ROMA TRE
UNIVERSITÀ DEGLI STUDI

Università degli Studi di Roma Tre

FACOLTÀ DI MATEMATICA

Appunti integrativi

Introduzione alla teoria dei numeri

TN410

Di:
Edoardo Signorini

A.A. 2015–2016, Semestre II

INDICE

1 | DIVISIONE E FATTORIZZAZIONE

1.1 INTRODUZIONE

Notazione. In questo corso l'insieme dei numeri naturali $\mathbb{N}$ è privo dello zero.

Definizione 1.1 – Assioma del buon ordinamento

Sia $S \subset \mathbb{N}$ non vuoto, allora:

$$\exists \min S.$$

Osservazione. Il buon ordinamento è equivalente al seguente assioma: Se $S \subset \mathbb{Z}$ è non vuoto e limitato inferiormente, allora

$$\exists \min S.$$

Teorema 1.2 – Divisione euclidea

Siano $a \in \mathbb{N}, b \in \mathbb{Z}$, allora:

$$\exists! \, q, r \in \mathbb{Z} : b = a\,q + r \text{ e } 0 \leqslant r < a.$$

Dimostrazione. Definiamo il seguente insieme

$$S = \{\, b - s\,a \mid s \in \mathbb{Z} \,\} \subseteq \mathbb{Z}.$$

Sia ora

$$S^+ = S \cap \big(\mathbb{N} \cup \{0\}\big),$$

ovvero

$$S^+ = \{\, b - s\,a \geqslant 0 \mid s \in \mathbb{Z} \,\},$$

per cui $S^+ \subseteq \mathbb{N} \cup \{0\}$. Sicuramente $S^+ \neq \emptyset$, infatti se $b \geqslant 0$ avremo

$$b \in S^+;$$

mentre se $b < 0$ segue

$$b - b\,a = b(1-a) \geqslant 0, \qquad \begin{matrix} b \leqslant 0 \ e \\ (1-a) \leqslant 0 \end{matrix}$$

per cui

$$b - b\,a \in S^+.$$

Quindi, per il buon ordinamento, $\exists\, r = \min S^+$ e supponiamo che

$$r = b - q\,a$$

con $q \in \mathbb{Z}$. Quindi $b = a\,q + r$ con $r \geqslant 0$, in quanto $r \in S^+$. Se per assurdo $r \geqslant a$ si avrebbe

$$r - a \geqslant 0 \iff b - (q+1)a \geqslant 0,$$

ovvero

$$\begin{aligned} b-(q+1)a \in S^+ &\implies b-(q+1)a \geqslant r \\ &\iff r-a \geqslant r \\ &\iff a \leqslant 0, \end{aligned}$$

ma ciò è assurdo in quanto $a \in \mathbb{N}$, per cui

$$0 \leqslant r < a.$$

Resta da mostrare l'uncità, supponiamo quindi che esistano $q', r' \in \mathbb{Z}$ tali che

$$q'a + r' = b = qa + r,$$

ne segue

$$|r' - r| = a\,|q' - q|.$$

Se per assurdo $q' \neq q$ seguirebbe

$$|r' - r| \geqslant a,$$

ma per ipotesi $r, r' < a$, da cui

$$|r' - r| < a.$$

Ciò è assurdo, per cui $q' = q$ e $r' = r$. □

Definizione 1.3 – Massimo comun divisore

Siano $a, b \in \mathbb{N}$ e sia $d \in \mathbb{N}$ tale che:

- $d \mid a, d \mid b$;
- $\exists\, k \in \mathbb{N} : k \mid a, k \mid b \implies k \mid d$.

d si definisce *massimo comun divisore* di a e di b.

Notazione. Il massimo comun divisore fra a e b si indica con (a, b).

Osservazione. Per definizione si pongono

- $(a, 0) = a$;
- se $a, b \in \mathbb{Z}$, $(a, b) = (|a|, |b|)$.

Teorema 1.4 – Unicità del massimo comun divisore

Siano $a, b \in \mathbb{N}$, allora:

$$\exists!\, d = (a, b),$$

e vale l'identità di Bezout, ovvero

$$\exists\, x, y \in \mathbb{Z} : d = ax + by.$$

Dimostrazione. Definiamo il seguente insieme

$$S = \{\, ax + by \mid x, y \in \mathbb{Z} \,\} \cap \mathbb{N}.$$

Sicuramente $S \neq \emptyset$ in quanto $a, b \in S$. Sia quindi $d = \min S$, il quale esiste per il buon ordinamento, per cui

$$\exists\, x, y \in \mathbb{Z} : d = ax + by.$$

Mostriamo che $d = (a, b)$ tramite la divisione euclidea:

$$\exists\, q, r \in \mathbb{Z} : a = d\,q + r,$$

con $0 \leqslant r < d$. Per come abbiamo definito d avremo

$$r = a - d\,q = a(1 - q\,x) + b(-q\,y).$$

Se per assurdo $r > 0$ seguirebbe $r \in S$ che è assurdo per la minimalità di d in S, da cui

$$r = 0 \implies a = d\,q \iff d \mid b.$$

Analogamente si mostra che $d \mid b$. Mostriamo che se $\exists\, k \in \mathbb{N} : k \mid a$ e $k \mid b$ allora $k \mid d$:

$$k \mid a \iff \exists\, \alpha \in \mathbb{Z} : k\,\alpha = a,$$
$$k \mid b \iff \exists\, \beta \in \mathbb{Z} : k\,\beta = b,$$

da cui

$$d = a\,x + b\,y = k(\alpha\,x + \beta\,y),$$

ovvero

$$k \mid d.$$

Infine l'unicità segue banalmente dall'ultima proprietà, infatti se esistesse $d' \in \mathbb{N}$ che soddisfa le ipotesi del teorema si avrebbe

$$d \mid d' \text{ e } d' \mid d,$$

ovvero

$$d' = d.$$ □

Proposizione 1.5 – Algoritmo di Euclide

Dati $a, b \in \mathbb{N}$, siano $q_1, \ldots, q_{n+1}$ e $r_1, \ldots, r_n \in \mathbb{Z}$ tali che:

- $r_1 > r_2 > \cdots > r_n \geqslant 0$;
- $b = a\,q_1 + r_1$,
  $a = r_1 q_2 + r_2$,
  $r_1 = r_2 q_3 + r_3$,
  $\ldots$
  $r_{n-2} = r_{n-1} q_n + r_n$,
  $r_{n-1} = r_n q_{n+1} + 0$.

Allora

$$r_n = (a, b).$$

Dimostrazione. Mostriamo che se $a = b\,q + r$ con $0 \leqslant r < b$, allora

$$(a, b) = (b, r).$$

Per definizione

$$(a, b) \mid a, b,$$

per cui (a, b) dividerà ogni combinazione lineare di a, b, in particolare

$$(a, b) \mid a - b\,q = r,$$

per cui $(a, b) \mid b, r$, ovvero

$$(a, b) \mid (b, r).$$

Viceversa

$$(b, r) \mid b, r \implies (b, r) \mid b\,q + r = a,$$

ovvero

$$(b, r) \mid (a, b).$$

Applicando tale osservazione al nostro caso otteniamo

$$\begin{aligned}(a, b) &= (b, r_1)\\ &= (r_1, r_2)\\ &= \dots\\ &= (r_{n-1}, r_n),\end{aligned}$$

ma $r_{n-1} = r_n\, q_{n+1}$ per cui

$$(r_{n-1}, r_n) = r_n.$$

□

Osservazione. L'algoritmo di Euclide ci fornisce anche un metodo pratico per trovare l'identità di Bezout, infatti $\forall\, j = 0, \dots, n$ avremo

$$r_j = x_j a + y_j b, \text{ con } x_j, y_j \in \mathbb{Z}.$$

Infatti, sfruttando le equazioni dell'algoritmo di Euclide, avremo

$$\begin{aligned}r_0 = a &\implies (x_0, y_0) = (1, 0);\\ r_1 = -q_1 a + b &\implies (x_1, y_1) = (-q_1, 1),\end{aligned}$$

più in generale

$$\begin{aligned}r_j &= r_{j-2} - q_j r_{j-1}\\ &= (x_{j-2} a + y_{j-2} b) - q_j (x_{j-1} a + y_{j-1} b)\\ &= (x_{j-2} - q_j x_{j-1}) a + (y_{j-2} - q_j y_{j-1}) b.\end{aligned}$$

Quindi

$$\begin{cases} x_0 = 1 \\ y_0 = 0 \end{cases}, \begin{cases} x_1 = -q_1 \\ y_1 = 1 \end{cases} \text{ e } \begin{cases} x_j = x_{j-2} - q_j x_{j-1} \\ y_j = y_{j-2} - q_j y_{j-1} \end{cases}.$$

Esempio. Calcoliamo $(5111, 589)$ tramite l'algoritmo di Euclide:

$$\begin{aligned}5111 &= 8 \cdot 589 + 399,\\ 589 &= 1 \cdot 399 + 190,\\ 399 &= 2 \cdot 190 + 19,\\ 190 &= 10 \cdot 19 + 0.\end{aligned}$$

Per cui

$$(5111, 589) = 19.$$

Proposizione 1.6 – Divisore del prodotto di coprimi

Siano $a, b \in \mathbb{N}$ tali che $(a, b) = 1$. Sia $w \in \mathbb{N}$ tale che $w \mid a\, b$, allora: esistono unici $u, v \in \mathbb{N}$ tali che

- $w = u\, v$;
- $u \mid a, v \mid b$.

Dimostrazione. Poniamo $u = (a, w)$ e $v = (b, w)$, dobbiamo verificare che $u \mid a, v \mid b, u\, v = w$ e che u, v siano unici:

- Per definizione u è il massimo comun divisore di a e w, in particolare risulterà essere divisore di a.
- Analogamente v è un divisore di b.
- Per il teorema 1.4 sappiamo che

$$\begin{aligned} u = (a, w) &\implies u = x_1 a + y_1 w; \\ v = (b, w) &\implies v = x_2 b + y_2 w, \end{aligned}$$

quindi

$$\begin{aligned} u v &= a\, b\, x_1 x_2 + w(y_1 x_2 b + x_1 y_1 a + y_1 y_2 w) \\ &= w K, \text{ con } K \in \mathbb{Z}, \end{aligned} \qquad w \mid a\, b$$

ovvero $w \mid u v$. D'altronde $1 = x\, a + y\, b$, ovvero

$$\begin{aligned} w &= x\, w\, a + y\, w\, b \\ &= (w, a)(w, b) S, \text{ con } S \in \mathbb{Z}, \end{aligned}$$

in quanto $x\, w\, a$ è multiplo di (w, b) e $y\, w\, b$ è multiplo di (w, a), per cui $u v \mid w$, ovvero

$$u v = w.$$

- Supponiamo che u', v' siano altri due interi che soddisfano la tesi, in particolare avremo $u' v' = w$, inoltre $u' \mid a$ e $u' \mid w$, da cui

$$u' \mid (a, w) = u.$$

Se per assurdo $u' \neq (a, w)$ si avrebbe $u' < (a, w)$ e, per ragionamenti analoghi ai precedenti, $v' \leqslant (b, w)$, da cui

$$\begin{aligned} w &= u' v' \\ &< (a, w)(b, w) \\ &= w, \end{aligned}$$

ma ciò è assurdo, quindi $u' = (a, w) = u$. Analogamente si mostra che $v' = v$. □

Osservazione. Se poniamo $\mathcal{D}(n) = \{\, d \in \mathbb{N} : d \mid n \,\}$, allora, se prendiamo $a, b \in \mathbb{N}$ tali che $(a, b) = 1$, avremo

$$\mathcal{D}(a) \times \mathcal{D}(b) \longleftrightarrow \mathcal{D}(a\, b),$$

dove la corrispondenza biunivoca è determinata da

$$(u, v) \mapsto u v,$$

che è biiettiva per la proposizione.

1.2 PRIMI

Definizione 1.7 – Insieme dei divisori

Si definisce *l'insieme dei divisori* di $n \in \mathbb{N}$ come l'insieme dei naturali che dividono n, ovvero

$$\mathcal{D}(n) = \{\, d \in \mathbb{N} : d \mid n \,\}.$$

Definizione 1.8 – Primo

Un naturale $n \in \mathbb{N}$ si definisce *primo* se

$$\left|\mathcal{D}(n)\right| = 2.$$

Osservazione. 1 non è primo in quanto $\left|\mathcal{D}(1)\right| = 1$.

Teorema 1.9 – Divisore primo

Siano $a, b \in \mathbb{N}$ e sia p primo, allora:

$$p \mid a\,b \implies p \mid a \text{ oppure } p \mid b.$$

Dimostrazione. Supponiamo che $p \nmid a$, per la primalità di p avremo che $p \neq a$, quindi

$$(a, p) = 1,$$

per cui esistono $x, y \in \mathbb{Z}$ tali che $1 = x\,a + y\,p$, da cui

$$\begin{aligned} b &= a\,b\,x + y\,b\,p \\ &= p\,N, \text{ con } N \in \mathbb{Z}, \end{aligned}$$

ovvero $p \mid b$. □

Proposizione 1.10 – Divisore primo per una succcessione

Siano $a_1, \ldots, a_n \in \mathbb{N}$ e sia p primo, allora:

$$p \mid a_1 \cdot \ldots \cdot a_k \implies \exists\, j = 1, \ldots, n : p \mid a_j.$$

Dimostrazione. Basta applicare iterativamente il teorema 1.9, infatti

$$p \mid a_1 \cdot \ldots \cdot a_k \implies p \mid a_1 \text{ oppure } p \mid a_2 \cdot \ldots \cdot a_k,$$

se $p \nmid a_1$ avremo di conseguenza

$$p \mid a_2 \text{ oppure } p \mid a_3 \cdot \ldots \cdot a_k.$$

Iterando il procedimento di arriva alla tesi. □

Teorema 1.11 – Teorema fondamentale dell'aritmetica

Sia $n \in \mathbb{N}$ tale che $n > 1$, allora esistono unici, a meno dell'ordine, $p_1, \ldots, p_r$ primi tali che

$$n = p_1 \cdot \ldots \cdot p_r.$$

Dimostrazione. Dimostriamolo per ampia induzione su n:

- Se $n = 2$ soddisfa banalmente la tesi in quanto 2 è primo e si scrive unicamente come se stesso, in quanto non ha altri divisori primi.
- Supponiamo che, comunque preso $2 < m < n$, esso sia prodotto di numeri primi. Se n è primo non ho nulla da dimostrare, supponiamo quindi che non lo sia.

n non primo ammette un divisore non banale, ovvero esiste $1 < n_1 < n$ tale che $n_1 \mid n$. Poniamo quindi $n_2 = \frac{n}{n_1}$, di conseguenza $1 < n_2 < n$ e

$$n = n_1 n_2.$$

Per induzione avremo

$$n_1 = p_1 \cdot \ldots \cdot p_r;$$
$$n_2 = p_1' \cdot \ldots \cdot p_r',$$

da cui

$$n = p_1 \cdot \ldots \cdot p_r p_1' \cdot \ldots \cdot p_r'.$$

Per dimostrare l'unicità, supponiamo che

$$q_1 \cdot \ldots \cdot q_s = n = p_1 \cdot \ldots \cdot p_r,$$

dove

$$q_1 \leqslant q_2 \leqslant \cdots \leqslant q_s;$$
$$p_1 \leqslant p_2 \leqslant \cdots \leqslant p_r.$$

Voglio mostrare che $r = s$ e che $q_j = p_j$. Ora, per la proposizione 1.10, $q_1 \mid p_1 \cdot \ldots \cdot p_r$ implica

$$\exists\, j : q_1 \mid p_j \implies q_1 = p_j,$$

in quanto entrambi primi. Analogamente si mostra che

$$\exists\, i : p_1 \mid q_i \implies p_1 = q_i.$$

Per cui

$$p_1 \leqslant p_j = q_1 \leqslant q_i = p_1,$$

ovvero $p_1 = q_1$, da cui

$$q_2 \cdot \ldots \cdot q_s = p_2 \cdot \ldots \cdot p_r.$$

Iterando ottengo $s = r$ e $p_i = q_j$. □

Teorema 1.12 – Equivalente del teorema fondamentale dell'aritmetica

Sia $n \in \mathbb{N}$ tale che $n > 1$, allora esistono unici $p_1, \ldots, p_r$ primi distinti e $m_1, \ldots, m_r \in \mathbb{N}$ tali che

$$n = p_1^{m_1} \cdot \ldots \cdot p_r^{m_r},$$

con $p_1 < \cdots < p_r$.

