}{15}\right) = -1,\end{aligned}$$

quindi 30 non è un quadrato modulo 79, cioè la congruenza non ha soluzioni.

**Esercizio 4.2.** *É risolubile la congruenza* $x^2 \equiv 3375 \mod 8191$?

**Risoluzione** Per rispondere, possiamo usare il simbolo di Legendre, poiché 8191 è un numero primo: usando le proprietà elencate nelle proposizioni 3.5,4.1 e nel corollario 4.2

$$\begin{aligned}\left(\frac{3375}{8191}\right) &= \left(\frac{27}{8191}\right)\left(\frac{125}{8191}\right)\\ &= -\left(\frac{8191}{27}\right)\left(\frac{8191}{125}\right)\\ &= -\left(\frac{10}{27}\right)\left(\frac{66}{125}\right)\\ &= -\left(\frac{2}{27}\right)\left(\frac{5}{27}\right)\left(\frac{2}{125}\right)\left(\frac{3}{125}\right)\left(\frac{11}{125}\right)\\ &= -\left(\frac{2}{3}\right)^3\left(\frac{5}{3}\right)^3\left(\frac{2}{5}\right)^3\left(\frac{3}{5}\right)^3\left(\frac{11}{5}\right)^3\\ &= -(-1)\left(\frac{2}{3}\right)^3(-1)(-1)\left(\frac{1}{5}\right)^3\\ &= (-1)^5 = -1,\end{aligned}$$

quindi 3375 non è un quadrato modulo 8191, cioè la congruenza non è risolubile.

**Esercizio 4.3.** *Sia $p$ un numero primo dispari. Si ha*

$$\left(\frac{3}{p}\right) = \begin{cases}1 & \text{se } p \equiv 1,11 \mod 12\\ -1 & \text{se } p \equiv 5,7 \mod 12\end{cases} \qquad \left(\frac{5}{p}\right) = \begin{cases}1 & \text{se } p \equiv 1,9 \mod 10\\ -1 & \text{se } p \equiv 3,7 \mod 10\end{cases}.$$

**Risoluzione** Usando il corollario 4.2

$$\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right) = \begin{cases}(-1)^{\frac{p-1}{2}} & \text{se } p \equiv 1 \mod 3\\ -(-1)^{\frac{p-1}{2}} & \text{se } p \equiv 2 \mod 3\end{cases} = \begin{cases}1 & \text{se } p \equiv 1,11 \mod 12\\ -1 & \text{se } p \equiv 5,7 \mod 12\end{cases},$$

$$\left(\frac{5}{p}\right) = (-1)^{p-1}\left(\frac{p}{5}\right) = \left(\frac{p}{5}\right) = \begin{cases}1 & \text{se } p \equiv 1,4 \mod 5\\ -1 & \text{se } p \equiv 2,3 \mod 5\end{cases} = \begin{cases}1 & \text{se } p \equiv 1,9 \mod 10\\ -1 & \text{se } p \equiv 3,7 \mod 10\end{cases},$$

e la dimostrazione è conclusa.

**Risoluzione alternativa** Vediamo una dimostrazione alternativa di questi risultati, basata sul lemma di Gauss. Nel primo caso, calcoliamo

$$m = \left| \left\{ [3k]_p > \frac{p}{2} \middle| 1 \leq k \leq \frac{p-1}{2} \right\} \right| = \sum_{\frac{p}{2}<3k<p} 1 = \left\lfloor \frac{p}{3} \right\rfloor - \left\lfloor \frac{p}{6} \right\rfloor .$$

Posto $p = 12q + r$, con $q, r \in \mathbb{N}$, $r \in \{1, 5, 7, 11\}$,

$$m = \left\lfloor \frac{12q+r}{3} \right\rfloor - \left\lfloor \frac{12q+r}{6} \right\rfloor = 2q + \left\lfloor \frac{r}{3} \right\rfloor - \left\lfloor \frac{r}{6} \right\rfloor .$$

Poiché di $m$ ci interessa la parità, possiamo trascurare il fattore $2q$ :

$$\left\lfloor \frac{r}{3} \right\rfloor - \left\lfloor \frac{r}{6} \right\rfloor \equiv \begin{cases} 0 \mod 2 & \text{se } r = 1, 11 \\ 1 \mod 2 & \text{se } r = 5, 7 \end{cases} .$$

Analogamente, per $q = 5$, calcoliamo

$$m = \left| \left\{ [5k]_p > \frac{p}{2} \middle| 1 \leq k \leq \frac{p-1}{2} \right\} \right| .$$

In questo caso, al variare di $k$, $5k$ può crescere abbastanza da essere uguale a numeri naturali maggiori di $p$ che appartengono alle stesse classi di resto modulo $5$. Tenuto conto di questo fatto,

$$m = \sum_{\frac{p}{2}<5k<p} 1 + \sum_{\frac{3p}{2}<5k<2p} 1 = \left\lfloor \frac{p}{5} \right\rfloor - \left\lfloor \frac{p}{10} \right\rfloor + \left\lfloor \frac{2p}{5} \right\rfloor - \left\lfloor \frac{3p}{10} \right\rfloor ,$$

Posto $p = 10q + r$, con $r \in \{1, 3, 5, 9\}$,

$$\begin{aligned} m &= \left\lfloor \frac{10q+r}{5} \right\rfloor - \left\lfloor \frac{10q+r}{10} \right\rfloor + \left\lfloor \frac{20q+2r}{5} \right\rfloor - \left\lfloor \frac{30q+3r}{10} \right\rfloor \\ &= 2q + \left\lfloor \frac{r}{5} \right\rfloor - \left\lfloor \frac{r}{10} \right\rfloor + \left\lfloor \frac{2r}{5} \right\rfloor - \left\lfloor \frac{3r}{10} \right\rfloor . \end{aligned}$$

Poiché di $m$ ci interessa la parità, possiamo trascurare il fattore $2q$ : procedendo in modo analogo al caso precedente, si conclude.

# CAPITOLO 5

## Congruenze quadratiche

**Introduzione**

In questo capitolo, dimostreremo alcuni risultati sulle congruenze quadratiche, e in particolare sul numero di soluzioni della congruenza $x^2 \equiv n \mod m$, dove $m \in \mathbb{N}, n \in \mathbb{Z}$ sono coprimi. In seguito, mostreremo, con un esempio, il metodo di Gauss per la risoluzione di una congruenza quadratica della forma $x^2 \equiv n \mod p$, con $n \in \mathbb{Z}$ e $p \in \mathbb{P}$.

## 5.1. Risultati generali

Vediamo alcuni risultati generali sul numero delle soluzioni di una congruenza polinomiale:

**Teorema 5.1.** *Sia $p$ un primo dispari, e sia*

$$q(x) = \sum_{j=0}^{k} a_j x^j \in \mathbb{Z}[x]$$

*un polinomio di grado $k < p$. Consideriamo, per ogni $l \in \mathbb{N}$, la congruenza*

$$q(x) \equiv 0 \mod p^l, \tag{5.1}$$

*e sia $S(l) = \{z \in (\mathbb{Z}/p^l\mathbb{Z})^\star \mid q(z) = 0$ in $\mathbb{Z}/p^l\mathbb{Z}\}$ l'insieme delle sue soluzioni. Se per ogni $z \in S(1)$ $q'(z) \neq 0$ in $\mathbb{Z}/p\mathbb{Z}$, allora $|S(1)| = |S(l)|$.*

**Dimostrazione**

Procediamo per induzione su $l$ :

- (passo base, $l = 1$) Ovvio.
- (passo induttivo $l - 1 \Rightarrow l$) Vogliamo definire una mappa $\Phi : S(l-1) \to \left(\mathbb{Z}/p^l\mathbb{Z}\right)^\star$ che ad ogni elemento di $S(l-1)$ associ un elemento di $S(l)$. Sia $z \in \left(\mathbb{Z}/p^{l-1}\mathbb{Z}\right)^\star$ tale che $q(z) \equiv 0 \mod p^{l-1}$. Cerchiamo $h(z) \in \mathbb{Z}$ tale che $z + h(z)p^{l-1} \in S(l)$, cioè

$$q(z + h(z)p^{l-1}) = 0 \text{ in } \mathbb{Z}/p^l\mathbb{Z}. \tag{5.2}$$

Usando il teorema del binomio di Newton,

$$\begin{aligned} q(z+h(z)p^{l-1}) &= \sum_{r=0}^{k} a_r \left(z + h(z)p^{l-1}\right)^r \\ &= \sum_{r=0}^{k}\sum_{s=0}^{r} a_r \binom{r}{s} h(z)^{r-s} p^{(l-1)(r-s)} z^s \\ &= \sum_{r=0}^{k} a_r z^r + \sum_{r=1}^{k}\sum_{s=0}^{r-1} a_r \binom{r}{s} h(z)^{r-s} p^{(l-1)(r-s)} z^s \\ &= q(z) + h(z)p^{l-1}\sum_{r=0}^{k} a_r r z^{r-1} + \sum_{r=2}^{k}\sum_{s=0}^{r-2} a_r \binom{r}{s} h(z)^{r-s} p^{(l-1)(r-s)} z^s \\ &= q(z) + h(z)p^{l-1}q'(z) + A(z)p^l, \end{aligned}$$

con

$$A(z) = \sum_{r=0}^{k}\sum_{s=0}^{r-2} a_r \binom{r}{s} h(z)^{r-s} p^{(l-1)(r-s)-l} z^s \in \mathbb{Z}.$$

In particolare,

$$\begin{aligned} q(z + h(z)p^{l-1}) \equiv 0 \mod p^l &\Leftrightarrow q(z) + h(z)p^{l-1}q'(z) \equiv 0 \mod p^l \\ &\overset{Ip.\,Ind.}{\Leftrightarrow} \quad \frac{q(z)}{p^{l-1}} + h(z)q'(z) \equiv 0 \mod p \\ &\Leftrightarrow \quad h(z) \equiv -\frac{q(z)}{p^{l-1}}(q'(z))^{-1} \mod p, \end{aligned}$$

Con questa scelta di $h(z)$, l'equazione (5.2) è soddisfatta, ed è ben definita la mappa

$$\begin{aligned} \Phi: \quad S(l-1) &\to S(l) \\ z &\mapsto z + h(z)p^{l-1}. \end{aligned}$$

Osserviamo che $\Phi$ è iniettiva: infatti,

$$\begin{aligned} z + h(z)p^{l-1} \equiv t + h(t)p^{l-1} \mod p^l &\Rightarrow z + h(z)p^{l-1} \equiv t + h(t)p^{l-1} \mod p^{l-1} \\ &\Rightarrow z \equiv t \mod p^{l-1}. \end{aligned}$$

In particolare, $|S(l)| \leq |S(l-1)| \overset{Ip.\,Ind.}{=} |S(1)|$. Ma poiché chiaramente anche $|S(l)| \geq |S(l-1)|$, $|S(l)| = |S(1)|$.

□

Osserviamo che il teorema 5.1 ci fornisce anche un metodo per calcolare le soluzioni della congruenza (5.1)

**Proposizione 5.1.** *Siano $f(x) \in \mathbb{Z}[x]$ un polinomio, $m, m_1, m_2 \in \mathbb{N}$, con $(m_1, m_2) = 1$, $m = m_1 m_2$. Se le congruenze*

$$\begin{aligned} f(x) &\equiv 0 \mod m_1 \\ f(x) &\equiv 0 \mod m_2 \end{aligned}$$

*hanno rispettivamente $s_1$ e $s_2$ soluzioni, allora la congruenza*

$$f(x) \equiv 0 \mod m$$

*ha $s_1 s_2$ soluzioni.*

**Dimostrazione**

É una conseguenza immediata del teorema cinese del resto, e nello specifico del fatto che $\mathbb{Z}/m\mathbb{Z} \cong \mathbb{Z}/m_1\mathbb{Z} \times \mathbb{Z}/m_2\mathbb{Z}$.

□

Passiamo al caso delle congruenze quadratiche: dato un polinomio di secondo grado $p(x) = ax^2 + bx + c \in \mathbb{Z}[x]$ e un intero $m > 1$, vogliamo risolvere la congruenza quadratica

$$ax^2 + bx + c \equiv 0 \mod m.$$

Per il teorema cinese del resto, è sufficiente studiare il caso in cui $m$ è una potenza di un primo $p$,

$$ax^2 + bx + c \equiv 0 \mod p^l.$$

Possiamo assumere, senza perdita di generalità, che $p$ non divida $a$ (altrimenti la congruenza non sarebbe quadratica), e in particolare che $p(x)$ sia monico.

**Teorema 5.2. (Wilson)**

$$(p-1)! \equiv -1 \mod p \Leftrightarrow p \in \mathbb{P}.$$

**Dimostrazione**

($\Leftarrow$) Possiamo accoppiare i numeri tra 1 e $p-1$ ognuno con il proprio inverso modulo $p$ : a parte 1 e $p-1$ ognuno di questi numeri si accoppia con un numero diverso. Quindi

$$(p-1)! \equiv 1 \cdot (p-1) \equiv -1 \mod p.$$

($\Rightarrow$) Supponiamo che $p$ non sia primo: allora esiste un primo $q$, con $1 < q < p$, tale che $q \mid p$ e $q \mid (p-1)!$ Pertanto, la congruenza $(p-1)! + 1 \equiv 0 \mod q$ non è verificata, e a maggior ragione non lo è nemmeno $(p-1)! + 1 \equiv 0 \mod p$. Quindi $p$ è primo.

□

## 5.2. Il caso $x^2 + bx + c \equiv 0 \mod p^l,\ p \neq 2$

Poiché $p \neq 2$, esiste l'inverso di 2 modulo $p^l$. Completando il quadrato e riducendo modulo $p^l$, ci si riconduce a una congruenza della forma

$$x^2 \equiv n \mod p^l, \tag{5.3}$$

con $n \in \mathbb{Z}$.

### Il caso $x^2 \equiv n \mod p$

Consideriamo la congruenza

$$x^2 \equiv n \mod p. \tag{5.4}$$

Per il teorema 3.7, il numero di soluzioni è al più 2. Più precisamente, dalla definizione del simbolo di Legendre, possiamo affermare che il numero di soluzioni è $1 + \left(\frac{n}{p}\right)$. L'unico caso interessante quando $n$ è un residuo quadratico modulo $p$, cioè quando $\left(\frac{n}{p}\right) = 1$ e la congruenza (5.4) ha due soluzioni: per trovarle entrambe è sufficiente trovarne una sola, dato che se $x \equiv m \mod p$ è una soluzione, lo è anche $x \equiv -m \mod p$. Nei casi $p \equiv 3 \mod 4$, $p \equiv 5 \mod 8$, si riescono a esprimere in generale le soluzioni, mentre il caso $p \equiv 1 \mod 8$ è più complicato.

**Proposizione 5.2.** *Se* $p \equiv 3 \mod 4$, *allora una soluzione della congruenza* (5.4) *è* $x \equiv n^{\frac{p+1}{4}} \mod p$.

**Dimostrazione**

Per il criterio di Eulero (3.4),

$$\left(\frac{n}{p}\right) = 1 \equiv n^{\frac{p-1}{2}} \mod p,$$

e per il piccolo teorema di Fermat,

$$\left(n^{\frac{p+1}{4}}\right)^2 = n^{\frac{p+1}{2}} \equiv n^{\frac{p+1}{2}} n^{\frac{p-1}{2}} \mod p \equiv n \mod p.$$

□

**Proposizione 5.3.** *Se* $p \equiv 5 \mod 8$, *e* $n^{\frac{p-1}{4}} \equiv 1 \mod p$, *allora una soluzione della congruenza* (5.4) *è*

$$x \equiv n^{\frac{p+3}{8}} \mod p,$$

*mentre se* $n^{\frac{p-1}{4}} \equiv -1 \mod p$, *una soluzione è, posto* $P = \frac{p-1}{2}$,

$$x \equiv n^{\frac{p+3}{8}} P! \mod p.$$

**Dimostrazione**

Poniamo, per comodità di notazione $m = n^{\frac{p+3}{8}}$.

1. Se $n^{\frac{p-1}{4}} \equiv 1 \mod p$,

$$m^2 \equiv n^{\frac{p+3}{4}} \mod p \equiv n^{\frac{p-1}{4}} n \mod p \equiv n \mod p.$$

2. Se $n^{\frac{p-1}{4}} \equiv -1 \mod p$, invece

$$m^2 \equiv -n \mod p.$$

Bisogna trovare $r \in \mathbb{Z}$ tale che $r^2 \equiv -1 \mod p$, in modo da aggiustare il segno. Per il teorema di Wilson 5.2

$$P!^2 \equiv (p-1)! \equiv -1 \mod p.$$

Basta quindi prendere $r = P!$

□

In questi casi le soluzioni, almeno da un punto di vista teorico, si trovano, ma per valori di $p$ molto grandi conoscere le soluzioni ridotte modulo $p$ è complicato.

## 5.3. Il caso $x^2 + bx + c \equiv 0 \mod 2^l$

Se $b$ è pari, , posto $b = 2b'$, con $b' \in \mathbb{Z}$,

$$x^2 + bx + c = x^2 + 2b'x + c = (x + b')^2 + c - b'^2,$$

e ci si riconduce anche in questo caso a risolvere una congruenza della forma (5.3).

Se $b$ è dispari, il problema è maggiormente complicato.

## Il caso $x^2 \equiv n \mod 2^l$

**Teorema 5.3.** *Sia $n$ un intero dispari: la congruenza (5.3) ha un numero di soluzioni pari a*

$$\begin{cases} 0 & \text{se } l = 2, n \equiv 3 \mod 4 \text{ oppure } l \geq 3, n \not\equiv 1 \mod 8 \\ 1 & \text{se } l = 1 \\ 2 & \text{se } l = 2, n \equiv 1 \mod 4, \\ 4 & \text{se } l \geq 3, n \equiv 1 \mod 8 \end{cases}.$$

**Dimostrazione**

I casi $l = 1$ e $l = 2$ sono banali. Se $l > 2$, e $x \in \mathbb{Z}$ è una soluzione della congruenza (5.3), $x$ è sicuramente dispari. Posto $x = 2k + 1$, con $k \in \mathbb{Z}$,

$$x^2 = 4k^2 + 4k + 1 = 4k(k + 1) + 1 \equiv 1 \mod 8.$$

Di conseguenza, se $n \not\equiv 1 \mod 8$, non ci sono soluzioni. Supponiamo allora $n \equiv 1 \mod 8$, e proviamo ciò che resta per induzione su $l$ :

- (passo base, $l = 3$) La congruenza $x^2 \equiv 1 \mod 8$, ha quattro soluzioni, e sono $x \equiv 1, 3, 5, 7 \mod 8$.
- (passo induttivo $1, \ldots, l-1 \Rightarrow l$). Prendiamo $l \geq 4$, e sia $z \in \mathbb{Z}$, $\overline{z} \in \left(\mathbb{Z}/2^{l-1}\mathbb{Z}\right)^\star$ tale che $z^2 \equiv n \mod 2^{l-1}$. Cerchiamo $h(z) \in \mathbb{Z}$ tale che $z + h(z)2^{l-2}$ sia una soluzione della congruenza (5.3): poiché $l \geq 4$,

  $$\left(z + h(z)2^{l-2}\right)^2 \equiv z^2 + 2^{l-1}h(z)z \mod 2^l \equiv z^2 + 2^{l-1}h(z) \mod 2^l.$$

  Quindi,

  $$\left(z + h(z)2^{l-2}\right)^2 \equiv n \mod 2^l \Leftrightarrow h(z) \equiv \frac{z^2 - n}{2^{l-1}} \mod 2.$$

  In particolare, la congruenza (5.3) ammette almeno una soluzione. In realtà ne ammette almeno quattro: infatti, se $x \equiv z_1 \mod 2^l$ è soluzione della congruenza (5.3), lo sono anche

  $$x \equiv -z_1, z_1 + 2^{l-1}, -z_1 + 2^{l-1} \mod 2^l.$$

  É immediato verificare che esse sono soluzioni distinte: dimostriamo che non ce ne sono altre. Denotiamo con $x \equiv z_1 \mod 2^l$ la soluzione trovata in precedenza, e prendiamo $y \in \mathbb{Z}$ tale che $x \equiv y \mod 2^l$ sia un'altra soluzione. Allora si deve avere $y^2 \equiv z_1^2 \mod 2^l$, da cui

  $$(y - z_1)(y + z_1) \equiv 0 \mod 2^l \overset{\substack{\textit{Entrambi i} \\ \textit{fattori} \\ \textit{sono pari}}}{\Rightarrow} \frac{y - z_1}{2}\frac{y + z_1}{2} \equiv 0 \mod 2^{l-2}.$$

  Poiché

  $$\frac{y - z_1}{2} + \frac{y + z_1}{2} = y,$$

  e quest'ultimo è un numero dispari, uno dei due addendi è pari e l'altro è dispari. In altre parole, o $\frac{y-z_1}{2} \equiv 0 \mod 2^{l-2}$, oppure $\frac{y+z_1}{2} \equiv 0 \mod 2^{l-2}$.

  - Se $y - z_1 \equiv 0 \mod 2^{l-1}$, allora esiste $k \in \mathbb{Z}$ tale che $y = z_1 + k2^{l-1}$. Se $k = 0$, oppure se $k = 1$, ritroviamo due delle soluzioni della congruenza (5.3) elencate in precedenza. Per valori di $k$ tali che $|k| \geq 2$, non otteniamo nessuna nuova soluzione modulo $2^l$.
  - Se $y + z_1 \equiv 0 \mod 2^{l-1}$, allora esiste $k \in \mathbb{Z}$ tale che $y = -z_1 + k2^{l-1}$. Se $k = 0$, oppure se $k = 1$, ritroviamo le altre due soluzioni della congruenza (5.3) elencate in precedenza. Per valori di $k$ tali che $|k| \geq 2$, non otteniamo nessuna nuova soluzione modulo $2^l$.

□

Possiamo enunciare adesso il seguente teorema, che è una diretta conseguenza di quanto fatto in questo capitolo (in particolare i teoremi 5.1, 5.3 e la proposizione 5.1):

**Teorema 5.4.** *Sia $m > 1$ un intero,*

$$m = 2^l \prod_{\substack{p \in \mathbb{P}^\star \\ p^{v_p} \| m}} p^{v_p},$$

*e sia $n \in \mathbb{Z}$, coprimo con $m$. Il numero di soluzioni della congruenza $x^2 \equiv n \mod m$ è*

$$a(l,n) \prod_{\substack{p \in \mathbb{P}^\star \\ p | m}} \left(1 + \left(\frac{n}{p}\right)\right),$$

*dove*

$$a(l,n) = \begin{cases} 0 & \text{se } l = 2, n \equiv 3 \mod 4 \text{ oppure } l \geq 3, n \not\equiv 1 \mod 8 \\ 1 & \text{se } l = 1 \\ 2 & \text{se } l = 2, n \equiv 1 \mod 4, \\ 4 & \text{se } l \geq 3, n \equiv 1 \mod 8 \end{cases}.$$

## 5.4. Applicazioni

**Esercizio 5.1. (Congruenza di Fermat)** *Se $p \in \mathbb{P}$, e $p(x) = x^{p-1} - 1$, l'equazione*

$$p(x) = 0$$

*ha $p-1$ soluzioni in $\mathbb{Z}/p^l\mathbb{Z}$, per ogni $l \in \mathbb{N}$.*

**Risoluzione** L'equazione $x^{p-1} - 1 = 0$ ha $p-1$ soluzioni in $\mathbb{Z}/p\mathbb{Z}$. Poiché $p'(x) = -1$ in $\mathbb{Z}/p\mathbb{Z}[x]$, per il teorema 5.1 concludiamo immediatamente.

### Il metodo di Gauss per la congruenza $x^2 \equiv n \mod p$

Mostriamo un metodo alternativo per studiare la congruenza (5.4), con $\left(\frac{n}{p}\right) = 1$. La congruenza

$$x^2 \equiv n \mod p$$

è soddisfatta se e solo se esiste $k \in \mathbb{Z}$ tale che

$$x^2 = n + kp. \tag{5.5}$$

Cerchiamo l'unica soluzione $m \in \mathbb{Z}$, con $1 \leq m \leq \frac{p}{2}$ : essa è tale che

$$kp = m^2 - n < m^2 < \frac{p^2}{4}.$$

In particolare, $k$ è tale che

$$1 \leq k < \frac{p}{4}. \tag{5.6}$$

L'idea è fare una sorta di crivellamento sulla lista di numeri

$$1, 2, \ldots, \left\lfloor \frac{p}{4} \right\rfloor - 1.$$

Consideriamo i primi dispari minori di $\left\lfloor \frac{p}{4} \right\rfloor$, $q^{(1)}, \ldots, q^{(l_p)}$, e per ognuno dei $q^{(j)}$ siano $n_1^{(j)}, \ldots n_{r_j}^{(j)}$ i non residui quadratici modulo $q^{(j)}$. Dalla lista di numeri, scartiamo tutti i $k$ tali che $n + kp$ sia un non residuo quadratico modulo uno dei $q^{(j)}$ : per tali valori, infatti, la congruenza (5.5) non può avere soluzioni. Per fare questo è sufficiente risolvere delle congruenze lineari. Vediamo un esempio:

**Esercizio 5.2.** *Risolvere la congruenza* $x^2 \equiv 17 \mod 89$.

**Risoluzione** Usiamo il metodo di Gauss: riscriviamo la congruenza come equazione:

$$x^2 = 17 + 89k.$$

Per l'equazione (5.6), la soluzione corrisponde a un valore di $k$ compreso tra 1 e 22. Consideriamo i primi $3, 5, 7, 11, 13, 18, 19$, e iniziamo il crivellamento sulla lista

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21.$$

| $q^{(1)} = 3$ | $q^{(2)} = 5$ | $q^{(3)} = 7$ |
|---|---|---|
| $n_1^{(1)} = 2$ | $n_1^{(2)} = 2$ | $n_1^{(3)} = 3$ |
| | $n_2^{(2)} = 3$ | $n_2^{(3)} = 5$ |
| | | $n_3^{(3)} = 6$ |

- Riduciamo modulo 3 :

  $$17 + 89k \equiv 2 \mod 3 \Rightarrow k \equiv 0 \mod 3$$

  Possiamo quindi eliminare dalla lista i multipli di 3 :

  $$1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20.$$

- Riduciamo modulo 5 :

  $$17 + 89k \equiv 2 \mod 5 \Rightarrow k \equiv 0 \mod 5$$

  $$17 + 89k \equiv 3 \mod 5 \Rightarrow k \equiv 4 \mod 5$$

  La lista si accorcia ancora:

  $$1, 2, 7, 8, 11, 14, 16, 17, 19$$

- Riducendo modulo 7 la lista diventa:

  $$1, 8, 11, 17$$

Ci siamo ridotti a un numero abbastanza piccolo di casi. Possiamo continuare ad accorciare la lista, ma in questo caso ad esempio si può notare che

$$17 + 8 \cdot 89 = 729 = 27^2,$$

quindi abbiamo che la soluzione più piccola modulo 89 è $x \equiv 27 \mod 89$. L'altra soluzione, di conseguenza, è $x \equiv 72 \mod 89$.

**Esercizio 5.3.** *Risolvere la congruenza* $x^3 \equiv 1 \mod 19^2$.

**Risoluzione** Possiamo riscrivere la congruenza nel modo seguente:

$$(x-1)(x^2 + x + 1) \equiv 0 \mod 19^2.$$

Iniziamo studiando la congruenza

$$(x-1)(x^2 + x + 1) \equiv 0 \mod 19.$$

Essendo $\mathbb{Z}/19\mathbb{Z}$ un campo, o $x - 1 \equiv 0 \mod 19$, o $x^2 + x + 1 \equiv 0 \mod 19$. Il caso non banale è quest'ultimo: poiché il discriminante del polinomio $p(x) = x^2 + x + 1$ è $\Delta = -3 \equiv 16 \mod 19$, la congruenza $x^2 + x + 1 \equiv 0 \mod 19$ ha come soluzioni $x_{1,2} \equiv 2^{-1}(-1 \pm 4) \mod 19$, e cioè, poiché $2^{-1} \equiv 10 \mod 19$,

$$x \equiv 7, 11 \mod 19.$$

Abbiamo quindi tre soluzioni modulo 19 : per il teorema 5.1, ce ne sono tre anche modulo $19^2$. Solleviamole:

- $x_0 \equiv 1 \mod 19$ : non c'è bisogno di far nulla, la corrispondente soluzione modulo $19^2$ è $y_0 \equiv 1 \mod 19^2$;
- $x_1 \equiv 11 \mod 19$. Cerchiamo $h(x_1)$ come nella dimostrazione del teorema 5.1:

  $$\frac{p(11)}{19} + h(x_1)p'(11) \equiv 0 \mod 19 \Rightarrow 23h(x_1) + 7 \equiv 0 \mod 19 \Rightarrow h(x_1) \equiv 3 \mod 19.$$

  Quindi, la soluzione corrispondente è $y_1 \equiv 11 + 3 \cdot 19 \equiv 68 \mod 19^2$
- $x_2 \equiv 7 \mod 19$. Come prima:

  $$\frac{p(7)}{19} + h(x_2)p'(7) \equiv 0 \mod 19 \Rightarrow h(x_2) \equiv 15 \mod 19.$$

  La soluzione corrispondente è $y_2 \equiv 7 + 15 \cdot 19 \equiv 292 \mod 19^2$.

# CAPITOLO 6

## Struttura dei gruppi moltiplicativi $(\mathbb{Z}/m\mathbb{Z})^\star$

**Introduzione**

In questo capitolo, dimostreremo il teorema di struttura dei gruppi moltiplicativi $(\mathbb{Z}/m\mathbb{Z})^\star$, che caratterizza quali di essi siano ciclici o meno.

Come abbiamo visto, per la risoluzione di una congruenza polinomiale può essere utile conoscere la struttura del gruppo moltiplicativo $(\mathbb{Z}/m\mathbb{Z})^\star$. Proviamo alcuni risultati preliminari:

**Lemma 6.1.** *Sia $p$ un primo dispari, e sia $k$ un numero intero che non è multiplo di $p$. Allora, per ogni $s \in \mathbb{N} \cup \{0\}$,*

$$(1+kp)^{p^s} \equiv 1 + kp^{s+1} \mod p^{s+2}.$$

**Dimostrazione**
Procediamo per induzione su $s$ :

- (passo base, $s = 0$) Ovvio;
- (passo induttivo $s-1 \Rightarrow s$) Supponiamo

$$(1+kp)^{p^{s-1}} \equiv 1 + kp^s \mod p^{s+1},$$

e proviamo che

$$(1+kp)^{p^s} \equiv 1 + kp^{s+1} \mod p^{s+2}.$$

Per ipotesi induttiva, esiste $y \in \mathbb{Z}$ tale che

$$\begin{aligned}(1+kp)^{p^s} = \left((1+kp)^{p^{s-1}}\right)^p &= (1+kp^s+yp^{s+1})^p \\ &= (1+p^s(k+yp))^p .\end{aligned}$$

Poiché

$$\binom{p}{r} \equiv \begin{cases} 0 \mod p & \text{se } 1 \le r \le p-1 \\ 1 \mod p & \text{se } r = 0,\ p \end{cases}$$

e usando il teorema del binomio di Newton

$$\begin{aligned}(1+kp)^{p^s} = \sum_{r=0}^{p} \binom{p}{r} p^{rs}(k+yp)^r &\equiv \binom{p}{0} + \binom{p}{1} p^s(k+yp) \mod p^{s+2} \\ &\equiv 1 + kp^{s+1} \mod p^{s+2}.\end{aligned}$$

□

**Lemma 6.2.** *Sia $a$ un intero dispari. Allora, per ogni $l \in \mathbb{N},\ l \geq 3$,*

$$a^{2^{l-2}} \equiv 1 \mod 2^l$$

**Dimostrazione**
Fissiamo $a$ e procediamo per induzione su $l$ :

- (passo base, $l = 3$) Ogni intero dispari è congruo a 1 modulo 8;
- (passo induttivo $l - 1 \Rightarrow l$) Supponiamo che

  $$a^{2^{l-3}} \equiv 1 \mod 2^{l-1},$$

  allora esiste $y \in \mathbb{Z}$ tale che $a^{2^{l-3}} = 1 + 2^{l-1}y$. Quindi,

  $$\begin{aligned} a^{2^{l-2}} = \left(a^{2^{l-3}}\right)^2 &\equiv (1 + 2^{l-1}y)^2 \mod 2^l \\ &\equiv 1 + 2^{2l-2}y^2 + 2^l y \mod 2^l \\ &\equiv 1 \mod 2^l. \end{aligned}$$

□

**Lemma 6.3.** *Se $l \geq 3$ è un intero, allora*

$$5^{2^{l-3}} \equiv 1 + 2^{l-1} \mod 2^l.$$

*In particolare, l'ordine di 5 modulo $2^l$ è $2^{l-2}$, per ogni $l \geq 3$.*
**Dimostrazione**
Procediamo per induzione su $l$ :

- (passo base, $l = 3$) Ovvio;
- (passo induttivo $l \Rightarrow l + 1$) Supponiamo che

  $$5^{2^{l-3}} \equiv 1 + 2^{l-1} \mod 2^l.$$

  Allora, esiste $y \in \mathbb{Z}$ tale che

  $$5^{2^{l-3}} = 1 + 2^{l-1} + y2^l.$$

  Di conseguenza,

  $$5^{2^{l-2}} \equiv (5^{2^{l-3}})^2 \equiv (1 + 2^{l-1} + y2^l)^2 \equiv 1 + 2^l \mod 2^{l+1},$$

  e concludiamo. In particolare, che l'ordine moltiplicativo di 5 modulo $2^l$ è maggiore di $2^{l-3}$ e per il lemma 6.2 deve dividere $2^{l-2}$. Quindi, l'ordine moltiplicativo di 5 modulo $2^l$ è proprio $2^{l-2}$.