Dimostrazione. Segue immediatamente dal teorema fondamentale dell'aritmetica. □

1.3 PROPRIETÀ ELEMENTARI DEI PRIMI

Teorema 1.13 – Cardinalità dell'insieme dei numeri primi

Esistono infiniti numeri primi.

Dimostrazione. Sia $p_1 = 2$ e supponiamo per assurdo che $p_1, \ldots, p_s$ siano tutti i numeri

primi. Sia ora

$$N = p_1 \cdot \ldots \cdot p_s + 1 \in \mathbb{N}.$$

Osserviamo che

$$(N, p_j) = 1, \forall\, j = 1, \ldots, s,$$

in quanto

$$1 = p_j \frac{1 - N}{p_j} + N.$$

Ora, per il teorema fondamentale dell'aritmetica, avremo

$$N = q_1^{m_1} \cdot \ldots \cdot q_r^{m_r},$$

dove $q_1, \ldots, q_r$ sono primi, ma, per quanto osservato a proposito di (N, p_j), avremo che

$$\{q_1, \ldots, q_r\} \cap \{p_1, \ldots, p_s\} = \emptyset,$$

ma ciò è assurdo, in quanto avevamo supposto che non vi fossero altri numeri primi. □

Osservazione. Esistono numerose dimostrazioni alternative di questo teorema, un'altra strategia è la seguente: consideriamo la seguente sequnza di interi

$$(a_n)_{n \in \mathbb{N}} \subseteq \mathbb{N}^{>1},$$

tale che

$$(a_n, a_m) = 1, \forall\, n > m.$$

Allora, se $(l_n)_{n \in \mathbb{N}}$ è una sequenza di numeri primi tali che

$$l_k \mid a_k,$$

si ha che $\{l_k\}$ sono tutti distinti e sono infiniti.

Esempio. Costruiamo la sequenza a_n come segue:

$$\begin{aligned}
a_1 &= 2,\\
a_2 &= 2 + 1 = 3,\\
a_3 &= 2 \cdot 3 + 1 = 7,\\
a_4 &= 2 \cdot 3 \cdot 7 + 1 = 43,\\
a_5 &= 2 \cdot 3 \cdot 7 \cdot 43 + 1 = 1807,\\
&\ldots\\
a_n &= (a_{n-1} - 1)a_{n-1} + 1,
\end{aligned}$$

allora a_n soddisfa il criterio.

Esempio. Mostriamo che la sequenza $(2^{2^k} + 1)_{k \in \mathbb{N}}$ soddisfa il criterio. Per farlo, verifichiamo che

$$2^{2^n} - 1 = 3 \prod_{j=1}^{n-1} 2^{2^j} + 1,$$

è sufficiente sviluppare $2^{2^n}-1$ come differenza di quadrati:

$$\begin{aligned} 2^{2^n}-1 &= (2^{2^{n-1}}+1)(2^{2^{n-1}}-1) \\ &= (2^{2^{n-1}}+1)(2^{2^{n-2}}+1)(2^{2^{n-2}}-1) \\ &= \left(\prod_{j=1}^{n-1} 2^{2^j}+1\right)(2^2-1) \\ &= 3\prod_{j=1}^{n-1} 2^{2^j}+1. \end{aligned}$$

Affinchè il criterio sia valido, dobbiamo mostrare che tutti gli elementi della sequnza sono coprimi. Se per assurdo

$$p \mid (2^{2^k}+1, 2^{2^j}+1), \text{ con } k<t,$$

allora, in particolare, $p \mid (2^{2^k}+1)$ e, per linearità, dividerebbe anche ogni suo multiplo, da cui

$$p \mid 3\prod_{j=1}^{t-1} 2^{2^j}+1.$$

Ma, per quanto mostrato

$$3\prod_{j=1}^{t-1} 2^{2^j}+1 = 2^{2^t}-1,$$

ovvero

$$p \mid (2^{2^t}-1).$$

Quindi, ancora per linearità

$$p \mid (2^{2^t}+1)-(2^{2^t}-1) = 2,$$

da cui, per la primalità di p, segue $p=2$. Ma ciò è assurdo in quanto $p \mid 2^{2^k}+1$ che è dispari. Quindi la successione soddisfa il criterio.

1.4 ALCUNI RISULTATI E PROBLEMI SUI PRIMI

Definizione 1.14 – Funzione enumerativa dei primi

Si definisce *funzione enumerativa dei primi* l'applicazione che associa ad ogni numero naturale n il numero dei primi non superiori ad n, ovvero

$$\pi(n) = \left|\{p \leqslant n\}\right|.$$

Esempio. Alcuni valori della funzione π:

- $\pi(1) = 0$;
- $\pi(2) = 1$;
- $\pi(100) = 25$.

Teorema 1.15 – Teorema dei numeri primi

Sia π la funzione enumerativa dei numeri primi, allora:

$$\pi(x) \sim \frac{x}{\ln x}.$$

Dimostrazione. Si rimanda ad un corso superiore di teoria dei numeri. □

Osservazione. La dimostrazione sfrutta l'anialisi complessa attraverso lo studio della funzione zeta di Riemann

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

la quale è una funzione differenziabile (olomorfa) nella regione

$$\{ s \in \mathbb{C} \mid \Re(s) > 1 \} \subseteq \mathbb{C}.$$

Proposizione 1.16 – Stima della funzione enumerativa dei numeri primi

Sia π la funzione enumerativa dei numeri primi, allora:

$$\pi(x) \geqslant \log_2(\log_2 x) - 1,$$

per $x \geqslant 2$.

Dimostrazione. Sia $k = \max\{j : 2^{2^j} + 1 \leqslant x\}$, mostriamo che

$$\pi(x) \geqslant k.$$

Infatti

$$[1, x] \cap \{2^{2^j} + 1 : j \in \mathbb{N}\} = \{5, 17, \ldots, 2^{2^k} + 1\},$$

ovvero

$$\#\left([1, x] \cap \{2^{2^j} + 1 : j \in \mathbb{N}\}\right) = k,$$

da cui

$$\pi(x) = \#\{p \text{ primo } : p \leqslant x\} \geqslant \#\left([1, x] \cap \{2^{2^j} + 1 : j \in \mathbb{N}\}\right) = k.$$

Infine, per ipotesi, $2^{2^{k+1}} + 1 > x$ da cui $2^{2^{k+1}} \geqslant x$, ovvero

$$k + 1 \geqslant \log_2(\log_2 x),$$

quindi

$$\pi(x) \geqslant k \geqslant \log_2(\log_2 x) - 1.$$

□

Teorema 1.17 – di Gauss

Sia π la funzione enumerativa dei numeri primi, allora:

$$\pi(x) \sim \operatorname{li}(x) := \int_1^x \frac{dt}{\ln t}.$$

Dimostrazione. Applichiamo il teorema dei numeri primi (1.13), mostrando che

$$\mathrm{li}(x) \sim \frac{x}{\ln x}.$$

Sviluppiamo $\mathrm{li}(x)$ per parti, escludendo l'intervallo $(1,2)$ per evitare che l'integrale sia improprio,

$$\begin{aligned}\int_2^x \frac{dt}{\ln t} &= \frac{t}{\ln t}\Big|_2^x + \int_2^x \frac{dt}{\ln^2 t} \\ &= \frac{x}{\ln x} - \frac{2}{\ln 2} + \int_2^x \frac{dt}{\ln^2 t}.\end{aligned}$$

Osserviamo che

$$\begin{aligned}\int_2^x \frac{dt}{\ln^2 t} &= \int_2^{\sqrt{x}} \frac{dt}{\ln^2 t} + \int_{\sqrt{x}}^x \frac{dt}{\ln^2 t} \\ &\leqslant \sqrt{x} + \frac{x}{\ln^2 \sqrt{x}} \\ &\leqslant 6\frac{x}{\ln^2 x}. \qquad \textit{per } x \textit{ grande}\end{aligned}$$

per cui

$$\mathrm{li}(x) = \frac{x}{\ln x} + E(x), \text{ con } \big|E(x)\big| \leqslant 6\frac{x}{\ln^2 x}.$$

Ora

$$\lim_{x\to 0} \frac{\big|E(x)\big|}{\frac{x}{\ln x}} = 0,$$

da cui

$$\mathrm{li}(x) \sim \frac{x}{\ln x}.$$

□

Teorema 1.18 – di Chebičev

Sia p la funzione enumerativa dei numeri primi, allora:

$$\exists\, c_1, c_2 \in \mathbb{R}^+ : c_1\frac{x}{\ln x} \leqslant \pi(x) \leqslant c_2\frac{x}{\ln x},$$

con $0 < c_1 < 1 < c_2$ e $x \geqslant 2$.

Dimostrazione. A pagina 93. □

Osservazione. Chebičev dimostrò questo teorema in modo elementare, senza l'utilizzo dell'analisi complessa.

1.5 LA FUNZIONE PARTE INTERA

Definizione 1.19 – Parte intera

Si definisce *parte intera* di $\alpha \in \mathbb{R}$ come il più grande intero minore di α, ovvero

$$[\alpha] = \max\{m \in \mathbb{Z} : m \leqslant \alpha\}.$$

Osservazione. Analogamente si può definire $[\alpha]$ come l'unico intero $m \in \mathbb{Z}$ tale che

$$m \leqslant \alpha < m + 1.$$

Esempio. Consideriamo π, avremo

$$[\pi] = 3,$$
$$[-\pi] = -4.$$

Proprietà 1.20.

$$\alpha - 1 < [\alpha] \leqslant \alpha.$$

Dimostrazione. Dalla definizione sappiamo che

$$[\alpha] \leqslant \alpha < [\alpha] + 1,$$

da cui

$$0 \leqslant \alpha - [\alpha] < 1 \iff -\alpha \leqslant -[\alpha] < 1 - \alpha,$$

ovvero

$$\alpha - 1 < [\alpha] \leqslant \alpha.$$

□

Proprietà 1.21. Se $\alpha \geqslant 0$, allora

$$[\alpha] = \sum_{\substack{n \in \mathbb{N} \\ n \leqslant \alpha}} 1.$$

Dimostrazione. Osserviamo che

$$\sum_{\substack{n \in \mathbb{N} \\ n \leqslant \alpha}} 1 = \#\big(\mathbb{N} \cap [0, \alpha]\big),$$

ma per definizione $[\alpha] = \max\{m \in \mathbb{Z} : m \leqslant \alpha\}$, da cui

$$[\alpha] = \#\big(\mathbb{N} \cap [0, \alpha]\big).$$

□

Proprietà 1.22. Se $n \in \mathbb{Z}$, allora

$$[\alpha + n] = [\alpha] + n.$$

Dimostrazione. Per definizione $[\alpha]$ è l'unico intero tale che

$$[\alpha] \leqslant \alpha < [\alpha] + 1,$$

da cui

$$[\alpha] + n \leqslant \alpha + n < [\alpha] + n + 1,$$

ovvero

$$[\alpha + n] = [\alpha] + n.$$

□

Proprietà 1.23.

$$[\alpha] + [\beta] \leqslant [\alpha + \beta] \leqslant [\alpha] + [\beta] + 1.$$

Dimostrazione. Sappiamo che $[\alpha] \leqslant \alpha$ e $[\beta] \leqslant \beta$, da cui

$$[\alpha] + [\beta] \leqslant \alpha + \beta,$$

d'altronde, $[\alpha + \beta]$ è il più grande intero minore di $\alpha + \beta$, e chiaramente $[\alpha] + [\beta]$ è un intero, per cui

$$[\alpha] + [\beta] \leqslant [\alpha + \beta].$$

Infine

$$\begin{aligned}[\alpha + \beta] &= \big[[\alpha] + [\beta] + \alpha - [\alpha] + \beta - [\beta]\big] \\ &\overset{(P.3)}{=} [\alpha] + [\beta] + \big[\alpha - [\alpha] + \beta - [\beta]\big],\end{aligned}$$

dove, per la proprietà 1, avremo

$$0 \leqslant \alpha - [\alpha], \beta - [\beta] < 1,$$

per cui

$$0 \leqslant \alpha - [\alpha] + \beta - [\beta] < 2 \implies \big[\alpha - [\alpha] + \beta - [\beta]\big] \leqslant 1,$$

ovvero

$$[\alpha + \beta] \leqslant [\alpha] + [\beta] + 1.$$

□

Proprietà 1.24.

$$[\alpha] + [-\alpha] = \begin{cases} 0 & \alpha \in \mathbb{Z} \\ -1 & \alpha \notin \mathbb{Z} \end{cases}$$

Dimostrazione. Se $\alpha \in \mathbb{Z}$, ovviamente $[\alpha] = \alpha$ e $[-\alpha] = -\alpha$, per cui

$$[\alpha] + [-\alpha] = 0.$$

Se $\alpha \notin \mathbb{Z}$, per definizione $[\alpha] \leqslant \alpha < [\alpha] + 1$, ma, dal momento che $[\alpha] \neq \alpha$, avremo

$$[\alpha] < \alpha < [\alpha] + 1,$$

ed analogamente $[-\alpha] < -\alpha < [-\alpha] + 1$. Sommando membro a membro otteniamo

$$[\alpha] + [-\alpha] < 0 < [\alpha] + [-\alpha] + 2,$$

ovvero

$$[\alpha] + [-\alpha] < 0 \wedge [\alpha] + [-\alpha] > -2,$$

quindi, dal momento che $[\alpha] + [-\alpha] \in \mathbb{Z}$,

$$[\alpha] + [-\alpha] = -1.$$

□

Proprietà 1.25.

$$-[-\alpha] = \min\{k \in \mathbb{Z} : k \geqslant \alpha\}.$$

Dimostrazione. Basta applicare la definizione di parte intera al contrario, sappiamo infatti che $[\alpha] = \max\{m \in \mathbb{Z} : m \leqslant \alpha\}$ è l'unico intero x tale che $x \leqslant \alpha < x + 1$, analogamente

avremo che $y = \min\{k \in \mathbb{Z} : k \geqslant \alpha\}$ è l'unico intero tale che

$$y - 1 < \alpha \leqslant y.$$

Ci basta quindi verificare che $-[-\alpha]$ soddisfa tale disuguaglianza, ma ciò discende proprio dalla definzione di parte intera di $-\alpha$, infatti

$$-[-\alpha] - 1 < \alpha \leqslant -[-\alpha] \iff [-\alpha] \leqslant -\alpha < [-\alpha] + 1,$$

ovvero

$$-[-\alpha] = \min\{k \in \mathbb{Z} : k \geqslant \alpha\}.$$

□

Proprietà 1.26.

$$\left[\frac{[\alpha]}{n}\right] = \left[\frac{\alpha}{n}\right].$$

Dimostrazione. Sia $m \in \mathbb{Z}$, per definizione $[\alpha] = \max\{k \in \mathbb{Z} : k \leqslant \alpha\}$, per cui $m = [\alpha]$ se e soltanto se $m \leqslant \alpha$ e, preso $k \in \mathbb{Z}$, si ha $k \leqslant a \iff k \leqslant m$.
Ora

$$\left[\frac{[\alpha]}{n}\right] \leqslant \frac{[\alpha]}{n} \leqslant \frac{\alpha}{n},$$

quindi, dal momento che la parte intera di $\frac{\alpha}{n}$ è $\left[\frac{\alpha}{n}\right]$, si avrà

$$\left[\frac{[\alpha]}{n}\right] \leqslant \left[\frac{\alpha}{n}\right].$$

Sia ora $k \in \mathbb{Z}$, avremo

$$\begin{aligned} k \leqslant \left[\frac{[\alpha]}{n}\right] &\iff k \leqslant \frac{\alpha}{n} \\ &\iff nk \leqslant [\alpha] \\ &\iff nk \leqslant \alpha \\ &\iff k \leqslant \frac{a}{n} \\ &\iff k \leqslant \left[\frac{\alpha}{n}\right], \end{aligned}$$

da cui, per l'osservazione iniziale, si ottiene la tesi. □

Proprietà 1.27.

$$\left[\alpha + \frac{1}{2}\right] = \begin{cases} [\alpha] & \text{se } \{\alpha\} < \frac{1}{2} \\ [\alpha] + 1 & \text{se } \{\alpha\} \geqslant \frac{1}{2} \end{cases}$$

Dimostrazione. Ricordiamo che $\{x\} = x - [x]$. Se $\{\alpha\} < \frac{1}{2}$, allora, per la proprietà 1,

$$\begin{aligned} 0 \leqslant \alpha - [\alpha] < \frac{1}{2} &\iff 0 \leqslant \alpha - [\alpha] + \frac{1}{2} < 1 \\ &\iff [\alpha] \leqslant \alpha + \frac{1}{2} < [\alpha] + 1, \end{aligned}$$

ovvero

$$\left[\alpha + \frac{1}{2}\right] = [\alpha].$$

Analogamente, se $\{\alpha\} \geqslant \frac{1}{2}$, avremo

$$\begin{aligned} \frac{1}{2} \leqslant \alpha - [\alpha] < 1 &\iff 1 \leqslant \alpha - [\alpha] + \frac{1}{2} < \frac{3}{2} \\ &\iff 1 \leqslant \alpha - [\alpha] + \frac{1}{2} < 2 \\ &\iff [\alpha] + 1 \leqslant \alpha + \frac{1}{2} < [\alpha] + 1 + 1, \end{aligned}$$

ovvero

$$\left[\alpha + \frac{1}{2}\right] = [\alpha] + 1.$$

□

Proprietà 1.28.

$$\left[\frac{\alpha}{n}\right] = \sum_{\substack{m \in \mathbb{N} \\ m \leqslant \alpha \\ n \mid m}} 1.$$

Dimostrazione. Osserviamo che

$$\sum_{\substack{m \in \mathbb{N} \\ m \leqslant \alpha \\ n \mid m}} 1 = \#\{\, m \in \mathbb{N} : m \leqslant \alpha, n \mid m \,\},$$

ovvero

$$\#\left\{\, t \in \mathbb{N} : t \leqslant \frac{\alpha}{m} \,\right\},$$

quindi, applicando la proprietà 2, si giunge alla tesi. □

Definizione 1.29 – Valutazione p-adica

Siano p un primo ed $n \in \mathbb{N}$, si definisce *valutazione p-adica* $\nu_p(n)$ di n come il massimo intero non negativo tale che

$$p^{\nu_p(n)} \mid n, \text{ ma } p^{\nu_p(n)+1} \nmid n.$$

Osservazione. Se $n = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$, allora

$$\nu_{p_j}(n) = \alpha_j,$$

mentre, se $p \nmid n$, allora

$$\nu_p(n) = 0.$$

Teorema 1.30 – Valutazione p-adica del fattoriale

Siano p primo ed $n \in \mathbb{N}$, allora

$$\nu_p(n!) = \sum_{j=1}^{\infty} \left[\frac{n}{p^j}\right].$$

Dimostrazione. Osserviamo che

$$\nu_p(n!) = \sum_{k=1}^{n} \nu_p(k),$$

infatti

$$\nu_p(a\,b) = \nu_p(a)\nu_p(b).$$

Quindi

$$\nu_p(n!) = \sum_{k=1}^{n} \nu_p(k) = \sum_{k=1}^{n} \sum_{\substack{j=1 \\ p^j \mid n}}^{\infty} 1,$$

ciò in quanto, se $k = p_1^{\alpha_1} \cdot \ldots \cdot p^{\alpha} \cdot \ldots \cdot p_s^{\alpha_s}$, si ha

$$\nu_p(k) = \alpha = \#\left\{ j \in \mathbb{N} : p^j \mid k \right\}.$$

Per cui

$$\begin{aligned} \nu_p(n!) &= \sum_{k=1}^{n} \sum_{\substack{j=1 \\ p^j \mid n}}^{\infty} 1 \\ &= \sum_{j=1}^{\infty} \sum_{\substack{k=1 \\ p^j \mid k}}^{n} 1 \\ &\overset{(P.9)}{=} \sum_{j=1}^{\infty} \left[\frac{n}{p^j} \right]. \end{aligned}$$

□

2 FUNZIONI ARITMETICHE

2.1 INTRODUZIONE

Definizione 2.1 – Funzione aritmetica

Una *funzione aritmetica* è un'applicazione

$$f\colon \mathbb{N} \to \mathbb{C}.$$

Definizione 2.2 – Funzione moltiplicativa

Una funzione aritmetica si dice *moltiplicativa*, se

$$f(n\,m) = f(n)f(m),\ \forall\ n, m \in \mathbb{N} : (n, m) = 1.$$

Definizione 2.3 – Funzione totalmente moltiplicativa

Una funzione aritmetica si dice *totalmente moltiplicativa*, se

$$f(n\,m) = f(n)f(m),\ \forall\ n, m \in \mathbb{N}.$$

Esempio.

- $f(n) = n^k$ è una funzione totalmente moltiplicativa.
- $f(n) = 1$ è una funzione totalmente moltiplicativa.
- $f(n) = \ln n$ non è una funzione moltiplicativa.
- $d(n) = \#\{\, d \in \mathbb{N} : d \mid n \,\}$ è una funzione moltiplicativa, ma non totalmente, infatti
$$d(p^2) = 3 \neq d(p)d(p) = 2 \cdot 2 = 4.$$
- $\sigma(n)$, che è la somma dei divisori di n, è una funzione moltiplicativa, ma non totalmente, infatti
$$\sigma(p^2) = 1 + p + p^2 \neq \sigma(p)\sigma(p) = 1 + 2p + p^2.$$

Definizione 2.4 – Trasformata di Dirichlet

Sia f una funzione aritmetica, si definisce *trasformata di Dirichlet* di f la seguente funzione

$$g(n) = \sum_{d \mid n} f(d).$$

Teorema 2.5 – La trasformata di Dirichlet è moltiplicativa

Sia f una funzione moltiplicativa. Allora la trasformata di Dirichlet g di f è moltiplicativa.

Dimostrazione. Per l'osservazione del teorema 1.9, sappiamo che, presi $n, m \in \mathbb{N}$ con $(n, m) = 1$, si ha una corrispondenza biunivoca

$$\mathcal{D}(n) \times \mathcal{D}(m) \longleftrightarrow \mathcal{D}(n\,m),$$

tramite l'applicazione $(u, v) \mapsto u\,v$.
Vogliamo mostrare che

$$g(n) = \sum_{d|n} f(d),$$

è moltiplicativa, cioè che $g(n\,m) = g(n)g(m)$ se $(n, m) = 1$. Ora

$$\begin{aligned} g(n\,m) &= \sum_{d|n\,m} f(d) \\ &= \sum_{d\in\mathcal{D}(n\,m)} f(d) \\ &= \sum_{(u,v)\in\mathcal{D}(n)\times\mathcal{D}(m)} f(u\,v), \end{aligned}$$

ma $(n, m) = 1$, quindi $(u, v) = 1$, ovvero

$$f(u\,v) = f(u)f(v),$$

per la molteplicità di f. Per cui

$$\begin{aligned} \sum_{(u,v)\in\mathcal{D}(n)\times\mathcal{D}(m)} f(u\,v) &= \sum_{u\in\mathcal{D}(n)} \sum_{v\in\mathcal{D}(m)} f(u)f(v) \\ &= \sum_{u\in\mathcal{D}(n)} f(u) \sum_{v\in\mathcal{D}(m)} f(v) \\ &= g(n)g(m). \end{aligned}$$

□

Corollario. La funzione

$$d(n) = \#\{\, d \in \mathbb{N} : d \mid n \,\},$$

è moltiplicativa.

Dimostrazione. Dalla definizione di d segue che

$$d(n) = \sum_{d|n} 1,$$

ovvero d è la trasformata di Dirichlet della funzione $(n) = 1$, la quale è banalmente moltiplicativa. □

Corollario. La funzione $\sigma(n)$, somma dei divisori di n, è moltiplicativa.

Dimostrazione. Dalla definizione di σ segue che

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

ovver σ è la trasformata di Dirichlet della funzione identità $\mathrm{id}(n) = n$, che è moltiplicativa. □

Osservazione. Supponiamo che f sia moltiplicativa, allora

- Se f non è la funzione nulla, $f(1) = 1$, infatti, preso $a \in \mathbb{N}$ tale che $f(a) \neq 0$, si avrà
$$f(a) = f(a \cdot 1) = f(a)f(1),$$
ovvero $f(1) = 1$.
- $f(p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}) = f(p_1^{\alpha_1}) \ldots f(p_s^{\alpha_s})$, con $p_1 < p_2 < \ldots < p_s$, ovvero
$$f(n) = \prod_p f(p^{\nu_p(n)}).$$

Proposizione 2.6 – Scrittura alternativa delle funzioni enumerativa e somma dei divisori

Sia $n = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$, allora
$$d(n) = \prod_{j=1}^{s}(\alpha_j + 1) \text{ e } \sigma(n) = \prod_{j=1}^{s} \frac{p_j^{\alpha_j+1} - 1}{p_j - 1}.$$

Dimostrazione. Segue dalla molteplicità di d e di σ, infatti
$$\begin{aligned} d(p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}) &= d(p_1^{\alpha_1}) \ldots d(p_s^{\alpha_s}) \\ &= \prod_{j=1}^{s}(\alpha_j + 1). \end{aligned}$$

Analogamente
$$\begin{aligned} \sigma(p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}) &= \sigma(p_1^{\alpha_1}) \ldots \sigma(p_s^{\alpha_s}) \\ &= \prod_{j=1}^{s} \sum_{k=0}^{\alpha_j} p_j^k \\ &= \prod_{j=1}^{s} \frac{p_j^{\alpha_j+1} - 1}{p_j - 1}. \end{aligned}$$
□

2.2 NUMERI PERFETTI

Definizione 2.7 – Numero perfetto

Un numero naturale n si definisce *perfetto* se
$$\sigma(n) = 2n.$$

Osservazione. I numeri primi non sono mai perfetti, infatti
$$\sigma(p) = 1 + p \neq 2p, \ \forall \ p \text{ primo}.$$

Osserviamo che vale anche $\sigma(n) = 1 + n \implies n$ primo, questo poichè, se per assurdo $n = a\,b$, dove a, b sono divisori propri di n, si avrebbe
$$\sigma(n) \geqslant n + 1 + a + b \neq n + 1.$$

Esempio. 6 è un numero perfetto, infatti

$$\sigma(6) = \sigma(2)\sigma(3) = 3 \cdot 4 = 12 = 2 \cdot 6.$$

Anche 28 è un numero perfetto, infatti

$$\sigma(28) = \sigma(4)\sigma(7) = 7 \cdot 8 = 56 = 2 \cdot 28.$$

Teorema 2.8 – Numeri perfetti pari

Sia $n \in \mathbb{N}$ pari. Allora n è perfetto se e soltanto se

$$n = 2^{m-1}(2^m - 1), \text{ con } 2^m - 1 \text{ primo.}$$

⇐) *dovuta a Euclide*

Dimostrazione. Supponiamo che

$$n = 2^{m-1}(2^m - 1),$$

con $2^m - 1$ primo, allora

$$\begin{aligned}\sigma(n) &= \sigma(2^{m-1})\sigma(2^m - 1)\\ &= (1 + 2 + \ldots + 2^{m-1})(2^m - 1 + 1)\\ &= (2^m - 1)2^m\\ &= 2n,\end{aligned}$$

dove la penultima uguaglianza discende da

$$\sum_{n=0}^{k} a^n = \frac{a^{k+1} - 1}{a - 1} \overset{a=2}{=} 2^{k+1} - 1.$$

⇒) *dovuta a Eulero*

Sia n un numero perfetto pari, per cui

$$n = 2^{m-1}u,$$

dove u è dispari e $m > 1$. Ora, n è perfetto, quindi $2n = \sigma(n)$, da cui

$$2^m u = \sigma(2^{m-1})\sigma(u) = (2^m - 1)\sigma(u),$$

ovvero

$$\begin{aligned}\sigma(u) &= \frac{2^m u}{2^m - 1}\\ &= \frac{2^m u - u + u}{2^m - 1}\\ &= u + \frac{u}{2^m - 1},\end{aligned}$$

quindi

$$\frac{u}{2^m - 1} = \sigma(u) - u \in \mathbb{N}$$

ricordiamo che $(1 + u) \leqslant \sigma(u)$

per cui

$$2^{m-1} \mid u \implies \frac{u}{2^m - 1} \mid u.$$

$a \mid b \implies \frac{b}{a} a = b \implies \frac{b}{a} \mid b$

Quindi sappiamo che

$$\sigma(u) = u + \frac{u}{2^m - 1},$$

che sono entrambi divisori di u. Ricordiamo che $\sigma(u)$ è la somma dei divisori di u e che $\sigma(u) \geqslant u + 1$. Per cui avremo necessariamente

$$u + 1 = u + \frac{u}{2^m - 1},$$

ovvero

$$u = 2^m - 1.$$

□

Osservazione. In generale basta trovare un primo della forma $2^m - 1$ per avere un numero perfetto.

Esempio. Alcuni numeri perfetti trovati tramite il teorema:

- $2 \cdot 3 = 6$;
- $2^2(2^3 - 1) = 28$;
- $2^4(2^5 - 1) = 16 \cdot 31 = 496$.

Definizione 2.9 – Numero primo di Mersenne

Un numero primo della forma

$$2^m - 1,$$

si definisce *numero primo di Mersenne*.

Osservazione. Si conoscono solamente 49 primi di Mersenne e non è stato dimostrato se sono o meno infiniti. Il più grande conosciuto è, ad oggi,

$$2^{74207281} - 1,$$

che ha più di 22 milioni di cifre.

Proprietà.

$$2^n - 1 \text{ primo} \implies n \text{ primo}.$$

Dimostrazione. Se per assurdo $n = a\,b$, con a, b divisori propri di n, si avrebbe

$$\begin{aligned} 2^n - 1 &= 2^{a\,b} - 1 \\ &= (2^a - 1)(1 + 2^a + 2^{2a} + \ldots + 2^{(b-1)a}), \end{aligned}$$

che è una fattorizzazione propria di $2^n - 1$ se $a > 1$. Ma ciò è assurdo in quanto avevamo supposto che $2^n - 1$ fosse primo. □

Osservazione. Fino ad oggi non è stato dimostrato se esistono o meno numeri perfetti dispari, di seguito andremo a mostrare alcuni risultati in questo ambito.

Proprietà. Se n è un numero perfetto dispari, allora

- $n > 10^{1500}$;
- il più grande dei suoi divisori primi è maggiori di 10^8.

Proprietà (Teorema di Eulero)**.** Se n è un numero perfetto dispari, allora

$$n = p^{4\lambda+1} Q^2,$$

dove $p = 1 + 4k$ e Q^2 è un quadrato perfetto.

2.3 LA FUNZIONE DEI DIVISORI

Definizione 2.10 – Notazione di Vinogradov

Prese due funzioni aritmetiche f, g, diremo che

$$f \ll g, \text{ per } n \to +\infty,$$

se esistono A, B costanti tali che

$$\frac{|f(n)|}{|g(n)|} \leqslant A, \forall\, n \geqslant B.$$

Osservazione. $f \ll g \iff f = O(g)$.