□

Il lemma 6.3 ha il seguente, importante, corollario

**Corollario 6.1.** *Sia $l \geq 3$ un intero. Se $a$ è un intero dispari, allora esiste $b \in \mathbb{Z}$ tale che*

$$a \equiv (-1)^{\frac{a-1}{2}} 5^b \mod 2^l.$$

*In particolare, se $l \geq 2$ è un intero,*

$$\left(\mathbb{Z}/2^l\mathbb{Z}\right)^\star \cong \mathbb{Z}/2^{l-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

**Dimostrazione**
Se $a \equiv 1 \mod 4$, per il lemma 6.3 i $2^{l-2}$ numeri $1, 5, \ldots, 5^{2^{l-2}-1}$ non hanno lo stesso resto modulo $2^l$, e in più sono tutti congrui a 1 modulo 4. Per il principio dei cassetti, esiste $b \in \mathbb{Z}$ tale che $a \equiv 5^b \mod 2^l$. Invece, se $a \equiv 3 \mod 4$, $-a \equiv 1 \mod 4$, e ci si riconduce al caso precedente. Infine, la mappa

$$\begin{aligned} f: \quad \mathbb{Z}/2^{l-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} &\to \left(\mathbb{Z}/2^l\mathbb{Z}\right)^\star \\ (a,b) &\mapsto (-1)^b 5^a \end{aligned}$$

è chiaramente un omomorfismo e, per quanto appena dimostrato, è surgettiva. Poiché i due gruppi hanno la stessa cardinalità, $f$ è anche iniettiva e dunque è un isomorfismo.

□

Dimostriamo infine il seguente teorema, dovuto a Gauss, che caratterizza i gruppi moltiplicativi $(\mathbb{Z}/m\mathbb{Z})^\star$ ciclici:

**Teorema 6.1. (Teorema di struttura dei gruppi moltiplicativi ciclici)** *Se $m \geq 2$ è un intero, il gruppo $\mathbb{G} = (\mathbb{Z}/m\mathbb{Z})^\star$ è ciclico se e solo se $m = 2, 4, p^l, 2p^l$, con $p \in \mathbb{P}^\star, l \in \mathbb{N}$. In particolare, se $l \geq 2$ e $\overline{g}$ è un generatore di $(\mathbb{Z}/p\mathbb{Z})^\star$ allora*

$$\left(\mathbb{Z}/p^l\mathbb{Z}\right)^\star = \begin{cases} (\overline{g}) & \text{se } g^{p-1} \not\equiv 1 \mod p^2 \\ (\overline{g}+\overline{p}) & \text{se } g^{p-1} \equiv 1 \mod p^2 \end{cases}$$

*mentre se $\overline{h}$ è un generatore di $\left(\mathbb{Z}/p^l\mathbb{Z}\right)^\star$,*

$$\left(\mathbb{Z}/2p^l\mathbb{Z}\right)^\star = \begin{cases} (\overline{h}) & \text{se } h \text{ è dispari} \\ (\overline{g}+\overline{p}^l) & \text{se } h \text{ è pari} \end{cases}$$

**Dimostrazione**
Poniamo

$$m = \prod_{p^{v_p} \| m} p^{v_p},$$

e sia

$$M = lcm\left(\left\{\phi(p^{v_p}) \,\middle|\, p^{v_p} \parallel m\right\}\right).$$

Osserviamo che se $\mathbb{G}$ è ciclico, si deve avere

$$M = \phi(m), \tag{6.1}$$

poiché, altrimenti, ogni elemento di $\mathbb{G}$ avrebbe ordine minore di $M$ e non esisterebbe un generatore del gruppo. Inoltre, a meno che $p = 2, l = 1$, $\phi(p^l)$ è pari, e quindi $m$ non può avere due divisori primi dispari distinti, altrimenti l'equazione (6.1) non può essere soddisfatta: concludiamo che, se $\mathbb{G}$ è ciclico, allora $m$ è della forma $m = 2^l, p^l, 2^{v_2}p^l$, con $p \in \mathbb{P}$. In più, se $m$ è della forma $m = 2^{v_2}p^l$, necessariamente $v_2 = 1$ : infatti, se $v_2 > 1$, allora $\phi(2^{v_2}) = 2^{v_2-1}$, e l'equazione (6.1) non può essere soddisfatta. Trattiamo separatamente i tre casi:

- $(m = 2^l)$ Se $l = 1$, oppure $l = 2$, non c'è nulla da dimostrare: nno gruppi moltiplicativi ciclici. Per il corollario 6.1 non ci sono altre possibilità;

- $(m = p^l)$ Il caso $l = 1$ è noto:
$$(\mathbb{Z}/p\mathbb{Z})^\star \cong \mathbb{Z}/(p-1)\mathbb{Z}.$$
Prendiamo $l = 2$, e sia $\overline{g}$ un generatore di $(\mathbb{Z}/p\mathbb{Z})^\star$. Se $g^{p-1} \not\equiv 1 \mod p^2$, osserviamo che $\overline{g}$ è anche un generatore del gruppo $\left(\mathbb{Z}/p^2\mathbb{Z}\right)^\star$, che è dunque ciclico, dato che il suo ordine deve dividere $p(p-1)$, e deve essere maggiore di $p-1$. Se invece $g^{p-1} \equiv 1 \mod p^2$, un generatore è dato da $\overline{r} = \overline{g} + \overline{p}$ : infatti
$$r^{p-1} - 1 = (g+p)^{p-1} - 1 \equiv -g^{p-2}p \mod p^2,$$
e poiché $p$ non divide $g$, $r^{p-1} - 1 \not\equiv 0 \mod p^2$, e quindi, l'ordine di $\overline{r}$ divide $p(p-1)$, ed è anche maggiore di $p-1$. Proviamo infine che se $\overline{r}$ genera $\left(\mathbb{Z}/p^2\mathbb{Z}\right)^\star$, allora genera anche $\left(\mathbb{Z}/p^l\mathbb{Z}\right)^\star$, per ogni $l \geq 3$ : l'ordine di $r$ modulo $p$ è $p-1$, quindi l'ordine di $\overline{r}$ modulo $p^l$ è un multiplo di $p-1$, ed è quindi della forma $p^a(p-1)$, con $0 \leq a < l$. Poiché $r$ genera $\left(\mathbb{Z}/p^2\mathbb{Z}\right)^\star$, esiste $k \in \mathbb{Z}$, non divisibile per $p$, tale che $r^{p-1} = 1 + kp$ : per il lemma 6.1 allora, esiste $h \in \mathbb{Z}$ tale che
$$r^{p^{l-2}(p-1)} = (1+kp)^{p^{l-2}} = 1 + kp^{l-1} + hp^l.$$
Quest'ultimo non è congruo a 1 modulo $p^l$, dato che $p \nmid k$ : pertanto, l'ordine di $r$ modulo $p^l$ deve dividere $(p-1)p^{l-1}$ e deve essere maggiore di $(p-1)p^{l-2}$, cioè non può che essere $(p-1)p^{l-1}$.

- $(m = 2p^l)$ Per il teorema cinese del resto, $\left(\mathbb{Z}/2p^l\mathbb{Z}\right)^\star \cong \left(\mathbb{Z}/p^l\mathbb{Z}\right)^\star$, e quindi anche $\left(\mathbb{Z}/2p^l\mathbb{Z}\right)^\star$ è ciclico. Inoltre, se $\overline{g}$ è un generatore di $\left(\mathbb{Z}/p^l\mathbb{Z}\right)^\star$, si vede subito che, se $g$ è dispari, allora è anche un generatore di $\left(\mathbb{Z}/2p^l\mathbb{Z}\right)^\star$, mentre se $g$ è pari, un generatore di $\left(\mathbb{Z}/2p^l\mathbb{Z}\right)^\star$ è, ad esempio, $r = \overline{g} + \overline{p}^l$.

□

## 6.1. Applicazioni

**Esercizio 6.1.** *Dire se il gruppo $(\mathbb{Z}/242\mathbb{Z})^\star$ è ciclico, e, in caso affermativo, determinare un suo generatore.*

**Risoluzione** Il gruppo $(\mathbb{Z}/242\mathbb{Z})^\star$ è ciclico, poiché $242 = 2 \cdot 11^2$ : determiniamo un suo generatore $\overline{g}$. Un generatore di $(\mathbb{Z}/11\mathbb{Z})^\star$ è, ad esempio $g \equiv 2 \mod 11$. Poiché $2^{10} \not\equiv 1 \mod 121$, per il teorema 6.1
$$(\mathbb{Z}/11\mathbb{Z})^\star = (\overline{2}),$$
e infine, poiché $h$ è pari,
$$(\mathbb{Z}/242\mathbb{Z})^\star = (\overline{2} + \overline{121}) = (\overline{123}).$$

# CAPITOLO 7

## Funzioni aritmetiche

**Introduzione**

In questo capitolo, definiremo e studieremo le principali proprietà delle funzioni aritmetiche e delle serie formali di Dirichlet. In particolare, vedremo che sia l'insieme delle prime sia quello delle seconde possiedono una struttura di anello. Infine, elencheremo e studieremo alcune fra le più importanti funzioni aritmetiche, e dimostreremo la prima formula di inversione di Möbius.

## 7.1. Definizioni

Chiameremo **funzione aritmetica** una qualsiasi funzione

$$f: \quad \mathbb{N} \to X \subseteq \mathbb{C}.$$

Diremo che una funzione aritmetica è **moltiplicativa** se è non nulla e, per ogni $m, n \in \mathbb{N}$,

$$(m, n) = 1 \Rightarrow f(mn) = f(m)f(n),$$

mentre diremo che è **completamente moltiplicativa** se è non nulla e, per ogni $m, n \in \mathbb{N}$,

$$f(mn) = f(m)f(n).$$

Similmente, diremo che una funzione aritmetica è **additiva** se è non nulla e, per ogni $m, n \in \mathbb{N}$,

$$(m, n) = 1 \Rightarrow f(mn) = f(m) + f(n),$$

e che è **completamente additiva** se è non nulla e, per ogni $m, n \in \mathbb{N}$,

$$f(mn) = f(m) + f(n).$$

Ad esempio, le funzioni

$$\begin{aligned} \mathbf{e}: \quad \mathbb{N} &\to \{0, 1\} \\ n &\mapsto \begin{cases} 1 & n = 1 \\ 0 & n \geq 2 \end{cases}, \end{aligned} \tag{7.1}$$

$$\begin{aligned} \mathbf{1}: \quad \mathbb{N} &\to \{1\} \\ n &\mapsto 1, \end{aligned} \tag{7.2}$$

e, per ogni $\alpha \in \mathbb{C}$,

$$\begin{aligned} i^\alpha: \quad \mathbb{N} &\to \mathbb{C} \\ n &\mapsto n^\alpha \end{aligned}$$

sono funzioni aritmetiche completamente moltiplicative (in particolare, l'identità su $\mathbb{N}$ è una funzione aritmetica completamente moltiplicativa). Invece, la funzione logaritmo

$$\begin{aligned} L: \quad \mathbb{N} &\to \mathbb{R} \\ n &\mapsto \log n \end{aligned}$$

è completamente additiva. Denoteremo con $\mathbb{A}$ l'insieme delle funzioni aritmetiche.

## 7.2. Serie di Dirichlet formali

Chiamiamo **serie formale di Dirichlet** una serie della forma

$$\sum_{n\in\mathbb{N}} f(n)\omega(n), \tag{7.3}$$

dove $f \in \mathbb{A}$, e $\omega$ è un'indeterminata completamente moltiplicativa. Denoteremo con $\mathbb{S}$ l'insieme delle serie formali di Dirichlet. Nel seguito, per non appesantire la notazione, scriveremo con lettere maiuscole le serie formali di Dirichlet, e useremo le corrispondenti lettere minuscole per indicare la funzione aritmetica associata.

In $\mathbb{S}$ si possono definire due operazioni di somma e prodotto: se $F$ e $G$ sono due serie formali di Dirichlet, definiamo la loro somma e il loro prodotto come

$$\begin{aligned} F+G &= \sum_{n\in\mathbb{N}} \left(f(n)+g(n)\right)\omega(n), \\ FG &= \sum_{n\in\mathbb{N}} \left( \sum_{hk=n} f(k)g(h) \right) \omega(n). \end{aligned}$$

Osserviamo che $(\mathbb{S}, +, \cdot)$ è un anello commutativo con unità. Il prodotto di due serie formali si può riscrivere nel modo seguente:

$$FG = \sum_{n\in\mathbb{N}} \left( \sum_{d|n} f(d)g\left(\frac{n}{d}\right) \right) \omega(n).$$

Date due funzioni aritmetiche $f, g$ chiameremo **convoluzione moltiplicativa**, o **prodotto di Dirichlet** di $f$ e $g$ la funzione aritmetica

$$\begin{aligned} f\star g: \quad \mathbb{N} &\to \mathbb{C} \\ n &\mapsto \sum_{d|n} f(d)g\left(\frac{n}{d}\right), \end{aligned}$$

così da poter scrivere

$$FG = \sum_{n\in\mathbb{N}} \left(f\star g(n)\right)\omega(n).$$

## 7.3. Struttura algebrica degli anelli $\mathbb{A}, \mathbb{S}$

Definiamo l'applicazione **norma** su $\mathbb{S}$ :

$$\begin{array}{rcl} \nu: \quad \mathbb{S} & \to & \mathbb{N} \cup \{+\infty\} \\ \displaystyle\sum_{n\in\mathbb{N}} f(n)\omega(n) & \mapsto & \begin{cases} \min\{n \in \mathbb{N} \mid f(n) \neq 0\} & \text{se } F \neq 0 \\ +\infty & \text{se } F = 0 \end{cases} \end{array}$$

**Proposizione 7.1.** *Se $F, G \in \mathbb{S}$, allora $\nu(FG) = \nu(F)\nu(G)$. In particolare, $\mathbb{S}$ è un dominio d'integrità.*

**Dimostrazione**
Se una fra $F$ e $G$ è nulla, la tesi è ovvia. Supponiamo che $F$ e $G$ siano non nulle, e poniamo $n_0 = \nu(F)$, $m_0 = \nu(G)$. Allora

$$F = \sum_{n=n_0}^{+\infty} f(n)\omega(n)$$
$$G = \sum_{n=m_0}^{+\infty} g(n)\omega(n),$$

e quindi il primo coefficiente della serie formale $FG$ non nullo per $n = m_0 n_0$, dato che sicuramente $f \star g(n) = 0$ per $n < m_0 n_0$, e

$$f \star g(m_0 n_0) = \sum_{d | m_0 n_0} f(d) g\left(\frac{m_0 n_0}{d}\right) = f(m_0) g(n_0) \neq 0.$$

Pertanto, $\nu(FG) = \nu(F)\nu(G)$. In particolare, se $F, G$ sono non nulle, $\nu(F), \nu(G) \neq 0$, e quindi anche $\nu(FG) \neq 0$, cioè $\mathbb{S}$ è un dominio di integrità.

□

**Teorema 7.1.** *La convoluzione aritmetica è associativa, ed è dotata di elemento neutro (la funzione aritmetica* **e***).*

**Dimostrazione**
Se $f, g, h \in \mathbb{A}$,

$$\begin{aligned} (f \star g) \star h(n) = \sum_{d|n} f \star g(d) h\left(\frac{n}{d}\right) &= \sum_{d|n} \sum_{m|d} f(m) g\left(\frac{d}{m}\right) h\left(\frac{n}{d}\right) \\ &= \sum_{m|n} \sum_{k|\frac{m}{d}} f(m) g(k) h\left(\frac{m}{dk}\right) \\ &= \sum_{m|n} f(m) \left( \sum_{k|\frac{m}{d}} g(k) h\left(\frac{m}{dk}\right) \right) \\ &= \sum_{m|n} f(m) \left( g \star h\left(\frac{m}{d}\right) \right) = f \star (g \star h)(n). \end{aligned}$$

Infine,

$$f \star \mathbf{e}(n) = \sum_{d|n} f(d) \mathbf{e}\left(\frac{n}{d}\right) = f(n)\mathbf{e}(1) = f(n)$$

□

Il teorema precedente ha delle conseguenze importanti:

**Corollario 7.1.** *$(\mathbb{A}, +, \star)$ è un anello commutativo con unità. Inoltre, $\mathbb{A}$ e $\mathbb{S}$ sono isomorfi (come anelli), e un isomorfismo è dato dalla mappa*

$$\begin{array}{rcl} \mathbb{S} & \to & \mathbb{A} \\ \sum_{n\in\mathbb{N}} f(n)\omega(n) & \mapsto & f \end{array}$$

Denoteremo con $1, \zeta$ le serie formali associate alle funzioni aritmetiche (7.1), (7.2):

$$1 = \sum_{n\in\mathbb{N}} \mathbf{e}(n)\omega(n) = \omega(1),$$
$$\zeta = \sum_{n\in\mathbb{N}} \mathbf{1}(n)\omega(n) = \sum_{n\in\mathbb{N}} \omega(n).$$

Una funzione aritmetica $f$ si dice **invertibile** se esiste una funzione aritmetica $g$ tale che

$$f \star g = \mathbf{e}.$$

Diremo inoltre che una serie formale $F$ è **invertibile** se è invertibile la funzione aritmetica ad essa associata. Le serie formali invertibili formano un sottogruppo moltiplicativo di $\mathbb{S}$ : denoteremo con $\mathbb{U}$ tale sottogruppo.

**Proposizione 7.2.** *Si ha*

$$\mathbb{U} = \{F \in \mathbb{S} \mid \nu(F) = 1\}$$

**Dimostrazione**
Proviamo la doppia inclusione:

- $(\subseteq)$ Se $F \in \mathbb{U}$, allora esiste $G \in \mathbb{U}$ tale che $FG = 1$. Per la proposizione 7.1, $\nu(F)\nu(G) = 1$, e quindi $\nu(F) = \nu(G) = 1$.
- $(\supseteq)$ Sia $F \in \mathbb{S}$ tale che $\nu(F) = 1$. Cerchiamo $G \in \mathbb{S}$ tale che $FG = 1$, cioè tale che

$$f \star g(n) = \begin{cases} 1 & \text{se } n = 1 \\ 0 & \text{altrimenti} \end{cases}.$$

Se $n = 1$, si deve avere $f(1)g(1) = 1$. Poiché $\nu(F) = 1$, sicuramente $f(1) \neq 0$, e quindi ha senso porre $g(1) = \frac{1}{f(1)}$. Procedendo induttivamente, si costruisce la funzione aritmetica

$$\begin{array}{rcl} g: \quad \mathbb{N} & \to & \mathbb{C} \\ n & \mapsto & \begin{cases} \frac{1}{f(1)} & \text{se } n = 1 \\ -\frac{1}{f(1)} \sum_{\substack{d|n \\ d\neq 1}} f(d) g\left(\frac{n}{d}\right) & \text{se } n > 1 \end{cases} \end{array}$$

che è tale che $f \star g = \mathbf{e}$. Quindi $F$ è invertibile.

□

Ricordando il teorema 7.1, conosciamo anche il sottogruppo moltiplicativo di $\mathbb{A}$ delle funzioni aritmetiche invertibili (rispetto alla convoluzione),

$$\{f \in \mathbb{A} \mid f(1) \neq 0\}.$$

Denoteremo tale sottogruppo con $\mathbb{U}_{\mathbb{A}}$.

**Lemma 7.1.** *Sia $\mathcal{R}$ un anello commutativo con unità, e sia $I \subset \mathcal{R}$ un ideale tale che per ogni $x \notin I$ $x$ è invertibile. Allora $\mathcal{R}$ è un anello locale, con ideale massimale $I$.*

**Dimostrazione**
Se $J$ è un altro ideale di $\mathcal{R}$, diverso da $\mathcal{R}$ stesso, necessariamente $J \subseteq I$.

□

**Proposizione 7.3.** *$\mathbb{S}$ è un anello locale, con ideale massimale $\mathbb{S} - \mathbb{U}$. Inoltre, $\mathbb{S}$ non è noetheriano.*

**Dimostrazione**
Se $F, G \in \mathbb{S} - \mathbb{U}$, allora $\nu(F), \nu(G) > 1$, e in particolare anche $\nu(F+G) > 1$. Quindi la somma di due elementi non invertibili di $\mathbb{S}$ non è un elemento invertibile di $\mathbb{S}$ (ma in generale $\nu(F+G) \neq \nu(F)+\nu(G)$). É immediato osservare che $\mathbb{S} - \mathbb{U}$ è un ideale di $\mathbb{S}$, che per costruzione verifica le ipotesi del lemma 7.1: quindi $\mathbb{S}$ è un anello locale con ideale massimale $\mathbb{S} - \mathbb{U}$. Inoltre, poiché la catena di ideali

$$\{(\{\omega(i)\}_{i\in\mathbb{N},2\leq i\leq n})\}_{n\in\mathbb{N},n\geq 2}$$

è ascendente, ma non stazionaria, $\mathbb{S}$ non è noetheriano.

□

Date $F, G \in \mathbb{S}$, diremo che $F$ **divide** $G$ (e scriveremo $F \mid G$) se e solo se esiste $H \in \mathbb{S}$ tale che $G = FH$.

**Proposizione 7.4.** *Se $F \mid G$ allora $\nu(F) \leq \nu(G)$. Se vale l'uguaglianza, $F$ e $G$ sono elementi associati.*

**Dimostrazione**
Se $F \mid G$ allora esiste $H \in \mathbb{S}$ tale che $G = FH$. Per la proposizione 7.1,

$$\nu(G) = \nu(FH) = \nu(F)\nu(H) \geq \nu(F)$$

(e se l'uguaglianza, deve aversi $\nu(H) = 1$, cioè $H$ è invertibile e $F, G$ sono elementi associati).

□

Se $F \mid G$ e $\nu(F) < \nu(G)$ diremo che $F$ **divide propriamente** $G$.
Essendo $\mathbb{S}$ un dominio, ogni elemento primo in $\mathbb{S}$ è anche irriducibile $\in$ $\mathbb{S}$. In realtà, vale anche il viceversa:

**Teorema 7.2.** *$(\mathbb{S}, +, \cdot)$ è un UFD.*

**Dimostrazione**
Daremo soltanto un'idea della dimostrazione di questo teorema.

$$R_n = \mathbb{C}[[x_1, \ldots, x_n]]$$

l'anello delle serie di potenze formali nelle $n$ indeterminate $x_1, \ldots, x_n$, e sia

$$\Pi_\omega = \prod_{j=1}^{+\infty_w} \mathbb{N} \cup \{0\}$$

l'insieme delle successioni a valori in $\mathbb{N}\cup\{0\}$, aventi un numero finito di elementi non nulli. Se proviamo che $\mathbb{S} \cong R_{+\infty}$, poiché $R_{+\infty}$ è un UFD, abbiamo la tesi. Per ogni intero $n > 1$, possiamo scrivere

$$n = \prod_{j=1}^{+\infty} {p_j}^{r_j},$$

con $\{r_j\}_{j\in\mathbb{N}} \in \Pi_\omega$, e quindi, se $F \in \mathbb{S}$,

$$F = \sum_{n\in\mathbb{N}} f(n)\omega(n) = \sum_{r\in\Pi_\omega} f\left(\prod_{i=1}^{+\infty} p_i^{r_i}\right) \prod_{i=1}^{+\infty} \omega(p_i)^{r_i}.$$

La mappa

$$\begin{array}{rcl} \mathbb{S} & \to & R_{+\infty} \\ \omega(p_j) & \mapsto & x_j \\ f\left(\prod_{i=1}^{+\infty} p_i^{r_i}\right) & \mapsto & f\left(\prod_{i=1}^{+\infty} p_i^{r_i}\right) \end{array}$$

è un isomorfismo (di anelli).

□

Ricordando il corollario 7.1, i risultati precedenti si riflettono sull'anello $\mathbb{A}$ delle funzioni aritmetiche:

**Corollario 7.2.** *$\mathbb{A}$ è un anello locale, non noetheriano, a fattorizzazione unica.*

## 7.4. Funzioni aritmetiche moltiplicative

Dimostriamo alcune proprietà generali delle funzioni aritmetiche moltiplicative. Ovviamente, ogni funzione aritmetica completamente moltiplicativa è anche moltiplicativa.

**Proposizione 7.5.** *Se $f \in \mathbb{A}$ è moltiplicativa, allora $f(1) = 1$.*

**Dimostrazione**
Sia $a \in \mathbb{N}$ tale che $f(a) \neq 0$. Allora

$$f(a) = f(a \cdot 1) = f(a)f(1) \Rightarrow f(1) = 1.$$

□

Denotiamo con $\mathbb{M}$ l'insieme delle funzioni aritmetiche moltiplicative.

**Lemma 7.2.** *$(\mathbb{M}, \star)$ è un monoide.*

**Dimostrazione**
Siano $f, g \in \mathbb{M}$, e siano $m, n \in \mathbb{N}$, coprimi. Osserviamo che se $d$ è un divisore di $m$ e $d'$ è un divisore di

$n$, che $d, d'$ e $\frac{m}{d}, \frac{n}{d'}$ sono coppie di interi coprimi. Quindi,

$$\begin{aligned}(f \star g(m))\,(f \star g(n)) &= \sum_{d|m} f(d)g\left(\frac{m}{d}\right) \sum_{d'|n} f(d')g\left(\frac{n}{d'}\right) \\ &= \sum_{\substack{d|m \\ d'|n}} f(d)g\left(\frac{m}{d}\right) f(d')g\left(\frac{n}{d'}\right) \\ &= \sum_{\substack{d|m \\ d'|n}} f(dd')g\left(\frac{mn}{dd'}\right) \\ &= \sum_{d|mn} f(d)g\left(\frac{mn}{d}\right) = f \star g(mn).\end{aligned}$$

□

Si potrebbe pensare che la convoluzione aritmetica di due funzioni aritmetiche completamente moltiplicative sia completamente moltiplicativa: in realtà questo è falso: vedremo in seguito degli esempi.

**Proposizione 7.6.** *Se $f, g$ sono due funzioni aritmetiche tali che $f, f \star g \in \mathbb{M}$, allora anche $g \in \mathbb{M}$.*

**Dimostrazione**

Supponiamo per assurdo che $g \notin \mathbb{M}$ : allora, per la proposizione 7.5, $g(1) \neq 1$, ed esisterebbero due interi positivi coprimi $m, n$, tali che

$$g(mn) \neq g(m)g(n).$$

Scegliamo $m$ e $n$ in modo tale che il loro prodotto $mn$ sia il più piccolo possibile (è possibile per il principio del minimo). Se $mn = 1$, si dovrebbe avere

$$g(1)^2 \neq g(1),$$

e poiché

$$1 = f \star g(1) = f(1)g(1) = g(1),$$

abbiamo subito un assurdo. Supponiamo allora $mn > 1$ : per la minimalitá di $mn$, comunque si scelgano due interi positivi coprimi $a, b$ tali che $ab < mn$, $g(ab) = g(a)g(b)$. Quindi

$$\begin{aligned}f \star g(mn) &= \sum_{\substack{a|m,\ b|n \\ ab<mn}} f\left(\frac{mn}{ab}\right) g(ab) + f(1)g(mn) \\ &\overset{Pro\ 7.5}{=} \sum_{\substack{a|m,\ b|n \\ ab<mn}} f\left(\frac{m}{a}\right) f\left(\frac{n}{b}\right) g(a)g(b) + g(mn) \\ &= \sum_{a|m} f\left(\frac{m}{a}\right) g(a) \sum_{b|n} f\left(\frac{n}{b}\right) g(b) + g(mn) - g(m)g(n) \\ &= f \star g(m) f \star g(n) - g(m)g(n) + g(mn).\end{aligned}$$

Ma $f \star g$ è moltiplicativa, quindi $f \star g(mn) = f \star g(m) f \star g(n)$, e semplificando si ottiene $g(mn) = g(m)g(n)$, assurdo. Quindi anche $g$ è moltiplicativa.

□

**Proposizione 7.7.** $\mathbb{M} < \mathbb{U}_{\mathbb{A}}$.

**Dimostrazione**

Sicuramente, $\mathbb{M} \subset \mathbb{U}_{\mathbb{A}}$, dato che se $f \in \mathbb{M}$, per la proposizione 7.5, $f(1) = 1 \neq 0$. Inoltre, l'elemento neutro per la convoluzione, la funzione aritmetica **e**, è una funzione moltiplicativa, e appartiene a $\mathbb{U}_{\mathbb{A}}$.

Resta da provare che per ogni funzione aritmetica moltiplicativa ne esiste un'altra tale che $f \star g = \mathbf{e}$. Per il corollario 7.1, la serie formale di Dirichlet associata ad $f$ è invertibile: sia $g$ la funzione aritmetica corrispondente all'inversa. Sempre per il corollario 7.1, $f \star g = \mathbf{e}$, e per la proposizione 7.6, $g$ è moltiplicativa.

□

L'insieme delle funzioni aritmetiche può essere dotato della struttura di $\mathbb{C}-$spazio vettoriale, con il prodotto per scalari

$$\begin{aligned} \mathbb{C} \times \mathbb{A} &\to \mathbb{A} \\ (\alpha, f) &\mapsto \alpha f. \end{aligned}$$

In più $(\mathbb{A}, +, \star)$ è una $\mathbb{C}-$algebra.
Data una funzione aritmetica $f$, consideriamo l'applicazione

$$\begin{aligned} \Phi_f : \mathbb{A} &\to \mathbb{A} \\ g &\mapsto fg. \end{aligned} \tag{7.4}$$

**Proposizione 7.8.** *Sia $f$ una funzione aritmetica completamente moltiplicativa. La mappa $\Phi_f$ è un omomorfismo di algebre. Inoltre, se $f(n) \neq 0$ per ogni $n \in \mathbb{N}$, allora $\Phi_f$ è un automorfismo.*

**Dimostrazione**
L'unica verifica non banale è che, se $g, h \in \mathbb{A}$,

$$\Phi_f(g \star h) = \Phi_f(g) \star \Phi_f(h).$$

Per ogni $n \in \mathbb{N}$,

$$\begin{aligned} \Phi_f(g \star h)(n) = f(g \star h)(n) &= \sum_{d|n} f(n) g(d) h\left(\frac{n}{d}\right) \\ &= \sum_{d|n} f(d) f\left(\frac{n}{d}\right) g(d) h\left(\frac{n}{d}\right) \\ &= fg \star fh(n) = \Phi_f(g) \star \Phi_f(h)(n). \end{aligned}$$

Se in più $f$ non si annulla mai, è ben definita la mappa $\Phi_{\frac{1}{f}}$, che si verifica subito essere l'inversa di $\Phi_f$. Quindi $\Phi$ è un automorfismo.

□

Se una funzione aritmetica è moltiplicativa, per determinarla completamente su tutto $\mathbb{N}$ basta conoscere il suo comportamento sulle potenze dei primi (e se è completamente moltiplicativa basta conoscere il suo comportamento sui primi).

**Teorema 7.3.** *Sia $f \in \mathbb{A}$ una funzione aritmetica moltiplicativa. Se*

$$\lim_{p^m \to +\infty} f(p^m) = 0$$

*per ogni $p \in \mathbb{P}$ e per ogni $m \in \mathbb{M}$, allora*

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

**Dimostrazione**
Per ipotesi, esistono due costanti positive $A$ e $B$ tali che

$$\forall p \in \mathbb{P},\ \forall m \in \mathbb{N}, \quad |f(p^m)| \leq A,$$

$$\forall p \in \mathbb{P},\ \forall m \in \mathbb{N}, \quad p^m > B \Rightarrow |f(p^m)| \leq 1.$$

Inoltre, per ogni $\epsilon > 0$ esiste una costante positiva $N(\epsilon)$ tale che

$$\forall p \in \mathbb{P},\ \forall m \in \mathbb{N}, \quad p^m > N(\epsilon) \Rightarrow |f(p^m)| < \epsilon.$$

Le costanti $A, B$ sono indipendenti da $p, m$, e dalla scelta di $\epsilon$. Inoltre, gli insiemi

$$\mathcal{V}_\epsilon = \{n \in \mathbb{N} \mid \forall p \in \mathbb{P}, \forall m \in \mathbb{N},\ p^m \parallel n \Rightarrow p^m \leq N(\epsilon)\},$$
$$\mathcal{W} = \{(p, m) \in \mathbb{P} \times \mathbb{N} \mid p^m \leq B\}$$

sono necessariamente finiti: poniamo $\rho(\epsilon)$ il massimo dell'insieme $\mathcal{V}_\epsilon$, $C = |\mathcal{W}|$; osserviamo che anche $C$ è indipendente da $p, m$, e dalla scelta di $\epsilon$. Prendiamo $n \in \mathbb{N},\ n > \rho(\epsilon)$ : allora esistono almeno un primo $\widehat{p}$ e un intero positivo $m$ tali che $\widehat{p}^m \parallel n$ e $\widehat{p}^m > N(\epsilon)$. Scrivendo

$$n = \widehat{p}^m \prod_{(p,a)\notin\mathcal{W}} p^a \prod_{(q,b)\in\mathcal{W}} q^b,$$

otteniamo che

$$|f(n)| = |f(\widehat{p}^m)| \prod_{(p,a)\notin\mathcal{W}} |f(p^a)| \prod_{(q,b)\in\mathcal{W}} |f(q^b)| < A^C \epsilon,$$

e poiché questo vale per ogni scelta di $n > \rho(\epsilon)$, abbiamo la tesi.

□

## 7.5. Funzioni aritmetiche additive

Dimostriamo anche alcune proprietà generali delle funzioni aritmetiche additive. Ovviamente ogni funzione aritmetica completamente additiva è anche additiva.