Teorema 2.11 – Stima superiore della funzione dei divisori

Preso $\varepsilon > 0$ qualsiasi, risulta

$$d(n) \ll n^{\varepsilon}, \text{ per } n \to +\infty.$$

Dimostrazione. Fissiamo $\varepsilon > 0$ e, senza perdita di generalità, assumiamo che $\varepsilon < 1$. Sia $n = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$, avremo

$$\frac{d(n)}{n^{\varepsilon}} = \frac{\alpha_1 + 1}{p_1^{\alpha_1 \varepsilon}} \cdot \ldots \cdot \frac{\alpha_s + 1}{p^{\alpha_s \varepsilon}},$$

vogliamo stimare ciascun fattore. Avremo quindi due casi:

- Se $2 \leqslant p_j \leqslant 2^{\frac{1}{\varepsilon}}$, avremo
$$2^{\alpha_j \varepsilon} \leqslant p_j^{\alpha_j \varepsilon} \leqslant 2^{\alpha_j},$$
da cui
$$\frac{\alpha_j + 1}{p_j^{\alpha_j \varepsilon}} \leqslant \frac{\alpha_j + 1}{2^{\alpha_j \varepsilon}}.$$
Ora
$$2^{a_j \varepsilon} \geqslant 1 + \varepsilon\, \alpha_j \ln 2,$$
in quanto, per Taylor,
$$2^{\alpha_j \varepsilon} = e^{\alpha_j \varepsilon \ln 2} = 1 + \varepsilon\, \alpha_j \ln 2 + o(\varepsilon\, \alpha_j \ln 2).$$
Infine
$$1 + \varepsilon\, \alpha_j \ln 2 > (1 + \alpha_j)\varepsilon \ln 2,$$
è vero poichè
$$\varepsilon \ln 2 < 1 \iff \varepsilon < \frac{1}{\ln 2},$$
che è soddisfatta in quanto $\varepsilon < 1$. Per cui avremo
$$\frac{\alpha_j + 1}{p^{\alpha_j \varepsilon}} < \frac{1}{\varepsilon \ln 2}.$$
- Se $p_j > 2^{\frac{1}{\varepsilon}}$, avremo
$$p_j^{\alpha_j \varepsilon} > 2^{a_j} > 1 + \alpha_j,$$

dove l'ultima disuguaglianza è vera poichè

$$\begin{aligned} 2^\alpha &= (1+1)^\alpha \\ &= \sum_{k=0}^{\alpha} \binom{\alpha}{k} \\ &> \binom{\alpha}{0} + \binom{\alpha}{1} \\ &= 1+\alpha. \end{aligned}$$

Per cui avremo

$$\frac{\alpha_j + 1}{p_j^{\alpha_j \varepsilon}} < 1.$$

Concludendo, abbiamo che

$$\frac{d(n)}{n^\varepsilon} = \prod_{j=1}^{s} \frac{\alpha_j + 1}{p_j^{\alpha_j \varepsilon}} < \prod_{\substack{j=1 \\ p_j < 2^{1/\varepsilon}}} \frac{1}{\varepsilon \ln 2},$$

da cui

$$\begin{aligned} \frac{d(n)}{n^\varepsilon} &\leqslant \prod_{\substack{i=1 \\ p_j \leqslant 2^{1/\varepsilon}}} \frac{1}{\varepsilon \ln 2} \\ &\leqslant \prod_{p \leqslant 2^{1/\varepsilon}} \frac{1}{\varepsilon \ln 2} \\ &= K_\varepsilon, \end{aligned}$$

p *è un generico primo indipendente da* n

che è un valore indipendente da n. Abbiamo quindi ottenuto

$$\frac{d(n)}{n^\varepsilon} \leqslant K_\varepsilon,$$

cioè $d(n) \ll n^\varepsilon$. □

Esempio. Se prendiamo $\varepsilon = \frac{1}{3}$, avremo

$$K_{\frac{1}{3}} = \prod_{p \leqslant 8} \frac{3}{\ln 2} = \left(\frac{3}{\ln 2}\right)^4,$$

per cui

$$\frac{d(n)}{n^{\frac{1}{3}}} < \left(\frac{3}{\ln 2}\right)^4.$$

Teorema 2.12 – Impossibilità di stimare meglio la funzione dei divisori

Preso $c \in \mathbb{R}^+$, la disuguaglianza

$$d(n) \ll \ln^c n, \text{ per } n \to +\infty,$$

è falsa.

Dimostrazione. Fissiamo c, la strategia è cotruire una sequenza di numeri infinita, tale

che

$$d(n) > k \ln n, \forall\, k > 0.$$

Fissiamo $l = [c]$, la sequenza è la seguente

$$n = (p_1 p_2 \cdot \ldots \cdot p_{l+1})^m, m \in \mathbb{N},$$

ovvero $p_1 = 2, p_2 = 3$, *ecc.*

dove p_i è l'i-esimo numero primo. Ora $d(n) = (m+1)^{l+1}$, e $\ln n = m \ln(p_1 \cdot \ldots \cdot p_{l+1})$, da cui

$$\begin{aligned} d(n) &= (m+1)^{l+1} \\ &> m^{l+1} \\ &= m^{l+1} \frac{\left(\ln(p_1 \cdot \ldots \cdot p_{l+1})\right)^{l+1}}{\left(\ln(p_1 \cdot \ldots \cdot p_{l+1})\right)^{l+1}} \\ &= \frac{1}{\left(\ln(p_1 \cdot \ldots \cdot p_{l+1})\right)^{l+1}} (\ln n)^{l+1} \\ &> k(\ln n)^c, \end{aligned}$$

dove l'ultima uguaglianza è vera se e soltanto se

$$(\ln n)^{l+1-c} > k\left(\ln(p_1 \cdot \ldots \cdot p_{l+1})\right)^{l+1},$$

che è soddisfatta per ogni n sufficientemente grande. □

Definizione 2.13 – Costante di Eulero-Mascheroni

La *costante di Eulero-Mascheroni* γ è definita come il limite della differenza tra la serie armonica troncata e il logaritmo naturale,

$$\gamma = \lim_{n \to +\infty} \left(\sum_{k=1}^{n} \frac{1}{k} - \ln n \right).$$

Osservazione. La costante di Eulero-Mascheroni converge, in particolare

$$\gamma \simeq 0,577215649\ldots$$

Teorema 2.14 – Stima asintotica della serie armonica tramite γ

Vale la seguente stima

$$\sum_{n \leqslant Y} \frac{1}{n} = \ln Y + \gamma + O\left(\frac{1}{Y}\right), \text{ con } Y \to +\infty.$$

Dimostrazione. Preso $Y \geqslant 1, Y \in \mathbb{R}$, vale la seguente identità

$$\sum_{n \leqslant Y} \frac{1}{n} = \frac{[Y]}{Y} + \int_1^Y \frac{[u]}{u^2}\, du,$$

infatti

$$\begin{aligned}
\frac{[Y]}{Y} + \int_1^Y \frac{[u]}{u^2}\,du &= \frac{[Y]}{Y} + \sum_{n=1}^{[Y]-1} \int_n^{n+1} \frac{[u]}{u^2}\,du + \int_{[Y]}^Y \frac{[u]}{u^2}\,du \\
&= \frac{[Y]}{Y} + \sum_{n=1}^{[Y]-1} n \int_n^{n+1} \frac{du}{u^2} + [Y] \int_{[Y]}^Y \frac{du}{u^2} \\
&= \frac{[Y]}{Y} + \sum_{n=1}^{[Y]-1} n \left(\frac{1}{n} - \frac{1}{n+1} \right) + [Y] \left(\frac{1}{[Y]} - \frac{1}{Y} \right) \\
&= \sum_{n=1}^{[Y]-1} \frac{1}{n+1} + 1 \\
&= 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{[Y]} \\
&= \sum_{n \leqslant Y} \frac{1}{n}.
\end{aligned}$$

Da cui

$$\begin{aligned}
\sum_{n \leqslant Y} \frac{1}{n} &= \frac{[Y]}{Y} + \int_1^Y \frac{[u]}{u^2}\,du \\
&= \frac{[Y]}{Y} + \int_1^Y \frac{u - \{u\}}{u^2}\,du \\
&= 1 - \frac{\{Y\}}{Y} + \ln Y - \int_1^Y \frac{\{u\}}{u^2}\,du \\
&= 1 - \int_1^{+\infty} \frac{\{u\}}{u^2}\,du + \ln Y - \frac{\{Y\}}{Y} + \int_Y^{+\infty} \frac{\{u\}}{u^2}\,du.
\end{aligned}$$

Sia quindi

$$\gamma = 1 - \int_1^{+\infty} \frac{\{u\}}{u^2}\,du,$$

dove

$$\int_1^{+\infty} \frac{\{u\}}{u^2}\,du \leqslant \int_1^{+\infty} \frac{du}{u^2} = 1,$$

che implica $\gamma \in \mathbb{R}$ e $\gamma \geqslant 0$. Sia inoltre

$$E(Y) = \int_Y^{+\infty} \frac{\{u\}}{u^2}\,du - \frac{\{Y\}}{Y}.$$

Avremo quindi

$$\sum_{n \leqslant Y} \frac{1}{n} = \ln Y + \gamma + E(Y).$$

Resta da mostrare che $E(Y) \ll \frac{1}{Y}$, infatti

$$\begin{aligned}
|E(Y)| &\leqslant \int_Y^{+\infty} \frac{du}{u^2} + \frac{1}{Y} \\
&= -\frac{1}{u}\Big|_Y^{+\infty} + \frac{1}{Y} \\
&= \frac{2}{Y} \\
&= O\left(\frac{1}{Y}\right).
\end{aligned}$$

□

Teorema 2.15 – dell'iperbole di Dirichlet

Vale la seguente stima

$$\sum_{n\leqslant X} d(n) = \ln X + (2\gamma - 1)X + O\left(\sqrt{X}\right), \text{ con } X \to +\infty.$$

Dimostrazione. Sappiamo che

$$d(n) = \sum_{d\mid n} 1,$$

per cui

$$\sum_{n\leqslant X} d(n) = \sum_{n\leqslant X}\sum_{d\mid n} 1 = \sum_{\substack{a,b\in\mathbb{N}\\ ab\leqslant X}} 1,$$

questo poichè esiste un corrispondenza biunivoca

$$\{\,(a,b)\in\mathbb{N} \mid ab\leqslant X\,\} \longleftrightarrow \{\,(n,d)\in\mathbb{N} : n\leqslant X, d\mid n\,\},$$

tramite le applicazioni

$$(a,b)\mapsto (ab,a),$$
$$\left(d,\frac{n}{d}\right)\mapsto (n,d).$$

Ora, come mostrato nella figura 2.1, $\sum_{ab\leqslant X} 1$ è il numero di punti a coordinate intere che si trovano al di sotto dell'iperbole $ab = X$. Preso il punto $P = (\sqrt{X},\sqrt{X})$, posso quindi considerare tale superficie suddivisa come nelle tre regioni in figura. Avrò quindi

in III *ho precisamente* $[\sqrt{X}]$ *punti di* b *per ognuno dei* $[\sqrt{X}]$ *punti di* a

$$\sum_{\substack{a,b\in\mathbb{N}\\ ab\leqslant X}} 1 = I + II - III = 2I - III = 2\sum_{a\leqslant\sqrt{X}}\sum_{b\leqslant\frac{X}{a}} 1 - \left([\sqrt{X}]\right)^2,$$

da cui

applico la proprietà 9 della parte intera

$$\begin{aligned}
\sum_{n\leqslant X} d(n) &= 2\sum_{a\leqslant\sqrt{X}}\left[\frac{X}{a}\right] - \left(\sqrt{X} - \{\sqrt{X}\}\right)^2 \\
&= 2\sum_{a\leqslant\sqrt{X}}\frac{X}{a} - \underbrace{2\sum_{a\leqslant\sqrt{X}}\overbrace{\left\{\frac{X}{a}\right\}}^{\leqslant 1}}_{\leqslant 2\sqrt{X}} - X + \underbrace{2\{X\}\sqrt{X}}_{\leqslant 2\sqrt{X}} - \underbrace{\{X\}^2}_{\leqslant 1} \\
&= 2X\sum_{a\leqslant\sqrt{X}}\frac{1}{a} - X + O\left(\sqrt{X}\right) \\
&= 2X\left[\ln\sqrt{X} + \gamma + O\left(\frac{1}{\sqrt{X}}\right)\right] - X + O\left(\sqrt{x}\right) \\
&= X\ln X + (2\gamma - 1)X + O\left(\sqrt{X}\right).
\end{aligned}$$

la stima della serie armonica viene dal teorema precedente

□

Osservazione. Un risultato molto più debole

$$\sum_{n\leqslant X} d(n) = X\ln X + O(X),$$

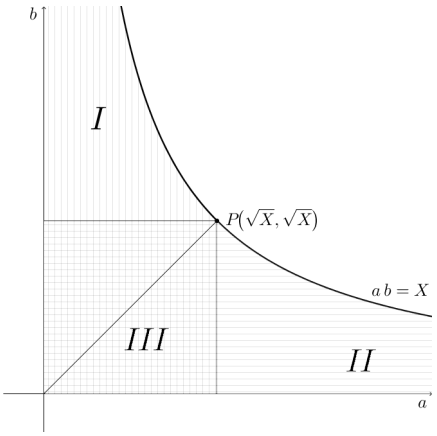

Figura 2.1: La porzione di piano sottesa da $a\,b = X$, suddivisa in 3 regioni.

può essere ottenuto più facilmente troncando il secondo termine significativo, infatti

$$\begin{aligned}
\sum_{n\leqslant X}\sum_{d\mid n} 1 &= \sum_{d\leqslant X}\sum_{\substack{n\leqslant X\\ d\mid n}} 1\\
&= \sum_{d\leqslant X}\left[\frac{X}{d}\right]\\
&= \sum_{d\leqslant X}\frac{X}{d} - \underbrace{\sum_{d\leqslant X}\left\{\frac{X}{d}\right\}}_{\leqslant X = O(X)}\\
&= X\sum_{d\leqslant X}\frac{1}{d} + O(X)\\
&= X\left[\ln X + \gamma + O\left(\frac{1}{X}\right)\right] + O(X)\\
&= X\ln X + \gamma X + O(1) + O(X)\\
&= X\ln X + O(X).
\end{aligned}$$

i termini $O(1)$ *e* γX *vengono inglobati da* $O(X)$

Osservazione. Esiste una congettura, equivalente all'ipotesi di Riemann, che stima l'errore di

$$\sum_{n\leqslant X} d(n),$$

come $O\left(X^{1/4}\right)$.

Teorema 2.16 – Stima superiore della funzione somma dei divisori

Consideriamo la funzione somma dei divisori σ, allora

$$\sigma(n) \ll n\ln n.$$

Dimostrazione. Osserviamo che l'applicazione

$$\mathcal{D}(n) \to \mathcal{D}(n), d \mapsto \frac{n}{d},$$

è un involuzione, ovvero è un applicazione biunivoca che ha se stessa come inversa. Da

cui

$$\sigma(n) = \sum_{d|n} d = \sum_{d|n} \frac{n}{d}.$$

Segue

$$\begin{aligned}\sigma(n) &= \sum_{d|n} \frac{n}{d} \\ &= n \sum_{d|n} \frac{1}{d} \leqslant n \sum_{d\leqslant n} \frac{1}{d} \\ &= n\left[\ln n + \gamma + O\left(\frac{1}{b}\right)\right] \leqslant 2n \ln n,\end{aligned}$$

quando n è sufficientemente grande. Ovvero $\sigma(n) \ll n \ln n$. □

Teorema 2.17 – Stima asintotica della funzione somma dei divisori

Consideriamo la funzione somma dei divisori σ, allora

$$\sum_{n\leqslant X} \sigma(n) = \frac{\pi^2}{12} X^2 + O(X \ln X).$$

Dimostrazione. Per definizione di σ avremo

vedi la dimostrazione del teorema precedente

$$\begin{aligned}\sum_{n\leqslant X} \sigma(n) &= \sum_{n\leqslant X} \sum_{d|n} d = \sum_{n\leqslant X} \sum_{d|n} \frac{n}{d} \\ &= \sum_{d\leqslant X} \sum_{\substack{n\leqslant X \\ d|n}} \frac{d}{n} = \sum_{d\leqslant X} \sum_{m\leqslant \frac{X}{d}} m,\end{aligned}$$

dove l'ultima uguaglianza è vera in quanto $d \mid n$ implica $n = m\,d$, inoltre $n \leqslant X$, da cui

$$m = \frac{n}{d} \leqslant \frac{X}{d}.$$

Ricordiamo la ben nota formula per la somma dei primi N numeri interi

$$\sum_{k=1}^{N} k = \frac{N(N+1)}{2},$$

da cui

$$\begin{aligned}\sum_{d\leqslant X} \sum_{m\leqslant \frac{X}{d}} m &= \sum_{d\leqslant X} \frac{1}{2}\left[\frac{X}{d}\right]\left(\left[\frac{X}{d}\right]+1\right) \\ &= \frac{1}{2}\sum_{d\leqslant X}\left(\frac{X}{d}+O(1)\right)\left(\frac{X}{d}+O(1)\right) = \frac{1}{2}\sum_{d\leqslant X}\left(\frac{X^2}{d^2}+O\left(\frac{X}{d}\right)\right) \\ &= \frac{X^2}{2}\sum_{d\leqslant X}\frac{1}{d^2} + O\underbrace{\left(X\sum_{d\leqslant X}\frac{1}{d}\right)}_{\ll X\ln X} \\ &= \frac{X^2}{2}\sum_{d=1}^{+\infty}\frac{1}{d^2} + O(X\ln X) - \frac{X^2}{2}\left(\sum_{d>X}\frac{1}{d^2}\right).\end{aligned}$$

per il teorema precedente

Ricordiamo il criterio del confronto integrale per serie:

$$\int_1^X f(t)\,dt \ll \sum_{n=1}^{X} f(n) \ll \int_1^X f(t)\,dt,$$

dove f è continua e $f \geqslant 0$. Quindi

$$\sum_{d \geqslant X} \frac{1}{d^2} \ll \int_X^{+\infty} \frac{dt}{t^2} = \frac{1}{X},$$

ovvero

$$\frac{X^2}{2}\left(\sum_{d \geqslant X} \frac{1}{d^2}\right) = O\left(X^2 \frac{1}{X}\right) = O(X),$$

infine, dal momento che il termine $O(X)$ viene inglobato da $O(X \ln X)$, avremo

$$\begin{aligned}\sum_{n \leqslant X} \sigma(n) &= \frac{X^2}{2} \sum_{d=1}^{+\infty} \frac{1}{d^2} + O(X \ln X) \\ &= \frac{\pi^2}{12} X^2 + O(X \ln X).\end{aligned}$$

□

2.4 FUNZIONE DI MÖEBIUS

Definizione 2.18 – Funzione di Möebius

Si definisce *funzione di Möebius* la seguente funzione aritmetica

$$\mu(n) = \begin{cases} 1 & \text{se } n = 1 \\ (-1)^s & \text{se } n = p_1 \cdot \ldots \cdot p_s \\ 0 & \text{se } n \text{ ha un fattore quadratico} \end{cases}$$

Osservazione. Dire che n ha fattori moltiplicativi, significa affermare che esiste p primo tale che

$$p^2 \mid n.$$

Teorema 2.19 – μ è moltiplicativa

La funzione μ di Möebius è moltiplicativa.