**Proposizione 7.9.** *Se $f \in \mathbb{A}$ è additiva, allora $f(1) = 0$.*

**Dimostrazione**
Sia $a \in \mathbb{N}$ tale che $f(a) \neq 0$. Allora

$$f(a) = f(a \cdot 1) = f(a) + f(1) \Rightarrow f(1) = 0.$$

□

**Proposizione 7.10.** *Sia $f \in \mathbb{A}$ una funzione aritmetica completamente additiva. La mappa $\Phi_f$ definita nell'equazione (7.4) è tale che, per ogni $g, h \in \mathbb{A}$,*

$$\Phi(g + h) = \Phi(g) + \Phi(h)$$
$$\Phi(g \star h) = \Phi(g) \star h + g \star \Phi(h). \tag{7.5}$$

**Dimostrazione**
La prima delle (7.5) è già stata verificata nella dimostrazione della proposizione 7.8, verifichiamo la seconda: per ogni $n \in \mathbb{N}$,

$$\begin{aligned}
\Phi(g \star h)(n) = f(g \star h)(n) &= f(n) \sum_{d|n} g(d) h\left(\frac{n}{d}\right) \\
&= \sum_{d|n} \left(f(d) + f\left(\frac{n}{d}\right)\right) g(d) h\left(\frac{n}{d}\right) \\
&= \sum_{d|n} fg(d) h\left(\frac{n}{d}\right) + g(d) fh\left(\frac{n}{d}\right) \\
&= fg \star h(n) + g \star fh(n) = \Phi(g) \star h(n) + g \star \Phi(h)(n).
\end{aligned}$$

□

Una funzione aritmetica $f \in \mathbb{A}$ tale che la funzione $\Phi$ goda delle proprietà nell'equazione (7.5) è detta una **derivazione** nell'algebra $\mathbb{A}$. In particolare il logaritmo è una derivazione nell'algebra $\mathbb{A}$.

Alla funzione aritmetica $L$ corrisponderà la serie formale

$$\zeta' = \sum_{n \in \mathbb{N}} \log n\omega(n).$$

Così come per le funzioni aritmetiche moltiplicative, se una funzione aritmetica è additiva, per determinarla completamente su tutto $\mathbb{N}$ basta conoscere il suo comportamento sulle potenze dei primi (e se è completamente additiva basta conoscere il suo comportamento sui primi).

## 7.6. Principali funzioni aritmetiche

### Funzioni di Dirichlet dei divisori, $d_r$

Chiameremo **funzione di Dirichlet dei divisori** la funzione aritmetica

$$\begin{aligned} d = \mathbf{1} \star \mathbf{1} : \quad \mathbb{N} &\to \mathbb{N} \\ n &\mapsto \sum_{d|n} 1 \end{aligned}$$

**Proposizione 7.11.** *La funzione aritmetica $d$ è moltiplicativa, ma non completamente moltiplicativa.*

**Dimostrazione**

Per il lemma 7.2, poiché $\mathbf{1} \in \mathbb{M}$, la funzione $d$ è moltiplicativa, ma non è completamente moltiplicativa: infatti, se $p$ è un numero primo, $d(p) = 2, d(p^2) = 3$, e $d(p^2) \neq d(p)^2$.

□

Più in generale, possiamo convolvere la funzione aritmetica $\mathbf{1}$ più volte: la funzione aritmetica

$$\begin{aligned} d_r = \star_{i=1}^{r} \mathbf{1} : \quad \mathbb{N} &\to \mathbb{N} \\ n &\mapsto \sum_{d_1 \dots d_r = n} 1. \end{aligned}$$

conta il numero di modi in cui un dato intero positivo $n$ può essere scritto come prodotto di $r$ interi positivi (osserviamo che $d = d_2$).

Poiché la funzione dei divisori di Dirichlet è moltiplicativa, per determinarla completamente basta studiare il suo comportamento sulle potenze dei primi: è semplice osservare che

$$d(p^a) = a + 1,$$

e di conseguenza

**Proposizione 7.12.** *Per ogni $n \in \mathbb{N}$,*

$$d(n) = \prod_{p^a \| n} (a + 1)$$

**Corollario 7.3.** *$d(n)$ è dispari se e solo se $n$ è un quadrato.*

Più in generale, valutiamo la funzione dei divisori di Dirichlet generalizzata $d_r$ :

**Proposizione 7.13.** *Per ogni* $a, r \in \mathbb{N}$, $r \geq 2$,

$$d_r(p^a) = \binom{a+r-1}{r-1}.$$

**Dimostrazione**
Procediamo per induzione su $r$ :

- (passo base, $r = 2$) Già dimostrato, dato che $d_2(p^a) = d(p^a) = a + 1 = \binom{a+1}{1}$;
- (passo induttivo $r \Rightarrow r + 1$) Per ogni primo $p$ e per ogni $a \in \mathbb{N}$,

$$\begin{aligned} d_{r+1}(p^a) = d_r \star \mathbf{1}(p^a) &= \sum_{k|p^a} d_r(k) \\ &= \sum_{h=0}^{a} d_r(p^h) \\ &= \sum_{h=0}^{a} \binom{h+r-1}{r-1} = \binom{a+r}{r}, \end{aligned}$$

  dove l'ultima uguaglianza si prova facilmente per induzione su $a$.

□

### Funzione di Möbius, $\mu$

Definiamo le funzioni $\omega, \Omega$ :

$$\begin{array}{rccl} \omega: & \mathbb{N} & \to & \mathbb{N} \\ & n & \mapsto & \begin{cases} 0 & \text{se } n = 1 \\ \sum_{p|n} 1 & \text{se } n \neq 1 \end{cases} \end{array}$$

$$\begin{array}{rccl} \Omega: & \mathbb{N} & \to & \mathbb{N} \\ & n & \mapsto & \begin{cases} 0 & \text{se } n = 1 \\ \sum_{p^a \| n} a & \text{se } n \neq 1 \end{cases} \end{array}.$$

che contano, rispettivamente, il numero di primi che compaiono nella fattorizzazione di un intero positivo $n$ e la somma degli esponenti di tali primi.

Definiamo inoltre la funzione **radicale**, che associa a ogni intero positivo il suo più grande divisore libero da quadrati:

$$\begin{array}{rccl} \rho: & \mathbb{N} & \to & \mathbb{N} \\ & n & \mapsto & \begin{cases} 1 & \text{se } n = 1 \\ \prod_{p|n} p & \text{se } n \neq 1 \end{cases} \end{array}$$

Per la proposizione 7.5, $\omega, \Omega$ non sono funzioni moltiplicative, ma è immediato osservare che $\omega$ è additiva e $\Omega$ è completamente additiva, mentre la funzione aritmetica $\rho$ è moltiplicativa.

Osserviamo che un intero $n$ è libero da quadrati se e solo se $n = \rho(n)$. In generale, dato $n \in \mathbb{N}$, $\Omega(n) \geq \omega(n)$, e $\Omega(n) = \omega(n)$ se e solo se $n$ è libero da quadrati.

La **funzione di Möbius** è la funzione aritmetica

$$\begin{array}{rccl} \mu: & \mathbb{N} & \to & \{-1,0,1\} \\ & n & \mapsto & \begin{cases} 1 & \text{se } n = 1 \\ (-1)^r & \text{se } \Omega(n) = \omega(n) = r \\ 0 & \text{se } \Omega(n) > \omega(n) \end{cases} \end{array}$$

**Proposizione 7.14.** *$\mu \in \mathbb{M}$, e in particolare $\mu$ è una funzione aritmetica invertibile.*

**Dimostrazione**
Siano $m, n$ interi positivi coprimi. Se almeno uno fra $m, n$ è non libero da quadrati, non lo è nemmeno $mn$. Allo stesso modo, se $m$ e $n$ sono liberi da quadrati, anche $mn$ è libero da quadrati. Dunque la funzione di Möbius è moltiplicativa.

□

La funzione $\mu$ deve la sua importanza al seguente risultato, noto come **prima formula di inversione di Möbius:**

**Teorema 7.4. (Möbius)**

$$\mu \star \mathbf{1} = \mathbf{e},$$

*cioè*

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{se } n = 1 \\ 0 & \text{se } n \neq 1 \end{cases}. \tag{7.6}$$

*Inoltre, se $f, g \in \mathbb{A}$,*

$$f \star \mathbf{1} = g \Leftrightarrow f = \mu \star g.$$

**Dimostrazione**
Sia $n$ un intero positivo. Si ha $\mu \star \mathbf{1}(1) = \mu(1) = 1$, mentre se $n > 1$, osserviamo che i divisori $d$ di $n$ tali che $\mu(d) \neq 0$ sono quelli liberi da quadrati: quindi

$$\sum_{d|n} \mu(d) = \sum_{d|\rho(n)} \mu(d).$$

Poniamo $\rho(n) = q_1 \dots q_r$ : i divisori di $\rho(n)$ sono tutti e soli i possibili prodotti dei primi che compaiono nella sua fattorizzazione: fissato $k \in \mathbb{N}$, con $0 \leq k \leq r$, nno $\binom{r}{k}$ divisori che sono prodotto di $k$ di questi primi. In definitiva,

$$\sum_{d|\rho(n)} \mu(d) = \sum_{k=0}^{r} \binom{r}{k} (-1)^k = (1 + (-1))^r = 0.$$

Proviamo la seconda parte:

$(\Rightarrow)$ $g = f \star \mathbf{1} \Rightarrow g \star \mu = f \star \mathbf{1} \star \mu = f \star (\mathbf{1} \star \mu) = f \star \mathbf{e} = f$

$(\Leftarrow)$ $f = g \star \mu \Rightarrow f \star \mathbf{1} = g \star \mu \star \mathbf{1} = g \star (\mu \star \mathbf{1}) = g \star \mathbf{e} = g.$

□

Alla funzione aritmetica $\mu$ associamo la serie formale di Dirichlet

$$\zeta^{-1} = \frac{1}{\zeta} = \sum_{n \in \mathbb{N}} \mu(n)\omega(n).$$

La prima formula di inversione di Möbius ha il seguente, importantissimo, corollario:

**Corollario 7.4.** *Se $f \in \mathbb{A}$ è una funzione aritmetica completamente moltiplicativa, la sua inversa è $f^{-1} = f\mu$.*

**Dimostrazione**

Basta osservare che $f\mu \overset{Eq.\ (7.4)}{=} \Phi(\mu) = \Phi(\mathbf{1}^{-1}) = \Phi(\mathbf{1})^{-1} = f^{-1}$.

□

Legate alle funzioni aritmetiche definite in questo paragrafo, ce ne sono delle altre: chiameremo **funzione di Liouville** la funzione aritmetica:

$$\begin{aligned} \lambda : \quad \mathbb{N} &\to \{-1, 1\} \\ n &\mapsto (-1)^{\Omega(n)}. \end{aligned}$$

Osserviamo che, essendo $\Omega$ completamente additiva, la funzione $\lambda$ è completamente moltiplicativa. La funzione aritmetica $\mu^2$ è invece la funzione caratteristica degli interi positivi liberi da quadrati:

$$\begin{aligned} \mu^2 : \quad \mathbb{N} &\to \{0, 1\} \\ n &\mapsto \begin{cases} 1 & \text{se } \Omega(n) = \omega(n) \\ 0 & \text{se } \Omega(n) > \omega(n) \end{cases}. \end{aligned}$$

## Funzione di Eulero, $\phi$

Già conosciamo la funzione $\phi$ di Eulero:

$$\begin{aligned} \phi : \mathbb{N} &\to \mathbb{C} \\ n &\mapsto \sum_{\substack{1 \le k \le n \\ (k,n)=1}} 1. \end{aligned}$$

**Proposizione 7.15.** *$\phi = \mu \star i$. In particolare, la funzione $\phi$ di Eulero è moltiplicativa.*

**Dimostrazione**

Per ogni $n \in \mathbb{N}$,

$$\begin{aligned} \phi(n) \overset{Eq.\ (7.6)}{=} \sum_{k=1}^{n} \sum_{d \mid (k,n)} \mu(d) &= \sum_{d \mid n} \left( \mu(d) \sum_{\substack{1 \le k \le n \\ d \mid k}} 1 \right) \\ &= \sum_{d \mid n} \mu(d) \frac{n}{d} = \mu \star i(n). \end{aligned}$$

□

Usando la prima formula di inversione di Möbius, si prova il seguente interessante corollario:

**Corollario 7.5.** *$i = \phi \star \mathbf{1}$, ovvero, per ogni $n \in \mathbb{N}$,*

$$\sum_{d \mid n} \phi(d) = n.$$

Determiniamo il comportamento della funzione $\phi$ : essendo moltiplicativa, basta valutarla sulle potenze dei primi. É facile rendersi conto che, per ogni primo $p$ e per ogni $a \in \mathbb{N}$,

$$\phi(p^a) = p^a - p^{a-1} = p^{a-1}(p-1),$$

e di conseguenza,

**Proposizione 7.16.** *Per ogni* $n \in \mathbb{N}$,

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

Di conseguenza

**Corollario 7.6.** *Se* $n > 2$, $\phi(n)$ *è pari.*

## Funzione di von Mangoldt, $\Lambda$

Chiameremo **funzione di von Mangoldt** la funzione aritmetica

$$\begin{array}{rccl} \Lambda: & \mathbb{N} & \to & \mathbb{C} \\ & n & \mapsto & \begin{cases} 0 & \text{se } n = 1 \vee \omega(n) > 2 \\ \log p & \text{se } n = p^a,\ a \geq 1 \end{cases} \end{array}$$

**Proposizione 7.17.** $\Lambda \star \mathbf{1} = L$ *(e per la prima formula di inversione di Möbius,* $\Lambda = L \star \mu$*).*

**Dimostrazione**
Sia $n > 1$ un intero positivo. Poiché $\Lambda$ è non nulla solo se valutata su una potenza di un primo,

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

□

## Funzione somma dei divisori, $\sigma$

Chiamiamo **funzione somma dei divisori** la funzione aritmetica

$$\begin{array}{rccl} \sigma = i \star \mathbf{1}: & \mathbb{N} & \to & \mathbb{N} \\ & n & \mapsto & \displaystyle\sum_{d|n} d, \end{array}$$

Anche $\sigma$ è moltiplicativa, in quanto convoluzione di funzioni moltiplicative. Valutiamola sulle potenze dei primi: per ogni primo $p$ e per ogni $a \in \mathbb{N}$,

$$\sigma(p^a) = \sum_{i=0}^{a} p^a = \frac{p^{a+1} - 1}{p - 1},$$

e di conseguenza

**Proposizione 7.18.** *Per ogni* $n \in \mathbb{N}$,

$$\sigma(n) = \prod_{p^a \| n} \frac{p^{a+1} - 1}{p - 1}.$$

Più in generale, dato $\alpha \in \mathbb{C}$, chiamiamo **funzione somma dei divisori generalizzata** la funzione aritmetica

$$\begin{array}{rccl} \sigma_\alpha : & \mathbb{N} & \to & \mathbb{C} \\ & n & \mapsto & i^\alpha \star \mathbf{1}(n) = \displaystyle\sum_{d|n} d^\alpha, \end{array}$$

che a ogni $n \in \mathbb{N}$ associa la somma delle potenze $\alpha-$esime dei suoi divisori. Anche $\sigma_\alpha$ è moltiplicativa, e per ogni primo $p$ e per ogni $a \in \mathbb{N}$,

$$\sigma_\alpha(p^a) = \sum_{i=0}^{a} p^{a\alpha} = \frac{p^{\alpha(a+1)} - 1}{p^\alpha - 1},$$

quindi

**Proposizione 7.19.** *Per ogni $n \in \mathbb{N}$,*

$$\sigma_\alpha(n) = \prod_{p^a \| n} \frac{p^{\alpha(a+1)} - 1}{p^\alpha - 1}.$$

## 7.7. Applicazioni

**Esercizio 7.1.** $\omega \star \mu = i_{\mathbb{P}}$, *dove*

$$\begin{array}{rccl} i_{\mathbb{P}} : & \mathbb{N} & \to & \{0,1\} \\ & n & \mapsto & \begin{cases} 1 & \textit{se } n \textit{ è un primo} \\ 0 & \textit{altrimenti} \end{cases} \end{array}$$

*è la funzione indicatrice dei primi.*

**Risoluzione** A priori, essendo $\omega$ una funzione aritmetica additiva e $\mu$ una funzione aritmetica moltiplicativa, non sappiamo nulla sul comportamento della loro convoluzione. Poniamo, per comodità di notazione, $\omega \star \mu = F$ : per la prima formula di inversione di Möbius, $\omega = F \star \mathbf{1}$, cioè, per ogni $n \in \mathbb{N}$,

$$\sum_{p|n} 1 = \sum_{d|n} F(d).$$

Ma

$$\sum_{p|n} 1 = \sum_{d|n} i_{\mathbb{P}}(d) = i_{\mathbb{P}} \star \mathbf{1},$$

quindi $F \star \mathbf{1} = i_{\mathbb{P}} \star \mathbf{1}$. Poiché $\mathbb{A}$ è un dominio di integrità, necessariamente $F = i_{\mathbb{P}}$.

# CAPITOLO 8

## Serie di Dirichlet

**Introduzione**

In questo capitolo definiremo le serie di Dirichlet e ne studieremo la convergenza e la convergenza assoluta, introducendo la nozione di ascissa di convergenza e ascissa di convergenza assoluta: enunceremo e dimostreremo il lemma di sommazione parziale di Abel, che permette di affrontare questi (ma anche tanti altri) problemi in modo agevole. Dimostreremo una relazione tra le due ascissa di convergenza. Infine, definiremo la funzione di generatrice di una funzione aritmetica, e dimostreremo l'unicità della rappresentazione di quest'ultima come serie di Dirichlet.

## 8.1. Definizioni e notazioni preliminari

Data una successione $\{a_n\}_{n\in\mathbb{N}} \subset \mathbb{C}$, e un numero complesso $s \in \mathbb{C}$, chiamiamo **serie di Dirichlet** associata alla successione (e a $s$) la serie

$$\sum_{n\in\mathbb{N}} \frac{a_n}{n^s}. \tag{8.1}$$

Nel seguito, supporremo che la successione $\{a_n\}_{n\in\mathbb{N}}$ sia a valori reali, e che anche $s$ sia reale. Per raccordarci alla definizione precedentemente data di serie formale di Dirichlet (7.3), prenderemo

$$\begin{array}{rccc} f: & \mathbb{N} & \to & \mathbb{C} \\ & n & \mapsto & a_n \end{array} \tag{8.2}$$

e, come indeterminata completamente moltiplicativa,

$$\begin{array}{rccc} \omega: & \mathbb{N} & \to & \mathbb{C} \\ & n & \mapsto & n^{-s}. \end{array} \tag{8.3}$$

Nel seguito, saremo interessati al caso in cui $f$ sia una funzione aritmetica moltiplicativa: con le notazioni dell'equazione (8.1), questo vuol dire che, per ogni $m, n \in \mathbb{N}$,

$$(m, n) = 1 \Rightarrow a_{mn} = a_m a_n.$$

## 8.2. Ascisse di convergenza

Prendiamo $s_0 \in \mathbb{R}$ : se la serie

$$\sum_{n\in\mathbb{N}} \frac{a_n}{n^{s_0}}$$

converge assolutamente, per il criterio del confronto converge assolutamente anche la serie

$$\sum_{n\in\mathbb{N}} \frac{a_n}{n^s},$$

per ogni numero reale $s > s_0$. Chiamiamo **ascissa di convergenza assoluta** della serie (8.1) il numero reale

$$\overline{s_0} = \inf\left\{ s\in\mathbb{R} \;\middle|\; \sum_{n\in\mathbb{N}} \frac{|a_n|}{n^s} < +\infty \right\}.$$

Osserviamo che potremmo fare tutta la teoria usando come indeterminata completamente moltiplicativa

$$\begin{array}{rccc} \omega' : & \mathbb{N} & \to & \mathbb{C} \\ & n & \mapsto & n^s. \end{array}$$

In tal caso, l'ascissa di convergenza assoluta diventa un estremo superiore e le disuguaglianze si ribaltano. La scelta di prendere la (8.3) come indeterminata avviene per motivi storici, legati principalmente ai lavori di Riemann.

Oltre all'ascissa di convergenza assoluta, è possibile definire una ascissa di convergenza semplice. Dimostriamo prima il seguente lemma, noto come **lemma di sommazione parziale di Abel**:

**Lemma 8.1. (Abel)** *Siano $\{x_n\}_{n\in\mathbb{N}}$ e $\{a_n\}_{n\in\mathbb{N}}$ due successioni di numeri reali, con la prima delle due crescente, a valori non negativi e tale che*

$$\lim_{n\to+\infty} x_n = +\infty.$$

*Siano inoltre $f : (0,+\infty) \to \mathbb{C}$ una funzione, e*

$$\begin{array}{rccc} A : & [0,+\infty) & \to & \mathbb{R} \\ & x & \mapsto & \displaystyle\sum_{\substack{n\in\mathbb{N} \\ x_n\le x}} a_n. \end{array}$$

*Si ha*

$$\sum_{k=1}^{n} a_k f(x_k) = A(x_n)f(x_n) - \sum_{k=1}^{n-1} A(x_k)\left(f(x_{k+1}) - f(x_k)\right).$$

*Se inoltre $f \in \mathcal{C}^1(0,+\infty)$,*

$$\sum_{\substack{n\in\mathbb{N} \\ x_n\le x}} a_n f(x_n) = A(x)f(x) - \int_{x_1}^{x} A(u)f'(u)du,$$

*e in particolare,*

$$\sum_{\substack{n\in\mathbb{N} \\ n\le x}} a_n f(n) = A(x)f(x) - \int_{1}^{x} A(u)f'(u)du.$$

**Dimostrazione**

Se poniamo, per convenzione, $A(x_0) = 0$,

$$\begin{aligned} \sum_{k=1}^{n} a_k f(x_k) &= \sum_{k=1}^{n} \left(A(x_k) - A(x_{k-1})\right) f(x_k) \\ &= A(x_n)f(x_n) - \sum_{k=1}^{n-1} A(x_k)\left(f(x_{k+1}) - f(x_k)\right), \end{aligned}$$

e la prima formula è dimostrata. Proviamo la seconda formula: osserviamo che $A$ è costante in ogni intervallo $(x_k, x_{k+1})$. Sia $n$ il più grande intero positivo tale che $x_n \leq x$ : allora

$$\begin{aligned}\sum_{k=1}^{n} a_k f(x_k) &= A(x_n)f(x_n) - \sum_{k=1}^{n-1} A(x_k)\left(f(x_{k+1}) - f(x_k)\right) \\ &= A(x_n)f(x_n) - \sum_{k=1}^{n-1} A(x_k)\int_{x_k}^{x_{k+1}} f'(u)du \\ &= A(x)f(x) - \int_{x_n}^{x} A(u)f'(u)du - \sum_{k=1}^{n-1} A(x_k)\int_{x_k}^{x_{k+1}} f'(u)du \\ &= A(x)f(x) - \int_{x_1}^{x} A(u)f'(u)du.\end{aligned}$$

La terza formula segue immediatamente dalla seconda.

□

Possiamo definire, oltre a un'ascissa di convergenza assoluta, anche un'ascissa di convergenza:

**Proposizione 8.1.** *Sia $s \in \mathbb{R}$, e supponiamo che*

$$\left|\sum_{n\in\mathbb{N}} \frac{f(n)}{n^s}\right| < +\infty.$$

*Allora, per ogni $s' \geq s$.*

$$\left|\sum_{n\in\mathbb{N}} \frac{f(n)}{n^{s'}}\right| < +\infty.$$

**Dimostrazione**
Sia $s' > s$, e fissiamo $N \in \mathbb{N}$ :

$$\sum_{n\leq N} \frac{f(n)}{n^{s'}} = \sum_{n\leq N} \frac{f(n)}{n^s}\frac{1}{n^{s'-s}}.$$

Applichiamo il lemma di sommazione parziale di Abel, con la funzione

$$\begin{array}{rccc} f: & (0,+\infty) & \to & \mathbb{R} \\ & x & \mapsto & x^{s-s'}, \end{array}$$

e la successione $\{a_n\}_{n\in\mathbb{N}} = \left\{\frac{f(n)}{n^s}\right\}_{n\in\mathbb{N}}$ :

$$\sum_{n\leq N} \frac{f(n)}{n^s}\frac{1}{n^{s'-s}} = \sum_{n\leq N} \frac{f(n)}{n^s}N^{s-s'} + (s-s')\int_1^N \left(\sum_{n\leq x} \frac{f(n)}{n^s}\right) x^{s-s'-1}dx.$$

Poiché $s - s' < 0$,

$$\lim_{N\to+\infty} \sum_{n\leq N} N^{s-s'}\frac{f(n)}{n^s} = 0.$$

Inoltre,

$$\begin{aligned}\left|\sum_{n\in\mathbb{N}}\frac{f(n)}{n^{s'}}\right| &= (s-s')\int_1^N\left(\sum_{n\le x}\frac{f(n)}{n^s}\right)x^{s-s'-1}dx\\ &\le (s'-s)\int_1^{+\infty}\left|\sum_{n\le x}\frac{f(n)}{n^s}\right|x^{s-s'-1}dx\\ &\le (s'-s)\left|\sum_{n\in\mathbb{N}}\frac{f(n)}{n^s}\right|\int_1^{+\infty}x^{s-s'-1}dx\\ &= \left|\sum_{n\in\mathbb{N}}\frac{f(n)}{n^s}\right|<+\infty,\end{aligned}$$

e quindi la tesi.

□

Chiamiamo **ascissa di convergenza** della serie (8.1)

$$s_0=\inf\left\{s\in\mathbb{R}\mid\left|\sum_{n\in\mathbb{N}}\frac{a_n}{n^s}\right|<+\infty\right\}.$$

Per la proposizione 8.1, tale definizione è ben posta. Data una serie di Dirichlet, i valori della sua ascissa di convergenza e della sua ascissa di convergenza assoluta sono legati dalla seguente disuguaglianza:

**Proposizione 8.2.** *L'ascissa di convergenza assoluta e l'ascissa di convergenza di una serie di Dirichlet sono legate dalla seguente relazione:*

$$s_0\le\overline{s_0}\le s_0+1.$$

**Dimostrazione**

Se una serie converge assolutamente, allora converge anche semplicemente: pertanto, $s_0\le\overline{s_0}$.
Fissiamo $\epsilon>0$ :

$$\sum_{n\in\mathbb{N}}\frac{|f(n)|}{n^{s_0+1+2\epsilon}}=\sum_{n\in\mathbb{N}}\frac{|f(n)|}{n^{s_0+\epsilon}}\frac{1}{n^{1+\epsilon}}$$

Poiché

$$\left|\sum_{n\in\mathbb{N}}\frac{f(n)}{n^{s_0+\epsilon}}\right|<+\infty,$$

il termine generico della serie tende a 0 per $n\to+\infty$ :

$$\lim_{n\to+\infty}\frac{f(n)}{n^{s_0+\epsilon}}=0.$$

Di conseguenza, per ogni $\delta>0$ esiste $N\in\mathbb{N}$ tale che

$$\frac{|f(n)|}{n^{s_0+\epsilon}}<\delta,$$

e inoltre

$$\begin{aligned}\sum_{n\in\mathbb{N}}\frac{|f(n)|}{n^{s_0+\epsilon}}\frac{1}{n^{1+\epsilon}} &= \sum_{n=1}^{N}\frac{|f(n)|}{n^{s_0+\epsilon}}\frac{1}{n^{1+\epsilon}}+\sum_{n=N+1}^{+\infty}\frac{|f(n)|}{n^{s_0+\epsilon}}\frac{1}{n^{1+\epsilon}}\\ &< \sum_{n=1}^{N}\frac{|f(n)|}{n^{s_0+\epsilon}}\frac{1}{n^{1+\epsilon}}+\delta\sum_{n=N+1}^{+\infty}\frac{1}{n^{1+\epsilon}}<+\infty.\end{aligned}$$

Pertanto, $s_0 + 1 + 2\epsilon \geq \overline{s_0}$, e poiché questo vale per ogni $\epsilon > 0$, necessariamente $s_0 + 1 \geq \overline{s_0}$.

□

La serie (8.1) converge totalmente in $[s_1, +\infty)$, per ogni $s_1 > \overline{s_0}$. In particolare, la convergenza uniforme in $[s_1, +\infty)$, per ogni $s_1 > \overline{s_0}$, ed è possibile riordinare i termini della serie. Come per le serie formali, se $s > \overline{s_0}$, è possibile sommare e moltiplicare le serie di Dirichlet: siano

$$\sum_{n\in\mathbb{N}} \frac{f(n)}{n^s}, \qquad \sum_{n\in\mathbb{N}} \frac{g(n)}{n^s}$$

due serie di Dirichlet con ascissa di convergenza assoluta, rispettivamente, $\overline{s_0}^{(1)}$ e $\overline{s_0}^{(2)}$. Sia $\overline{s_0} = \sup\{\overline{s_0}^{(1)}, \overline{s_0}^{(2)}\}$ : per $s > \overline{s_0}$ definiamo la somma e il prodotto delle due serie di Dirichlet

$$\sum_{n\in\mathbb{N}} \frac{f(n)}{n^s} + \sum_{n\in\mathbb{N}} \frac{g(n)}{n^s} = \sum_{n\in\mathbb{N}} \frac{f(n) + g(n)}{n^s}$$

$$\sum_{n\in\mathbb{N}} \frac{f(n)}{n^s} \sum_{n\in\mathbb{N}} \frac{g(n)}{n^s} = \sum_{n\in\mathbb{N}} \frac{f \star g(n)}{n^s}$$

## 8.3. Funzioni generatrici

**Teorema 8.1.** *Supponiamo che la serie (8.1) converga assolutamente per $s > \overline{s_0}$. Allora anche la serie*

$$-\sum_{n\in\mathbb{N}} \frac{f(n)}{n^s} \log n$$

*converge assolutamente per $s > \overline{s_0}$.*

**Dimostrazione**

Fissiamo $s > \overline{s_0}$, e poniamo $\delta = s - \overline{s_0}$. Poiché esiste $c(\delta) > 0$ tale che

$$\log n < c(\delta) n^{\frac{\delta}{2}},$$

$$\sum_{n\in\mathbb{N}} \frac{f(n)}{n^s} \log n < \sum_{n\in\mathbb{N}} c(\delta) \frac{f(n)}{n^{s-\frac{\delta}{2}}} < +\infty.$$

□

Data la serie di Dirichlet

$$\sum_{n\in\mathbb{N}} \frac{f(n)}{n^s},$$

chiamiamo

$$\begin{aligned} F: \quad (\overline{s_0}, +\infty) &\to \mathbb{R} \\ s &\mapsto \sum_{n\in\mathbb{N}} \frac{f(n)}{n^s} \end{aligned}$$

la **funzione generatrice** della funzione aritmetica $f$. Per il teorema 8.1, e per il teorema di derivazione per serie, $F$ è derivabile, e

$$F'(s) = -\sum_{n\in\mathbb{N}} \frac{f(n)}{n^s} \log n,$$

per ogni $s > \overline{s_0}$, e iterando si trova che $F \in \mathcal{C}^\infty(\overline{s_0}, +\infty)$.

**Proposizione 8.3.** *Se $F$ è la funzione generatrice di $f$, per $s > s_0^{(1)}$, e se $G$ è la funzione generatrice di $g$, per $s > s_0^{(2)}$, allora $F + G$ e $FG$ sono le funzioni generatrici, rispettivamente, di $f + g$ e $f \star g$, per $s > \overline{s_0} = \max\left\{s_0^{(1)}, s_0^{(2)}\right\}$.*

Il risultato successivo garantisce l'unicità della rappresentazione:

**Teorema 8.2.** *Sia $f \in \mathbb{A}$ una funzione aritmetica e sia $F$ la serie di Dirichlet ad essa associata, con ascissa di convergenza assoluta $\overline{s_0}$. Se $F(s) = 0$ per ogni $s \geq s_1 > \overline{s_0}$, allora $f(n) = 0$ per ogni $n \in \mathbb{N}$. In particolare, se $f, g \in \mathbb{A}$ sono due funzioni aritmetiche aventi funzioni generatrici, rispettivamente, $F$, $G$ con ascissa di convergenza assoluta $\overline{s_0}^{(1)}$, $\overline{s_0}^{(2)}$, e se esiste $s_1 > \overline{s} = \max\left\{\overline{s_0}^{(1)}, \overline{s_0}^{(2)}\right\}$ tale che $F(s) = G(s)$ per ogni $s \geq s_1$, allora $f(n) = g(n)$ per ogni $n \in \mathbb{N}$.*

**Dimostrazione**

Usiamo le notazioni introdotte nell'equazione (8.2). Supponiamo per assurdo che esista almeno un intero $n \in \mathbb{N}$ tale che $f(n) \neq 0$ : per il principio del minimo, esiste

$$n_0 = \min\{n \in \mathbb{N} \mid f(n) \neq 0\}.$$

Prendiamo inoltre $s_2 > \overline{s_0}$, $s > s_2$ :

$$0 = \frac{a_{n_0}}{n_0^s} + \sum_{k=n_0+1}^{+\infty} \frac{a_k}{k^s} = \frac{a_{n_0}}{n_0^s}\left(1 + \sum_{k=n_0+1}^{+\infty} \frac{a_k}{a_{n_0}}\left(\frac{n_0}{k}\right)^s\right) = \frac{a_{n_0}}{n_0^s}(1 + H(s)), \tag{8.4}$$

con

$$H(s) = \sum_{k=n_0+1}^{+\infty} \frac{a_k}{a_{n_0}}\left(\frac{n_0}{k}\right)^s = \sum_{k=1}^{+\infty} \frac{a_{k+n_0}}{a_{n_0}}\left(\frac{n_0}{k+n_0}\right)^s.$$

Studiamo $H(s)$ :

$$\begin{aligned} |H(s)| &\leq \sum_{k=1}^{+\infty} \frac{|a_{k+n_0}|}{|a_{n_0}|}\left(\frac{n_0}{k+n_0}\right)^{s-s_2}\left(\frac{n_0}{k+n_0}\right)^{s_2} \\ &\leq \left(\frac{n_0}{n_0+1}\right)^{s-s_2} \frac{n_0^{s_2}}{|a_{n_0}|} \sum_{k=1}^{+\infty} \frac{|a_{n_0+k}|}{(n_0+k)^{s_2}}. \end{aligned}$$

Osserviamo che

$$\lim_{s\to+\infty} \left(\frac{n_0}{n_0+1}\right)^{s-s_2} \frac{n_0^{s_2}}{|a_{n_0}|} \sum_{k=1}^{+\infty} \frac{|a_{n_0+k}|}{(n_0+k)^{s_2}} = 0,$$

e si può scegliere $s > s_2$ in modo tale che $|H(s)| < \frac{1}{2}$, e $|1 + H(s)| \geq \frac{1}{2}$. Allora, per l'equazione (8.4), si dovrebbe avere $a_{n_0} = 0$, assurdo.