Dimostrazione. Siano $n, m \in \mathbb{N} : (n, m) = 1$, dobbiamo mostrare che $\mu(mn) = \mu(m)\mu(n)$. D'altronde se $\mu(m)\mu(n) = 0$ certamente esisterà un primo p tale che p^2 divide n oppure m, in entrambi i casi

$$\exists\, p^2 \mid nm \implies \mu(nm) = 0.$$

Se, invece, $\mu(n)\mu(m) \neq 0$ avremo due possibilità

- $n = 1$ o $m = 1$, da cui segue banalmente la tesi;
- $n \neq 1$ e $m \neq 1$, quindi, per definizione di μ

$$\begin{aligned} n &= p_1 \cdot \ldots \cdot p_s, \\ m &= q_1 \cdot \ldots \cdot q_r, \end{aligned}$$

quindi $\mu(n) = (-1)^s$ e $\mu(m) = (-1)^r$. Inoltre $\mu(nm) = (-1)^{r+s}$ in quanto $(n, m) = 1$ implica che $p_i \neq q_j$, $\forall\, i, j$.

□

Osservazione. μ non è totalmente moltiplicativa, infatti

$$1 = \mu(2)\mu(2) \neq \mu(4) = 0.$$

Teorema 2.20 – Trasformata di Dirichlet di μ

La trasformate di Dirichlet di μ è

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & n = 1 \\ 0 & n \neq 1 \end{cases}$$

Dimostrazione. Ricordiamo che per il teorema 2.5 la trasformata di Dirichlet di una funzione moltiplicativa è a sua volta moltiplicativa, quindi

$$g(n) = \sum_{d|n} \mu(d),$$

è moltiplicativa in n. Ora

$$g(1) = \sum_{d|1} \mu(d) = \mu(1) = 1,$$

inoltre, se $\alpha \geqslant 1$,

$$g(p^\alpha) = \sum_{d|p^\alpha} \mu(d) = \sum_{\beta=0}^{\alpha} \mu(p^\beta) = 1 - 1 = 0.$$

Infine, per la moltiplicatività di g, avremo

$$\begin{aligned} g(n) &= g\left(p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}\right) \\ &= g\left(p_1^{\alpha_1}\right) \cdot \ldots \cdot g\left(p_s^{\alpha_s}\right) \\ &= 0. \end{aligned}$$

□

Teorema 2.21 – Prima legge di inversione di Möebius

Sia $f\colon \mathbb{N} \to \mathbb{C}$ una funzione aritmetica. Sia $g\colon \mathbb{N} \to \mathbb{C}$ la trasformata di Dirichlet di f, allora

$$g(n) = \sum_{d|n} f(d) \implies f(n) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right).$$

Dimostrazione. Ricordiamo che esiste una corrispondenda biunivoca dell'inisieme dei divisori di n in se stesso tramite $d \mapsto \frac{n}{d}$, per cui

$$\begin{aligned} \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right) &= \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d) \\ &= \sum_{d|n} \mu\left(\frac{n}{d}\right) \sum_{e|d} f(e) \\ &= \sum_{e|n} f(e) \sum_{\substack{d|n \\ e|d}} \mu\left(\frac{n}{d}\right), \end{aligned}$$

$e \mid d, d \mid n \implies e \mid n$

dove e, n sono fissati, inoltre $n = d\,f, d = e\,k$, per cui

$$f = \frac{n}{d} = \frac{n}{e\,k} \implies f \mid \frac{n}{e}.$$

In conclusione

$$\sum_{\substack{d \mid n \\ e \mid d}} \mu\left(\frac{n}{d}\right) = \sum_{f \mid \frac{n}{e}} \mu(f) = \begin{cases} 1 & e = n \\ 0 & \text{altrimenti} \end{cases}$$

ovvero

$$\sum_{e \mid n} f(e) \sum_{\substack{d \mid n \\ e \mid d}} \mu\left(\frac{n}{d}\right) = f(n).$$

□

Esempio. Consideriamo la funzione ζ di Riemann

$$\zeta(s) = \sum_{n=1}^{+\infty} \frac{1}{n^s}, s > 1$$

in generale $s \in \mathbb{C}$ *con* $\Re(s) > 1$

e consideriamo

$$F(s) = \sum_{n=1}^{+\infty} \frac{\mu(n)}{n^s},$$

dove $|\mu(s)| \in \{0, 1\}$, per cui $F(s)$ converge totalmente per la convergenza di $\zeta(s)$ quando $s > 1$.
Facciamo il prodotto tra le due funzioni

$$\sum_{n=1}^{+\infty} \frac{1}{n^s} \sum_{m=1}^{+\infty} \frac{\mu(m)}{m^s} = \sum_{\substack{n \in \mathbb{N} \\ m \in \mathbb{N}}} \frac{\mu(m)}{(m\,n)^s} = \sum_{k=1}^{+\infty} \frac{a_k}{k^s},$$

dove

$$a_k = \sum_{\substack{n, m \in \mathbb{N} \\ m\,n = k}} \mu(m) = \sum_{m \mid k} \mu(m) = \begin{cases} 1 & k = 1 \\ 0 & k \neq 1 \end{cases}$$

Ovvero

$$\sum_{k=1}^{+\infty} \frac{a_k}{k^s} = 1,$$

cioè F è la funzione inversa di ζ, quindi

$$\frac{1}{\zeta(s)} = \sum_{n=1}^{+\infty} \frac{\mu(n)}{n^s}.$$

Teorema 2.22 – Seconda legge di inversione di Möebius

Siano $g\colon \mathbb{N} \to \mathbb{C}$ e $f\colon \mathbb{N} \to \mathbb{C}$ funzioni aritmetiche tali che

$$f(n) = \sum_{d \mid n} \mu(d) g\left(\frac{n}{d}\right),$$

allora

$$g(n) = \sum_{d \mid n} f(d).$$

Dimostrazione. La dimostrazione è analoga a quella del teorema 2.21, infatti

$$\begin{aligned}\sum_{d|n} f(d) &= \sum_{d|n}\sum_{e|d} \mu\left(\frac{d}{e}\right) g(e) \\ &= \sum_{e|n} g(e) \sum_{d|\frac{n}{e}} \mu\left(\frac{n}{e\,d}\right) \\ &= \sum_{e|n} g(e) \left(\sum_{d|\frac{n}{e}} \mu(d)\right) \\ &= g(n).\end{aligned}$$

dalla corrispondenza biunivoca di $\mathcal{D}(\frac{n}{d})$ in se stesso

□

2.5 FUNZIONE DI EULERO

Definizione 2.23 – Funzione di Eulero

Si definisce funzione di Eulero

$$\varphi(n) = \#\{\, x \in \mathbb{N} \mid x \leqslant n, (x,n) = 1 \,\}.$$

Osservazione. Analogamente φ si può definire come la cardinalità degli invertibili di $\mathbb{Z}_n$, ovvero

$$\varphi(n) = \#\mathcal{U}\left(\frac{\mathbb{Z}}{n\,\mathbb{Z}}\right).$$

Teorema 2.24 – Trasformata di Dirichlet di φ

La trasformata di Dirichlet di φ è

$$\sum_{d|n} \varphi(d) = n.$$

Dimostrazione. Per ogni divisore d di n consideriamo

$$\mathcal{D}_d = \{\, x \in \mathbb{N} \mid x \leqslant n, (x,n) = d \,\} \subseteq \{\, 1, \dots, n \,\}.$$

Osserviamo che se $d \neq d'$ avremo $\mathcal{D}_d \cap \mathcal{D}_{d'} = \emptyset$, per cui

$$\bigsqcup_{d|n} \mathcal{D}_d = \{\, 1, \dots, n \,\},$$

ovvero

$$n = \#\{\, 1, \dots, n \,\} = \#\left(\bigsqcup_{d|n} \mathcal{D}_d\right) = \sum_{d|n} |\mathcal{D}_d|.$$

Consideriamo ora

$$\mathcal{D}'_d = \left\{ x \in \mathbb{N} \;\middle|\; 1 \leqslant x \leqslant \frac{n}{d}, \left(x, \frac{n}{d}\right) = 1 \right\},$$

quindi, per definizione, $|\mathcal{D}'_d| = \varphi(\frac{n}{d})$. Esiste una corrispondenza biunivoca fra $\mathcal{D}_d$ e $\mathcal{D}'_d$ tramite

$$\begin{aligned} x &\mapsto \frac{x}{d} \\ d\,y &\mapsfrom y. \end{aligned}$$

Per cui

$$\begin{aligned} n &= \sum_{d|n} |\mathcal{D}_d| = \sum_{d|n} |\mathcal{D}'_d| \\ &= \sum_{d|n} \varphi\left(\frac{n}{d}\right) = \sum_{d|n} \varphi(d). \end{aligned}$$

□

Teorema 2.25 – Inversione di Möebius applicata a φ

La funzione φ di Eulero può essere riscritta nella forma

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

Dimostrazione. Segue banalmente dalla prima legge di inversione di Möebius (teorema 2.21). Infatti, dal teorema precedente sappiamo che

$$\sum_{d|n} \varphi(d) = n,$$

quindi conosciamo la trasformata di Dirichlet di φ, applicando la legge di inversione otteniamo

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

□

Teorema 2.26 – φ è moltiplicativa

La funzione φ di Eulero è moltiplicativa.

Dimostrazione. Dal teorema precedente sappiamo che

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

ora, la funzione μ di Möebius è moltiplicativa, pertanto lo sarà anche $\mu(d)/d$. Inoltre

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

è moltiplicativa in quanto trasformata di Dirichlet di una funzione moltiplicativa. Quindi

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

è moltiplicativa.

□

Teorema 2.27 – Scrittura alternativa di φ

Supponiamo $n > 1$ e sia $n = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$, allora

$$\varphi(n) = n \prod_{j=1}^{s} \left(1 - \frac{1}{p_s}\right).$$

Dimostrazione. Dal teorema 2.25 sappiamo che

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

definiamo quindi la funzione

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

che per definizione è moltiplicativa. Quindi

$$h(n) = \prod_{j=1}^{s} h(p_j^{\alpha_j}),$$

dove

$$h(p_s^{\alpha_j}) = 1 + \frac{\mu(p_j)}{p_j} + \underbrace{\frac{\mu(p_j^2)}{p_j^2} + \ldots}_{=0} = 1 - \frac{1}{p_j}.$$

Per cui, sostituendo nell'equazione iniziale,

$$\varphi(n) = n\, h(n) = n \prod_{j=1}^{s} \left(1 - \frac{1}{p_j}\right).$$

□

Osservazione. L'ultima uguaglianza può essere ancora raffinata, infatti

$$n \prod_{j=1}^{s} \left(1 - \frac{1}{p_j}\right) = \prod_{j=1}^{s} p_s^{\alpha_j} \prod_{j=1}^{s} \left(1 - \frac{1}{p_j}\right) = \prod_{j=1}^{s} (p_s^{\alpha_j} - p_j^{\alpha_j - 1}).$$

Teorema 2.28 – Disuguaglianza applicata a $\varphi(n)\sigma(n)$

Vale la seguente disuguaglianza

$$\frac{1}{2} < \frac{\varphi(n)\sigma(n)}{n^2} < 1.$$

Dimostrazione. Preso $n \in \mathbb{N}$, scriviamone la fattorizzazione $n = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$. Richiamando i teoremi 2.6 e 2.27 avremo che

$$\sigma(n) = \prod_{j=1}^{s} \frac{p_j^{\alpha_j+1} - 1}{p_j - 1} = \prod_{j=1}^{s} \frac{p_j^{\alpha_j+1}(1 - p_j^{-\alpha_j-1})}{p_j(1 - p_j^{-1})} = n \prod_{j=1}^{s} \frac{1 - p_j^{-\alpha_j-1}}{1 - p_j^{-1}},$$

e

$$\varphi(n) = n \prod_{j=1}^{s} \left(1 - \frac{1}{p_j}\right).$$

Quindi

$$\begin{aligned}\frac{\varphi(n)\sigma(n)}{n^2} &= \prod_{j=1}^{s}\left(1-\frac{1}{p_j}\right)\prod_{j=1}^{s}\frac{1-p_j^{-\alpha_j-1}}{1-p_j^{-1}}\\ &= \prod_{j=1}^{s}(1-p_j^{-1})\frac{1-p_j^{-\alpha_j-1}}{1-p_j^{-1}}\\ &= \prod_{j=1}^{s}1-\frac{1}{p_j^{\alpha_j+1}} < 1.\end{aligned}$$

Inoltre

$$\begin{aligned}\prod_{j=1}^{s}\left(1-\frac{1}{p_j^{\alpha_j+1}}\right) &> \prod_{j=1}^{s}\left(1-\frac{1}{p_j^2}\right)\\ &> \prod_{m=2}^{n}\left(1-\frac{1}{m^2}\right)\\ &= \frac{n+1}{2n} > \frac{1}{2},\end{aligned}$$

dove l'ultima uguaglianza si mostra facilmente per induzione. □

Osservazione. La stima inferiore può essere migliorata, infatti

$$\prod_{j=1}^{s}\left(1-\frac{1}{p_j^{\alpha_j+1}}\right) > \prod_{p}\left(1-\frac{1}{p^2}\right) = \frac{1}{\zeta(2)} = \frac{6}{\pi^2}.$$

Teorema 2.29 – Stima inferiore di φ

Vale la seguente stima

$$\varphi(n) \gg \frac{n}{\ln n}, \text{ per } n \to +\infty.$$

Dimostrazione. Dal teorema 2.16 sappiamo che

$$\sigma(n) \ll n\ln n \iff \frac{1}{\sigma(n)} \gg \frac{1}{n\ln n},$$

ora, per il teorema precedente

$$\varphi(n) > \frac{n^2}{2\sigma(n)} \iff \varphi(n) \gg \frac{n}{\ln n}.$$ □

Osservazione. Si può dimostrare che in particolare vale il seguente

$$\varphi(n) > \frac{n}{e^{\gamma}\ln(\ln n)+\frac{3}{\ln(\ln n)}},$$

ovvero

$$\varphi(n) \gg \frac{n}{\ln(\ln n)}.$$

Inoltre $\varphi(n) \leqslant n-1$ quando $n \neq 1$, quindi, in conclusione,

$$\frac{n}{\ln(\ln n)} \ll \varphi(n) \leqslant n-1.$$

Esempio. Sappiamo che

$$\zeta(s) = \sum_{n=1}^{+\infty} \frac{1}{n^s} \qquad \text{e} \qquad \frac{1}{\zeta(s)} = \sum_{n=1}^{+\infty} \frac{\mu(n)}{n^s},$$

allora

$$\frac{\zeta(s-1)}{\zeta(s)} = \sum_{n=1}^{+\infty} \frac{\varphi(n)}{n^s}, \Re(s) > 2.$$

Osservazione. Si può dimostrare che anche

$$\sum_{n=1}^{+\infty} \frac{d(n)}{n^s},$$

può essere scritto in funzione di $\zeta(s)$.