□

Elenchiamo le funzioni generatrici di alcune delle funzioni aritmetiche definite finora: ad esempio la funzione generatrice della funzione aritmetica **1** è la **funzione zeta di Riemann** (sui reali)

$$\begin{aligned} \zeta : \quad (1, +\infty) &\to \mathbb{R} \\ s &\mapsto \sum_{n\in\mathbb{N}} \frac{1}{n^s}, \end{aligned}$$

la cui ascissa di convergenza assoluta è $\overline{s_0} = 1$. In tabella elenchiamo le funzioni generatrici di alcune delle altre funzioni aritmetiche:

| Funzione aritmetica | Serie di Dirichlet | Ascissa di convergenza assoluta |
|---|---|---|
| $e$ | **1**(s) | |
| $\mathbf{1}$ | $\zeta(s)$ | $\overline{s_0} = 1$ |
| $d_r = \star_{i=1}^{r} \mathbf{1}$ | $\zeta^r(s)$ | $\overline{s_0} = 1$ |
| $\mu$ | $\frac{1}{\zeta(s)}$ | $\overline{s_0} = 1$ |
| $L$ | $-\zeta'(s)$ | $\overline{s_0} = 1$ |
| $i$ | $\zeta(s-1)$ | $\overline{s_0} = 2$ |
| $i^\alpha$ | $\zeta(s-\alpha)$ | $\overline{s_0} = 1+\alpha$ |
| $\sigma = i \star \mathbf{1}$ | $\zeta(s-1)\zeta(s)$ | $\overline{s_0} = 2$ |
| $\sigma_\alpha = i^\alpha \star \mathbf{1}$ | $\zeta(s-\alpha)\zeta(s)$ | $\overline{s_0} = 1+\alpha$ |
| $\phi(n) = i \star \mu$ | $\frac{\zeta(s-1)}{\zeta(s)}$ | $\overline{s_0} = 2$ |

## 8.4. Applicazioni

**Esercizio 8.1.** *Per ogni* $n \in \mathbb{N}$, $\phi \star \sigma(n) = nd(n)$

**Risoluzione** La serie di Dirichlet associata a $\phi \star \sigma$ è

$$\frac{\zeta(s-1)}{\zeta(s)}\zeta(s)\zeta(s-1) = \zeta(s-1)^2 = \sum_{n\in\mathbb{N}} \frac{d(n)}{n^{s-1}} = \sum_{n\in\mathbb{N}} \frac{nd(n)}{n^s}.$$

Per il teorema 8.2, la tesi.

Denotiamo con **q** la **funzione indicatrice dei quadrati**:

$$\begin{aligned} \mathbf{q}: \quad \mathbb{N} &\to \{0,1\} \\ n &\mapsto \begin{cases} 1 & \text{se } n \text{ è un quadrato} \\ 0 & \text{se } n \text{ non è un quadrato} \end{cases}. \end{aligned}$$

**Esercizio 8.2.** $\lambda \star \mathbf{1} = \mathbf{q}$. *In particolare, la funzione generatrice di* **q** *è* $\zeta(2s)$, *con ascissa di convergenza assoluta* $\overline{s_0} = \frac{1}{2}$.

**Risoluzione** Poiché $\lambda$ e **1** sono funzioni aritmetiche completamente moltiplicative, per il lemma 7.2 la loro convoluzione è sicuramente moltiplicativa. Valutiamola sulle potenze dei primi:

$$\lambda \star \mathbf{1}(p^a) = \sum_{d|p^a} \lambda(d) = \sum_{h=0}^{a} \lambda(p^h) = \sum_{h=0}^{a} (-1)^h = \begin{cases} 1 & \text{se } a \text{ è pari} \\ 0 & \text{se } a \text{ è dispari} \end{cases} = \mathbf{q}(p^a).$$

Quindi, $\lambda \star \mathbf{1} = \mathbf{q}$, e

$$\sum_{n\in\mathbb{N}} \frac{\mathbf{q}(n)}{n^s} = \sum_{n\in\mathbb{N}} \frac{\lambda \star \mathbf{1}(n)}{n^s} = \sum_{n\in\mathbb{N}} \frac{1}{n^{2s}} = \zeta(2s).$$

**Esercizio 8.3.** *La funzione generatrice di* $\lambda$ *è* $\frac{\zeta(2s)}{\zeta(s)}$, *con ascissa di convergenza assoluta* $\overline{s_0} = 1$. *Inoltre,* $\mu^2$ *ha come funzione generatrice* $\frac{\zeta(s)}{\zeta(2s)}$, *anch'essa con ascissa di convergenza assoluta* $\overline{s_0} = 1$.

**Risoluzione** Per la prima formula di inversione di Möbius, $\lambda = \mathbf{q} \star \mu$, quindi, passando alle serie di Dirichlet,

$$\sum_{n\in\mathbb{N}} \frac{\lambda(n)}{n^s} = \frac{\zeta(2s)}{\zeta(s)},$$

Essendo $\lambda$ una funzione aritmetica completamente moltiplicativa, per il corollario 7.4 la sua inversa convolutiva è $\lambda^{-1} = \lambda\mu = \mu^2$ : pertanto

$$\sum_{n\in\mathbb{N}} \frac{\mu^2(n)}{n^s} = \frac{\zeta(s)}{\zeta(2s)}.$$

**Esercizio 8.4.** *Risolvere l'equazione* $\frac{\phi(n)}{n} = \frac{1}{2}$.

**Risoluzione** Per la proposizione 7.16

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

Se $n$ è pari,

$$\prod_{p|n}\left(1 - \frac{1}{p}\right) = \frac{1}{2}\prod_{\substack{p|n\\ p\neq 2}}\left(1 - \frac{1}{p}\right),$$

dunque, affinché l'equazione sia soddisfatta, $n$ non può essere diviso da un primo diverso da 2. D'altra parte, le potenze di 2 verificano l'equazione:

$$\phi(2^n) = 2^n - 2^{n-1} = 2^{n-1} = \frac{2^n}{2}.$$

Infine, se $n$ è dispari, $\frac{n}{2}$ non è un intero, quindi in questo caso l'equazione non può essere verificata: tutte e sole le soluzioni dell'equazione sono le potenze di 2.

**Esercizio 8.5.** *Risolvere l'equazione* $\phi(n) = 12$.

**Risoluzione** Posto,

$$n = 2^{a_2}\prod_{\substack{p|n\\ p>2}} p^{a_p},$$

si deve avere

$$\phi(n) = 2^{a_2-1}\prod_{\substack{p|n\\ p>2}} p^{a_p-1}(p-1) = 12.$$

Necessariamente, $a_2 - 1 \leq 2$, cioè $a_2 \leq 3$. Inoltre, poiché $p - 1$ deve dividere 12, $p \in \{3, 5, 7, 13\}$. Di conseguenza, possiamo scrivere $n = 2^{a_2}3^{a_3}5^{a_5}7^{a_7}13^{a_{13}}$. Procediamo cercando di togliere di volta in volta almeno un primo dalla fattorizzazione:

- $a_{13} > 0$ : in tal caso, $a_{13} = 1$. Poiché $\phi(13) = 12$, in questo caso, le uniche soluzioni sono $n = 13$ e $n = 2 \cdot 13 = 26$;
- $a_7 > 0$ : in tal caso, $a_7 = 1$. Poiché $\phi(7) = 6$, le uniche possibilità per i restanti esponenti sono $a_3 = 1, a_2 = a_5 = 0$ $a_2 = a_3 = 1, a_5 = 0$ e $a_2 = 2, a_3 = a_5 = 0$. In questo caso, abbiamo le soluzioni $n = 21, n = 42, n = 28$;
- $a_5 > 0$ : in tal caso, $a_5 = 1$. Poiché $\phi(5) = 4$, si dovrebbe avere $\phi(\frac{n}{5^{a_5}}) = 3$, e questo è impossibile dato che $\phi(n)$ è pari per ogni numero naturale $n$ maggiore di 2;

- $a_3 > 0$ : in tal caso, $a_3 = 1$, oppure $a_3 = 2$. Se $a_3 = 2$, si dovrebbe avere $\phi(2^{a_2}) = 6$, e questo è impossibile, poiché 6 non è una potenza di 2. Quindi, se ci sono soluzioni, $a_3 = 2$. Poiché $\phi(9) = 6$, si deve avere $\phi(2^{a_2}) = 2$, da cui si vede l'unica possibilità è che $a_2 = 2$. Quindi l'unica soluzione in questo caso è $n = 36$.

Ricapitolando, le soluzioni sono $n = 13, 26, 21, 42, 28, 36$.

**Esercizio 8.6.** *Per ogni $n \in \mathbb{N}$,*

$$\prod_{k|n} k = n^{\frac{d(n)}{2}}$$

**Risoluzione** Basta osservare che

$$\prod_{k|n} k = \sqrt{\prod_{k|n} k \prod_{k|n} \frac{n}{k}} = \sqrt{\prod_{k|n} n} = n^{\frac{d(n)}{2}}.$$

**Esercizio 8.7.** *La funzione aritmetica*

$$\begin{array}{rccl} f: & \mathbb{N} & \to & \mathbb{C} \\ & n & \mapsto & \lfloor\sqrt{n}\rfloor - \lfloor\sqrt{n-1}\rfloor \end{array}$$

*coincide con la funzione aritmetica* **q**.

**Risoluzione** Basta osservare che $\lfloor\sqrt{n}\rfloor - \lfloor\sqrt{n-1}\rfloor \neq 0$ se e solo se è un quadrato, e in tal caso $\lfloor\sqrt{n}\rfloor - \lfloor\sqrt{n-1}\rfloor = 1$.

Modifichiamo l'esercizio precedente:

**Esercizio 8.8.** *La funzione aritmetica*

$$\begin{array}{rccl} f: & \mathbb{N} & \to & \mathbb{C} \\ & n & \mapsto & \begin{cases} \mu(\sqrt{n}) & \textit{se } n \textit{ è un quadrato} \\ 0 & \textit{altrimenti} \end{cases} \end{array}$$

*è moltiplicativa, ed è l'inversa convolutiva della funzione aritmetica* **q**.

**Risoluzione** La funzione aritmetica $f$ è moltiplicativa: infatti, poiché $\mu$ è moltiplicativa, se $m, n$ sono coprimi, $mn$ è un quadrato se e solo se lo sono sia $m$ sia $n$. Consideriamo la funzione aritmetica

$$\begin{array}{rccl} f\star\mathbf{1}: & \mathbb{N} & \to & \mathbb{N} \\ & n & \mapsto & \displaystyle\sum_{d|n} f(d) = \sum_{d^2|n} \mu(d). \end{array}$$

Per il lemma 7.2, $f \star \mathbf{1}$ è moltiplicativa. Valutiamola sulle potenze dei primi: per ogni primo $p$ e per ogni $a \in \mathbb{N}$,

$$f\star\mathbf{1}(p^a) = \sum_{d^2|p^a} \mu(d) = \begin{cases} 1 & \text{se } a = 1 \\ 0 & \text{altrimenti} \end{cases}.$$

Ma allora $f \star \mathbf{1}$ è la funzione caratteristica degli interi positivi liberi da quadrati, cioè $f \star \mathbf{1} = \mu^2$. Per la prima formula di inversione di Möbius, $f = \mu^2 \star \mu$, e passando alle serie di Dirichlet

$$\sum_{n\in\mathbb{N}} \frac{f(n)}{n^s} = \frac{\zeta(s)}{\zeta(2s)}\frac{1}{\zeta(s)} = \frac{1}{\zeta(2s)}.$$

Dunque, $f^{-1} = \mathbf{q}$.

# CAPITOLO 9

## Prodotti infiniti

**Introduzione**

In questo capitolo, definiamo i prodotti infiniti e ne studieremo le principali proprietà. Infine enunceremo e dimostreremo l'identità di Eulero, e inizieremo a vedere alcune sue conseguenze.

## 9.1. Definizioni e risultati preliminari

Sia $\{a_n\}_{n\in\mathbb{N}} \subset \mathbb{C}$ una successione di numeri complessi: chiamiamo **prodotto (numerico) infinito** associato alla successione

$$\prod_{n=1}^{+\infty}(1+a_n) = \lim_{N\to+\infty}\prod_{n=1}^{N}(1+a_n). \tag{9.1}$$

Nel seguito, supporremo che $\{a_n\}_{n\in\mathbb{N}}$ sia una successione di numeri reali. Diremo che il prodotto infinito (9.1) **converge** se

$$\lim_{N\to+\infty}\prod_{n=1}^{N}(1+a_n) \in \mathbb{R}-\{0\},$$

**diverge** se

$$\lim_{N\to+\infty}\prod_{n=1}^{N}(1+a_n) \in \{0,\pm\infty\},$$

**non esiste** altrimenti. Diremo inoltre che il prodotto infinito (9.1) **converge assolutamente** se

$$0 < \lim_{N\to+\infty}\prod_{n=1}^{N}(1+|a_n|) < +\infty.$$

Valgono alcuni risultati analoghi a quelli per le serie numeriche:

**Proposizione 9.1.** *Se il prodotto infinito* (9.1) *converge, allora* $\lim_{n\to+\infty} a_n = 0$.

**Dimostrazione**

Sia $l \in \mathbb{R}-\{0\}$ tale che

$$\prod_{n=1}^{+\infty}(1+a_n) = l.$$

Allora

$$\lim_{n\to+\infty}(a_n+1) = \lim_{n\to+\infty}\frac{\prod_{k=1}^{n}(1+a_k)}{\prod_{k=1}^{n}(1+a_k)} = \frac{l}{l} = 1,$$

e quindi la tesi.

□

Come per le serie numeriche, la condizione espressa nella proposizione precedente è solo necessaria: ad esempio, presa la successione $\{\frac{1}{n}\}_{n\in\mathbb{N},n\geq 2}$,

$$\lim_{n\to+\infty}\left(1+\frac{1}{n}\right)=0,$$

$$\prod_{n=2}^{+\infty}\left(1+\frac{1}{n}\right)=\lim_{N\to+\infty}\prod_{n=2}^{N}\left(1+\frac{1}{n}\right)=\lim_{N\to+\infty}\frac{N}{2}=+\infty.$$

Il legame fra le serie e i prodotti infiniti è ben più stretto:

**Proposizione 9.2.** *Data una successione $\{a_n\}_{n\in\mathbb{N}}$ a termini non negativi, il prodotto infinito (9.1) converge se e solo se converge anche la serie associata alla successione $\{a_n\}_{n\in\mathbb{N}}$.*

**Dimostrazione**
Osserviamo che

$$\log\prod_{j=1}^{N}(1+a_n)=\sum_{j=1}^{N}\log(1+a_n).$$

Poiché $\log(1+a_n)\sim_{+\infty}a_n$, subito la tesi.

□

## 9.2. L'identità di Eulero

**Teorema 9.1. (Eulero)** *Sia $f\in\mathbb{M}$, e sia $\overline{s_0}$ l'ascissa di convergenza assoluta della serie di Dirichlet ad essa associata. Per $s>\overline{s_0}$,*

$$\sum_{n\in\mathbb{N}}\frac{f(n)}{n^s}=\prod_{p\in\mathbb{P}}\sum_{h=0}^{+\infty}\frac{f(p^h)}{p^{hs}},$$

*e se $f$ è anche completamente moltiplicativa*

$$\sum_{n\in\mathbb{N}}\frac{f(n)}{n^s}=\prod_{p\in\mathbb{P}}\left(1-\frac{f(p)}{p^s}\right)^{-1}.$$

*In particolare,*

$$\zeta(s)=\prod_{p\in\mathbb{P}}\left(1-\frac{1}{p^s}\right)^{-1}.$$

**Dimostrazione**
Fissiamo $N\in\mathbb{N}$ e consideriamo il troncamento

$$\prod_{p\leq N}\sum_{h=0}^{+\infty}\frac{f(p^h)}{p^{sh}}. \tag{9.2}$$

Usando la moltiplicatività di $f$, osserviamo che si può scrivere (9.2) come

$$\prod_{p\leq N}\sum_{h=0}^{+\infty}\frac{f(p^h)}{p^{sh}}=\sum_{\substack{n\in\mathbb{N}\\ p|n\Rightarrow p\leq N}}\frac{f(n)}{n^s}.$$

Tutti i numeri naturali minori o uguali a $N$ si fattorizzano con primi minori o uguali a $N$ : quindi possiamo spezzare la sommatoria nel modo seguente

$$\sum_{\substack{n\in\mathbb{N}\\ p|n\Rightarrow p\leq N}} \frac{f(n)}{n^s} = \sum_{n=1}^{N} \frac{f(n)}{n^s} + \sum_{\substack{n>N\\ p|n\Rightarrow p\leq N}} \frac{f(n)}{n^s}.$$

Poiché

$$\left| \prod_{p\leq N} \sum_{h=0}^{+\infty} \frac{f(p^h)}{p^{sh}} - \sum_{n=1}^{N} \frac{f(n)}{n^s} \right| \leq \sum_{\substack{n>N\\ p|n\Rightarrow p\leq N}} \frac{|f(n)|}{n^s} \leq \sum_{n>N} \frac{|f(n)|}{n^s},$$

e poiché quest'ultima è la coda di una serie convergente,

$$\lim_{N\to+\infty} \left| \prod_{p\leq N} \sum_{h=0}^{+\infty} \frac{f(p^h)}{p^{sh}} - \sum_{n=1}^{N} \frac{f(n)}{n^s} \right| = 0 \Rightarrow \prod_{p\in\mathbb{P}} \sum_{h=0}^{+\infty} \frac{f(p^h)}{p^{sh}} = \sum_{n\in\mathbb{N}} \frac{f(n)}{n^s}.$$

Se la funzione $f$ è anche completamente moltiplicativa,

$$\sum_{h=0}^{+\infty} \frac{f(p^h)}{p^{hs}} = \sum_{h=0}^{+\infty} \frac{f(p)^h}{p^{hs}} = \sum_{h=0}^{+\infty} \left(\frac{f(p)}{p^s}\right)^h.$$

Osserviamo che, per quanto provato in precedenza,

$$\frac{|f(p)|}{p^s} < 1,$$

quindi

$$\sum_{h=0}^{+\infty} \left(\frac{f(p)}{p^s}\right)^h = \frac{1}{1-\frac{f(p)}{p^s}} = \left(1-\frac{f(p)}{p^s}\right)^{-1},$$

da cui la seconda formula. L'ultima segue immediatamente dalla seconda prendendo come funzione aritmetica completamente moltiplicativa **1**.

□

L'identità di Eulero ha diverse conseguenze: ad esempio

**Corollario 9.1.** *Si ha*

$$\sum_{p\in\mathbb{P}} \frac{1}{p} = +\infty.$$

**Dimostrazione**

Supponiamo per assurdo che la serie converga. Allora, per la proposizione 9.2 convergerebbe anche il prodotto infinito

$$\prod_{p\in\mathbb{P}} \left(1-\frac{1}{p}\right)$$

e quindi anche

$$\prod_{p\in\mathbb{P}} \left(1-\frac{1}{p}\right)^{-1}.$$

Ma allora, per l'identità di Eulero, convergerebbe anche la serie

$$\sum_{n\in\mathbb{N}} \frac{1}{n},$$

assurdo.

□

Tramite l'identità di Eulero possiamo dimostrare in un altro modo alcuni risultati già dimostrati in precedenza:

**Esercizio 9.1.** *La funzione generatrice di $\lambda$ è $\frac{\zeta(2s)}{\zeta(s)}$, con ascissa di convergenza assoluta $\overline{s_0} = 1$.*
**Risoluzione** $\lambda$ è una funzione aritmetica completamente moltiplicativa: usando l'identità di Eulero, per $s > \overline{s_0}$,

$$\sum_{n\in\mathbb{N}} \frac{\lambda(n)}{n^s} = \prod_{p\in\mathbb{P}} \left(1 - \frac{\lambda(p)}{p^s}\right)^{-1} = \prod_{p\in\mathbb{P}} \left(1 + \frac{1}{p^s}\right)^{-1}.$$

Poiché, per ogni $x \in \mathbb{R}$, $x \neq \pm 1$,

$$(1+x)^{-1} = \frac{1-x}{1-x^2},$$

$$\prod_{p\in\mathbb{P}} \left(1 + \frac{1}{p^s}\right)^{-1} = \frac{\prod_{p\in\mathbb{P}} \left(1 - \frac{1}{p^s}\right)}{\prod_{p\in\mathbb{P}} \left(1 - \frac{1}{p^{2s}}\right)} = \frac{\zeta(2s)}{\zeta(s)}.$$

La tecnica usata nella dimostrazione precedente può essere riadattata in altre situazioni: definiamo, per ogni $k \in \mathbb{N}$, la funzione caratteristica degli interi positivi che non sono divisibili per una potenza $k-$esima:

$$\begin{array}{rccl} q_k: & \mathbb{N} & \to & \mathbb{C} \\ & n & \mapsto & \begin{cases} 1 & \text{se non esiste } p \in \mathbb{P} \text{ tale che } p^k \mid n \\ 0 & \text{altrimenti} \end{cases} \end{array}.$$

**Teorema 9.2.** *Per ogni $s \in \mathbb{R}$, $s > 1$, e per ogni $k \in \mathbb{N}$,*

$$\frac{\zeta(s)}{\zeta(ks)} = \sum_{n\in\mathbb{N}} \frac{q_k(n)}{n^s}.$$

Studiamo un'altra funzione aritmetica:

**Proposizione 9.3.** *La funzione aritmetica*

$$\begin{array}{rccl} f: & \mathbb{N} & \to & \mathbb{C} \\ & n & \mapsto & 2^{\omega(n)} \end{array}$$

*è moltiplicativa. Inoltre, per $s > 1$,*

$$\sum_{n\in\mathbb{N}} \frac{2^{\omega(n)}}{n^s} = \frac{\zeta^2(s)}{\zeta(2s)}.$$

**Dimostrazione**
La funzione $f$ è sicuramente moltiplicativa, dato che $\omega$ è additiva. Valutiamola sulle potenze dei primi: per ogni $p \in \mathbb{P}$, e per ogni $h \in \mathbb{N}$,

$$f(p^h) = 2^{\omega(p^h)} = \begin{cases} 2 & h \geq 1 \\ 1 & h = 0 \end{cases}.$$

Per ogni $n \in \mathbb{N}$, $2^{\omega(n)} \leq d(n)$ : infatti

$$2^{\omega(n)} \leq \prod_{p\mid n} (a_p + 1)$$

dato che i fattori che compaiono nel secondo membro sono $\omega(n)$ e sono tutti maggiori o uguali a 2. Determiniamo la sua funzione generatrice: per $s > 1$ (proprio in virtù della disuguaglianza appena provata, l'ascissa di convergenza assoluta della serie di Dirichlet associata a $\omega$ è minore o uguale a 1), usando l'identità di Eulero,

$$F(s) = \prod_{p\in\mathbb{P}} \sum_{k=0}^{+\infty} \frac{2^{\omega(p^k)}}{p^{ks}} = \prod_{p\in\mathbb{P}} \left(1 + \sum_{k=1}^{+\infty} \frac{2}{p^{ks}}\right).$$

Moltiplicando per $\zeta(2s)$, otteniamo

$$F(s)\zeta(2s) = \prod_{p\in\mathbb{P}} \left(1 + \sum_{k=1}^{+\infty} \frac{2}{p^{ks}}\right) \prod_{p\in\mathbb{P}} \sum_{h=0}^{+\infty} \frac{1}{p^{2hs}}.$$

Per un semplice ragionamento combinatorio,

$$\prod_{p\in\mathbb{P}} \left(1 + \sum_{k=1}^{+\infty} \frac{2}{p^{ks}}\right) \prod_{p\in\mathbb{P}} \sum_{h=0}^{+\infty} \frac{1}{p^{2hs}} = \prod_{p\in\mathbb{P}} \sum_{k=0}^{+\infty} \frac{k+1}{p^{ks}}.$$

Come è ben noto, se $|q| < 1$, vale

$$\sum_{k=0}^{+\infty} kq^k = \frac{q}{(q-1)^2}.$$

Dunque,

$$\prod_{p\in\mathbb{P}} \sum_{k=0}^{+\infty} \frac{k+1}{p^{ks}} = \prod_{p\in\mathbb{P}} \left(\frac{p^s}{(p^s-1)^2} + \frac{p^s}{p^s-1}\right) = \prod_{p\in\mathbb{P}} \left(\frac{1}{1-\frac{1}{p^s}}\right)^2 = \zeta^2(s).$$

In conclusione, per $s > 1$,

$$\sum_{n\in\mathbb{N}} \frac{2^{\omega(n)}}{n^s} = \frac{\zeta^2(s)}{\zeta(2s)}.$$

□

Vale anche il seguente

**Teorema 9.3. (Ramanujan)** *Per ogni $s \in \mathbb{R}$, $s > 1$,*

$$\frac{\zeta^4(s)}{\zeta(2s)} = \sum_{n\in\mathbb{N}} \frac{d(n)^2}{n^s},$$

e quest'ultimo è conseguenza di un risultato ancora più generale:

**Teorema 9.4.** *Se $s, s-a, s-b, s-a-b$ sono tutti numeri reali maggiori di 1, allora*

$$\frac{\zeta(s)\zeta(s-a)\zeta(s-b)\zeta(s-a-b)}{\zeta(2s-a-b)} = \sum_{k=1}^{+\infty} \frac{\sigma_a(k)\sigma_b(k)}{n^s}.$$

# CAPITOLO 10

## La costante $\gamma$ di Eulero

**Introduzione**

In questo capitolo, studieremo più nel dettaglio il comportamento della serie armonica e vedremo che la costante $\gamma$ di Eulero, che sarà il risultato di questo studio, ha dei legami con la funzione $\zeta$ di Riemann. A proposito di quest'ultima, calcoleremo il valore $\zeta(2)$.

**Teorema 10.1.** *Esiste un numero reale* $\gamma$*, detto* **costante di Eulero***, tale che* $0 < \gamma < 1$,

$$\sum_{n\leq x} \frac{1}{n} = \log x + \gamma + \mathcal{O}\left(\frac{1}{x}, +\infty\right).$$

**Dimostrazione**

Applichiamo il lemma di sommazione parziale di Abel, con la successione $\{a_n\}_{n\in\mathbb{N}} = \{1\}_{n\in\mathbb{N}}$, e la funzione

$$\begin{aligned} f: \quad (0,+\infty) &\to \mathbb{R} \\ x &\mapsto \frac{1}{x} \end{aligned}$$

Otteniamo

$$\begin{aligned} \sum_{n\leq x} \frac{1}{n} &= \frac{1}{x}\sum_{n\leq x} 1 - \int_1^x \left(-\frac{1}{u^2}\right)\sum_{n\leq u} 1du \\ &= \frac{\lfloor x\rfloor}{x} + \int_1^x \frac{\lfloor u\rfloor}{u^2}du = 1 - \frac{\{x\}}{x} + \int_1^x \frac{1}{u}du - \int_1^x \frac{\{u\}}{u^2}du \\ &\overset{[1]}{=} 1 - \frac{\{x\}}{x} + \int_1^x \frac{1}{u}du - \int_1^x \frac{\{u\}}{u^2}du = 1 + \log x - \int_1^{+\infty} \frac{\{u\}}{u^2}du + \mathcal{O}\left(\frac{1}{x}, +\infty\right). \end{aligned}$$

In più,

$$0 < \int_1^{+\infty} \frac{\{u\}}{u^2}du < \int_1^{+\infty} \frac{1}{u^2}du = 1.$$

Quindi,

$$0 < 1 - \int_1^{+\infty} \frac{\{u\}}{u^2}du < 1.$$

Il numero

$$\gamma = 1 - \int_1^{+\infty} \frac{\{u\}}{u^2}du$$

è il numero cercato.

□

[1] Infatti,

$$\frac{\{x\}}{x}, \int_x^{+\infty} \frac{\{u\}}{u^2}du \in \mathcal{O}\left(\frac{1}{x}, +\infty\right)$$

Come è lecito aspettarsi, la costante $\gamma$ è legata al comportamento della funzione zeta per $s \to 1^+$. Infatti:

**Corollario 10.1.**

$$\zeta(s) = \frac{1}{s-1} + \gamma + \mathcal{O}\left(s-1, 1^+\right)$$

**Dimostrazione**

Applichiamo il lemma di sommazione parziale di Abel, con la successione $\{a_n\}_{n\in\mathbb{N}} = \{1\}_{n\in\mathbb{N}}$, e la funzione

$$\begin{aligned} f: \quad (0,+\infty) &\to \mathbb{R} \\ x &\mapsto \frac{1}{x^s} \end{aligned}$$

Otteniamo

$$\begin{aligned} \sum_{n\le x} \frac{1}{n^s} &= \frac{\lfloor x \rfloor}{x^s} - \int_1^x \frac{\lfloor u \rfloor}{u^{s+1}}(-s)du = x^{1-s} - \frac{\{x\}}{x^s} + s\int_1^x \frac{du}{u^s} - s\int_1^x \frac{\{u\}}{u^{s+1}}du \\ &= x^{1-s} - \frac{\{x\}}{x^s} + \frac{s}{s-1} - \frac{s}{s-1}x^{1-s} - s\int_1^x \frac{\{u\}}{u^{s+1}}du \\ &= -\frac{x^{1-s}}{s-1} + \frac{s}{s-1} - s\int_1^x \frac{\{u\}}{u^{s+1}}du - \frac{\{x\}}{x^s}. \end{aligned}$$

Poiché

$$\begin{aligned} \lim_{x\to+\infty} \frac{x^{1-s}}{s-1} &= \lim_{x\to+\infty} \frac{\{x\}}{x^s} = 0, \\ \zeta(s) &= \frac{s}{s-1} - s\int_1^{+\infty} \frac{\{u\}}{u^{s+1}}du, \qquad (10.1) \\ \lim_{s\to1^+}\left(\zeta(s) - \frac{1}{s-1}\right) &= 1 - \int_1^{+\infty} \frac{\{u\}}{u^{s+1}}du = \gamma \end{aligned}$$

e di conseguenza

$$\zeta(s) = \frac{1}{s-1} + \gamma + \mathcal{O}\left(s-1, 1^+\right).$$

□

Per l'equazione (10.1) possiamo prolungare la funzione $\zeta$ di Riemann su tutto $(0,+\infty)$, escluso il punto $s = 1$.

Della costante $\gamma$ non si sa molto: ad esempio, non si sa se è irrazionale, e nemmeno se è trascendente.

## 10.1. Calcolo della funzione $\zeta$ sui numeri naturali pari

**Teorema 10.2.** *$\zeta(3)$ è irrazionale.*

**Teorema 10.3.** *Almeno uno fra $\zeta(5), \zeta(7), \zeta(9), \zeta(11)$ è irrazionale.*

Non è nota una formula generale per la valutazione della funzione $\zeta$ sugli interi positivi dispari, mentre se ne ha una per la valutazione sugli interi positivi pari. Chiamiamo successione dei **numeri di Bernoulli** la successione $\{B_n\}_{n\in\mathbb{N}}$ così definita: poniamo $B_0 = 1$ e, per ogni $m \in \mathbb{N}$,

$$B_m = -\frac{1}{m+1}\sum_{j=0}^{m-1}\binom{m+1}{j}B_j.$$

Inoltre, per ogni $n \in \mathbb{N}$ chiamiamo $n-$esimo **polinomio di Bernoulli** il polinomio

$$\begin{aligned} B_n : \quad \mathbb{R} &\to \mathbb{R} \\ x &\mapsto \sum_{k=0}^{n} \binom{n}{k} B_{n-k} x^k. \end{aligned}$$

Mediante i polinomi di Bernoulli si può calcolare la funzione $\zeta$ di Riemann sugli interi positivi pari. Vediamo un esempio:

**Teorema 10.4.**

$$\zeta(2) = \frac{\pi^2}{6}.$$

**Dimostrazione**

[2] Consideriamo la restrizione del primo polinomio di Bernoulli sull'intervallo $(0,1)$

$$\begin{aligned} \widetilde{B}_1 = B_{1|_{[0,1)}} : \quad (0,1) &\to \mathbb{R} \\ x &\mapsto x - \frac{1}{2}, \end{aligned}$$

e prolunghiamola periodicamente su tutto $\mathbb{R}$. Osserviamo che $\widetilde{B}_1 \in \mathcal{L}^2(0,1)$, quindi vale lo sviluppo in serie di Fourier

$$B_1(x) = \sum_{n \in \mathbb{Z}} a_n e^{2\pi i n x}, \qquad \text{con } a_n = \int_0^1 f(x) e^{-2\pi i n x} dx, \ \forall n \in \mathbb{Z}.$$

Calcoliamo la norma $\mathcal{L}^2(0,1)$ di $\widetilde{B}_1$ :

$$\left\| \widetilde{B}_1 \right\|^2_{\mathcal{L}^2(0,1)} = \int_0^1 B_1(x)^2 dx = \frac{1}{12}.$$

É inoltre immediato il calcolo esplicito dei coefficienti di Fourier: $a_0 = 0$ e, per ogni $n \in \mathbb{Z} - \{0\}$,

$$a_n = \int_0^1 \left( x - \frac{1}{2} \right) e^{-2\pi i n x} dx = -\frac{1}{2\pi n}.$$

Per l'identità di Parseval,

$$2 \frac{1}{4\pi^2} \zeta(2) = \frac{1}{12},$$

e quindi

$$\zeta(2) = \frac{\pi^2}{6}.$$

□

Con la stessa tecnica, usando il $k-$esimo polinomio di Bernoulli si può calcolare $\zeta(2k)$, per ogni $k \in \mathbb{N}$. Osserviamo esplicitamente che in questo modo non é possibile calcolare la funzione $\zeta$ sugli interi positivi dispari, in quanto nell'uguaglianza di Parseval ci sono gli elevamenti al quadrato, e quindi gli esponenti saranno sempre pari. La formula generale è la seguente:

**Teorema 10.5.** *Per ogni $k \in \mathbb{N}$,*

$$\zeta(2k) = \sum_{n \in \mathbb{N}} \frac{1}{n^{2k}} = \frac{(-1)^{k-1} (2\pi)^{2k} B_{2k}}{2(2k)!}.$$

[2] La dimostrazione di questo teorema qui presentata richiede conoscenze acquisite nel corso di Analisi 3. Una dimostrazione alternativa può essere trovata a questo link: talus.maths.usyd.edu.au/u/daners/publ/abstracts/zeta2/zeta2.pdf.

# CAPITOLO 11

## Ordine di grandezza delle funzioni aritmetiche

**Introduzione**

In questo capitolo, studieremo l'ordine di grandezza delle principali funzioni aritmetiche.

## 11.1. Funzione di Dirichlet dei divisori, $d$

**Proposizione 11.1.**

$$\min \lim_{n\to+\infty} d(n) = 2$$
$$\max \lim_{n\to+\infty} d(n) = +\infty.$$

**Dimostrazione**
Poiché $d(n) \geq 2$ per ogni $n \in \mathbb{N}$ sicuramente

$$\min \lim_{n\to+\infty} d(n) \geq 2.$$

Per ottenere il minimo limite basta prendere la successione dei primi. Per il massimo limite, invece, consideriamo la successione $\{a_n\}_{n\in\mathbb{N}} = \{2^n\}_{n\in\mathbb{N}}$. Si ha

$$\lim_{n\to+\infty} d(a_n) = \lim_{n\to+\infty} n+1 = +\infty.$$

□

Non è lecito aspettarsi una stima troppo buona. Vale infatti

**Proposizione 11.2.** *Per ogni $\alpha > 0$, la stima*

$$d(n) = \mathcal{O}(\log^\alpha(n), +\infty) \tag{11.1}$$

*è falsa.*

**Dimostrazione**
Fissiamo $\alpha > 0$, e sia $k = \lfloor \alpha \rfloor + 1 > \alpha$. Consideriamo la successione $\{a_n\}_{n\in\mathbb{N}}$ definita da

$$\{a_n\}_{n\in\mathbb{N}} = \left\{ \left( \prod_{r=1}^{k} p_r \right)^n \right\}_{n\in\mathbb{N}}$$

$$d(a_n) = (n+1)^k = \left( \frac{\log a_n}{\sum_{r=1}^{k} \log p_r} + 1 \right)^k > K \log^k a_n > K \log^\alpha a_n,$$

dove $K$ è una costante indipendente da $n$. Quindi la stima (11.1) non è verificata da una successione di interi, cioè è falsa.

□

Una stima corretta è invece data dal seguente:

**Teorema 11.1.** *Per ogni $\delta > 0$,*

$$d(n) \in \mathcal{O}\left(n^{\delta}, +\infty\right).$$

**Dimostrazione**

Fissiamo $\delta > 0$, e consideriamo la funzione aritmetica

$$\begin{array}{rccc} f: & \mathbb{N} & \to & \mathbb{C} \\ & n & \mapsto & \dfrac{d(n)}{n^{\delta}}. \end{array}$$

Osserviamo che $f$ è una funzione moltiplicativa, e per ogni primo $p$ e ogni $m \in \mathbb{N}$,

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

Poiché per ogni primo $p$ e per ogni numero naturale $m$

$$\lim_{p^m \to +\infty} \frac{2}{\log 2} \frac{\log p^m}{(p^m)^{\delta}} = 0,$$

per il teorema del confronto, anche

$$\lim_{p^m \to +\infty} f(p^m) = 0.$$

Infine, per il teorema 7.3,

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

e cioè $d(n) \in o(n^{\delta}, +\infty)$, e quindi anche $d(n) \in \mathcal{O}(n^{\delta}, +\infty)$.

□

In media, invece:

**Teorema 11.2.**

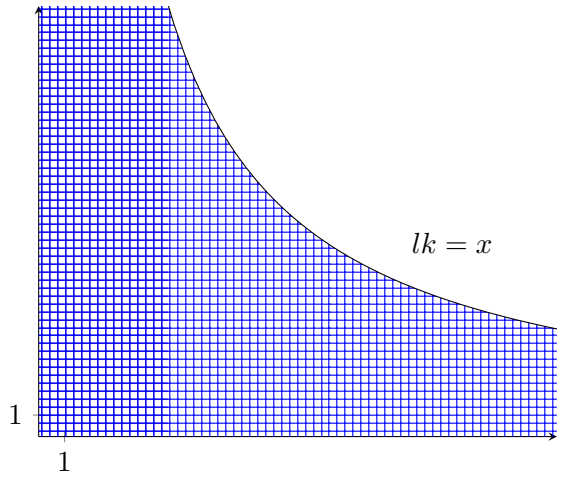
$$\sum_{n \leq x} d(n) = x \log x + (2\gamma - 1)x + \mathcal{O}\left(\sqrt{x}, +\infty\right)$$

**Dimostrazione**

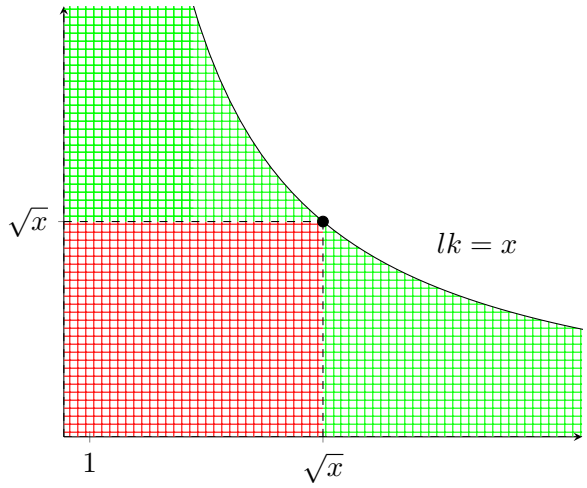
Possiamo scrivere

$$\sum_{n \leq x} d(n) = \sum_{n \leq x} \sum_{l \mid n} 1 = \sum_{lk \leq x} 1.$$

Quindi, dobbiamo contare i punti a coordinate intere positive sotto il ramo di iperbole $lk = x$, con $l, k > 0$ :



Spezziamo nel modo seguente:




Per simmetria, nelle aree in verde c'è lo stesso numero di punti a coordinate intere, $\Sigma_1$. Sia invece $\Sigma_2$ il numero di punti a coordinate intere nell'area in rosso:

$$\Sigma_1 = \sum_{l\leq\sqrt{x}} \sum_{\sqrt{x}<k<\frac{x}{l}} = \sum_{l\leq\sqrt{x}} \left( \left\lfloor \frac{x}{l} \right\rfloor - \lfloor\sqrt{x}\rfloor \right) = \sum_{l\leq\sqrt{x}} \frac{x}{l} - \lfloor\sqrt{x}\rfloor^2 + \mathcal{O}(\sqrt{x}, +\infty).$$

Invece

$$\Sigma_2 = \lfloor\sqrt{x}\rfloor^2 = \left(\sqrt{x} + \mathcal{O}(1, +\infty)\right)^2 = x + \mathcal{O}(\sqrt{x}, +\infty).$$

Quindi

$$2\Sigma_1 + \Sigma_2 = 2x \sum_{l\leq\sqrt{x}} \frac{1}{l} - x + \mathcal{O}(\sqrt{x}, +\infty).$$

Per il teorema 10.1,

$$\begin{aligned} 2\Sigma_1 + \Sigma_2 &= 2x \left( \frac{1}{2} \log x + \gamma + \mathcal{O}\left( \frac{\sqrt{x}}{x}, +\infty \right) \right) - x + \mathcal{O}(\sqrt{x}, +\infty) \\ &= x \log x + (2\gamma - 1)x + \mathcal{O}(\sqrt{x}, +\infty). \end{aligned}$$

□

## 11.2. Funzione somma dei divisori, $\sigma$

**Proposizione 11.3.** *Per ogni $\delta > 0$,*

$$\lim_{n\to+\infty} \frac{\sigma(n)}{n^{1+\delta}} = 0.$$

*In particolare, $\sigma(n) \in \mathcal{O}\left(n^{1+\delta}, +\infty\right)$, per ogni $\delta > 0$.*

**Dimostrazione**

Per ogni primo $p$ e per ogni $n \in \mathbb{N}$,

$$\begin{aligned} \frac{\sigma(p^m)}{p^{m(1+\delta)}} &= \frac{p^{m+1} - 1}{p - 1} \frac{1}{p^{m(1+\delta)}} = \frac{p^{m+1}\left(1 - \frac{1}{p^{m+1}}\right)}{p^{m+1+m\delta} - p^{m(1+\delta)}} \\ &= \frac{p^{m+1}\left(1 - \frac{1}{p^{m+1}}\right)}{p^{m+1+m\delta}\left(1 - \frac{1}{p}\right)} = \frac{1 - \frac{1}{p^{m+1}}}{p^{m\delta}\left(1 - \frac{1}{p}\right)} \leq 2p^{-m\delta}. \end{aligned}$$

Poiché $\sigma$ è una funzione aritmetica moltiplicativa, e

$$\lim_{p^m \to +\infty} 2p^{-m\delta} = 0,$$

abbiamo la tesi per il teorema 7.3.

□

In media, invece:

**Proposizione 11.4.**

$$\sum_{n\leq x} \sigma(n) = \frac{\zeta(2)}{2}x^2 + \mathcal{O}\left(x\log x, +\infty\right)$$

**Dimostrazione**

$$\begin{aligned}
\sum_{n\leq x}\sigma(n) &= \sum_{n\leq x}\sum_{l|n} l = \sum_{k\leq x}\sum_{l\leq \frac{x}{k}} l = \sum_{k\leq x}\frac{1}{2}\left\lfloor\frac{x}{k}\right\rfloor\left(\left\lfloor\frac{x}{k}\right\rfloor+1\right)\\
&= \sum_{k\leq x}\frac{1}{2}\frac{x^2}{k^2} + \mathcal{O}\left(\frac{x}{k}, +\infty\right) = \frac{x^2}{2}\sum_{k\leq x}\frac{1}{k^2} + \mathcal{O}\left(x\sum_{k\leq x}\frac{1}{k}, +\infty\right)\\
&= \frac{x^2}{2}\left(\zeta(2) - \sum_{k>x}\frac{1}{k^2}\right) + \mathcal{O}\left(x\log x, +\infty\right)\\
&= \frac{\zeta(2)}{2}x^2 + \mathcal{O}\left(\frac{x^2}{2}\int_{\lfloor x\rfloor}^{+\infty}\frac{du}{u^2}, +\infty\right) + \mathcal{O}\left(x\log x, +\infty\right)\\
&= \frac{\zeta(2)}{2}x^2 + \mathcal{O}\left(x\log x, +\infty\right).
\end{aligned}$$

□

## 11.3. Funzione di Eulero, $\phi(n)$

Premettiamo un lemma:

**Lemma 11.1.** *Per ogni* $n \in \mathbb{N}$,

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

**Dimostrazione**
Per le proposizioni 7.16, 7.18,

$$\frac{\phi(n)\sigma(n)}{n^2} = \prod_{p^a\|n} p^{a_p}(p-1)\frac{p^{a_p}-1}{p-1}\frac{1}{p^{2a_p}} = \prod_{p^a\|n}\left(1-\frac{1}{p^{a_p+1}}\right).$$

Per concludere, basta osservare che

$$\prod_{p^a\|n}\left(1-\frac{1}{p^{a_p+1}}\right) < 1,$$

e inoltre

$$\prod_{p^a\|n}\left(1-\frac{1}{p^{a_p+1}}\right) > \prod_{p\in\mathbb{P}}\left(1-\frac{1}{p^2}\right) = \frac{1}{\zeta(2)}.$$

□

Grazie al lemma che abbiamo appena dimostrato possiamo affermare che le funzioni aritmetiche

$$\begin{array}{rccc} \widetilde{\sigma}: & \mathbb{N} & \to & \mathbb{C} \\ & n & \mapsto & \dfrac{\sigma(n)}{n} \end{array}$$

$$\begin{array}{rccc} \widetilde{\phi}: & \mathbb{N} & \to & \mathbb{C} \\ & n & \mapsto & \dfrac{n}{\phi(n)} \end{array}$$

hanno lo stesso ordine di grandezza. In particolare,

**Corollario 11.1.** *Per ogni $\delta > 0$,*

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

Il legame fra le funzioni aritmetiche $\phi$ e $\sigma$ diventa ancora più evidente con la seguente proposizione, che è l'analogo della proposizione 11.4:

**Proposizione 11.5.**

$$\sum_{n\leq x} \phi(n) = \frac{1}{2\zeta(2)} x^2 + \mathcal{O}\left(x \log x, +\infty\right)$$

**Dimostrazione**
Per la proposizione 7.15, $\phi = i \star \mu$. Quindi

$$\begin{aligned} \sum_{n\leq x} \phi(n) &= \sum_{n\leq x} \sum_{lk=n} \mu(k) l = \sum_{lk\leq x} \mu(k) l \\ &= \sum_{k\leq x} \mu(k) \sum_{l\leq \frac{x}{k}} l. \end{aligned}$$

Osserviamo che

$$\sum_{l\leq y} l = \frac{\lfloor y \rfloor \lfloor y+1 \rfloor}{2} = \frac{y^2}{2} + \mathcal{O}\left(y, +\infty\right),$$

quindi

$$\begin{aligned} \sum_{n\leq x} \phi(n) &= \sum_{k\leq x} \mu(k) \left( \frac{x^2}{2k^2} + \mathcal{O}\left(\frac{x}{k}, +\infty\right)\right) = \frac{x^2}{2} \sum_{k\leq x} \frac{\mu(k)}{k^2} + \mathcal{O}\left(x \sum_{k\leq x} \frac{1}{k}, +\infty\right) \\ &= \frac{x^2}{2\zeta(2)} + \mathcal{O}\left(x^2 \sum_{k>x} \frac{1}{k^2}, +\infty\right) + \mathcal{O}\left(x \log x, +\infty\right). \end{aligned}$$

Infine, poiché

$$\sum_{k>x} \frac{1}{k^2} \leq \int_{\lfloor x \rfloor}^{+\infty} \frac{du}{u^2} = \mathcal{O}\left(\frac{1}{x}, +\infty\right),$$

$$\sum_{n\leq x} \phi(n) = \frac{x^2}{2\zeta(2)} + \mathcal{O}\left(\frac{1}{x}, +\infty\right) + \mathcal{O}\left(x \log x, +\infty\right) = \frac{1}{2\zeta(2)} x^2 + \mathcal{O}\left(x \log x, +\infty\right).$$

□

# CAPITOLO 12

## Densità

**Introduzione**

In questo capitolo, affronteremo questioni di densità nell'insieme dei numeri naturali. Infine dimostreremo la seconda formula di Möbius, per un risultato sul densità degli interi positivi liberi da quadrati.

## 12.1. Probabilità che due interi positivi siano coprimi

Fissiamo $N \in \mathbb{N}$, $N \geq 2$, e consideriamo

$$\Phi(N) = \sum_{n \leq N} \phi(n).$$

Cosa rappresenta? Osserviamo che

$$\Phi(N) = \sum_{n \leq N} \sum_{\substack{k \leq n \\ (k,n)=1}} 1,$$

quindi $\Phi(N)$ conta il numero di coppie di interi positivi coprimi, minori di $N$. Osserviamo che il numero di coppie complessive è dell'ordine

$$\sum_{\substack{n \in \mathbb{N} \\ n \leq N}} \sum_{\substack{k \in \mathbb{N} \\ k \leq n}} 1 \sim_{+\infty} \frac{N^2}{2}.$$

Siamo interessati al limite per $N$ che tende a $+\infty$ del rapporto

$$\lim_{N \to +\infty} \frac{\Phi(N)}{\sum_{\substack{n \in \mathbb{N} \\ n \leq N}} \sum_{\substack{k \in \mathbb{N} \\ k \leq n}} 1}$$

Se tale limite esistesse, potrebbe essere interpretato come la probabilità che, scelti due interi in maniera casuale, essi siano coprimi. Questo limite, effettivamente, esiste:

**Proposizione 12.1.**

$$\lim_{N \to +\infty} \frac{\Phi(N)}{\sum_{\substack{n \in \mathbb{N} \\ n \leq N}} \sum_{\substack{k \in \mathbb{N} \\ k \leq n}} 1} = \frac{1}{\zeta(2)}.$$

**Dimostrazione**

Per la proposizione 11.5,

$$\lim_{N \to +\infty} \frac{\Phi(N)}{\sum_{\substack{n \in \mathbb{N} \\ n \leq N}} \sum_{\substack{k \in \mathbb{N} \\ k \leq n}} 1} = \frac{\frac{N^2}{2\zeta(2)}}{\frac{N^2}{2}} = \frac{1}{\zeta(2)}.$$

□

## 12.2. Valori medi e densità

Sia $f \in \mathbb{A}$. Se esiste, finito, il limite

$$\lim_{x\to+\infty} \frac{1}{x} \sum_{n\leq x} f(n) = \lambda,$$

diremo che $f$ ha **valor medio** $\lambda$, e scriveremo $v_M(f) = \lambda$. Il valor medio di una funzione aritmetica può essere interpretato anche in termini di densità: abbiamo già dato in precedenza la definizioni di densità asintotica, superiore e inferiore, che riportiamo qui di seguito.

Sia $A \subset \mathbb{N}$, chiamiamo **densità asintotica** di $A$, se esiste, il limite

$$d_A = \lim_{n\to+\infty} \frac{|A \cap \{1, 2, 3, \ldots, n\}|}{n} = \lim_{x\to+\infty} \frac{1}{x} \sum_{\substack{n\leq x \\ n\in A}} 1,$$

mentre chiamiamo **densità superiore** e **densità inferiore** di $A$, rispettivamente, i limiti

$$\overline{d_A} = \limsup_{n\to+\infty} \frac{|A \cap \{1, 2, 3, \ldots, n\}|}{n} = \limsup_{x\to+\infty} \frac{1}{x} \sum_{\substack{n\leq x \\ n\in A}} 1,$$

$$\underline{d_A} = \liminf_{n\to+\infty} \frac{|A \cap \{1, 2, 3, \ldots, n\}|}{n} = \liminf_{x\to+\infty} \frac{1}{x} \sum_{\substack{n\leq x \\ n\in A}} 1.$$

Inoltre, chiamiamo **densità logaritmica** di $A$, se esiste, il limite

$$d_{l,A} = \lim_{x\to+\infty} \frac{1}{\log x} \sum_{\substack{n\leq x \\ n\in A}} \frac{1}{n}.$$

La densità asintotica e la densità logaritmica sono legate dal seguente risultato:

**Proposizione 12.2.** *Sia $f \in \mathbb{A}$, e sia $A \subset \mathbb{N}$. Se esiste il limite*

$$\lim_{x\to+\infty} \frac{1}{x} \sum_{\substack{n\leq x \\ n\in A}} f(n),$$

*allora esiste anche il limite*

$$\lim_{x\to+\infty} \frac{1}{\log x} \sum_{\substack{n\leq x \\ n\in A}} \frac{f(n)}{n},$$

*e sono uguali. Di conseguenza, se un sottoinsieme di $\mathbb{N}$ ammette densità asintotica, allora ammette anche densità logaritmica, e tali densità sono uguali.*

**Dimostrazione**
Supponiamo che il primo limite esista, e sia uguale a $\lambda$ : di conseguenza,

$$\sum_{\substack{n\leq x \\ n\in A}} f(n) = \lambda x + o(x, +\infty).$$

Applicando il lemma di sommazione parziale di Abel,

$$\begin{aligned}\sum_{\substack{n\leq x\\ n\in A}}\frac{f(n)}{n} &= \frac{1}{x}\sum_{\substack{n\leq x\\ n\in A}} f(n) + \int_1^x \sum_{\substack{n\leq x\\ n\in A}} f(u)\frac{du}{u^2}\\ &= (\lambda x + o(x,+\infty))\frac{1}{x} + \lambda\int_1^x \frac{du}{u} + o\left(\int_1^x \frac{du}{u}\right)\\ &= \lambda + \lambda\log x + o(\log x, +\infty).\end{aligned}$$

Pertanto,

$$\frac{1}{\log x}\sum_{\substack{n\leq x\\ n\in A}}\frac{f(n)}{n} = \lambda + o(1,+\infty),$$

e quindi la tesi.

□

Il viceversa non è vero: vedremo un esempio nelle applicazioni.

## 12.3. Densità degli interi positivi che sono liberi da quadrati

Oltre alla prima formula di inversione di Möbius, esiste anche la **seconda formula di inversione di Möbius**:

**Lemma 12.1. (Möbius)** *Siano $F, G : [1,+\infty] \to \mathbb{R}$ due funzioni. Si ha*

$$G(x) = \sum_{n\leq x} F\left(\frac{x}{n}\right) \Leftrightarrow F(x) = \sum_{n\leq x}\mu(n)G\left(\frac{x}{n}\right).$$

**Dimostrazione**
Si ha

$$\begin{aligned}\sum_{n\leq x}\mu(n)G\left(\frac{x}{n}\right) &= \sum_{n\leq x}\mu(n)\sum_{m\leq\frac{x}{n}} F\left(\frac{x}{mn}\right)\\ &= \sum_{mn\leq x}\mu(n)F\left(\frac{x}{mn}\right) \overset{k=mn}{=} \sum_{k\leq x} F\left(\frac{x}{k}\right)\sum_{h|k}\mu(h)\\ &= \sum_{k\leq x} F\left(\frac{x}{k}\right)\mu\star\mathbf{1}(k).\end{aligned}$$

Usando la prima formula di inversione di Möbius 7.6,

$$\sum_{k\leq x} F\left(\frac{x}{k}\right)\mu\star\mathbf{1}(k) = \sum_{k\leq x} F\left(\frac{x}{k}\right)\mathbf{e}(k) = F(x).$$

□

Consideriamo la seguente funzione:

$$\begin{aligned} Q: \quad (0,+\infty) &\to \mathbb{R}\\ n &\mapsto \sum_{k\leq n}\mu^2(k)\end{aligned}$$

Osserviamo che, essendo $\mu^2$ la funzione caratteristica degli interi positivi liberi da quadrati, $Q(x)$ è il numero di interi positivi minori di $x$ che hanno questa proprietà.

**Proposizione 12.3.** *Si ha*

$$\sum_{n\leq x}\mu^2(n)=\frac{1}{\zeta(2)}x+\mathcal{O}\left(\sqrt{x},+\infty\right).$$

*In particolare,*

$$\lim_{x\to+\infty}\frac{Q(x)}{x}=\frac{1}{\zeta(2)},$$

*e cioè la densità asintotica dell'insieme dei numeri naturali liberi da quadrati è* $\frac{1}{\zeta(2)}$.

**Dimostrazione**

Fissiamo $x^2\in\mathbb{R}$, e consideriamo la mappa

$$\begin{array}{rccl} q: & \{n\in\mathbb{N}\mid n\leq x^2\} & \to & \{m\in\mathbb{N}\mid m\leq x\} \\ & n & \mapsto & \max\{q\in\mathbb{N}\mid q\leq x,\ q^2\mid n\}. \end{array}$$

Definiamo la seguente relazione su $M$ : dati $n_1,n_2\leq x^2$, diremo che $n_1\sim n_2$ se e solo se $q(n_1)=q(n_2)$. É immediato verificare che $\sim$ è una relazione di equivalenza: quindi, gli interi positivi minori o uguali a $x^2$ sono partizionati in $r=\lfloor x\rfloor$ classi di equivalenza, $A_1,\dots,A_r$, con

$$A_j=\{n\in\mathbb{N}\mid n\leq x^2,\ q(n)=r\},$$

per ogni $j=1,\dots r$. Vogliamo stimare $A_1$. Si ha

$$\lfloor x^2\rfloor=\sum_{n\leq x}Q\left(\frac{x^2}{n^2}\right).$$

(infatti, a ogni passo si contano gli interi che hanno come massimo divisore quadratico $n^2$, fino a contare tutti gli interi positivi minori o uguali a $x^2$). Per la seconda formula di inversione di Möbius,

$$\begin{aligned} Q(x^2)&=\sum_{n\leq x}\mu(n)\left\lfloor\frac{x^2}{n^2}\right\rfloor=\sum_{n\leq x}\mu(n)\left(\frac{x^2}{n^2}+\mathcal{O}(1,+\infty)\right)\\ &=x^2\sum_{n\leq x}\frac{\mu(n)}{n^2}+\mathcal{O}(x,+\infty)\\ &=x^2\sum_{n\in\mathbb{N}}\frac{\mu(n)}{n^2}+\mathcal{O}\left(x\sum_{n>x}\frac{1}{n^2},+\infty\right)+\mathcal{O}(x,+\infty)\\ &=\frac{x^2}{\zeta(2)}+\mathcal{O}(x,+\infty). \end{aligned}$$

□

## 12.4. Applicazioni

**Esercizio 12.1.** *Calcolare i valori medi delle funzioni aritmetiche* $\frac{\sigma}{i}$, $\frac{\phi}{i}$.

**Risoluzione**

1. Applichiamo il lemma di sommazione parziale di Abel, con la successione $\{a_n\}_{n\in\mathbb{N}} = \{\sigma(n)\}_{n\in\mathbb{N}}$, e la funzione

$$\begin{aligned} f: \quad (0,+\infty) &\to \mathbb{R} \\ x &\mapsto \frac{1}{x}, \end{aligned}$$

e usando la proposizione 11.4

$$\begin{aligned} \sum_{n\le x}\frac{\sigma(n)}{n} &= \frac{1}{x}\sum_{n\le x}\sigma(n) + \int_1^x \frac{1}{u^2}\sum_{n\le u}\sigma(n)du \\ &= \frac{\zeta(2)}{2}x + \mathcal{O}\left(\log x, +\infty\right) \\ &\qquad + \int_1^x \left(\frac{\zeta(2)}{2} + \mathcal{O}\left(\frac{\log u}{u}, +\infty\right)\right) du \\ &= \zeta(2)x + \mathcal{O}(\log^2 x, +\infty). \end{aligned}$$

Quindi $v_M(\frac{\sigma}{i}) = \zeta(2)$.

2. Applichiamo il lemma di sommazione parziale di Abel, con la successione $\{a_n\}_{n\in\mathbb{N}} = \{\phi(n)\}_{n\in\mathbb{N}}$, e la funzione

$$\begin{aligned} f: \quad (0,+\infty) &\to \mathbb{R} \\ x &\mapsto \frac{1}{x}, \end{aligned}$$

e usando la proposizione 11.5

$$\begin{aligned} \sum_{n\le x}\frac{\phi(n)}{n} &= \frac{1}{x}\sum_{n\le x}\phi(n) + \int_1^x \frac{1}{u^2}\sum_{n\le u}\phi(n)du \\ &= \frac{1}{2\zeta(2)}x + \mathcal{O}\left(\log x, +\infty\right) \\ &\qquad + \int_1^x \left(\frac{1}{2\zeta(2)} + \mathcal{O}\left(\frac{\log u}{u}, +\infty\right)\right) du \\ &= \frac{1}{\zeta(2)}x + \mathcal{O}(\log^2 x, +\infty). \end{aligned}$$

Quindi $v_M(\frac{\phi}{i}) = \frac{1}{\zeta(2)}$.

**Esercizio 12.2.** *Siano $a, q \in \mathbb{N}$. L'insieme*

$$P_{q,a} = \{a + lq | l \in \mathbb{N}\}$$

*ha densità asintotica $d_{P_{q,a}} = \frac{1}{q}$.*

**Risoluzione** Ricordando che $\alpha - 1 < \lfloor\alpha\rfloor \le \alpha$, e usando il teorema del confronto

$$d_{P_{q,a}} = \lim_{x\to+\infty}\frac{1}{x}\sum_{\substack{n\le x\\ n\in A}} 1 = \lim_{x\to+\infty}\frac{1}{x}\left\lfloor\frac{x-a}{q}\right\rfloor = \frac{1}{q}.$$

**Esercizio 12.3.** *L'insieme*

$$A = \{n \in \mathbb{N} \mid n \textit{ ha } 1 \textit{ come prima cifra nella sua rappresentazione decimale}\}$$

*ha densità logaritmica, ma non ha densità asintotica. In particolare, che*

$$\overline{d_A} \geq \frac{5}{9}, \qquad \underline{d_A} =\leq \frac{1}{9},$$

*e*

$$d_{l,A} = \frac{\log 2}{\log 10}.$$

**Risoluzione** Osserviamo che i numeri naturali con prima cifra decimale 1 si dispongono a blocchi che sono via via sempre più lontani. Sfruttando questo fatto, consideriamo le successioni $\{x_k\}_{k\in\mathbb{N}} = \{10^k\}_{k\in\mathbb{N}}$, $\{y_k\}_{k\in\mathbb{N}} = \{2\cdot 10^k - 1\}_{k\in\mathbb{N}}$ :

$$\lim_{k\to+\infty} \frac{1}{x_k} \sum_{\substack{n\leq x_k \\ n\in A}} 1 = \lim_{k\to+\infty} \frac{\sum_{h=0}^{k-1} 10^h}{10^k} = \frac{1}{9},$$

$$\lim_{k\to+\infty} \frac{1}{y_k} \sum_{\substack{n\leq y_k \\ n\in A}} 1 = \lim_{k\to+\infty} \frac{\sum_{h=0}^{k} 10^h}{2\cdot 10^k - 1} = \frac{5}{9}.$$

Calcoliamo la densità logaritmica di $A$ : posto $\mathbb{B} = [1, 10^{m+1})_{\mathbb{N}}$,

$$\begin{aligned}\sum_{n\in\mathbb{B}\cap A} \frac{1}{n} &= 1 + \sum_{h=1}^{m} \sum_{n=10^k}^{2\cdot 10^k-1} \frac{1}{n} \\ &= 1 + \sum_{h=1}^{m} \left( \log \frac{2\cdot 10^k - 1}{10^k - 1} + \mathcal{O}\left( \frac{1}{10^k - 1}, +\infty \right) \right).\end{aligned}$$

Poiché

$$\log \frac{2\cdot 10^k - 1}{10^k - 1} = \log 2 \left( 1 + \frac{1}{2(10^k - 1)} \right) = \log 2 + \mathcal{O}\left( \frac{1}{10^k - 1}, +\infty \right),$$

si ricava

$$\begin{aligned}\sum_{n\in\mathbb{B}\cap A} \frac{1}{n} &= 1 + m\log 2 + \mathcal{O}\left( \sum_{k=1}^{m} \frac{1}{10^k - 1}, +\infty \right) \\ &\overset{[1]}{=} 1 + m\log 2 + \mathcal{O}(1, +\infty)\end{aligned}$$

Fissiamo un generico $x \in \mathbb{R}$, $x \geq 10$ e prendiamo $m \in \mathbb{N}$ tale che $10^m - 1 \leq x \leq 10^{m+1}$ : per monotonia, $\log(10^m - 1) \leq \log x \leq (m+1)\log 10$, e

$$\frac{m\log 2 + \mathcal{O}(1, +\infty)}{(m+1)\log 10} \leq \frac{1}{\log x} \sum_{\substack{m\in A \\ m\leq x}} \frac{1}{n} \leq \frac{m\log 2 + \mathcal{O}(1, +\infty)}{\log(10^m - 1)}.$$

Poiché

$$\lim_{m\to+\infty} \frac{m\log 2 + \mathcal{O}(1, +\infty)}{(m+1)\log 10} = \lim_{m\to+\infty} \frac{m\log 2 + \mathcal{O}(1, +\infty)}{\log(10^m - 1)} = \frac{\log 2}{\log 10},$$

concludiamo per il teorema del confronto.

[1] Infatti,

$$\sum_{k=1}^{+\infty} \frac{1}{10^k - 1} < +\infty.$$

Più in generale, si può provare il seguente

**Proposizione 12.4. Benford** *Siano $b, d$ interi positivi, con $1 \leq d \leq b-1$. Posto*

$$A_{b,d} = \{n \in \mathbb{N} \mid n \text{ ha } d \text{ come prima cifra nella sua rappresentazione in base } b\},$$

$$d_{l,A_{b,d}} = \frac{\log\left(1+\frac{1}{d}\right)}{\log b}.$$

# CAPITOLO 13

## Rappresentazioni come somma di due quadrati

**Introduzione**

In questo capitolo, completeremo lo studio del problema del numero di rappresentazioni di un intero positivo come somma di due quadrati. Premetteremo alcuni risultati preliminari sull'anello degli interi di Gauss, $\mathbb{Z}[i]$.

## 13.1. Alcuni risultati preliminari sull'anello $\mathbb{Z}[i]$

Caratterizziamo gli elementi irriducibili (e quindi i primi) in $\mathbb{Z}[i]$.