Teorema 2.30 – Stima asintotica di φ

Vale la seguente stima

$$\sum_{n \leqslant X} \varphi(n) = \frac{3}{\pi^2} X^2 + O(X \ln X).$$

Dimostrazione. Applicando il teorema di inversione (2.21), otteniamo

$$\begin{aligned}
\sum_{n \leqslant X} \varphi(n) &= \sum_{n \leqslant X} \sum_{d \mid n} \frac{n}{d} \mu(d) \\
&= \sum_{d \leqslant X} \frac{\mu(d)}{d} \sum_{\substack{n \leqslant X \\ d \mid n}} n \\
&= \sum_{d \leqslant X} \frac{\mu(d)}{d} \sum_{m \leqslant \frac{X}{d}} m\, d.
\end{aligned}$$

Ora

$$\sum_{r \leqslant T} r = \frac{1}{2}[T]([T]+1) = \frac{1}{2}T^2 + O(T).$$

Quindi, sostituendo nell'equazione iniziale, otteniamo

$$\begin{aligned}
\sum_{d \leqslant X} \mu(d) \sum_{m \leqslant \frac{X}{d}} m &= \sum_{d \leqslant X} \mu(d) \left[\frac{1}{2} \frac{X^2}{d^2} + O\left(\frac{X}{d}\right) \right] \\
&= \frac{1}{2} \left(\sum_{d \leqslant X} \frac{\mu(d)}{d^2} \right) X^2 + O\left(\sum_{d \leqslant X} \frac{X}{d} \right) \\
&= \frac{1}{2} \left[\frac{1}{\zeta(2)} + O\left(\frac{1}{X}\right) \right] X^2 + O(X \ln X) \\
&= \frac{1}{2\zeta(2)} X^2 + O(X \ln X) = \frac{3}{\pi^2} X^2 + O(X \ln X).
\end{aligned}$$

ho stimato $\mu(d) = 1$

dove

$$\sum_{d\leqslant X}\frac{\mu(d)}{d^2}=\frac{1}{\zeta(2)}+O\left(\frac{1}{X}\right)\qquad\text{e}\qquad O\left(\sum_{d\leqslant X}\frac{X}{d}\right)=O(X\ln X),$$

valgono rispettivamente per l'esercizio 7.5 e per il l'osservazione alla stima della serie armonica (teorema 2.14). □

Osservazione. Esiste una congettura, equivalente all'ipotesi di Riemann, per cui

$$\sum_{n\leqslant X}\varphi(n)=\frac{3}{\pi^2}X^2+O(X^{\frac{1}{2}+\varepsilon}).$$

2.6 PRODOTTO DI CONVOLUZIONE DI DIRICHLET

Definizione 2.31 – Prodotto di convoluzione

Siano $f,g\colon\mathbb{N}\to\mathbb{C}$ due funzioni aritmetiche. Si definisce convoluzione (di Dirichlet) di f,g la seguente funzione

$$(f*g)(n)=\sum_{d|n}f(d)g\left(\frac{n}{d}\right).$$

Osservazione. Le seguenti sono definizioni equivalenti

$$\begin{aligned}(f*g)(n)&=\sum_{d|n}f\left(\frac{n}{d}\right)g(d)\\&=\sum_{\substack{a,b\in\mathbb{N}\\ab=n}}f(a)g(b).\end{aligned}$$

Esempio. Se consideriamo la funzione unitaria $u(n)=1$, allora $u*f$ è la trasformata di Dirichlet di f. Inoltre, per le leggi di inversioni

$$u*f=g\iff f=\mu*g.$$

Osservazione. In particolare avremo

$$u*\delta=u\iff\delta=\mu*u,$$

ovvero μ è invertibile e $\mu^{-1}=u$.

Proposizione 2.32 – Funzioni aritmetiche costituiscono un monoide commutativo

Sia $\mathcal{A}=\{f\colon\mathbb{N}\to\mathbb{C}\}$. Allora

$$(A,*),$$

costituisce un monoide commutativo.

Dimostrazione. La dimostrazione è una semplice verifica:

- $(f * g) * h = f * (g * h)$, in quanto

$$(f * g) * h = \sum_{\substack{a,b,c\in\mathbb{N}\\ a\,b\,c=n}} f(a)g(b)h(c);$$

- $f * g = g * f$ segue dalla definizione;
- $\exists\, \delta \in \mathcal{A} : f * \delta = \delta * f = f$ con

$$\delta(n) = \begin{cases} 1 & n = 1 \\ 0 & \text{altrimenti} \end{cases}$$

□

Esempio. Sia $f \in \mathcal{A}$, possiamo associare ad f una serie

$$\zeta_f(s) = \sum_{n\in\mathbb{N}} \frac{f(n)}{n^s},$$

con s sufficientemente grande. Se ora consideriamo la funzione unitaria u e l'identità δ, avremo

$$\zeta_u(s) = \sum_{n\in\mathbb{N}} \frac{u(n)}{n^s} = \sum_{n\in\mathbb{N}} \frac{1}{n^s} = \zeta(s);$$
$$\zeta_\delta(s) = \sum_{n\in\mathbb{N}} \frac{\delta(n)}{n^s} = 1.$$

Ora, se esistesse $\alpha \in \mathbb{R}$ tale che $f(n) = O(n^\alpha)$, si avrebbe $\zeta_f(s) < +\infty$ per $\Re(s) > \alpha + 1$, infatti

$$|\zeta_f(s)| \leqslant \sum_{n\in\mathbb{N}} \frac{|f(n)|}{n^s} \ll \sum_{n\in\mathbb{N}} \frac{1}{n^{s-\alpha}} < +\infty,$$

per $s > \alpha + 1$.

Lemma 2.33. Siano $f, g \in \mathcal{A}$, allora

$$\zeta_f(s)\zeta_g(s) = \zeta_{f*g}(s),$$

per s sufficientemente grande.

Dimostrazione. Andremo a sfruttare la definizione equivalente di convoluzione, infatti

$$\begin{aligned}
\zeta_f(s)\zeta_g(s) &= \sum_{n\in\mathbb{N}} \frac{f(n)}{n^s} \sum_{m\in\mathbb{N}} \frac{g(m)}{m^s} \\
&= \sum_{n,m\in\mathbb{N}} \frac{f(n)g(m)}{(n\,m)^s} \qquad \textit{raggruppando le coppie con lo stesso prodotto} \\
&= \sum_{k\in\mathbb{N}} \frac{1}{k^s} \sum_{\substack{n,m\in\mathbb{N}\\ n\,m=k}} f(n)g(m) \\
&= \sum_{k\in\mathbb{N}} \frac{(f*g)(k)}{k^s} \\
&= \zeta_{f*g}(s).
\end{aligned}$$

□

Osservazione. Notiamo che possiamo scrivere la funzione somma dei divisori $d(n)$ come la convoluzione della funzione unitaria u in se stessa, infatti

$$(u * u)(n) = \sum_{d|n} u(d)u\left(\frac{n}{d}\right) = \sum_{d|n} 1 = d(n),$$

quindi, per il lemma precedente

$$\zeta_d(s) = \zeta_{u*u}(s) = \zeta_u(s)\zeta_u(s) = \big(\zeta_u(s)\big)^2 = \big(\zeta(s)\big)^2.$$

Teorema 2.34 – Invertibilità rispetto alla convoluzione

Sia $f \in \mathcal{A}$, allora

$$f \in \mathcal{U}(\mathcal{A}) \iff f(1) \neq 0.$$

Dimostrazione. Se $f \in \mathcal{U}(\mathcal{A})$, esiste $g \in \mathcal{A}$ tale che ⇒)

$$f * g = \delta.$$

In particolare avremo $(f * g)(1) = \delta(1) = 1$, ma

$$(f * g)(1) = \sum_{\substack{a,b\in\mathbb{N}\\ a\,b=1}} f(a)g(b) = f(1)g(1) = 1,$$

quindi, necessariamente, $f(1) \neq 0$.
Costruiamo l'inversa g con un metodo induttivo. Definiamo $g(1)$ come ⇐)

$$g(1) := \frac{1}{f(1)}.$$

Procediamo con $g(2)$, vogliamo che

$$(f * g)(2) = \delta(2) = 0,$$

per cui

$$\begin{aligned} 0 = (f * g)(2) &= \sum_{\substack{a,b\in\mathbb{N}\\ a\,b=2}} f(a)g(b) \\ &= f(1)g(2) + f(2)g(1), \end{aligned}$$

ovvero

$$g(2) = -\frac{f(2)g(1)}{f(1)}.$$

Generalizzando per $n \neq 1$ avremo $(f * g)(n) = \delta(n) = 0$, da cui

$$\begin{aligned} 0 = (f * g)(n) &= \sum_{d|n} f(d)g\left(\frac{n}{d}\right) \\ &= f(1)g(n) + \sum_{\substack{d|n\\ d\neq 1}} f(d)g\left(\frac{n}{d}\right), \end{aligned}$$

ovvero

$$g(n) = -\frac{1}{f(1)} \sum_{\substack{d|n\\ d\neq 1}} f(d)g\left(\frac{n}{d}\right).$$

Quindi avendo definito

$$g(n) = \begin{cases} \dfrac{1}{f(1)} & n = 1 \\ -\dfrac{1}{f(1)} \displaystyle\sum_{\substack{d \mid n \\ d \neq 1}} f(d) g\left(\dfrac{n}{d}\right) & n \neq 1 \end{cases}$$

avremo che g è l'inversa di f. □

Osservazione. Quindi l'insieme

$$\mathcal{A}' = \{ f \in \mathcal{A} \mid f(1) \neq 0 \},$$

è un gruppo abeliano rispetto alla composizione.

Definizione 2.35 – Insieme delle funzioni moltiplicative

Analogamente al caso delle funzioni funzioni aritmetiche, definiamo

$$\mathcal{M} = \{ f \colon \mathbb{N} \to \mathbb{C} \mid f \text{ moltiplicativa} \},$$

come l'insieme delle funzioni moltiplicative.

Teorema 2.36 – $\mathcal{M}$ è chiuso rispetto alla convoluzione

Consideriamo l'insieme delle funzioni moltiplicative $\mathcal{M}^*$ privo della funzione identicamente nulla. Allora $\mathcal{M}^*$ è chiuso rispetto alla convoluzione.

Dimostrazione. Siano $f, g \in \mathcal{M}^*$ e siano $n, m \in \mathbb{N}$ tali che $(n, m) = 1$, dobbiamo mostrare che

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

Ora

ricordiamo che da $(n, m) = 1$ si deduce una corrispondenza biunivoca tra $\mathcal{D}(nm)$ e $\setminus \times \updownarrow$

$$\begin{aligned}
(f * g)(mn) &= \sum_{d \mid mn} f(d) g\left(\frac{mn}{d}\right) \\
&= \sum_{\substack{d_1 \mid m \\ d_2 \mid n}} f(d_1 d_2) g\left(\frac{m}{d_1}\frac{n}{d_2}\right) \\
&= \sum_{\substack{d_1 \mid m \\ d_2 \mid n}} f(d_1) f(d_2) g\left(\frac{m}{d_1}\right) g\left(\frac{n}{d_2}\right) \\
&= \left[\sum_{d_1 \mid m} f(d_1) g\left(\frac{m}{d_1}\right)\right] \left[\sum_{d_2 \mid n} f(d_2) g\left(\frac{n}{d_2}\right)\right] \\
&= (f * g)(m)(f * g)(n).
\end{aligned}$$

□

2.7 APPENDICE

Definizione 2.37 – Numero privo di fattori quadratici

$n \in \mathbb{N}$ si dice privo di *fattori quadratici* se la fattorizzazione in primi di n è costituita da primi a due a due distinti, ovvero

$$n = p_1 \dots \cdot p_s, \text{ con } p_1 < \dots < p_s.$$

Osservazione. Analogamente un numero $n \in \mathbb{N}$ si definisce privo di fattori quadratici se $p^2 \nmid n$ per ogni p primo.

Definizione 2.38 – Funzione caratteristica dei numeri privi di fattori quadratici

Definiamo la *funzione caratteristica* dei numeri privi di fattori quadratici come

$$\mu_2(n) = \begin{cases} 1 & \text{se } n \text{ è privo di fattori quadratici} \\ 0 & \text{altrimenti} \end{cases}$$

Osservazione. Dalla definizione segue che

$$\mu_2(n) = |\mu(n)|,$$

dove μ è la funzione di Möebius. Da cui segue, per la moltiplicatività di μ, che μ_2 è moltiplicativa.

Proposizione 2.39 – Scrittura alternativa di μ_2

Consideriamo la funzione μ_2, allora

$$\mu_2(n) = \sum_{d^2 \mid n} \mu(d).$$

Dimostrazione. Se $n = 1$

$$\sum_{d^2 \mid 1} \mu(d) = \mu(1) = 1 = \mu_2(1).$$

Se $n = p^\alpha$

$$\sum_{d^2 \mid p^\alpha} \mu(d) = \begin{cases} 1 & \alpha = 1 \\ 0 & \alpha \geqslant 2 \end{cases} = \mu_2(p^\alpha).$$

Infine, se $n = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s} \neq 1$, per la moltiplicatività di μ e di μ_2 avremo

$$\begin{aligned} \sum_{d^2 \mid n} \mu(n) &= \sum_{d^2 \mid n} \mu(p_1^{\alpha_1}) \cdot \ldots \cdot \mu(p_s^{\alpha_s}) \\ &= \sum_{d_1^2 \mid p_1^{\alpha_1}} \mu(p_1^{\alpha_1}) \cdot \ldots \cdot \sum_{d_s^2 \mid p_s^{\alpha_s}} \mu(p_s^{\alpha_s}) \\ &= \mu(p_1^{\alpha_1}) \cdot \ldots \cdot \mu(p_s^{\alpha_s}) \\ &= \mu(n). \end{aligned}$$

□

Osservazione. Se definiamo la seguente funzione

$$\chi_2(k) = \begin{cases} 1 & \text{se } k \text{ è un quadrato} \\ 0 & \text{altrimenti} \end{cases}$$

allora avremo

$$\mu_2(n) = \sum_{d|n} \chi_2(d)\mu(d).$$

Teorema 2.40 – Stima della cardinalità di numeri privi di fattori quadratici

Vale la seguente stima

$$\sum_{n\leqslant X} \mu_2(n) = \frac{6}{\pi^2}X + O(\sqrt{X}).$$

Dimostrazione. Applicando la proposizione precedente avremo

$$\begin{aligned}
\sum_{n\leqslant X} \mu_2(n) &= \sum_{n\leqslant X} \sum_{\substack{d\in\mathbb{N} \\ d^2|n}} \mu(d) \\
&= \sum_{d\leqslant\sqrt{X}} \mu(d) \sum_{\substack{n\leqslant X \\ d^2|n}} 1 && \text{per la proposizione 1.28 sulla parte intera} \\
&= \sum_{d\leqslant\sqrt{X}} \mu(d) \left[\frac{X}{d^2}\right] = \sum_{d\leqslant\sqrt{X}} \frac{\mu(d)}{d^2}(X + O(1)) \\
&= X \sum_{d\leqslant\sqrt{X}} \frac{\mu(d)}{d^2} + O\left(\sum_{d\leqslant\sqrt{X}} \frac{\mu(d)}{d^2}\right) \leqslant X \sum_{d\leqslant\sqrt{X}} \frac{\mu(d)}{d^2} + O(\sqrt{X}) && \text{ho stimato } \tfrac{\mu(d)}{d^2} \leqslant 1 \\
&= X\left(\frac{1}{\zeta(2)} + O\left(\frac{1}{\sqrt{X}}\right)\right) + O(\sqrt{X}) \\
&= \frac{6}{\pi^2}X + O(\sqrt{X}).
\end{aligned}$$

dove

$$\sum_{d\leqslant\sqrt{X}} \frac{\mu(d)}{d^2} = \frac{1}{\zeta(2)} + O\left(\frac{1}{\sqrt{X}}\right),$$

per l'esercizio 7.5. □

Osservazione. Quindi circa il 60% dei numeri è senza fattori quadratici.

3 CONGRUENZE

3.1 INTRODUZIONE

Definizione 3.1 – Congruenza modulo n

Presi $a, b \in \mathbb{Z}$ e $n \in \mathbb{N}$, diremo che a è congruo a b in modulo n se e soltanto se

$$n \mid a - b.$$

Notazione. Si scrive $a \equiv b \pmod{n}$.

Osservazione. Se facciamo la divisione euclidea fra a ed n otteniamo

$$a = n\,q + r, \text{ con } 0 \leqslant r < n,$$

ovvero $a \equiv r \pmod{n}$.