**Lemma 13.1.** *Se $p \in \mathbb{P}^\star$ non è un elemento irriducibile in $\mathbb{Z}[i]$, allora $p \in \mathcal{Q}_2$.*

**Dimostrazione**

Se $p$ non è irriducibile in $\mathbb{Z}[i]$, allora esistono $a+bi, c+di \in \mathbb{Z}[i]$, non invertibili, tale che $p = (a+bi)(c+di)$. Per il lemma 3.2, $a^2+b^2 > 1$ e $c^2+d^2 > 1$. Osserviamo che, essendo $p$ un numero reale, anche $p = (a-bi)(c-di)$. Quindi, $p^2 = (a^2+b^2)(c^2+d^2)$, ed essendo entrambi questi fattori maggiori di 1, si deve avere $p = a^2+b^2 = c^2+d^2$.

□

**Lemma 13.2.** *Se $p \in \mathbb{P}^\star$ è congruo a 1 modulo 4, allora $p$ non è irriducibile in $\mathbb{Z}[i]$.*

**Dimostrazione**

Per il teorema di Wilson 5.2, esiste $x \in \mathbb{Z}$ tale che $x^2 \equiv -1 \mod p$, cioè $p \mid x^2+1 = (x+i)(x-i)$ : se $p$ fosse irriducibile in $\mathbb{Z}[i]$, poiché quest'ultimo è un PID, $p$ sarebbe anche primo, e dividerebbe almeno uno dei due fattori. Supponiamo, ad esempio, che $p \mid x+i$ : allora, esiste $a+bi \in \mathbb{Z}[i]$ tale che $p(a+bi) = x+i$. Ma allora si deve avere $pb = 1$, assurdo.

□

**Teorema 13.1.** *Tutti e soli gli elementi irriducibili di $\mathbb{Z}[i]$ sono, a meno di associati, i primi di $\mathbb{Z}$ congrui a 3 modulo 4 e gli elementi la cui norma è un primo di $\mathbb{Z}$.*

**Dimostrazione**

($\Rightarrow$) Sia $z \in \mathbb{Z}[i]$ un elemento irriducibile: osserviamo che

$$z \mid z\overline{z} = N(z).$$

Poiché $z$ è un primo in $\mathbb{Z}[i]$, $z$ divide almeno uno dei primi $p$ nella fattorizzazione in $\mathbb{Z}$ di $N(z)$ : quindi, esiste $\omega \in \mathbb{Z}[i]$ tale che $p = z\omega$. Se $\omega$ è un elemento invertibile, allora $p$ e $z$ sono associati, e quindi $p$ è un primo (e quindi irriducibile) in $\mathbb{Z}[i]$. Per il lemma 13.2, e poiché $2 = (1+i)(1-i)$, $p$ è un primo congruo a 3 modulo 4, e lo è anche $z$, a meno di associati. Se invece $\omega$ non è invertibile, per il lemma 3.2, $N(\omega) \neq 1$, e

$$p^2 = N(z)N(\omega),$$

da cui $N(\omega) = N(z) = p$.

($\Leftarrow$) Se $p$ è un primo congruo a 3 modulo 4, nella dimostrazione della proposizione 3.3 abbiamo visto che $p$ non si può scrivere come somma di due quadrati. Per il lemma 13.1, quindi, $p$ è irriducibile in $\mathbb{Z}[i]$. Se invece $z$ è un elemento di $\mathbb{Z}[i]$ tale che $N(z)$ è un numero primo, se scriviamo $z = z_1 z_2$, passando alle norme $N(z) = N(z_1)N(z_2)$, quindi o $N(z_1) = 1$, o $N(z_2) = 1$. Quindi, $z$ è irriducibile.

□

## 13.2. La funzione $r$

Introduciamo la seguente funzione aritmetica

$$\begin{array}{rccl} r: & \mathbb{N} & \to & \mathbb{N} \\ & n & \mapsto & \left|\left\{(x,y) \in \mathbb{Z}^2 \mid x^2+y^2 = n\right\}\right| \end{array}$$

Per la proposizione 7.5, $r$ non è moltiplicativa: infatti, $r(1) = 4$. Per studiare la funzione $r$, è utile la seguente funzione aritmetica, completamente moltiplicativa:

$$\begin{array}{rccl} \chi_4: & \mathbb{N} & \to & \{-1,0,1\} \\ & n & \mapsto & \begin{cases} 0 & \text{se } n \text{ è pari} \\ 1 & \text{se } n \equiv 1 \mod 4 \\ -1 & \text{se } n \equiv 3 \mod 4 \end{cases} \end{array}$$

**Teorema 13.2.** $r = 4\chi_4 \star \mathbf{1}$.

**Dimostrazione**

Una semplice verifica mostra che $\chi_4 \star \mathbf{1}$ è una funzione aritmetica moltiplicativa: per ogni $p, q \in \mathbb{P}$, e per ogni $a, r, s \in \mathbb{N}$,

$$\begin{aligned} \chi_4 \star \mathbf{1}(p^r) &= \sum_{h=0}^{r} \chi_4(q^h) = r+1 = d(p^r) \\ \chi_4 \star \mathbf{1}(q^s) &= \sum_{h=0}^{s} \chi_4(q^h) = \begin{cases} 1 & \text{se } s \text{ è pari} \\ 0 & \text{se } s \text{ è dispari} \end{cases} \\ \chi_4 \star \mathbf{1}(2^a) &= 1. \end{aligned}$$

Per il teorema 3.8, $r(n)$ è uguale a 0 se e solo se nella fattorizzazione di $n$ compare almeno un primo $p \equiv 3 \mod 4$ con esponente dispari. Possiamo limitarci a considerare interi positivi della forma

$$n = 2^\alpha \prod_{\substack{p^r \| n \\ p \equiv 1 \mod 4}} p^r \prod_{\substack{q^{2s} \| n \\ q \equiv 3 \mod 4}} q^{2s} = 2^\alpha \mu\nu,$$

dove

$$\mu = \prod_{\substack{p^r \| n \\ p \equiv 1 \mod 4}} p^r, \qquad \nu = \prod_{\substack{q^{2s} \| n \\ q \equiv 3 \mod 4}} q^{2s}$$

Dunque, $\chi_4 \star \mathbf{1}(n) = d(\mu)$. Per il lemma 13.2, i primi $p$ non sono irriducibili in $\mathbb{Z}[i]$, ed esistono due interi positivi $a, b$ tale che

$$p = a^2 + b^2 = (a+ib)(a-ib).$$

Per il teorema 13.1, queste sono le fattorizzazioni in irriducibili in $\mathbb{Z}[i]$ dei $p$. Sempre per il teorema 13.1,la fattorizzazione di 2 in irriducibili è $2 = (1+i)(1-i)$, e infine i primi $q$ sono irriducibili in $\mathbb{Z}[i]$. Per il teorema 3.8, esistono $R, S \in \mathbb{N}$ tale che

$$n = R^2 + S^2 = (R+Si)(R-Si).$$

Si deve avere, necessariamente,

$$R + Si = i^t(1+i)^{\alpha_1}(1-i)^{\alpha_2} \prod ((a+ib)^{r_1}(a-ib)^{r_2}) \prod_{q|n} q^s$$
$$R - Si = i^{-t}(1+i)^{\alpha_2}(1-i)^{\alpha_1} \prod ((a-ib)^{r_1}(a+ib)^{r_2}) \prod_{q|n} q^s$$

con $t \in \{0,1,2,3\}$, $\alpha_1 + \alpha_2 = \alpha$, $r_1 + r_2 = r$. Ogni possibile scelta di $R, S$ è univocamente determinata dalla scelta di $t$ e $r_1$ (non $\alpha_1$, tenendo conto che $i(1-i) = 1+i$): poiché ci sono 4 possibilità per $t$, e $r+1$ possibilità per $r_1$, ci sono in tutto

$$4 \prod (r+1) = 4d(\mu) = 4\chi_4 \star \mathbf{1}(n)$$

possibili rappresentazioni di $n$ come somma di due quadrati.

□

Osserviamo che $\frac{r}{4}$ è una funzione aritmetica moltiplicativa. Studiare quest'ultima funzione aritmetica, anziché $r$, corrisponde a cercare le rappresentazioni di un intero positivo $n$ come somma di due quadrati usando come basi solo interi positivi.

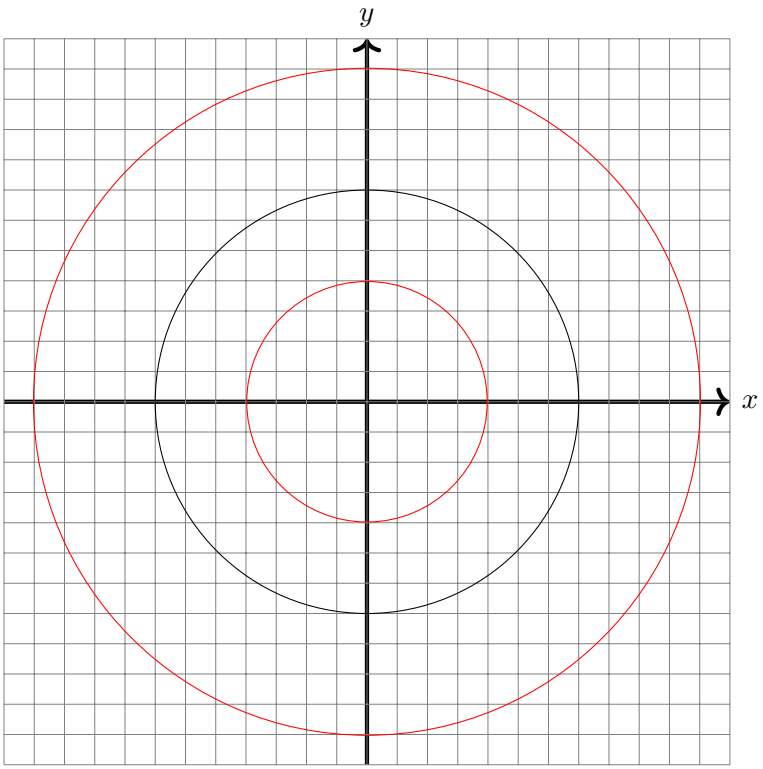
**Proposizione 13.1.**

$$\sum_{n \le x} r(n) = \pi x + \mathcal{O}(\sqrt{x}, +\infty)$$

**Dimostrazione**
Si ha

$$\sum_{n \le x} r(n) = \sum_{n \le x} \sum_{\substack{(m,l) \in \mathbb{Z}\times\mathbb{Z} \\ m^2+l^2=n^2}} 1 = \sum_{\substack{(m,l) \in \mathbb{Z}\times\mathbb{Z} \\ m^2+l^2 \le x}} 1$$

Si tratta quindi di contare il numero di punti a coordinate intere all'interno della circonferenza di centro l'origine e raggio $\sqrt{x}$ (circonferenza inclusa).




Ognuno di questi punti è il vertice in basso a sinistra di un quadrato di area unitaria. Possiamo quindi stimare questo numero di punti sommando l'area di questi quadrati: osserviamo che alcuni di questi quadrati non sono completamente contenuti all'interno della circonferenza, e inoltre l'unione di questi quadrati non ricopre interamente il cerchio. D'altra parte, l'unione di questi quadrati è sicuramente contenuta nel cerchio di centro l'origine e raggio $\sqrt{x}+\sqrt{2}$ e contiene il cerchio di centro l'origine e raggio $\sqrt{x}+\sqrt{2}$, dato che la diagonale di ognuno di questi quadrati è $\sqrt{2}$. Pertanto,

$$\pi(\sqrt{x}-\sqrt{2})^2 \leq \sum_{\substack{(m,l)\in\mathbb{Z}\times\mathbb{Z}\\ m^2+l^2\leq x}} 1 \leq \pi(\sqrt{x}+\sqrt{2})^2,$$

e cioè

$$\sum_{n\leq x} r(n) = \pi x + \mathcal{O}(\sqrt{x}, +\infty).$$

□

# CAPITOLO 14

## Il teorema di Chebychev e i teoremi di Mertens

**Introduzione**

In questo capitolo, torniamo a occuparci della counting function, $pi$ : in particolare, dimostreremo il teorema di Chebychev. In seguito, dimostreremo i teoremi di Mertens, e vedremo alcune loro conseguenze sull'insieme dei numeri primi. Infine studieremo più nel dettaglio il comportamento delle funzioni aritmetiche $\omega$, $\Omega$.

**Teorema 14.1.** $\pi(x) = o(x, +\infty)$.

**Dimostrazione**

Fissiamo $\epsilon > 0$ : sia $p_r$ l'$r-$esimo primo, e sia $x \geq r$. Per il principio di inclusione-esclusione,

$$\begin{aligned}
\pi(x) &\leq r + \lfloor x \rfloor - \sum_{1\leq i\leq r} \left\lfloor \frac{x}{p_i} \right\rfloor + \sum_{1\leq i_1,i_2\leq r} \left\lfloor \frac{x}{p_{i_1}p_{i_2}} \right\rfloor - \cdots + (-1)^r \left\lfloor \frac{x}{p_1\cdots p_r} \right\rfloor \\
&\leq r + x\left(1 - \sum_{1\leq i\leq r} \frac{1}{p_i} + \sum_{1\leq i_1,i_2\leq r} \frac{1}{p_{i_1}p_{i_2}} - \cdots + (-1)^r \frac{1}{p_1\cdots p_r}\right) + \mathcal{O}\left(\sum_{h=0}^{r}\binom{r}{h}, +\infty\right) \\
&= r + x\prod_{j=1}^{r}\left(1 - \frac{1}{p_j}\right) + 2^r\mathcal{O}(1, +\infty) \\
&< x\prod_{j=1}^{r}\left(1 - \frac{1}{p_j}\right) + 2^{r+1}\mathcal{O}(1, +\infty)
\end{aligned}$$

Per il corollario 9.1,

$$\prod_{p\in\mathbb{P}}\left(1 - \frac{1}{p}\right) = 0.$$

Ma allora, a patto di scegliere $r$ sufficientemente grande,

$$\pi(x) \leq \frac{\epsilon}{2}x + 2^{r+1}\mathcal{O}(1, +\infty).$$

Dunque, prendendo $x$ sufficientemente grande, $\pi(x) < \epsilon x$, e quindi la tesi.

□

## 14.1. Le funzioni di Chebychev

Definiamo le seguenti funzioni, note come **funzioni di Chebychev**:

$$\begin{aligned}
\psi : \quad (0, +\infty) &\to \mathbb{R} \\
x &\mapsto \sum_{k\leq x}\Lambda(k) = \sum_{p^m\leq x}\log p
\end{aligned}$$

$$\begin{aligned} \theta: \quad (0,+\infty) &\to \mathbb{R} \\ x &\mapsto \sum_{p\le x} \log p \end{aligned}$$

Dalle definizioni di queste due funzioni, è immediato verificare che $e^{\theta(x)}$ e $e^{\psi(x)}$ sono, rispettivamente, il prodotto di tutti i primi e il minimo comune multiplo di tutti gli interi positivi minori o uguali a $x$. Poiché, per ogni primo $p$, l'addendo $\log p$ compare esattamente $\left\lfloor \frac{\log x}{\log p} \right\rfloor$ volte, è altrettanto immediato osservare che

$$\psi(x) = \sum_{p\le x} \left\lfloor \frac{\log x}{\log p} \right\rfloor \log p. \tag{14.1}$$

Le funzioni $\psi$ e $\theta$ sono legate nel modo seguente:

**Proposizione 14.1.** *Si ha*

$$\psi(x) = \sum_{n=1}^{+\infty} \theta\left(x^{\frac{1}{n}}\right).$$

*Inoltre,*

$$\psi(x) = \theta(x) + \mathcal{O}(\sqrt{x}\log^2 x, +\infty).$$

**Dimostrazione**
Osserviamo che, nella prima formula, la somma è in realtà su un numero finito di termini, dato che

$$\theta\left(x^{\frac{1}{n}}\right) \neq 0 \Leftrightarrow x^{\frac{1}{n}} > 2 \Leftrightarrow n < \frac{\log x}{\log 2}.$$

La sua veridicità è conseguenza immediata delle definizioni.
Sempre dalle definizioni , per $x \ge 2$, $\theta(x) < x\log x$, quindi

$$\theta\left(x^{\frac{1}{n}}\right) < \frac{1}{n} x^{\frac{1}{n}} \log x < \frac{1}{2}\sqrt{x}\log x,$$

$$\sum_{k=2}^{+\infty} \theta\left(x^{\frac{1}{n}}\right) = \mathcal{O}(\sqrt{x}\log^2 x, +\infty).$$

□

Le funzioni di Chebychev giocano un ruolo importante nella dimostrazione del teorema 2.4:

**Lemma 14.1.**

$$\begin{aligned} \liminf_{x\to+\infty} \frac{\pi(x)\log x}{x} &= \liminf_{x\to+\infty} \frac{\theta(x)}{x} = \liminf_{x\to+\infty} \frac{\psi(x)}{x} \\ \limsup_{x\to+\infty} \frac{\pi(x)\log x}{x} &= \limsup_{x\to+\infty} \frac{\theta(x)}{x} = \limsup_{x\to+\infty} \frac{\psi(x)}{x} \end{aligned}$$

**Dimostrazione**
Chiaramente, $\theta(x) \le \psi(x)$. Inoltre, dall'equazione 14.1,

$$\psi(x) \le \sum_{p\le x} \frac{\log x}{\log p} \log p = \log x \sum_{p\le x} 1 = \pi(x)\log x.$$

Quindi $\theta(x) \leq \psi(x) \leq \pi(x)\log x$,

$$\limsup_{x\to+\infty} \frac{\theta(x)}{x} \leq \limsup_{x\to+\infty} \frac{\psi(x)}{x} \leq \limsup_{x\to+\infty} \frac{\pi(x)\log x}{x},$$

e analogamente per i limiti inferiori.
Fissiamo un numero reale $\alpha \in (0,1)$, e sia $x > 1$. Allora,

$$\theta(x) \geq \sum_{x^\alpha \leq p \leq x} \log p \geq \alpha \log x \sum_{x^\alpha < p \leq x} 1 = \alpha \log x \left(\pi(x) - \pi(x^\alpha)\right).$$

Ma $\pi(x^\alpha) < x^\alpha$, quindi $\theta(x) > \alpha \log x \left(\pi(x) - x^\alpha\right)$ e

$$\frac{\theta(x)}{x} > \alpha \frac{\pi(x)\log x}{x} - \alpha \frac{\log x}{x^{1-\alpha}}.$$

Poiché

$$\lim_{x\to+\infty} \frac{\log x}{x^{1-\alpha}} = 0,$$

$$\limsup_{x\to+\infty} \frac{\theta(x)}{x} \geq \alpha \limsup_{x\to+\infty} \frac{\pi(x)\log x}{x}$$

per ogni $\alpha \in (0,1)$, e quindi

$$\limsup_{x\to+\infty} \frac{\theta(x)}{x} \geq \limsup_{x\to+\infty} \frac{\pi(x)\log x}{x}.$$

Pertanto,

$$\limsup_{x\to+\infty} \frac{\pi(x)\log x}{x} = \limsup_{x\to+\infty} \frac{\theta(x)}{x} = \limsup_{x\to+\infty} \frac{\psi(x)}{x}.$$

In maniera analoga, si conclude allo stesso modo per i limiti inferiori.

□

## 14.2. Il teorema di Chebychev

**Lemma 14.2.** *Per ogni $n \in \mathbb{N}$,*

$$n! = \prod_{p \leq n} p^{\sum_{k=1}^{+\infty} \left\lfloor \frac{n}{p^k} \right\rfloor}$$

**Dimostrazione**
La dimostrazione di questo lemma è un fatto combinatorio molto semplice: osserviamo soltanto che le somme negli esponenti dei primi $p$ sono su un numero finito di termini, dato che

$$\left\lfloor \frac{n}{p^k} \right\rfloor \neq 0 \Leftrightarrow n > p^k \Leftrightarrow k < \frac{\log n}{\log p}. \tag{14.2}$$

□

Enunciamo inoltre il seguente famoso risultato, noto come **postulato di Bertrand**:

**Teorema 14.2. (Postulato di Bertrand)** *Per ogni $N \in \mathbb{N}$, esiste un numero primo $p$ tale che $N \leq p < 2N$.* Abbiamo già enunciato il teorema di Chebychev: ora possiamo dimostrarlo.

**Teorema 14.3. (Chebychev)**

$$\pi(x) \asymp_{+\infty} \frac{x}{\log x}$$

**Dimostrazione**

Per il lemma 14.1, è sufficiente provare che esistono due costanti $C_1, C_2 > 0$ tali che

$$\liminf_{x\to+\infty} \frac{\psi(x)}{x} \geq C_1, \qquad \limsup_{x\to+\infty} \frac{\theta(x)}{x} \leq C_2.$$

Costante $C_1$ Fissiamo $N \in \mathbb{N}$ : usando il lemma 14.2,

$$\begin{aligned} B = \frac{(2N)!}{N!N!} &= \frac{\prod_{p\leq 2N} p^{\sum_{k=1}^{+\infty}\left\lfloor \frac{2N}{p^k}\right\rfloor}}{\prod_{p\leq N} p^{\sum_{k=1}^{+\infty}\left\lfloor \frac{N}{p^k}\right\rfloor}\prod_{p\leq N} p^{\sum_{k=1}^{+\infty}\left\lfloor \frac{N}{p^k}\right\rfloor}} \\ &= \frac{\prod_{p\leq 2N} p^{\sum_{k=1}^{+\infty}\left\lfloor \frac{2N}{p^k}\right\rfloor}}{\prod_{p\leq N} p^{2\sum_{k=1}^{+\infty}\left\lfloor \frac{N}{p^k}\right\rfloor}} \\ &= \prod_{N<p<2N} p^{\sum_{k=1}^{+\infty}\left\lfloor \frac{2N}{p^k}\right\rfloor - 2\left\lfloor \frac{N}{p^k}\right\rfloor} \\ &\leq \prod_{p<2N} p^{\sum_{k=1}^{+\infty}\left\lfloor \frac{2N}{p^k}\right\rfloor - 2\left\lfloor \frac{N}{p^k}\right\rfloor} \end{aligned}$$

Osserviamo che, per ogni $x, y \in \mathbb{R}$, $\lfloor x+y\rfloor - \lfloor x\rfloor - \lfloor y\rfloor \in \{0,1\}$ : usando questo fatto, e ricordando l'equazione (14.2), otteniamo la maggiorazione

$$B \leq \prod_{p<2N} p^{\left\lfloor \frac{\log 2N}{\log p}\right\rfloor}$$

D'altra parte, anche

$$\binom{2N}{N} \geq 2^N.$$

Quindi, passando ai logaritmi,

$$\log 2N \leq \sum_{p\leq 2N} \log p \left\lfloor \frac{\log 2N}{\log p}\right\rfloor = \psi(2N).$$

Sia $x \in (2, +\infty)$, e sia $N \in \mathbb{N}$ tale che $2N \leq x < 2(N+1)$. Allora,

$$\begin{aligned} \psi(x) \geq \psi(2N) \geq N\log 2 \geq \frac{x-2}{2}\log 2 \geq \frac{x}{4}\log 2 \Rightarrow \frac{\psi(x)}{x} \geq \frac{\log 2}{4} \\ \Rightarrow \liminf_{x\to+\infty} \frac{\psi(x)}{x} \geq \frac{\log 2}{4} = C_1. \end{aligned}$$

Costante $C_2$ Fissiamo $N \in \mathbb{N}$, e consideriamo il coefficiente binomiale $B = \binom{2N}{N}$ : osserviamo che ogni primo $p$, con $N < p \leq 2N$ è tale che $p \mid B$. Quindi,

$$\prod_{N<p<2N} p \leq B \leq \sum_{h=0}^{2N} \binom{2N}{h} = 2^{2N},$$

e passando ai logaritmi

$$\theta(2N) - \theta(N) \leq 2N\log 2.$$

In particolare, per ogni $m \in \mathbb{N}$,

$$\theta(2^m) - \theta(2^{m-1}) \leq 2^m \log 2,$$

e quindi, per ogni $k \in \mathbb{N}$,

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

Sia $x \in (2, +\infty)$, e sia $k \in \mathbb{N}$ tale che $2^k < x \leq 2^{k+1}$. Allora,

$$\theta(x) \leq \theta(2^{k+1}) < 4 \cdot 2^k \log 2 < 4 \log 2x \Rightarrow \frac{\theta(x)}{x} \leq 4 \log 2$$
$$\Rightarrow \limsup_{x \to +\infty} \frac{\theta(x)}{x} \leq 4 \log 2 = C_2.$$

□

Di conseguenza,

**Corollario 14.1.**

$$\pi(x) \asymp_{+\infty} Li(x).$$

**Dimostrazione**
Integrando per parti,

$$\int_2^x \frac{dt}{\log^2 t} = \int_2^x \frac{tdt}{t \log^2 t} = -\frac{x}{\log x} + \frac{2}{\log 2} + \int_2^x \frac{dt}{\log t} = -\frac{x}{\log x} + \frac{2}{\log 2} + Li(x).$$

Mantenendo le stesse notazioni del teorema di Chebychev, usiamo il lemma di sommazione parziale di Abel, con le successioni

$$\{a_n\}_{n \in \mathbb{N}} = \{\log p_n\}_{n \in \mathbb{N}} \qquad \{x_n\}_{n \in \mathbb{N}} = \{p_n\}_{n \in \mathbb{N}},$$

e la funzione logaritmo. Per ogni $x \geq 2$,

$$\pi(x) = \sum_{p_n \leq x} 1 = \sum_{p_n \leq x} \log p_n \frac{1}{\log p_n} = \frac{\theta(x)}{\log x} + \int_2^x \frac{\theta(u)}{u \log^2 u} du$$
$$\geq \frac{C_1 x}{\log x} + C_1 \int_2^x \frac{du}{\log^2 u} = \frac{2C_1}{\log 2} + C_1 Li(x).$$

Inoltre anche $\theta(x) \leq C_2 x$, quindi

$$\pi(x) = \sum_{p_n \leq x} 1 = \sum_{p_n \leq x} \log p_n \frac{1}{\log p_n} = \frac{\theta(x)}{\log x} + \int_2^x \frac{\theta(u)}{u \log^2 u} du$$
$$\leq \frac{C_2 x}{\log x} + C_2 \int_2^x \frac{du}{\log^2 u} = \frac{2C_2}{\log 2} + C_2 Li(x)$$

□

Il corollario precedente ci conforta sull'enunciato del teorema dei numeri primi. In modo più preciso, si potrebbe dimostrare che

**Teorema 14.4.**

$$\liminf_{x \to +\infty} \frac{\pi(x) \log x}{x} \leq 1 \qquad \limsup_{x \to +\infty} \frac{\pi(x) \log x}{x} \geq 1.$$

## 14.3. I teoremi di Mertens

Premettiamo un lemma:

**Lemma 14.3.**

$$\sum_{n\leq x} \log n = x\log x - x + \mathcal{O}(\log x, +\infty).$$

**Dimostrazione**
Usando il lemma di sommazione parziale di Abel,

$$\sum_{n\leq x} \log n = \lfloor x\rfloor \log x - \int_1^x \lfloor u\rfloor \frac{du}{u} = x\log x - x + \mathcal{O}(\log x, +\infty).$$

□

I seguenti teoremi sono noti come **Teoremi di Mertens**

**Teorema 14.5. (Mertens)**

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

*Si può dimostrare che il resto che compare nel primo teorema di Mertens è*

$$-\gamma + \mathcal{O}\left(\frac{1}{\log x}, x\to+\infty\right).$$

**Dimostrazione**
Per la proposizione 7.17,

$$\begin{aligned}\sum_{n\leq x}\log n &= \sum_{n\leq x}\sum_{d|n}\Lambda(d) = \sum_{kd\leq x}\Lambda(k)\\ &= \sum_{k\leq x}\Lambda(k)\sum_{d\leq \frac{x}{k}} 1 = \sum_{k\leq x}\Lambda(k)\left\lfloor\frac{x}{k}\right\rfloor\\ &= \sum_{k\leq x}\left(\frac{x}{k}+\mathcal{O}(1,+\infty)\right)\Lambda(k) = x\sum_{k\leq x}\frac{\Lambda(k)}{k} + \mathcal{O}(\psi(x),+\infty)\\ &= x\sum_{k\leq x}\frac{\Lambda(k)}{k} + \mathcal{O}(x,+\infty).\end{aligned}$$

Uguagliando con quanto ottenuto nel lemma 14.3, si ricava subito la tesi.

□

**Teorema 14.6. (Mertens)** *Sia $x\in(2,+\infty)$. Allora*

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

**Dimostrazione**
Si ha

$$\sum_{n\leq x}\frac{\Lambda(n)}{n} = \sum_{\substack{(a,p)\in\mathbb{N}\times\mathbb{P}\\ p^a\leq x}}\frac{\log p}{p^a} = \sum_{p\leq x}\frac{\log p}{p} + \sum_{\substack{(a,p)\in\mathbb{N}\times\mathbb{P}\\ a>1,\ p^a\leq x}}\frac{\log p}{p^a}.$$

Osserviamo che

$$\sum_{\substack{(a,p)\in\mathbb{N}\times\mathbb{P}\\ a>1,\ p^a\leq x}} \frac{\log p}{p^a} = \sum_{p\in\mathbb{P}} \log p \sum_{\substack{a>1\\ p^a\leq x}} \frac{1}{p^a} \leq \sum_{p\in\mathbb{P}} \log p \sum_{a=2}^{+\infty} \frac{1}{p^a} = \sum_{p\in\mathbb{P}} \frac{\log p}{p(p-1)} < +\infty$$

$$\Rightarrow \sum_{\substack{(a,p)\in\mathbb{N}\times\mathbb{P}\\ a>1,\ p^a\leq x}} \frac{\log p}{p^a} = \mathcal{O}(1,+\infty).$$

Per il primo teorema di Mertens 14.5, confrontando con quanto appena ottenuto, la tesi.

□

I teoremi di Mertens ci permettono di studiare il comportamento asintotico della serie dei reciproci dei primi, che sappiamo essere divergente, come conseguenza dell'identità di Eulero.

**Corollario 14.2.** *Esiste una costante $C > 0$ tale che*

$$\sum_{p\leq x} \frac{1}{p} = \log\log x + C + \mathcal{O}\left(\frac{1}{\log x}, +\infty\right).$$

*Si può dimostrare che*

$$C = \gamma + \sum_{p\in\mathbb{P}} \left(\log\left(1-\frac{1}{p}\right) + \frac{1}{p}\right).$$

**Dimostrazione**

Usando il lemma di sommazione parziale di Abel:

$$\sum_{p\leq x} \frac{1}{p} = \sum_{p\leq x} \frac{\log p}{p} \frac{1}{\log p} = \left(\sum_{p\leq x} \frac{\log p}{p}\right) \frac{1}{\log x} + \int_2^x \sum_{p\leq u} \frac{\log p}{p} \frac{du}{u\log^2 u}.$$

Usando il secondo teorema di Mertens,

$$\begin{aligned}\sum_{p\leq x} \frac{1}{p} &= 1 + \mathcal{O}\left(\frac{1}{\log x}, +\infty\right) + \int_2^x \frac{du}{u\log u} + \int_2^x \frac{\mathcal{O}(1,+\infty)}{u\log^2 u} du \\ &= 1 + \mathcal{O}\left(\frac{1}{\log x}, +\infty\right) + \int_2^x \frac{du}{u\log u} \\ &\quad + \int_2^{+\infty} \frac{\mathcal{O}(1,+\infty)}{u\log^2 u} du - \int_x^{+\infty} \frac{\mathcal{O}(1,+\infty)}{u\log^2 u} du.\end{aligned}$$

Dunque esiste una costante $A > 0$ tale che

$$\int_2^{+\infty} \frac{\mathcal{O}(1,u)}{u\log^2 u} du \leq A < +\infty$$

sebbene, in questo modo, non sia possibile calcolarla. In più, è noto che

$$\int_2^x \frac{du}{u\log u} = \log\log x - \log\log 2.$$

Ricapitolando,

$$\begin{aligned}\sum_{p\leq x} \frac{1}{p} &= \log\log x + 1 - \log\log 2 + A + \mathcal{O}\left(\frac{1}{\log x}, +\infty\right) + \mathcal{O}\left(\int_x^{+\infty} \frac{du}{u\log^2 u}, +\infty\right) \\ &= \log\log x + 1 - \log\log 2 + A + \mathcal{O}\left(\frac{1}{\log x}, +\infty\right).\end{aligned}$$

□

Vediamo un'ultima conseguenza dei teoremi di Mertens:

**Corollario 14.3.** *Si ha*

$$\sum_{p\leq x}\log\left(1-\frac{1}{p}\right)=-\log\log x-\gamma+\mathcal{O}\left(\frac{1}{\log x},+\infty\right).$$

**Dimostrazione**

$$\sum_{p\leq x}\log\left(1-\frac{1}{p}\right)=-\sum_{p\leq x}\frac{1}{p}+\sum_{p\leq x}\left(\log\left(1-\frac{1}{p}\right)+\frac{1}{p}\right).$$

Per il corollario 14.2,

$$\begin{aligned}\log\left(\prod_{p\leq x}\left(1-\frac{1}{p}\right)\right)&=-\log\log x-\gamma-\sum_{p>x}\left(\log\left(1-\frac{1}{p}\right)+\frac{1}{p}\right)+\mathcal{O}\left(\frac{1}{\log x},+\infty\right)\\&=-\log\log x-\gamma+\mathcal{O}\left(\frac{1}{\log x},+\infty\right).\end{aligned}$$

□

## 14.4. Le funzioni $\omega$, $\Omega$

**Proposizione 14.2.** *Si ha*

$$\omega(n)=\mathcal{O}(\log n,+\infty).$$

**Dimostrazione**
Osserviamo che, per ogni $n\in\mathbb{N}$, $\omega(n)=\omega(\rho(n))$. Sia $q$ il più piccolo primo che divide $n$. Si ha

$$\rho(n)\geq q^{\omega(n)}\geq 2^{\omega(n)},$$

quindi $\log\rho(n)\geq\log 2\omega(n)$, e

$$\omega(n)\leq\frac{\log\rho(n)}{\log 2}=\frac{\log n}{\log 2}\Rightarrow\omega(n)=\mathcal{O}(\log n,+\infty).$$

□

**Corollario 14.4.** *Per ogni $n\in\mathbb{N}$, con $n\geq 3$,*

$$\sum_{p|n}\frac{1}{p}\leq\log\log\log n+\mathcal{O}(1,+\infty).$$

**Dimostrazione**
Possiamo spezzare nel seguente modo:

$$\sum_{p|n}\frac{1}{p}=\sum_{\substack{p|n\\p\leq\log n}}\frac{1}{p}+\sum_{\substack{p|n\\p>\log n}}\frac{1}{p}.$$

Per il corollario 14.2,

$$\sum_{\substack{p\leq \log p\\ p|n}} \frac{1}{p} \leq \sum_{p\leq \log p} \frac{1}{p} = \log\log\log n + C + \mathcal{O}\left(\frac{1}{\log\log n}, +\infty\right),$$

mentre, per la proposizione 14.2,

$$\sum_{\substack{p> \log p\\ p|n}} \frac{1}{p} \leq \frac{1}{\log n}\sum_{p|n} 1 = \frac{\omega(n)}{\log n} = \mathcal{O}(1, +\infty).$$

Rimettendo assieme i pezzi, subito la tesi.

□

Vediamo cosa succede in media:

**Proposizione 14.3.**

$$\sum_{n\leq x} \omega(n) = x\log\log x + Cx + \mathcal{O}\left(\frac{x}{\log x}, +\infty\right)$$
$$\sum_{n\leq x} \Omega(n) = x\log\log x + Bx + \mathcal{O}\left(\frac{x}{\log x}, +\infty\right)$$

dove $C$ è la stessa costante del corollario 14.2, e

$$B = C + \sum_{p\in\mathbb{P}} \frac{1}{p(p-1)}.$$

**Dimostrazione**
Si ha

$$\sum_{n\leq x} \omega(n) = \sum_{n\leq x}\sum_{p|n} 1 = \sum_{\substack{(p,k)\in\mathbb{P}\times\mathbb{N}\\ pk\leq x}} 1 = \sum_{p\leq x}\sum_{k\leq \frac{x}{p}} 1$$
$$= \sum_{p\leq x} \left\lfloor \frac{x}{p} \right\rfloor = x\sum_{p\leq x}\frac{1}{p} + \mathcal{O}(\pi(x), +\infty).$$

Per il corollario 14.2 e per il teorema di Chebychev 2.4,

$$\sum_{n\leq x} \omega(n) = x\log\log x + Cx + \mathcal{O}\left(\frac{x}{\log x}, +\infty\right),$$

e la prima formula è dimostrata. Vediamo la seconda:

$$\sum_{n\leq x} \Omega(n) = \sum_{n\leq x}\sum_{p^m\| n} m = \sum_{n\leq x}\sum_{p|n} 1 + \sum_{\substack{m\geq 2\\ p^m\leq x}}\sum_{k\leq \frac{x}{p^m}} 1$$
$$= \sum_{\substack{n\in\mathbb{N}\\ n\leq x}} \omega(n) + \sum_{\substack{m\geq 2\\ p^m\leq x}}\sum_{k\leq \frac{x}{p^m}} 1.$$

Abbiamo appena visto come valutare il primo termine. Per il secondo, invece,

$$\sum_{\substack{m\geq 2\\ p^m\leq x}}\sum_{k\leq \frac{x}{p^m}} 1 = \sum_{\substack{m\geq 2\\ p^m\leq x}} \left\lfloor \frac{x}{p^m}\right\rfloor = x\sum_{\substack{m\geq 2\\ p^m\leq x}}\frac{1}{p^m} + \mathcal{O}\Big(\sum_{\substack{m\geq 2\\ p^m\leq x}} 1, +\infty\Big).$$

Valutiamo il resto: poiché

$$\sum_{\substack{m\geq 2\\ p^m\leq x}} 1 \leq \sum_{\substack{m\geq 2\\ p^m\leq x}} \frac{\log p}{\log 2} = \frac{1}{\log 2}\left(\psi(x) - \theta(x)\right),$$

per la proposizione 14.1, il resto è $\mathcal{O}(\sqrt{x}\log^2 x, +\infty)$. Valutiamo la somma restante: poiché

$$\sum_{m\geq 2}\frac{1}{p^m} = \sum_{p\in\mathbb{P}}\frac{1}{p(p-1)},$$

possiamo scrivere

$$\sum_{\substack{m\geq 2\\ p^m\leq x}}\frac{1}{p^m} = \frac{1}{p(p-1)} - \sum_{\substack{m\geq 2\\ p^m> x}}\frac{1}{p^m}.$$

Osserviamo che

$$p^m > x \Leftrightarrow m > \frac{\log x}{\log 2} = \mu,$$

quindi

$$\sum_{\substack{m\geq 2\\ p^m> x}}\frac{1}{p^m} = \sum_{p\in\mathbb{P}}\sum_{m\geq \max\{2,\mu\}}\frac{1}{p^m}.$$

Poiché

$$\frac{\log x}{\log p} < 2 \Leftrightarrow p > \sqrt{x},$$

possiamo spezzare la somma nel modo seguente:

$$\sum_{p\in\mathbb{P}}\sum_{m\geq\max\{2,\rho\}}\frac{1}{p^m} = \sum_{p\leq\sqrt{x}}\sum_{m\geq\rho}\frac{1}{p^m} + \sum_{p>\sqrt{x}}\sum_{m=2}^{+\infty}\frac{1}{p^m}.$$

Il secondo termine lo possiamo valutare nel modo seguente:

$$\sum_{p>\sqrt{x}}\sum_{m=2}^{+\infty}\frac{1}{p^m} = \sum_{p>\sqrt{x}}\frac{1}{p(p-1)} = \mathcal{O}(1, +\infty),$$

e infine, osservando che, per ogni $p\in\mathbb{N}$,

$$\frac{p}{p-1} < 2 \qquad p^{\lfloor\rho\rfloor+1} > \frac{\log x}{\log p},$$

valutiamo così il primo termine:

$$\begin{aligned}\sum_{p\leq\sqrt{x}}\sum_{m=\rho+\infty}\frac{1}{p^m} = \sum_{p\leq\sqrt{x}}\sum_{m=\lfloor\rho\rfloor+1}^{+\infty}\frac{1}{p^m} &= \sum_{p\leq\sqrt{x}}\frac{p}{p^{\lfloor\rho\rfloor+1}(p-1)}\\ &< \sum_{p\leq\sqrt{x}}\frac{2}{x} = \frac{2}{x}\pi(\sqrt{x}) = \mathcal{O}\left(\frac{1}{\sqrt{x}}, +\infty\right).\end{aligned}$$

Rimettendo assieme tutti i pezzi, la tesi.

□

Il risultato precedente è per certi versi inaspettato: infatti, ci dice che in media si avverte la differenza fra $\omega$ e $\Omega$ solo al secondo termine dello sviluppo.

## 14.5. Ordini normali

Diremo che un insieme $E \subset \mathbb{N}$ è a **misura nulla** se

$$|\{n \in E \mid n \leq x\}| = o(x, +\infty).$$

Se una proprietà $P$ è verificata per tutti gli interi positivi ad eccezione di quelli contenuti in un insieme $E \subset \mathbb{N}$ a misura nulla, diremo che $P$ è vera per quasi tutti gli interi.

Sia $f \in \mathbb{A}$ una funzione aritmetica: diremo che $g \in \mathbb{A}$ è un **ordine normale** di $f$ se, per ogni $\epsilon > 0$, esiste $E_\epsilon \subset \mathbb{N}$ a misura nulla tale che, per ogni $n \in \mathbb{N} - E$,

$$(1 - \epsilon)g(n) \leq f(n) \leq (1 + \epsilon)g(n).$$

In un certo senso, potremmo dire che la funzione aritmetica $g$ approssima $f$. Con l'introduzione degli ordini normali di una funzione aritmetica, abbiamo un nuovo strumento per studiare il comportamento di una funzione aritmetica. Si potrebbe pensare che il valor medio di una funzione aritmetica sia correlato agli ordini normali. In realtà non è così, vediamo qualche esempio:

- La funzione aritmetica

$$\begin{array}{rccl} f: & \mathbb{N} & \to & \mathbb{N} \\ & n & \mapsto & \begin{cases} 2 & \text{se } 2 \mid n \\ 0 & \text{altrimenti} \end{cases} \end{array}$$

  ha valor medio $1$, ma non può avere ordine normale: infatti, continua a oscillare tra due insiemi che hanno densità asintotica positiva, pari a $\frac{1}{2}$.

- La funzione aritmetica

$$\begin{array}{rccl} f: & \mathbb{N} & \to & \mathbb{N} \\ & n & \mapsto & \begin{cases} 2^m & \text{se } n = 2^m \\ 0 & \text{altrimenti} \end{cases} \end{array}$$

  ha come ordine normale la funzione aritmetica identicamente nulla (infatti, $f$ è non nulla su un insieme che ha densità asintotica uguale a $0$) ma non ammette valor medio: infatti

$$\lim_{m \to +\infty} \frac{1}{2^m - 1} \sum_{n \leq 2^m - 1} f(n) = \lim_{m \to +\infty} \frac{2^m - 1}{2^m - 1} = 1,$$

$$\lim_{m \to +\infty} \frac{1}{2^m} \sum_{n \leq 2^m} f(n) = \lim_{m \to +\infty} \frac{2^{m+1} - 1}{2^m} = 2.$$

Cerchiamo degli ordini principali per alcune delle funzioni aritmetiche studiate:

**Teorema 14.7.** *Per ogni* $\epsilon > 0$

$$\left|\left\{n \in \mathbb{N} \mid n \leq x,\ |\omega(n) - \log\log n| > (\log\log n)^{\frac{1}{2}+\epsilon}\right\}\right| = o(x, +\infty).$$

*Un risultato analogo vale per la funzione aritmetica* $\Omega$. *In altri termini,* $\log\log x$ *è un ordine normale per le funzioni aritmetiche* $\omega, \Omega$.

**Dimostrazione**

Se $x^{\frac{1}{e}} \leq n \leq x$, allora $\log\log x - 1 \leq \log\log n \leq \log\log x$ : basta quindi provare che

$$\left|\left\{n \in \mathbb{N} \mid n \leq x,\ |\omega(n) - \log\log n| > (\log\log x)^{\frac{1}{2}+\epsilon}\right\}\right| = o(x, +\infty).$$

Inoltre, è sufficiente dimostrare la tesi per $\omega$ : infatti, per la proposizione 14.3,

$$\sum_{n\leq x} (\Omega(n) - \omega(n)) = \mathcal{O}(x, +\infty),$$

e quindi

$$\left|\left\{n \in \mathbb{N} \mid n \leq x,\ \Omega(n) - \omega(n) > \sqrt{\log\log x}\right\}\right| = o(x, +\infty).$$

Fissiamo $n \in \mathbb{N}$, e consideriamo il numero di coppie di fattori primi distinti di $n$, $(p, q)$. Dalla definizione della funzione $\omega$,

$$\omega(n)(\omega(n) - 1) = \sum_{\substack{pq|n \\ p\neq q}} 1 = \sum_{pq|n} 1 - \sum_{p^2|n} 1.$$

Sommiamo su tutti gli $n \in \mathbb{N}$, $n \leq x$ :

$$\sum_{n\leq x} \left(\omega(n)^2 - \omega(n)\right) = \sum_{n\leq x} \left(\sum_{pq|n} 1 - \sum_{p^2|n} 1\right) = \sum_{pq\leq x} \left\lfloor \frac{x}{pq} \right\rfloor - \sum_{p^2\leq x} \left\lfloor \frac{x}{p^2} \right\rfloor$$

Valutiamo il secondo termine:

$$\sum_{p^2\leq x} \left\lfloor \frac{x}{p^2} \right\rfloor \leq \sum_{p^2\leq x} \frac{x}{p^2} \leq x \sum_{p\in\mathbb{P}} \frac{1}{p^2} = \mathcal{O}(x, +\infty).$$

Invece, per il primo termine,

$$\sum_{pq\leq x} \left\lfloor \frac{x}{pq} \right\rfloor = x \sum_{pq\leq x} \frac{1}{pq} + \mathcal{O}(x \log\log x, +\infty).$$

Per la proposizione 14.3, si ricava

$$\sum_{n\leq x} \omega(n)^2 = x \sum_{pq\leq x} \frac{1}{pq} + \mathcal{O}(x \log\log x, +\infty).$$

Osserviamo che

$$\left(\sum_{p\leq\sqrt{x}} \frac{1}{p}\right)^2 \leq \sum_{pq\leq x} \frac{1}{pq} \leq \left(\sum_{p\leq x} \frac{1}{p}\right)^2.$$

Per il corollario 14.2,

$$\left(\sum_{p\leq x} \frac{1}{p}\right)^2 = (\log\log x)^2 + \mathcal{O}(\log\log x, +\infty),$$

e quindi

$$\sum_{\substack{n\in\mathbb{N}\\ n\leq x}} \omega(n)^2 = x(\log\log x)^2 + \mathcal{O}(x\log\log x, +\infty).$$

Per quanto appena dimostrato, e per la proposizione 14.3,

$$\begin{aligned}
&\sum_{n\leq x} (\omega(n) - \log\log x)^2 = \sum_{n\leq x} \omega(n)^2 - 2\log\log x \sum_{n\leq x} \omega(n) + \lfloor x\rfloor (\log\log x)^2 \\
&= x(\log\log x)^2 + \mathcal{O}(x\log\log x, +\infty) \\
&\quad - 2\log\log x\,(x\log\log x + \mathcal{O}(x, +\infty)) + x(\log\log x)^2 + \mathcal{O}((\log\log x)^2, +\infty) \\
&= \mathcal{O}(x\log\log x, +\infty).
\end{aligned}$$

Fissiamo $\epsilon > 0$ : se per assurdo ci fossero più di $\eta x$ interi positivi, con $\eta > 0$, che non superano $x$, tali che sia soddisfatta la condizione

$$|\omega(n) - \log\log n| > (\log\log x)^{\frac{1}{2}+\epsilon},$$

allora si avrebbe

$$\sum_{n\leq x} (\omega(n) - \log\log x)^2 \geq \eta x (\log\log x)^{1+2\epsilon},$$

e questo contraddice quanto appena provato, comunque si scelga $\epsilon > 0$.

□

**Corollario 14.5.** *Per ogni $\epsilon > 0$, per quasi tutti gli $n \in \mathbb{N}$*

$$2^{(1-\epsilon)\log\log n} < d(n) < 2^{(1+\epsilon)\log\log n}$$

*In particolare, $L \circ d$ ha ordine normale* $\log 2 \log\log x$.

**Dimostrazione**

Per ogni $n \in \mathbb{N}$, $n > 1$, vale la disuguaglianza

$$2^{\omega(n)} \leq d(n) \leq 2^{\Omega(n)}$$

(per provarla, basta provare che vale per le potenze dei primi, dato che le funzioni aritmetiche in gioco sono moltiplicative): per ogni $p \in \mathbb{P}$, e per ogni $a \in \mathbb{N}$, allora

$$2^{\omega(n)} = 2 \leq d(p^a) = a + 1 \leq 2^a = 2^{\Omega(n)},$$

e di conseguenza

$$\omega(n)\log 2 \leq \log d(n) \leq \Omega(n)\log 2.$$

Per il teorema 14.7, la tesi.

□

## 14.6. Applicazioni

### Metodi di crivello

Siano $\mathcal{N} \subset \mathbb{N}$, $P \subset \mathbb{P}$ due insiemi e, per ogni numero primo $p \in P$, sia $\Omega_p \subset \mathbb{Z}/p\mathbb{Z}$, un insieme di classi residue modulo $p$. Chiamiamo **crivello** la terna $(\mathcal{N}, P, \{\Omega_p\}_{p\in P})$. Chiamiamo **metodo di crivello** la ricerca di una stima della quantità

$$|\mathcal{N}_0| = |\{n \in \mathbb{N} \mid \overline{n} \notin \Omega_p\ \forall p \in P\}|.$$

L'insieme $\mathcal{N}_0$ è chiamato **insieme di crivello**. Nel seguito, adottiamo la notazione $\omega_p = |\Omega_p|$. In generale, parleremo di metodi di **piccolo crivello** quando, per ogni $p \in \mathbb{P}$, $\omega_p$ è limitato, di metodi di **grande crivello** se invece $\omega_p$ è grande (ad esempio, se $\Omega_p$ è l'insieme dei residui quadratici modulo $p$).

**Teorema 14.8. (Montgomery, 1968)** *Sia $(\mathcal{N}, P, \{\Omega_p\}_{p\in P})$ un crivello, dove*

$$\mathcal{N} = (M+1, M+N)_{\mathbb{N}}$$

*è un intervallo, e $M, N \in \mathbb{N}$. Siano poi $Q$ un intero positivo e $\widehat{Q}$ l'insieme degli interi positivi, minori di $Q$, che sono prodotto di primi in $\mathbb{P}$. Vale la stima*

$$|\mathcal{N}_0| \leq \frac{N+Q^2}{L},$$

*dove*

$$L = \sum_{q\in\widehat{Q}} \mu^2(q) \prod_{p|q} \frac{\omega_p}{p-\omega_p}.$$

### Il crivello di Eratostene

Un crivello famoso è il **crivello di Eratostene**, che si ottiene, fissato un intero positivo $N \in \mathbb{N}$, prendendo

$$\mathcal{N} = [1, N]_{\mathbb{N}} \qquad P = \{p \in \mathbb{P} \mid 1 \leq p \leq \sqrt{n}\},$$

e, per ogni $p \in P$, $\Omega_p = \{\overline{0}\}$ : in questo modo, l'insieme di crivello è

$$\mathcal{N}_0 = \{p \in \mathbb{P} \mid \sqrt{N} \leq p \leq N\},$$

e inoltre $\omega_p = 1$ per ogni $p \in \mathbb{P}$, $\mu^2(q) = 1$ per ogni $q \in Q$,

$$L = \sum_{q\leq Q} \prod_{p|q} \frac{1}{p-1}.$$

Per il teorema di Montgomery 14.8,

$$\pi(N) - \pi(\sqrt{N}) \leq \frac{N+Q^2}{\sum_{q\leq Q}\prod_{p|q}\frac{1}{p-1}}.$$

Prendiamo $Q = \sqrt{N}$ : il problema è stimare dal basso il denominatore. L'idea è la seguente: osserviamo che, per ogni $q \in Q$,

$$\phi(q) = \prod_{p|q} \phi(p) = \prod_{p|q} (p-1).$$

Si ha

**Proposizione 14.4.** $L > \log Q$.

**Dimostrazione**

Basta osservare che

$$L = \sum_{q\leq Q} \frac{1}{\phi(q)} = \sum_{q\leq Q} \frac{1}{q} \prod_{p|q} \frac{p}{p-1} > \sum_{q\leq Q} \frac{1}{q} > \log Q.$$

□

Quindi

$$\pi(N) - \pi(\sqrt{N}) \leq \frac{N+N}{\frac{1}{2}\log N} = \frac{4N}{\log N}.$$

Scegliendo $Q$ in maniera opportuna, si possono ottenere stime migliori.

### Un crivello per i primi gemelli

Un altro crivello è quello per la ricerca dei primi gemelli, che si ottiene prendendo $\Omega_p = \{\overline{0}, \overline{2}\}$ : l'insieme di crivello, in questo caso, è

$$\mathcal{N}_0 = \{p \in \mathbb{P} \mid \sqrt{N} \leq p \leq N, p+2 \in \mathbb{P}\}.$$

Si può dimostrare che

**Proposizione 14.5.** $L > \log^2 Q$.

Prendendo $Q = \sqrt{N}$, si ottiene la stima

$$\pi_2(N) \leq \frac{8N}{\log^2 N}, \tag{14.3}$$

che ha una bella conseguenza:

**Proposizione 14.6.**

$$\sum_{p \in \mathbb{P}_2} \frac{1}{p} < +\infty.$$

**Dimostrazione**
Applicando il lemma di sommazione parziale di Abel, con la successione $\{a_n\}_{n\in\mathbb{N}}$ definita da

$$a_n = \begin{cases} 1 & \text{se } n \in \mathbb{P}_2 \\ 0 & \text{se } n \notin \mathbb{P}_2 \end{cases}$$

per ogni $n \in \mathbb{N}$, e la funzione

$$\begin{array}{rccc} f: & \mathbb{N} & \to & \mathbb{R} \\ & n & \mapsto & \dfrac{1}{n}, \end{array}$$

e usando la stima (14.3)

$$\begin{aligned} \sum_{\substack{p \in \mathbb{P}_2 \\ p \leq x}} \frac{1}{p} &= \sum_{2 \leq n \leq x} \frac{a_n}{n} = \frac{\pi_2(x)}{x} - \frac{\pi_2(2)}{2} + \int_2^x \frac{\pi_2(u)}{y^2} \\ &= \frac{\pi_2(x)}{x} + \int_2^x \frac{\pi_2(u)}{y^2} \leq \frac{8}{\log^2 x} + \int_2^x \frac{8du}{u \log^2 u} = \frac{8}{\log^2 x} + \frac{8}{\log 2} - \frac{8}{\log x}. \end{aligned}$$

Quindi,

$$\sum_{p \in \mathbb{P}_2} \frac{1}{p} = \lim_{x \to +\infty} \sum_{\substack{p \in \mathbb{P}_2 \\ p \leq x}} \frac{1}{p} < \lim_{x \to +\infty} \frac{8}{\log^2 x} + \frac{8}{\log 2} - \frac{8}{\log x} = \frac{8}{\log 2} < +\infty.$$

□

### La densità di Schnirelmann

Fissiamo $n \in \mathbb{N}$ : consideriamo il problema di valutare la quantità

$$S_n = \sum_{\substack{p,q\in\mathbb{P} \\ p,q>\sqrt{n} \\ p+q=n}} 1.$$

Questo è un problema di tipo additivo: somme di questo tipo compaiono in problemi come la congettura di Goldbach2.4. In problemi come questo, è utile la seguente densità, nota come **densità di Schnirelmann**: dato $A \subset \mathbb{N} \cup \{0\}$, definiamo la sua densità di Schnirelmann

$$d_S(A) = \inf_{N\in\mathbb{N}} \frac{\sum_{\substack{a\in A \\ a\leq N}} 1}{N}.$$

La densità di Schnirelmann gode delle seguenti proprietà:

**Teorema 14.9.** *Siano $A, B \subset \mathbb{N} \cup \{0\}$. Se $0 \in A$, posto*

$$A + B = \{a + b \in \mathbb{N} \cup \{0\} \mid a \in A, b \in B\},$$

$$d_S(A + B) = d_S(A) + d_S(B) - d_S(A)d_S(B).$$

**Proposizione 14.7.** *Sia $A \subset \mathbb{N} \cup \{0\}$. Se $d_S(A) = 1$, allora $A = \mathbb{N} \cup \{0\}$.*

**Dimostrazione**

Assumiamo, senza perdere in generalità, che $A = \mathbb{N} - \{0\}$. Allora

$$\frac{\sum_{\substack{a\in A \\ a\leq n_0}} 1}{n_0} = \frac{n_0 - 1}{n_0} < 1,$$

e quindi $d_S(A) < 1$.

□

Si può dimostrare che

**Teorema 14.10.** *Esiste una costante positiva $C$ tale che $S_n \leq C\frac{n}{\log^2 n}$.*

### Un'applicazione del postulato di Bertrand

**Teorema 14.11. (Miller)** *Esiste una costante positiva $\alpha$ tale che, posto*

$$\begin{cases} a_0 = \alpha \\ a_n = 2^{a_{n-1}} \quad \forall n \geq 1 \end{cases}$$

*la successione $\{\lfloor a_n \rfloor\}_{n\in\mathbb{N}}$ è fatta di soli primi.*

**Dimostrazione**

Sia $q_1 \neq 2$ un primo. Per il postulato di Bertrand, esiste un primo $q_2$ tale che $2^{q_1} < q_2 < 2^{q_1+1}$ : procedendo in questo modo, costruiamo una successione $\{q_n\}_{n\in\mathbb{N}} \subset \mathbb{P}$. Per ogni $n \in \mathbb{N}$,

$$2^{q_n} < q_{n+1} < q_{n+1} + 1 < 2^{q_n+1}, \tag{14.4}$$

poiché se fosse $q_{n+1} + 1 = 2^{q_n+1}$ allora $2^{q_n+1} - 1 = q_{n+1}$ sarebbe un primo di Mersenne, e, per la proposizione 2.6, $q_n + 1$ dovrebbe essere primo, che è chiaramente assurdo. Definiamo le successioni

$$\{u_n\}_{n\in\mathbb{N}} = \{\log_2^{(n)} q_n\}_{n\in\mathbb{N}},$$

$$\{v_n\}_{n\in\mathbb{N}} = \{\log_2^{(n)} (q_n + 1)\}_{n\in\mathbb{N}}.$$

Per l'equazione (14.4), $u_n < u_{n+1} < v_{n+1} < v_n$. Di conseguenza, $\{u_n\}_{n\in\mathbb{N}}$ è una successione crescente, $\{v_n\}_{n\in\mathbb{N}}$ è una successione decrescente, e hanno limite finito. Sia $\alpha \in \mathbb{R}$ tale che $\lim_{n\to+\infty} u_n \leq \alpha \leq \lim_{n\to+\infty} v_n$. Per ogni $n \in \mathbb{N}$, elevando a potenza si ottiene

$$q_n < a_n < q_n + 1,$$

cioè $\lfloor a_n \rfloor = q_n$, per ogni $n \in \mathbb{N}$.

□

Osserviamo che in particolare

$$u_1 < \alpha < v_1,$$

e se prendiamo $q_1 = 3$ abbiamo $u_1 = \log_2 3 \sim 1.5849625$, $v_1 = \log_2 4 = 2$. Purtroppo $\alpha$ non è una costante nota, ma si sa che $\alpha \sim 1.9287800$.

# CAPITOLO 15

## Il teorema di Dirichlet

**Introduzione**

In questo capitolo, dimostreremo il teorema di Dirichlet sull'infinità dei numeri primi nelle progressioni aritmetiche. Per farlo, introdurremo i caratteri e le funzioni $\mathscr{L}$ di Dirichlet, ne studieremo le principali proprietà e vedremo come possano essere utili per la dimostrazione.

Abbiamo già enunciato il teorema di Dirichlet sui primi nelle progressioni:

**Teorema 15.1. (Dirichlet)** *Se $m, n$ sono tali che $1 \leq m \leq n$ e $(m, n) = 1$, allora esistono infiniti numeri primi congrui ad $m$ modulo $n$.*

## 15.1. I caratteri di Dirichlet

Sia $p$ un primo dispari. Sappiamo che

$$\mathbb{G} = (\mathbb{Z}/p\mathbb{Z})^\star$$

è un gruppo ciclico: sia $\overline{g}$ un suo generatore, e, per ogni $n \in \mathbb{N}$, con $p \nmid n$, sia $\nu(n)$ il più piccolo intero positivo tale che

$$g^{\nu(n)} \equiv n \mod p.$$

Sia infine $\omega \in \mathbb{C}$ una radice $(p-1)-$esima dell'unità: la scelta di $\omega$ corrisponde a scegliere un qualsiasi intero positivo $m$ minore di $p$ :

$$\omega = e^{\frac{2\pi m i}{p-1}}.$$

Per ogni scelta di $m$ definiamo carattere di Dirichlet modulo $p$ la funzione aritmetica

$$\begin{array}{rccl} \chi_{m,p}: & \mathbb{N} & \to & \mathbb{C} \\ & n & \mapsto & \begin{cases} e^{\frac{2\pi m i \nu(n)}{p-1}} & \text{se } p \nmid n \\ 0 & \text{altrimenti} \end{cases} \end{array}.$$

Denotiamo con $\mathbb{D}_p$ l'insieme dei caratteri di Dirichlet modulo $p$. Per come abbiamo definito i caratteri di Dirichlet, chiaramente $|\mathbb{D}_p| = p - 1$. Chiamiamo carattere principale $\chi_{0,p}$ il carattere

$$\begin{array}{rccl} \chi_{p-1,p} = \chi_{0,p}: & \mathbb{N} & \to & \mathbb{C} \\ & n & \mapsto & \begin{cases} 1 & \text{se } p \nmid n \\ 0 & \text{altrimenti} \end{cases} \end{array}.$$

**Proposizione 15.1.** *I caratteri di Dirichlet modulo $p$ hanno le seguenti proprietà:*

1. $\chi(1) = 1$ *per ogni* $\chi \in \mathbb{D}_p$;
2. *Ogni carattere di Dirichlet modulo* $q$ *è una funzione periodica di periodo* $q$;
3. *Ogni carattere di Dirichlet modulo* $q$ *è una funzione aritmetica completamente moltiplicativa;*
4. $(\mathbb{D}_p, \cdot)$ *è un gruppo.*
5. **(Formule di ortogonalità)**

$$\sum_{\chi \in \mathbb{D}_p} \chi(n) = \begin{cases} p-1 & \textit{se } n \equiv 1 \mod p \\ 0 & \textit{altrimenti} \end{cases}$$

$$\sum_{n=1}^{p-1} \chi_{m,p}(n) = \begin{cases} p-1 & \textit{se } \chi_{m,p} = \chi_0 \\ 0 & \textit{se } \chi_{m,p} \neq \chi_0 \end{cases}$$

**Dimostrazione.**

1. Ovvio;
2. É una conseguenza immediata del fatto che

$$n_1 \equiv n_2 \mod p \Leftrightarrow \nu(n_1) = \nu(n_2);$$

3. É una conseguenza immediata del fatto che, per ogni $n_1, n_2 \in \mathbb{N}$, se $p \nmid n_1, n_2$

$$\nu(n_1 n_2) \equiv \nu(n_1) + \nu(n_2) \mod p - 1;$$

4. Il prodotto dei caratteri è sicuramente associativo e l'elemento neutro è il carattere $\chi_{0,p}$. Infine, per ogni $m = 1, \ldots, p-1$, l'inverso del carattere di Dirichlet $\chi_{m,p}$ è il carattere $\chi_{p-1-m,p} = \overline{\chi}_{m,p}$. Quindi $\mathbb{D}_p$ è un gruppo;
5. Se $n \equiv 1 \mod p$ chiaramente

$$\sum_{n=1}^{p-1} \chi_{m,p}(n) = \sum_{n=1}^{p-1} 1 = p - 1.$$

Se invece $n \not\equiv 1 \mod p$, abbiamo

$$\sum_{n=1}^{p-1} \chi_{m,p}(n) = \sum_{n=1}^{p-1} e^{\frac{2\pi m i \nu(n)}{p-1}} \overset{1}{=} \sum_{n=1}^{p-1} \left(e^{\frac{2\pi m i}{p-1}}\right)^n = e^{\frac{2\pi m i}{p-1}} \frac{e^{2\pi m i} - 1}{e^{\frac{2\pi m i}{p-1}} - 1} = 0.$$

La seconda formula si dimostra in modo simile.

□

[1] Infatti, l'insieme dei $\nu(n)$ è uguale all'insieme degli interi positivi da 1 a $p-1$

Possiamo generalizzare la definizione di carattere di Dirichlet modulo $p$ a quella di carattere modulo un numero intero positivo $r$ qualunque, purché maggiore di 1 :

- ($r = p^{a_p}$, $p \in \mathbb{P}^\star$, $a_p \in \mathbb{N}$, oppure $p = 2$, $a_2 = 1, 2$) Per il teorema 6.1 il gruppo moltiplicativo

$$(\mathbb{Z}/p^{a_p}\mathbb{Z})^\star$$

è ciclico. Sia $\overline{g}_p$ un suo generatore, e per ogni $n \in \mathbb{N}$, con $p \nmid n$, sia $\nu(n)$ il più piccolo intero positivo tale che

$$g^{\nu(n)} \equiv n \mod \phi(r).$$

Sia infine $\omega \in \mathbb{C}$ una radice $\phi(r)-$esima dell'unità: la scelta di $\omega$ corrisponde a scegliere un qualsiasi intero positivo $m$ minore di $r$ coprimo con $r$ :

$$\omega = e^{\frac{2\pi m i}{\phi(r)}}.$$

Per ogni scelta di $m$ definiamo carattere di Dirichlet modulo $r$ la funzione aritmetica

$$\begin{array}{rccl} \chi_{m,r}: & \mathbb{N} & \to & \mathbb{C} \\ & n & \mapsto & \begin{cases} e^{\frac{2\pi m i \nu(n)}{\phi(r)}} & \text{se } p \nmid n \\ 0 & \text{altrimenti} \end{cases} \end{array}.$$

Nel caso $r = 2$, abbiamo un solo carattere, che è il carattere principale modulo 2 (la funzione caratteristica dell'insieme dei numeri dispari), mentre nel caso $r = 4$ abbiamo due caratteri, uno dei quali è la funzione aritmetica $\chi_4$, che abbiamo incontrato in precedenza;

- ($r = 2^{a_2}$, $a_2 \in \mathbb{N}$, $a_2 > 2$) In questo caso, il gruppo moltiplicativo

$$(\mathbb{Z}/2^{a_2}\mathbb{Z})^\star$$

non è ciclico. Tuttavia, per il corollario 6.1, possiamo riadattare la costruzione fatta precedentemente: per ogni $n \in \mathbb{N}$, con $n$ dispari sia $\nu(n)$ il più piccolo intero positivo tale che

$$2^{\nu(n)} \equiv n \mod 2^{a_2-2}.$$

Siano poi $\omega_1 \in (\mathbb{Z}/2\mathbb{Z})^\star$, e $\omega \in \mathbb{C}$ una radice $2^{a_2-2}-$esima dell'unità: anche in questo caso, le scelte di $\omega_1, \omega$ corrispondono alla scelta di due interi positivi, il primo, $m'$, in $\{\pm 1\}$, il secondo, $m$, minore di $2^{a_2-2}$ e dispari. Per ogni scelta di $m, m'$, definiamo carattere di Dirichlet modulo $r$ la funzione aritmetica

$$\begin{array}{rccl} \chi_{m',m,r}: & \mathbb{N} & \to & \mathbb{C} \\ & n & \mapsto & \begin{cases} m' e^{\frac{2\pi m i \nu(n)}{\phi(2^{a-2})}} & \text{se } 2 \nmid n \\ 0 & \text{altrimenti} \end{cases} \end{array}$$

- ($r = \prod_{p^{a_p} \| r} p^{a_p}$) Nel caso generale, tutti i caratteri di Dirichlet modulo $r$ si ottengono moltiplicando fra loro i caratteri di Dirichlet modulo $p^{a_p}$.