Teorema 3.2 – Caratterizzazione della congruenza

Presi $a, b \in \mathbb{Z}$ diremo che $a \equiv b \pmod{n}$ se e soltanto se a e b, divisi per n, hanno lo stesso resto.

Dimostrazione. Supponiamo che ⇐)

$$a = n\,q_1 + r \qquad \text{e} \qquad b = n\,q_2 + r,$$

sottraendo membro a membro avremo

$$a - b = n(q_1 - q_2),$$

ovvero $n \mid a - b$, quindi, per definizione, $a \equiv b \pmod{n}$.
Supponiamo che $n \mid a - b$, ovvero ⇒)

$$n\,q = a - b \iff a = n\,q + b,$$

se effettuiamo la divisione euclidea fra a ed n, avremo

$$a = n\,q' + r, \text{ con } 0 \leqslant r < n$$

quindi, uguagliando le espressioni, otteniamo

$$n\,q + b = n\,q' + r \iff b = n(q' - q) + r,$$

dove $0 \leqslant r < n$, da cui, per l'unicità dei resti, si ha la tesi. □

Proprietà 3.3. Siano $a_1, a_2, b_1, b_2 \in \mathbb{Z}$ e sia $n \in \mathbb{N}$ tali che

$$a_1 \equiv b_1 \pmod{n} \qquad \text{e} \qquad a_2 \equiv b_2 \pmod{n},$$

allora

- $a_1 + a_2 \equiv b_1 + b_2 \pmod{n}$;
- $a_1 a_2 \equiv b_1 b_2 \pmod{n}$.

Proprietà 3.4. Siano $a, b, c \in \mathbb{Z}$ e sia $n \in \mathbb{N}$ con $c \neq 0$, allora

- $ac \equiv bc \pmod{n} \implies a \equiv b \pmod{n/(n,c)}$;
- $(n,c) = 1 \implies a \equiv b \pmod{n}$.

3.2 SISTEMI DI RESIDUI

Definizione 3.5 – Residuo modulo n

Preso $a \in \mathbb{Z}$, diremo che il resto di a diviso n è il *residuo* di a modulo n.

Definizione 3.6 – Insieme completo di residui modulo n

Un insieme $S \subseteq \mathbb{Z}$ si definisce *insieme completo di residui modulo* m se, per ogni intero $z \in \mathbb{Z}$, esiste un unico $s \in S$ tale che

$$z \equiv s \pmod{m}.$$

Notazione. Spesso indicheremo un sistema completo di residui modulo m con la sigla ICR(m).

Proprietà. Dato $m \in \mathbb{N}$, allora $S \subseteq \mathbb{Z}$ è un ICR(m) se e soltanto se

- $|S| = m$;
- $\forall\, x, y \in S, x \neq y \implies x \not\equiv y \pmod{m}$.

Esempio. Preso $m \in \mathbb{N}$ l'insieme completo di residui canonico di m è

$$S = \{0, 1, \ldots, m-1\}.$$

Esempio. Analogamente sono sistemi completi di residui

- $S = \{1, 2, \ldots, m\}$;
- se m è pari $S = \{-m/2, \ldots, -1, 0, 1, \ldots, m/2 - 1\}$.

Teorema 3.7 – Dilatazione di un ICR

Sia S un insieme completo di residui modulo m e sia $k \in \mathbb{Z}$ tale che $(k, m) = 1$. Allora l'insieme

$$kS = \{ kx \mid x \in S \},$$

è ancora un insieme completo di residui modulo m.

Dimostrazione. Basta dimostrare che vale la caratterizzazione:

- $|kS| = m$ segue banalmente da dalla definizione di kS e da $|S| = m$.
- Siano $kx_1, kx_2 \in kS$ distinti modulo m. Se per assurdo $kx_1 \equiv kx_2 \pmod{m}$, si avrebbe
$$x_1 \equiv x_2 \pmod{\frac{m}{(k,m)}} \iff x_1 \equiv x_2 \pmod{m},$$
in quanto $(k, m) = 1$ per ipotesi. Ma ciò è ovviamente assurdo in quanto x_1, x_2 sono elementi distinti di un ICR(m).

□

Definizione 3.8 – Insieme completo di residui invertibili

Sia S un insieme completo di residui modulo m, si definisce *insieme completo di residui invertibili modulo* m, l'insieme

$$S^* = \{ s \in S \mid (s, m) = 1 \}.$$

Notazione. Spesso indicheremo un sistema completo di residui invertibili modulo m con la sigla IRR(m).

Proprietà. Dato $m \in \mathbb{N}$, allora $S^* \subseteq \mathbb{Z}$ è un IRR(m) se e soltanto se

- $|S^*| = \varphi(m)$;
- $(a, m) = 1$, $\forall\, a \in S^*$;
- $\forall\, x, y \in S^*, x \neq y \implies x \not\equiv y \pmod{m}$.

Teorema 3.9 – Dilatazione di un ICR

Sia S^* un insieme completo di residui invertibili modulo m e sia $k \in \mathbb{Z}$ tale che $(k, m) = 1$. Allora l'insieme

$$kS^* = \{ kx \mid x \in S^* \},$$

è ancora un insieme completo di residui completo modulo m.

Dimostrazione. La dimostrazione è analoga a quella sugli insiemi completi (teorema 3.7), resta solo da mostrare che

$$kx \in kS^* \implies (kx, m) = 1.$$

Ma $x \in S^*$ implica $(x, m) = 1$, mentre $(k, m) = 1$ per ipotesi, per cui

$$(x\,k, m) = 1.$$

□

Osservazione. Se S è ICR(m) allora $S + a$ è ancora ICR(m). Ma questo, in generale, non vale per gli IRR.

Teorema 3.10 – Combinazione lineare di ICR

Siano $a, b \in \mathbb{N}$ tali che $(a, b) = 1$ e supponiamo che S_a sia un ICR(a) e che S_b sia un ICR(b), allora

$$b\,S_a + a\,S_b,$$

è un ICR($a\,b$).

Dimostrazione. Mostriamo che vale la caratterizzazione:

- Vogliamo mostrare che $\#(b\,S_a + a\,S_b) = a\,b$. Ora

$$b\,S_a + a\,S_b = \{\, b\,x + a\,y \mid x \in S_a, y \in S_b \,\},$$

dove $|S_a| = a$ e $|S_b| = b$. Quindi ci basta verificare che se $(x_1, y_1) \neq (x_2, y_2)$ allora $x_1 b + y_1 a \not\equiv x_2 b + y_2 a$. Supponiamo per assurdo che $x_1 b + y_1 a \equiv x_2 b + y_2 a$, allora

dal momento che $(a, b) = 1$

$$\begin{aligned} b \mid a(y_1 - y_2) &\implies b \mid y_1 - y_2 \\ &\implies y_1 \equiv y_2 \pmod{b} \implies y_1 = y_2, \end{aligned}$$

per la caratterizzazione degli ICR. Analogamente segue che $x_1 = x_2$. Ma ciò è assurdo per la scelta di x_1, x_2, y_1, y_2.

- Il ragionamento precedente è valido anche per mostrare che

$$x_1 b + y_1 a \not\equiv x_2 b + y_2 a \pmod{a\,b}.$$

□

Corollario. Se S_a^* è un IRR(a) e S_b^* è un IRR(b), allora

$$b\,S_a^* + a\,S_b^*,$$

è un IRR($a\,b$).

Dimostrazione. La dimostrazione segue da quella precedente, eccetto per la verifica che

$$(b\,x + a\,y, a\,b) = 1.$$

Osserviamo che $(b\,x + a\,y, a) = (b\,x, a) = (x, a)$ in quanto $(a, b) = 1$, e che $(x, a) = 1$ poichè $x \in S$. Analogamente si mostra che $(b\,x + a\,y, b) = (a\,y, b) = (y, b) = 1$. Per cui

$$(a\,x + b\,y, a\,b) = 1.$$

□

3.3 TEOREMI DI EULERO E DI FERMAT

Teorema 3.11 – di Eulero-Fermat

Preso $m \in \mathbb{N}$, sia $a \in \mathbb{Z}$ tale che $(a, m) = 1$, allora

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Dimostrazione. Sia S^* un qualsiasi IRR(m), allora sappiamo che anche $a\,S^*$ è un IRR(m). Ora

$$\prod_{j \in S^*} j \equiv \prod_{a\,j \in S^*} a\,j \pmod{m}.$$

Inoltre, siccome $|S^*| = \varphi(m)$, avremo

$$\prod_{j \in S^*} j \equiv a^{\varphi(m)} \prod_{j \in S^*} j \pmod{m},$$

dove $(m, j) = 1$ comunque prendo $j \in S^*$, per cui

$$\left(m, \prod_{j \in S^*} j\right) = 1,$$

quindi

$$1 \equiv a^{\varphi(m)} \pmod{m}$$ □

Teorema 3.12 – Piccolo teorema di Fermat

Sia p primo e sia $a \in \mathbb{Z}$ tale che $p \nmid a$, allora

$$a^{p-1} \equiv 1 \pmod{p}$$

Dimostrazione. Dal momento che p è primo e che non divide a, avremo necessariamente

$$(a, p) = 1.$$

Quindi, applicando il teorema precedente, avremo

$$a^{\varphi(p)} \equiv 1 \pmod{p},$$

ovvero, ricordando che p primo implica $\varphi(p) = p - 1$,

$$a^{p-1} \equiv 1 \pmod{p}.$$ □

3.4 CONGRUENZE LINEARI

Definizione 3.13 – Congruenza lineare

Presi $a, b \in \mathbb{Z}$ e $m \in \mathbb{N}$ si definisce *congruenza lineare* un'equazione del tipo

$$a\,X \equiv b \pmod{m}.$$

Osservazione. Quando si parla del numero soluzioni di una congruenza lineare si fa riferimento al numero di elementi in un insieme completo di residui modulo m per cui la congruenza è valida. In altre parole si intende il numero di soluzioni mutualmente incongrue fra di loro.

Notazione. In generale, data $f\colon \mathbb{Z} \to \mathbb{Z}$, $m \in \mathbb{N}$, diremo che il numero di soluzioni di

$$f(x) \equiv 0 \pmod{m},$$

è la cardinalità di

$$N_f(m) = \{\, j \in \mathbb{N} \mid 0 \leqslant j < m, f(j) \equiv 0 \pmod{m} \,\}.$$

Inoltre diremo che la congruenza ammette soluzione se $N_f(m) \neq \emptyset$.

Teorema 3.14 – delle congruenze lineari

Siano $a, b \in \mathbb{Z}$ e sia $m \in \mathbb{N}$, allora

$$aX \equiv b \pmod{m},$$

ammette soluzione se e soltanto se

$$(a, m) \mid b.$$

In tal caso il numero di soluzioni è pari a (a, m).

Dimostrazione. Sfruttando la notazione precedentemente definita, la tesi risulta essere

$$N_{aX-b} \neq \emptyset \iff (a, m) \mid b.$$

$\Rightarrow$) Supponiamo che $x_0 \in N_{aX-b}$, ovvero

$$a x_0 \equiv b \pmod{m},$$

quindi esisterà $y_0 \in \mathbb{Z}$ tale che $x_0 a - b = y_0 m$, ovvero

$$b = x_0 a - y_0 m \implies (a, m) \mid b.$$

$\Leftarrow$) Supponiamo che $(a, m) \mid b$, necessariamente avremo che

$$\left(\frac{a}{(a,m)}, \frac{m}{(a,m)}\right) = 1.$$

Ora, preso $M = \left\{ 0, 1, \ldots, \frac{m}{(a,m)} - 1 \right\}$ un $\mathrm{ICR}\left(\frac{m}{(a,m)}\right)$, avremo che

$$\frac{a}{(a,m)} M = \left\{ 0, \frac{a}{(a,m)}, \frac{2a}{(a,m)}, \ldots, \frac{a}{(a,m)}\left(\frac{m}{(a,m)} - 1\right) \right\},$$

è ancora un $\mathrm{ICR}\left(\frac{m}{(a,m)}\right)$. Inoltre, dal momento che $(a, m) \mid b$, esisterà un $x_0 \in \mathbb{Z}$ tale che

$$\frac{b}{(a,m)} \equiv \frac{a}{(a,m)} x_0 \pmod{\frac{m}{(a,m)}},$$

ma da ciò segue subito che $b \equiv a x_0 \pmod{m}$.

Resta da mostrare l'affermazione sul numero di soluzioni. Se x_0 è una soluzione, avremo che

$$x_k = x_0 + k\frac{m}{(a,m)}, \text{ con } k = 0, \dots, (a,m) - 1,$$

sono tutte soluzioni non congrue fra di loro, infatti

$$\begin{aligned} a\,x_k &= a\,x_0 + k\frac{a}{(a,m)}m \\ &\equiv a\,x_0 \equiv b \pmod{m}. \end{aligned}$$

D'altronde ogni altra soluzione x ha la medesima forma, infatti

$$a\,x \equiv b \equiv a\,x_0 \pmod{m},$$

implica che

$$\begin{aligned} m \mid a(x - x_0) &\iff \frac{m}{(a,m)} \mid \frac{a}{(a,m)}(x - x_0) \\ &\implies \frac{m}{(a,m)} \mid x - x_0 \implies x = x_0 + k\frac{m}{(a,m)}, \end{aligned}$$

in quanto $\left(\frac{m}{(a,m)}, \frac{a}{(a,m)}\right) = 1$. □

Teorema 3.15 – cinese dei resti

Siano $m_1, \dots, m_s \in \mathbb{N}$ e siano $a_1, \dots, a_j \in \mathbb{Z}$ tali che $(m_i, m_j) = 1, \forall\, i \neq j$, allora

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ \dots \\ x \equiv a_s \pmod{m_s} \end{cases}$$

ammette un'unica soluzione modulo $m_1 \cdot \ldots \cdot m_s$.

Dimostrazione. Per ogni $j \in \{1, \dots, s\}$ poniamo

$$M_j = \frac{m_1 \cdot \ldots \cdot m_s}{m_j},$$

per definizione avremo quindi $(M_j, m_j) = 1$. Prendiamo quindi $M_j X \equiv a_j \pmod{m_j}$ che è una congruenza lineare che, per il teorema precedente, ammette un'unica soluzione $q_j \pmod{m_j}$. Posto

$$x_0 = M_1 q_1 + \ldots + M_s q_s,$$

avremo che

$$x_0 \equiv M_j q_j \equiv a_j, \forall\, j \in \{1, \dots, s\}.$$

Resta da mostrare l'unicità. Supponiamo che x_1, x_2 siano soluzioni del sistema di congruenze, allora

$$\begin{cases} x_1 \equiv a_j \pmod{m_j} \\ x_2 \equiv a_j \pmod{m_s} \end{cases}$$

ovvero $m_j \mid x_1 - x_2$ e, siccome $(m_i, m_j) = 1$, avremo

$$m_1 \cdot \ldots \cdot m_s \mid x_1 - x_2,$$

che implica $x_1 \equiv x_2 \pmod{m_1 \cdot \ldots \cdot m_s}$. □

Esempio. Si trovino tutte le soluzioni di

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 4 \\ x \equiv 4 \pmod 5 \end{cases}$$

nell'intervallo $[-500, 500]$.

Soluzione. Per il teorema cinese dei resti esiste un'unica soluzione modulo 60.
La prima equazione ci dice $x = 2 + 3t$, mentre la seconda $x = 3 + 4s$, da cui

$$3t + 2 = 3 + 4s \iff 3t \equiv 1 \pmod 4,$$

quindi $t \equiv 3 \pmod 4 \iff t = 3 + 4u$ che ci permette di ridurre le prime due equazioni alla singola

$$x = 2 + 3(3 + 4u) = 11 + 12u.$$

Dalla terza otteniamo

$$11 + 12u \equiv 4 \iff 12u \equiv 3 \iff u \equiv 4 \pmod 5,$$

ovvero $u = 4 + 5y$, da cui

$$x = 11 + 12(4 + 5y) = 59 + 60y \iff x \equiv 59 \pmod{60}.$$

Resta da trovare y tale che

$$-500 \leqslant 59 + 60y \leqslant 500,$$

ovvero

$$\begin{aligned} -559 \leqslant 60y \leqslant 441 &\iff -\frac{559}{60} \leqslant y \leqslant \frac{441}{60} \\ &\iff \left[-\frac{559}{60}\right] + 1 \leqslant u \leqslant \left(\frac{441}{60}\right) \\ &\iff -9 \leqslant u \leqslant 7. \end{aligned}$$

3.5 CONGRUENZE POLINOMIALI

Notazione. Preso un polinomio $f \in K[X]$ indicheremo il suo grado con il simbolo ∂f.