Anche per i caratteri di Dirichlet generalizzati continuano a valere proprietà analoghe a quelle per i caratteri di Dirichlet modulo $p$ enunciate nella proposizione 15.1. In particolare, continuano a valere le formule di ortogonalità:

**Proposizione 15.2.** *I caratteri di Dirichlet modulo $r$ hanno le seguenti proprietà:*

1. $\chi(1) = 1$ *per ogni* $\chi \in \mathbb{D}_r$;

2. *Ogni carattere di Dirichlet modulo $r$ è una funzione periodica di periodo $r$;*
3. *Ogni carattere di Dirichlet modulo $r$ è una funzione aritmetica completamente moltiplicativa;*
4. *$(\mathbb{D}_r, \cdot)$ è un gruppo.*
5. **(Formule di ortogonalità)**

$$\sum_{n=1}^{r-1} \chi_{m,r}(n) = \begin{cases} 0 & \textit{se } \chi_{m,r} \neq \chi_0 \\ \phi(r) & \textit{se } \chi_{m,r} = \chi_0 \end{cases}$$

$$\sum_{\chi \in \mathbb{D}_r} \chi(n) = \begin{cases} \phi(r) & \textit{se } n \equiv 1 \mod r \\ 0 & \textit{altrimenti} \end{cases}$$

I caratteri di Dirichlet sono importantissimi anche e soprattutto per il seguente corollario:

**Corollario 15.1.** *Se $aa' \equiv 1 \mod r$,*

$$\frac{1}{\phi(r)} \sum_{\chi \in \mathbb{D}_r} \chi(n)\overline{\chi}(a) = \frac{1}{\phi(r)} \sum_{\chi \in \mathbb{D}_r} \chi(a'n) = \begin{cases} 1 & \textit{se } n \equiv a \mod r \\ 0 & \textit{altrimenti} \end{cases} \tag{15.1}$$

## 15.2. Le funzioni $\mathscr{L}$ di Dirichlet

A ogni carattere $\chi_{m,r}$ di Dirichlet associamo una funzione, che chiameremo **funzione $\mathscr{L}$ di Dirichlet** associata al carattere, espressa in termini di serie di Dirichlet:

$$\begin{aligned} \mathscr{L}_{\chi_{m,r}} : (1, +\infty) &\to \mathbb{C} \\ s &\mapsto \sum_{n \in \mathbb{N}} \frac{\chi_{m,r}(n)}{n^s}. \end{aligned}$$

Ad esempio, al carattere principale $\chi_{0,r}$ si associa la funzione

$$\begin{aligned} \mathscr{L}_{\chi_{0,r}} : (1, +\infty) &\to \mathbb{C} \\ s &\mapsto \sum_{n \in \mathbb{N}} \frac{\chi_{0,r}(n)}{n^s} = \sum_{n \not\equiv 0 \mod r} \frac{1}{n^s}. \end{aligned}$$

Quest'ultima funzione assomiglia "pericolosamente" alla funzione $\zeta$ di Riemann. In effetti, per l'identità di Eulero, se $\chi \in \mathbb{D}_r$, per $s > 1$,

$$\mathscr{L}_\chi(s) = \prod_{p \in \mathbb{P}} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1},$$

e nel caso particolare del carattere principale

$$\mathscr{L}_{\chi_{0,r}}(s) = \prod_{p \nmid q} \left(1 - \frac{1}{p^s}\right)^{-1} = \zeta(s) \prod_{p \mid q} \left(1 - \frac{1}{p^s}\right),$$

**Proposizione 15.3.** *Sia $q \in \mathbb{N}$, con $q > 1$. Per $s > 1$,*

$$\prod_{\chi \in \mathbb{D}_q} |\mathscr{L}_\chi(s)| \geq 1.$$

**Dimostrazione**
Si ha

$$\begin{aligned}
\log \prod_{\chi \in \mathbb{D}_r} \mathscr{L}_\chi(s) = \sum_{\chi \in \mathbb{D}_r} \log \mathscr{L}_\chi(s) &= \sum_{\chi \in \mathbb{D}_r} \log \mathscr{L}_\chi(s) \\
&= \sum_{\chi \in \mathbb{D}_r} \sum_{p \in \mathbb{P}} \log \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} \\
&= \sum_{\chi \in \mathbb{D}_r} \sum_{p \in \mathbb{P}} \sum_{m=0}^{+\infty} \overline{\chi}(1) \frac{\chi(p^m)}{m p^{ms}} \\
&= \sum_{p \in \mathbb{P}} \sum_{m \in \mathbb{N}} \frac{1}{m} \sum_{\chi \in \mathbb{D}_r} \frac{\overline{\chi}(1)\chi(p^m)}{p^{ms}} \\
&\overset{Eq.\ (15.1)}{=} \phi(r) \sum_{m \in \mathbb{N}} \sum_{p^m \equiv 1 \mod r} \frac{1}{m p^{ms}} \geq 0
\end{aligned}$$

□

**Proposizione 15.4.** *Sia $\chi$ un carattere modulo $r$ diverso dal carattere principale. Allora*

$$\mathscr{L}_\chi(s) = s \int_1^{+\infty} \frac{1}{u^{s+1}} \sum_{n \leq u} \chi(n) du.$$

*In particolare, se $\chi$ è un carattere reale, $\mathscr{L}_\chi(s) = \mathcal{O}(1, +\infty)$, e*

$$\sum_{y < n \leq x} \frac{\chi(n)}{\sqrt{n}} = \mathcal{O}\left(\frac{1}{\sqrt{y}}, +\infty\right).$$

**Dimostrazione**
Applicando il lemma di sommazione parziale di Abel,

$$\sum_{n \leq x} \frac{\chi(n)}{n^s} = \frac{1}{x^s} \sum_{n \leq x} \chi(n) + s \int_1^x \frac{1}{u^{s+1}} \sum_{n \leq u} \chi(n) du. \tag{15.2}$$

Per la prima formula di ortogonalità,

$$\frac{1}{x^s} \sum_{n \leq x} \chi(n) = \mathcal{O}\left(\frac{1}{x^s}, +\infty\right),$$

quindi tende a 0 al limite per $x \to +\infty$. Di conseguenza, la tesi. Allora

$$\mathscr{L}_\chi(s) \leq s \int_1^{+\infty} \frac{\phi(r)}{2} \frac{1}{u^{s+1}} du = \frac{\phi(r)}{2},$$

quindi $\mathscr{L}_\chi(s) = \mathcal{O}(1, +\infty)$. Prendendo $s = \frac{1}{2}$, dall'equazione (15.2) , per ogni $x, y \in \mathbb{R}$, $0 < y < x$,

$$\begin{aligned}
\sum_{y < d \leq x} \frac{\chi(d)}{\sqrt{d}} &= \frac{1}{2} \int_y^x \frac{1}{u^{\frac{3}{2}}} \sum_{k \leq u} \chi(k) du + \frac{1}{x} \sum_{k \leq x} \chi(k) - \frac{1}{y} \sum_{k \leq y} \chi(k) \\
&\leq \frac{\phi(r)}{4} \left(\frac{1}{\sqrt{y}} - \frac{1}{\sqrt{x}}\right) + \frac{1}{y} \sum_{y < d \leq x} \chi(d) \leq \phi(r) \left(\frac{1}{\sqrt{y}} - \frac{1}{\sqrt{x}} + \frac{1}{y}\right) = \mathcal{O}\left(\frac{1}{\sqrt{y}}, +\infty\right).
\end{aligned}$$

□

**Lemma 15.1.** *Sia $r \in \mathbb{N}$, con $r > 1$, e sia $\chi \in \mathbb{D}_r$. Se $\chi \in \mathbb{D}_r$, con $\chi \neq \chi_{0,r}$, allora $\mathbb{L}_\chi(1) \neq 0$.*

**Dimostrazione**

Supponiamo inizialmente che il carattere sia reale (cioè, assume solo i valori 1 e $-1$), e consideriamo la funzione aritmetica $\chi \star \mathbf{1}$. Osserviamo che tale funzione aritmetica è moltiplicativa: valutiamola sulle potenze dei primi. Per ogni $p \in \mathbb{P}$, e per ogni $a \in \mathbb{N}$,

$$\chi \star \mathbf{1}(p^a) = 1 + \sum_{h=1}^{a} \chi^h(p) = \begin{cases} a+1 & \text{se } \chi(p) = 1 \\ 1 & \text{se } \chi(p) = -1, \text{ e a è pari, oppure se } \chi(p) = 0 \\ 0 & \text{se } \chi(p) = -1, \text{ e a è dispari} \end{cases}$$

Per la moltiplicatività di $\chi \star \mathbf{1}$,

$$\chi \star \mathbf{1}(n) \geq \begin{cases} 1 & \text{se } n \text{ è un quadrato perfetto} \\ 0 & \text{altrimenti} \end{cases}$$

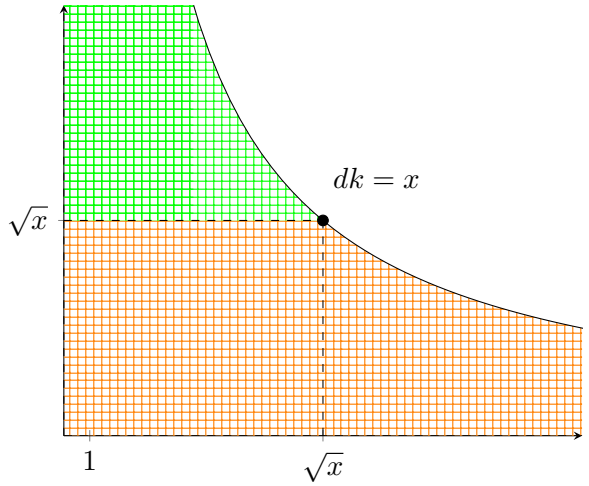
Allora

$$\sum_{n \leq x} \frac{\chi \star \mathbf{1}(n)}{\sqrt{n}} \geq \sum_{m^2 \leq x} \frac{1}{m} \overset{Teo\ 10.1}{=} \frac{1}{2} \log x + \mathcal{O}(1, +\infty).$$

D'altra parte, usando le definizioni,

$$\begin{aligned} \sum_{n \leq x} \frac{\chi \star \mathbf{1}(n)}{\sqrt{n}} &= \sum_{n \leq x} \frac{1}{\sqrt{n}} \sum_{d \mid n} \chi(d) \overset{k=\frac{n}{d}}{=} \sum_{kd \leq x} \frac{\chi(d)}{\sqrt{kd}} \\ &= \sum_{k \leq \sqrt{x}} \frac{1}{\sqrt{k}} \sum_{\sqrt{x} < d \leq \frac{x}{k}} \frac{\chi(d)}{\sqrt{d}} + \sum_{d \leq \sqrt{x}} \frac{\chi(d)}{\sqrt{d}} \sum_{k \leq \frac{x}{d}} \frac{1}{\sqrt{k}}, \end{aligned}$$

dove lo spezzamento è fatto come nella figura seguente:




Stimiamo separatamente i due contributi. Osserviamo che, per la proposizione 15.4,

$$\sum_{k \leq \sqrt{x}} \frac{1}{\sqrt{k}} \sum_{\sqrt{x} < d \leq \frac{x}{k}} \frac{\chi(d)}{\sqrt{d}} = \mathcal{O}\left( \frac{1}{\sqrt{x}} \sum_{k \leq \sqrt{x}} \frac{1}{\sqrt{k}}, +\infty \right) = \mathcal{O}(1, +\infty).$$

Invece, poiché per il lemma di sommazione parziale di Abel,

$$\sum_{k \leq y} \frac{1}{\sqrt{x}} = \frac{\lfloor y \rfloor}{\sqrt{y}} + \frac{1}{2} \int_1^y \frac{\lfloor u \rfloor}{u^{\frac{3}{2}}} du = 2\sqrt{y} - 1 + \mathcal{O}\left( \frac{1}{\sqrt{y}}, +\infty \right),$$

$$\begin{aligned}\sum_{d\le\sqrt{x}}\frac{\chi(d)}{\sqrt{d}}\sum_{k\le\frac{x}{d}}\frac{1}{\sqrt{k}} &= \sum_{d\le\sqrt{x}}\frac{\chi(d)}{\sqrt{d}}\left(2\sqrt{\frac{x}{d}}-1+\mathcal{O}\left(\sqrt{\frac{d}{x}},+\infty\right)\right)\\ &= 2\sqrt{x}\sum_{d\le\sqrt{x}}\frac{\chi(d)}{d}-\sum_{d\le\sqrt{x}}\frac{\chi(d)}{\sqrt{d}}+\mathcal{O}\left(\frac{1}{\sqrt{x}}\sum_{d\le\sqrt{x}}1,+\infty\right)\\ &= 2\sqrt{x}\mathscr{L}_\chi(1)+\mathcal{O}(1,+\infty),\end{aligned}$$

dove l'ultima uguaglianza è conseguenza della proposizione 15.4. In definitiva

$$\sum_{n\le x}\frac{\chi\star\mathbf{1}(n)}{\sqrt{n}} = 2\sqrt{x}\mathscr{L}_\chi(1)+\mathcal{O}(1,+\infty).$$

Confrontando con quanto ottenuto in precedenza, osserviamo che $\mathscr{L}_\chi(1)$ non può annullarsi: se fosse $\mathscr{L}_\chi(1)=0$, infatti, si dovrebbe avere che il logaritmo è una funzione limitata, per $x\to+\infty$. Infine, se $\chi$ è un carattere non reale,

$$\mathscr{L}_{\overline{\chi}} = \overline{\mathscr{L}}_\chi,$$

quindi se una delle funzioni $\mathscr{L}$ si annullasse in 1, ce ne sarebbero almeno due. Moltiplicandole tutte, si ottiene una funzione che si annulla in 1 (si ha una compensazione della singolarità dovuta al carattere principale), e quindi in un intorno di tale punto tale prodotto avrebbe modulo minore di 1, contraddicendo la proposizione 15.3.

□

## 15.3. Una dimostrazione del teorema di Dirichlet

**Teorema 15.2. (Dirichlet)** *Se $m,n$ sono tali che $1\le m\le n$ e $(m,n)=1$, allora esistono infiniti numeri primi congrui ad $m$ modulo $n$.*

**Dimostrazione**

Per $s>1$,

$$\begin{aligned}\sum_{p\equiv m \mod n}\frac{1}{p^s} &\overset{Pro\ 15.2}{=} \frac{1}{\phi(n)}\sum_{\chi\in\mathbb{D}_n}\overline{\chi}(m)\sum_{p\equiv m \mod n}\frac{\chi(p)}{p^s}\\ &\overset{2}{=} \frac{1}{\phi(n)}\sum_{p\equiv m \mod n}\frac{1}{p^s}+\frac{1}{\phi(n)}\sum_{\substack{\chi\in\mathbb{D}_n\\ \chi\neq\chi_0}}\overline{\chi}(m)\sum_{p\equiv m \mod n}\frac{\chi(p)}{p^s}\\ &\overset{3}{=} \frac{1}{\phi(n)}\sum_{p\in\mathbb{P}}\frac{1}{p^s}+\frac{1}{\phi(n)}\sum_{\substack{\chi\in\mathbb{D}_n\\ \chi\neq\chi_0}}\overline{\chi}(m)\sum_{\substack{p\in\mathbb{P}\\ r\in\mathbb{N}}}\frac{\chi^r(p)}{rp^{rs}}+\mathcal{O}(1,+\infty)\end{aligned}$$

$$= \frac{1}{\phi(n)} \sum_{p \in \mathbb{P}} \frac{1}{p^s} - \frac{1}{\phi(n)} \sum_{\substack{\chi \in \mathbb{D}_n \\ \chi \neq \chi_0}} \overline{\chi}(m) \sum_{p \in \mathbb{P}} \log\left(1 - \frac{\chi(p)}{p^s}\right) + \mathcal{O}(1, +\infty)$$

$$= \frac{1}{\phi(n)} \sum_{p \in \mathbb{P}} \frac{1}{p^s} + \frac{1}{\phi(n)} \sum_{\substack{\chi \in \mathbb{D}_n \\ \chi \neq \chi_0}} \overline{\chi}(m) \log \prod_{p \in \mathbb{P}} \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} + \mathcal{O}(1, +\infty)$$

$$= \frac{1}{\phi(n)} \sum_{p \in \mathbb{P}} \frac{1}{p^s} + \frac{1}{\phi(n)} \sum_{\chi \neq \chi_0} \overline{\chi}(m) \log \mathscr{L}_\chi(s) + \mathcal{O}(1, +\infty).$$

Per il lemma 15.1, la quantità

$$\frac{1}{\phi(n)} \sum_{\chi \neq \chi_0} \overline{\chi}(m) \log \mathscr{L}_\chi(s)$$

è limitata. Quindi,

$$\sum_{p \equiv m \mod n} \frac{1}{p^s} = \frac{1}{\phi(n)} \sum_{p \in \mathbb{P}} \frac{1}{p^s} + \mathcal{O}(1, +\infty).$$

Facendo tendere $s \to 1^+$, il secondo membro diverge: dunque deve divergere anche il primo; in altri termini ci sono infiniti primi congrui a $m$ modulo $n$.

□

[4] Separiamo il carattere principale dal resto.

[3] Aggiungiamo i restanti primi nel primo termine, e una quantità finita nel secondo (poiché $s > 1$); bilanciamo con un $\mathcal{O}(1, +\infty)$.

# APPENDICE A

## Introduzione al problema di Waring

In letteratura il **problema di Waring** è il seguente:

**Teorema A.1. (Hilbert-Waring)**

$$\forall k \geq 2,\ \exists g(k) \in \mathbb{N} \mid \forall n \in \mathbb{N}, \exists x_1, \ldots, x_{g(k)} \in \mathbb{N} \cup \{0\}, n = x_1^k + \cdots + x_{g(k)}^k$$

Questo problema è storicamente precedente al teorema dei quattro quadrati (è del 1770), ma fu chiuso da Hilbert solo nel 1909. Il seguente risultato fornisce un limite inferiore per $g(k)$, dovuto ad Eulero:

**Proposizione A.1.** *Per ogni* $k \geq 2$,

$$g(k) \geq 2^k + \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 2.$$

**Dimostrazione**
Fissiamo $k \geq 2$, e consideriamo l'intero

$$n_k = 2^k \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 1.$$

Osserviamo che $n_k < 3^k$, quindi $n_k$ si potrà scrivere usando solo gli addendi $1, 2^k$. L'addendo $2^k$ può essere usato un numero di volte pari a

$$\left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 1,$$

e il resto, pari a

$$n_k - 2^k \left( \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 1 \right) = 2^k - 1,$$

dovrà essere colmato usando solo addendi 1. In questo modo, per scrivere $n_k$ come somma di potenze $k-$esime se ne usano esattamente

$$\left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 1 + 2^k - 1 = 2^k + \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 2.$$

Di conseguenza,

$$g(k) \geq 2^k + \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 2.$$

□

Osserviamo che ad esempio per $k = 2$, la stima di $g(2)$ è ottimale, per il teorema dei quattro quadrati 3.11. Osserviamo anche che, se anziché $n_k$ avessimo preso, ad esempio,

$$n'_k = 3^k \left\lfloor \left(\frac{4}{3}\right)^k \right\rfloor - 2,$$

avremmo scoperto che

$$g(k) \geq \left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor + \left\lfloor \left(\frac{4}{3}\right)^k \right\rfloor - 2,$$

che è una stima più bassa (ad esempio, per $k = 2$ potremmo dire soltanto che $g(k) \geq 1$): si deduce che le difficoltà maggiori si hanno quando si hanno pochi "pezzi" a disposizione per scrivere come somma di potenze $k-$esime un numero.

Quindi, è maggiormente interessante concentrarsi sul comportamento asintotico del problema di Waring: introduciamo il simbolo $G(k)$ per denotare, dato $k \in \mathbb{N}$, $k \geq 2$, il numero delle potenze $k-$esime necessarie affinché, almeno definitivamente ogni numero intero sia somma di $G(k)$ di esse. Per $k = 2$ non ci sono problemi: per il teorema dei quattro quadrati 3.11, si avrà $G(2) = g(2) = 4$. Invece, si può provare che

**Teorema A.2.** *Valgono i seguenti risultati*

1. **(Linnik, 1943)** $G(3) \leq 7$;
2. **(Davenport, 1939)** $G(4) = 16$.

Hardy e Littlewood misero a punto un metodo, noto come **metodo di Hardy-Littlewood**, utile per affrontare il problema di Waring: presentiamo brevemente le idee alla base di questo metodo.

Sia $n$ il numero naturale che vogliamo rappresentare come somma di potenze $k-$esime. Poniamo $N = \lfloor \sqrt[k]{n} \rfloor$ e, dato $\alpha \in (0, 1)$, poniamo

$$f(\alpha) = \sum_{m=1}^{N} e^{2\pi i \alpha m^k}.$$

Osserviamo che

$$f^s(\alpha) = \sum_{1 \leq m_1, \ldots, m_s \leq N} e^{2\pi i \alpha (m_1^k + \cdots + m_s^k)} = \sum_{m=1}^{sn} R_s(m) e^{2\pi i \alpha m},$$

dove $R_s(m)$ è il numero di rappresentazioni di $m$ come somma di $s$ potenze $k-$esime.

Osserviamo che nessuna delle potenze con cui scriviamo $m$ è maggiore di $n$. Dalla relazione

$$\int_0^1 e^{2\pi i h \alpha} d\alpha = \begin{cases} 1 & \text{se } h = 0 \\ 0 & \text{se } h \neq 0 \end{cases},$$

segue che

$$\int_0^1 f(\alpha)^s e^{-2\pi i \alpha n} d\alpha = R_s(n). \tag{A.1}$$

Fissiamo $\eta \in (0, +\infty)$, e poniamo $P = N^\eta$ : per ogni coppia di interi positivi $a, q$ coprimi, e tale che $1 \leq a < q \leq P$ chiamiamo **arco principale** associato alla coppia $(a, q)$ l'insieme

$$\mathcal{A}_\eta(a, q) = \left\{ \alpha \in (0, 1) \mid \left| \alpha - \frac{a}{q} \right| \leq N^{\eta - k} \right\}.$$

Osserviamo che ogni arco principale è contenuto in $\mathbb{U} = (N^{\eta-k}, 1 + N^{\eta-k}]$. Inoltre, se $\frac{a}{q} \neq \frac{a'}{q'}$, e se $q, q' \leq P$,

$$\left|\frac{a}{q} - \frac{a'}{q'}\right| \geq \frac{1}{qq'} > \left(\frac{1}{q} + \frac{1}{q'}\right) N^{\eta-k}.$$

Quindi, archi principali associati a coppie distinte sono disgiunti. Denotando con $\mathcal{A}$ l'unione di tutti gli archi principali, dall'equazione (A.1) otteniamo

$$R_s(n) = \int_{\mathcal{A}} f(\alpha)^s \exp(-2\pi i \alpha n) d\alpha + \int_{\mathcal{U}-\mathcal{A}} f(\alpha)^s \exp(-2\pi i \alpha n) d\alpha$$

Mediante tecniche analitiche si riescono a dare stime dei due integrali a secondo membro, e quindi di $R_s(n)$.

# APPENDICE B

## Una lista di funzioni aritmetiche

| Nome | | Descrizione | Proprietà |
|---|---|---|---|
| Funzione **1** | $\mathbf{1}: \mathbb{N} \to \{1\}$, $n \mapsto 1$ | | Completamente moltiplicativa |
| Funzione **e** | $\mathbf{e}: \mathbb{N} \to \{0,1\}$, $n \mapsto \begin{cases} 1 & n = 1 \\ 0 & n \geq 2 \end{cases}$ | Elemento neutro del prodotto di Dirichlet | Completamente moltiplicativa |
| Funzione $i^\alpha$ ($\alpha \in \mathbb{C}$) | $i^\alpha: \mathbb{N} \to \mathbb{C}$, $n \mapsto n^\alpha$ | | Completamente moltiplicativa |
| Funzione di Liouville, $\lambda$ | $\lambda: \mathbb{N} \to \{-1,1\}$, $n \mapsto (-1)^{\Omega(n)}$ | | Completamente moltiplicativa |
| Funzione $\chi_4$ | $\chi_4: \mathbb{N} \to \{-1,0,1\}$, $n \mapsto \begin{cases} 0 & \text{se } n \text{ è pari} \\ 1 & \text{se } n \equiv 1 \mod 4 \\ -1 & \text{se } n \equiv 3 \mod 4 \end{cases}$ | | Completamente moltiplicativa |
| Funzione somma dei divisori, $\sigma = i \star \mathbf{1}$ | $\sigma: \mathbb{N} \to \mathbb{N}$, $n \mapsto i \star \mathbf{1}(n) = \sum_{d \mid n} d$ | $\sigma(n)$ è la somma dei divisori di $n$ | Moltiplicativa |
| Funzione somma dei divisori generalizzata, $\sigma_\alpha = i^\alpha \star \mathbf{1}$ ($\alpha \in \mathbb{C}$) | $\sigma_\alpha: \mathbb{N} \to \mathbb{C}$, $n \mapsto i^\alpha \star \mathbf{1}(n) = \sum_{d \mid n} d^\alpha$ | $\sigma_\alpha(n)$ è la somma delle potenze $\alpha-$esime dei divisori di $n$ | Moltiplicativa |
| Funzione $\phi$ di Eulero | $\phi: \mathbb{N} \to \mathbb{N}$, $n \mapsto \sum_{\substack{1 \leq k \leq n \\ (k,n)=1}} 1$ | $\phi(n)$ è il numero di interi positivi compresi tra 1 e $n$, coprimi con $n$ | Moltiplicativa |

| Nome | | Descrizione | Proprietà |
|---|---|---|---|
| Funzione di Dirichlet dei divisori $d = \mathbf{1} \star \mathbf{1}$ | $d: \mathbb{N} \to \mathbb{N}$, $n \mapsto \sum_{d\mid n} 1$ | $d(n)$ è il numero di divisori di $n$ | Moltiplicativa |
| Funzione di Dirichlet dei divisori generalizzata $d_r = \star_{i=1}^{r} \mathbf{1}$ | $d_r: \mathbb{N} \to \mathbb{N}$, $n \mapsto \sum_{d_1 \dots d_r = n} 1$ | $d_r(n)$ è il numero di modi in cui $n$ può essere scritto come prodotto di $r$ interi positivi | Moltiplicativa |
| Funzione $\mu^2$ | $\mu^2: \mathbb{N} \to \{0,1\}$, $n \mapsto \begin{cases} 1 & \text{se } \Omega(n) = \omega(n) \\ 0 & \text{se } \Omega(n) > \omega(n) \end{cases}$ | Funzione indicatrice dell'insieme dei numeri naturali liberi da quadrati | Moltiplicativa |
| Funzione $\mathbf{q} = \lambda \star \mathbf{1}$ | $\mathbf{q}: \mathbb{N} \to \{0,1\}$, $n \mapsto \begin{cases} 1 & \text{se } n \text{ è un quadrato} \\ 0 & \text{se } n \text{ non è un quadrato} \end{cases}$ | Funzione indicatrice dell'insieme $\mathcal{Q}_1$ | Moltiplicativa |
| Funzione $q_k$, $k \in \mathbb{N}$ | $\mathbf{q_k}: \mathbb{N} \to \{0,1\}$, $n \mapsto \begin{cases} 1 & \text{se non esiste } p \in \mathbb{P} \text{ tale che } p^k \mid n \\ 0 & \text{altrimenti} \end{cases}$ | Funzione indicatrice dell'insieme dei numeri naturali che sono divisibili per una potenza $k-$esima. | Moltiplicativa |
| Funzione radicale, $\rho$ | $\rho: \mathbb{N} \to \mathbb{N}$, $n \mapsto \begin{cases} 1 & \text{se } n = 1 \\ \prod_{p\mid n} p & \text{se } n \neq 1 \end{cases}$ | $\rho(n)$ è il più grande divisore di $n$ libero da quadrati | Moltiplicativa |
| Funzione Logaritmo $L$ | $L: \mathbb{N} \to \mathbb{R}$, $n \mapsto \log n$ | | Completamente additiva |
| Funzione $\Omega$ | $\Omega: \mathbb{N} \to \mathbb{N}$, $n \mapsto \begin{cases} 0 & \text{se } n = 1 \\ \sum_{i=1}^{r} a_i & \text{se } n = \prod_{i=1}^{r} p_i^{a_i} \end{cases}$ | $\Omega(n)$ è la somma degli esponenti dei primi che compaiono nella fattorizzazione di $n$ | Completamente additiva |
| Funzione $\omega$ | $\omega: \mathbb{N} \to \mathbb{N}$, $n \mapsto \begin{cases} 0 & \text{se } n = 1 \\ r & \text{se } n = \prod_{i=1}^{r} p_i^{a_i} \end{cases}$ | $\omega(n)$ è il numero di primi che compaiono nella fattorizzazione di $n$ | Additiva |
| Funzione di Möbius $\mu$ | $\mu: \mathbb{N} \to \{-1,0,1\}$, $n \mapsto \begin{cases} 1 & \text{se } n = 1 \\ (-1)^r & \text{se } \Omega(n) = \omega(n) = r \\ 0 & \text{se } \Omega(n) > \omega(n) \end{cases}$ | | Additiva |

| Nome | | Descrizione | Proprietà |
|---|---|---|---|
| Funzione di von Mangoldt, $\Lambda$ | $\Lambda: \mathbb{N} \to \mathbb{N}$<br>$n \mapsto \begin{cases} 0 & \text{se } n = 1 \vee \omega(n) > 2 \\ \log p & \text{se } n = p^a,\ a \geq 1 \end{cases}$ | | Né moltiplicativa, né additiva |
| Funzione $i_{\mathbb{P}} = \omega \star \mu$ | $i_{\mathbb{P}}: \mathbb{N} \to \{0,1\}$<br>$n \mapsto \begin{cases} 1 & \text{se } n \text{ è un primo} \\ 0 & \text{altrimenti} \end{cases}$ | Funzione indicatrice dell'insieme $\mathbb{P}$ | Né moltiplicativa, né additiva |
| Funzione $r$ | $r: \mathbb{N} \to \mathbb{N}$<br>$n \mapsto \lvert\{(x,y) \in \mathbb{Z} \mid x^2 + y^2 = n\}\rvert$ | $r(n)$ è il numero di rappresentazioni di $n$ come somma di due quadrati di due interi | Né moltiplicativa, né additiva |

| Nome | | Descrizione |
|---|---|---|
| Counting function $\pi$ | $\pi: [1,+\infty) \to \mathbb{R}$<br>$x \mapsto \sum_{p \leq x} 1$ | $\pi(x)$ è il numero di primi minori o uguali a $x$ |
| Counting function $\pi_2$ per i primi gemelli | $\pi_2: [1,+\infty) \to \mathbb{R}$<br>$x \mapsto \sum_{\substack{p \leq x \\ p \in \mathbb{P}_2}} 1$ | $\pi_2(x)$ è il numero di primi che compaiono in una coppia di primi gemelli, minori o uguali a $x$ |
| Funzione di Chebychev $\theta$ | $\theta: (0,+\infty) \to \mathbb{R}$<br>$x \mapsto \sum_{p \leq x} \log p$ | $e^{\theta(x)}$ è il prodotto di tutti i numeri primi minori o uguali a $x$ |
| Funzione di Chebychev $\psi$ | $\psi: (0,+\infty) \to \mathbb{R}$<br>$x \mapsto \sum_{k \leq x} \Lambda(k) = \sum_{p^m \leq x} \log p$ | $e^{\psi(x)}$ è il minimo comune multiplo di tutti gli interi positivi minori o uguali a $x$ |

# Bibliografia


[Bom87] E. Bombieri, *Le grand crible dans la théorie analytique des nombres*, Astérisque, vol. 18, Société mathématique de France, 1987.

[Cha68] K. Chandrasekharan, *Introduction to Analytic Number Theory*, Grundlehren der Mathematische Wissenschaften, vol. 148, Springer - Verlag, 1968.

[Cha70] _____, *Arithmetical Functions*, Grundlehren der Mathematische Wissenschaften, vol. 167, Springer, 1970.

[Dav00] H. Davenport, *Multipicative Number Theory*, Graduate Texts in Mathematics, vol. 74, Springer - Verlag, 2000.

[Hua82] L.K. Hua, *Introduction to Number Theory*, Springer, 1982.

[HW08] G.H. Hardy and E.M. Wright, *An introduction to the theory of numbers*, Oxford University Press, 2008.

[Tit51] E.C. Titchmarsh, *The Theory of the Riemann Zeta Function*, Oxford: Clarendon Press, 1951.

[Vau81] R.C. Vaughan, *The Hardy-Littlewood Method*, Cambridge tracts in mathematics, vol. 80, Cambridge University Press, 1981.