Teorema 3.16 – Interpolazione modulo p

Sia $f \in \mathbb{Z}[X]$, allora esisterà $g \in \mathbb{Z}[X]$ tale che

$$\partial g < p \qquad \text{e} \qquad f(a) \equiv g(a) \pmod p, \ \forall\, a \in \mathbb{Z}.$$

Dimostrazione. Dimostriamo il teorema prima nel caso semplice del polinomio avente un solo coefficiente non nullo per poi mostrare il caso generale.
Supponiamo che $f(x) = \alpha_n x^n$. Se $n = 0$ avremmo che banalmente $f(x) = \alpha_n$ e la tesi sarebbe banalmente soddisfatta. Supponiamo quindi che $n > 1$, avremo

$$n = q(p-1) + r, \text{ con } 1 \leqslant r \leqslant p-1,$$

infatti, per la divisione euclidea,

$$n = q_1(p-1) + r_1, \text{ con } 0 \leqslant r_1 < p-1,$$

in particolare, se fosse $r_1 = 0$, avremmo $n = (q_1 - 1)(p-1) + p_1$, quindi, in tal caso, mi basterebbe imporre

$$\begin{cases} q = q_1 - 1 \\ r = p - 1 \end{cases}$$

Per cui abbiamo $x^n = \left(x^{p-1}\right)^q x^r$, posto $g(x) = a_n x^r$ otteniamo

$$f(a) \equiv g(a) \pmod{p}, \forall\, a \in \mathbb{Z},$$

infatti, se $p \mid a$ si ha banalmente $0 \equiv 0 \pmod{p}$. Se, invece, $p \nmid a$ otteniamo

$$\begin{aligned} f(a) = a_n a^n &= a_n \left(a^{p-1}\right)^q a^r \\ &\equiv a_n a^r = g(a) \pmod{p}, \end{aligned}$$

per il teorema di Fermat (3.12).
In generale, se $f(x) = a_0 + a_1 x + \ldots + a_n x^n$, possiamo scrivere, comunque preso i fra 2 e n che

$$i = q_i(p-1) + r_i, \text{ con } 1 \leqslant r_i \leqslant p-1,$$

che vale per ragionamenti analoghi al caso iniziale. Definiamo quindi

$$g(x) = \sum_{j=0}^{n} a_j x^{r_j},$$

per definizione si avrà

$$\partial g \leqslant p-1 \qquad \text{e} \qquad f(a) \equiv g(a) \pmod{p},$$

semplicemente iterando il caso iniziale ad ogni potenza di x. □

Proposizione 3.17 – Interpolazione modulo p (caso generale)

Sia $\sigma\colon \mathbb{Z} \to \mathbb{Z}$ e sia p primo e supponiamo che

$$\sigma(a) \equiv \sigma(b) \pmod{p}, \forall\, a \equiv b \pmod{p}.$$

Allora esiste un'unica $g_\sigma \in \mathbb{Z}[X]$ con $\partial g_\sigma < p$ tale che

$$g_\sigma(a) \equiv \sigma(a) \pmod{p}, \forall\, a \in \mathbb{Z}.$$

Dimostrazione. DA FARE! □

Teorema 3.18 – di Lagrange

Sia $f \in \mathbb{Z}[X]$ con $\partial f = n$, dove

$$f(x) = a_n x^n + \ldots + a_1 x + a_0.$$

Supponiamo che $p \nmid a_n$, allora f ha al più n radici $\pmod{p}$

Dimostrazione. Preso

$$\begin{aligned} N_f &= \{\, j \in \mathbb{Z} \mid 0 \leqslant j \leqslant p-1, f(j) \equiv 0 \pmod{p} \,\} \\ &= \{\, j \in S \mid f(j) \equiv 0 \pmod{p} \,\}, \end{aligned}$$

con S un qualsiasi ICR(p), allora si tratta di mostrare che

$$\#N_f \leqslant \min\{\, \partial f, p \,\}.$$

$\#N_f \leqslant p$ *necessariamente in quanto* $N_f \subset S$ *che è un ICR*(p)

Mostriamolo quindi per induzione su n:

- Se $n = 0$ allora f è un polinomio costante non nullo, quindi
$$\#N_f = 0 \leqslant 0.$$
- Se $n = 1$ avremo $f(x) = ax + b$, quindi, per il teorema 3.14, avremo
$$\#N_f = 1 \leqslant 1.$$
- Posto quindi $n > 1$ supponiamo che la tesi sia valida per $k < n$. Se per assurdo $x_0, \dots, x_n$ sono $n+1$ radici tali che $x_i \not\equiv x_j \pmod p$, avremo che
$$\begin{aligned} f(x) - f(x_0) &= \sum_{j=0}^{n} a_j x^j - a_j x_0^j \\ &= \sum_{j=0}^{n} a_j \left(x^j - x_0^j\right) \\ &= \sum_{j=0}^{n} a_j (x - x_0)\left(x^{j-1} + x^{j-2}x_0 + \dots + x\,x_0^{j-2} + x_0^{j-1}\right) \\ &= (x - x_0)g(x), \end{aligned}$$
con $g(x) \in \mathbb{Z}[X]$ e $\partial g = n - 1$. Ora, comunque preso $j \in \{1, \dots, n\}$, avremo
$$f(x_j) - f(x_0) \equiv 0 \pmod p,$$
ma
$$f(x_j) - f(x_0) \equiv \cancel{(x_j - x_0)} g(x_j) \equiv 0 \pmod p.$$
Quindi $x_1, \dots, x_n$ sono n radici di $g(x) \equiv 0 \pmod p$ tutte mutualmente incongrue. Ciò è assurdo per ipotesi induttiva, da cui la tesi. □

posso cancellare $(x_j - x_0)$ in quanto non sono congrui e ogni elemento non nullo è invertibile $\pmod p$

Teorema 3.19 – Corollario di Lagrange

Sia $f \in \mathbb{Z}[X]$ e supponiamo che f abbia un numero di radici $\pmod p$ superiore a ∂f, allora
$$p \mid a_j, \ \forall\, j = 0, \dots, n.$$

Dimostrazione. Sia $f(x) = a_0 + \dots + a_n x^n$ e supponiamo per assurdo che esista
$$k = \max\{\, h \mid p \nmid a_h \,\},$$
ciò significa che possiamo riscrivere f come
$$f(x) = g(x) + a_{k+1}x^{k+1} + \dots + a_n x^n,$$
dove $g(x) = a_0 + \dots + a_k x^k$ e con i termini restanti di f che sono tutti divisibili per p. Quindi, per ognuna delle radici x_i di f, che ricordiamo essere maggiori di n, avremo
$$f(x_i) \equiv g(x_i) \pmod p,$$
per cui anche g ha più di n radici $\pmod p$. Ma $\partial g = k \leqslant n$ e g soddisfa le ipotesi del teorema di Lagrange, per cui
$$\#N_g \leqslant k.$$
Ma ciò è assurdo in quanto abbiamo stabilito che $\#N_g > n$, da cui la tesi. □

Teorema 3.20 – di Wilson

Sia p primo, allora

$$(p-1)! \equiv -1 \pmod{p}.$$

Dimostrazione. Se $p = 2$ avremo

$$1 \equiv -1 \pmod{2},$$

analogamente se $p = 3$

$$2 \equiv -1 \pmod{3}.$$

Possiamo quindi supporre $p \geqslant 5$. Il polinomio

$$f(x) = x^{p-1} - 1 - \prod_{j=1}^{p-1}(x-j),$$

ha $\partial f = p-2$, dove il coefficiente di x^{p-2} è $\frac{p(p-1)}{2} \neq 0$. Ora, comunque preso $x_0 \in \mathbb{Z}$ tale che $p \nmid x_0$, avremo $f(x_0) \equiv 0 \pmod{p}$ in quanto

$$p \nmid x_0 \implies x_0^{p-1} - 1 \equiv 0 \pmod{p},$$

per il teorema di Fermat, mentre

$$\prod_{j=1}^{p-1}(x_0 - j) \equiv 0 \pmod{p},$$

in quanto se $p \nmid x_0$ esisterà $j \in \{1, \dots, p-1\}$ tale che $j \equiv x_0 \pmod{p}$. In particolare f ha $p-1$ radici $\pmod{p}$, che sono in numero maggiore del suo grado. Applicando il teorema precedente avremo che p divide tutti i coefficienti di f, incluso il suo termine noto che è

$$\begin{aligned} f(0) &= -1 - \prod_{j=1}^{p-1} -j = -1 - (-1)^{p-1}(p-1)! \\ &= -1 - (p-1)!, \end{aligned}$$

in quanto $p-1$ è necessariamente pari. Abbiamo quindi dimostrato che $p \mid -1 - (p-1)!$, ovvero

$$(p-1)! \equiv -1 \pmod{p}.$$ □

3.6 ORDINE

Definizione 3.21 – Ordine di un elemento modulo m

Siano $a \in \mathbb{Z}$ e $m \in \mathbb{N}$ tali che $(a, m) = 1$. Si definisce *l'ordine di* a *modulo* m come il più piccolo naturale n per cui $a^n \equiv 1 \pmod{m}$, ovvero

$$\operatorname{ord}_m(a) = \min\{\, n \in \mathbb{N} \mid a^n \equiv 1 \pmod{m} \,\}.$$

Osservazione. Tale intero esiste in quanto, per Eulero, si ha

$$a^{\varphi(m)} \equiv 1 \pmod{m},$$

quindi, se chiamiamo S l'insieme di cui l'ordine di a è il minimo, avremo

$$\varphi(m) \in S \implies S \neq \emptyset,$$

ovvero S ammette minimo per il buon ordinamento.

Notazione. In alcuni libri si trova l'ordine di a modulo m con la dicitura "esponente a cui a appartiene modulo m".

Teorema 3.22 – Proprietà dell'ordine

Siano $a \in \mathbb{Z}$ e $m \in \mathbb{N}$ tali che $(a, m) = 1$. Se $n = \mathrm{ord}_m(a)$, allora

$$1, a, a^2, \ldots, a^{n-1},$$

sono mutualmente non congruenti modulo m.

Dimostrazione. Presi $j \neq k$, supponiamo per assurdo che $a^j \equiv a^k \pmod{m}$. Supponiamo inoltre, per semplicità, che $1 \leqslant j < k \leqslant n-1$, avremo quindi

$$a^j(a^{k-j} - 1) \equiv 0 \pmod{m},$$

quindi, dal momento che $(a, m) = 1$ implica $(a^j, m) = 1$, avremo

$$a^{k-j} \equiv 1 \pmod{m},$$

che è assurdo in quanto $k - j < n$. □

Teorema 3.23 – Congruenza modulo l'ordine

Siano $a \in \mathbb{Z}$ e $m \in \mathbb{N}$ tali che $(a, m) = 1$ e sia $n = \mathrm{ord}_m(a)$. Supponiamo che $l, k \in \mathbb{N}$ tali che $a^l \equiv a^k \pmod{m}$, allora

$$l \equiv k \pmod{n}.$$

Dimostrazione. Se $l = k$ la tesi è banalmente verificata. Supponiamo quindi $l > k$, applicando la divisione euclidea con n avremo

$$l = n\,q_1 + r_1, \text{ con } 0 \leqslant r_1 < n,$$
$$k = n\,q_2 + r_2, \text{ con } 0 \leqslant r_2 < n,$$

da cui

$$a^l \equiv \left(a^n\right)^{q_1} a^{r_1} \equiv a^{r_1} \pmod{m},$$
$$a^k \equiv \left(a^n\right)^{q_2} a^{r_2} \equiv a^{r_2} \pmod{m},$$

da cui, per ipotesi, $a^{r_1} \equiv a^{r_2} \pmod{m}$. Ma $0 \leqslant r_1, r_2 < n$, quindi per il teorema precedente, avremo necessariamente $r_1 = r_2$. Quindi

$$k \equiv l \pmod{n},$$

in quanto k, l danno luogo allo stesso modulo se divisi per n. □

Osservazione. In particolare, se $k = 0$, avremo $a^l \equiv 1 \pmod{m}$ e quindi, per il teorema, $l \equiv 0 \pmod{n}$, ovvero

$$\operatorname{ord}_m(a) \mid l.$$

3.7 TEOREMA DI GAUSS

Definizione 3.24 – Radice primitiva

Siano $a \in \mathbb{Z}$ e $m \in \mathbb{N}$ tali che $(a, m) = 1$. Diremo che a è una *radice primitiva modulo* m se

$$\operatorname{ord}_m(a) = \varphi(m).$$

Proposizione 3.25 – Numero di elementi di ordine n modulo p

Sia p primo e sia $n \in \mathbb{N}$ tale che $n \mid p-1$. Allora in $(\mathbb{Z}/p\mathbb{Z})^*$ esistono $\varphi(n)$ elementi di ordine n.

Dimostrazione. Supponiamo che $n \mid p-1$, sia $\psi(n)$ il numero di elementi in $(\mathbb{Z}/p\mathbb{Z})^*$ che hanno ordine n. Vogliamo mostrare che $\psi(n) = \varphi(n)$.
Definiamo

$$N_{x^n-1}(p) = \#\left\{ x \in (\mathbb{Z}/p\mathbb{Z})^* \;\middle|\; x^n \equiv 1 \pmod{p} \right\},$$

che corrisponde al numeri di radici $\pmod{p}$ di $x^n - 1$. Per costruzione avremo che

$$N_{x^n-1}(p) = \sum_{d \mid n} \psi(d),$$

infatti, se α è una radice di $x^n - 1 \pmod{p}$, avremo che $\operatorname{ord}_p(\alpha) \mid n$ per il teorema 3.23. Quindi

$$\left\{ x \in (\mathbb{Z}/p\mathbb{Z}) \;\middle|\; x^n \equiv 1 \pmod{p} \right\} = \bigsqcup_{d \mid n} \left\{ \alpha \in (\mathbb{Z}/p\mathbb{Z}) \;\middle|\; \operatorname{ord}_p(\alpha) = d \right\}.$$

Supponendo che $N_{x^n-1}(p) = n$, avremmo

$$n = \sum_{d \mid n} \psi(d),$$

ovvero n sarebbe la trasformata di Dirichlet di $\psi(d)$, quindi, tramite la formula di inversione di Möebius, otterremmo

$$\psi(n) = \sum_{d \mid n} \mu(d) \frac{n}{d} = \varphi(n).$$

Resta quindi da mostrare $N_{x^n-1}(p) = n$. Per Lagrange sappiamo che $N_{x^n-1}(p) \leqslant n$, inoltre per ipotesi $n \mid p-1$, da cui

$$x^{p-1} - 1 = (x^n - 1)(x^{p-1-n} + x^{p-1-2n} + \ldots + x^n + 1), \qquad \text{k } n = p-1$$

dove, per Fermat, $x^{p-1} - 1$ ha $p-1$ radici $\pmod{p}$, mentre Lagrange ci dice che $x^n - 1$ ne ha al più n e che il secondo fattore ne ha al più $p-1-n$, da cui

$$\begin{aligned} N_{x^n-1}(p) &= N_{x^{p-1}-1}(p) - N_{x^{p-1-n}+\ldots+x^n-1}(p) \\ &= p - 1 - N_{x^{p-1-n}+\ldots+x^n-1}(p) \geqslant p - 1 - (p - 1 - n) \\ &= n. \end{aligned}$$

Ovvero

$$N_{x^n-1}(p) = n.$$

□

Corollario. In $(\mathbb{Z}/p\,\mathbb{Z})^*$ ci sono precisamente $\varphi(p-1)$ radici primitive.

Dimostrazione. Per definizione una radice primitiva modulo p ha ordine $\varphi(p) = p-1$. Ovviamente $p-1 \mid p-1$, quindi per la proposizione esistono precisamente $\varphi(p-1)$ radici primitive modulo p. □

Teorema 3.26 – Sollevamento di una radice primitiva modulo p

Sia p primo e sia g una radice primitiva modulo p. Allora esiste $t \in \mathbb{Z}$ tale che

$$(g+tp)^{p-1} = 1 + up,$$

dove $p \nmid u$ e $g+tp$ è una radice primitiva modulo p^α, comunque preso $\alpha \in \mathbb{N}$.

Dimostrazione. Troncando il binomio di Newton otteniamo

$$(g+tp)^{p-1} = g^{p-1} + (p-1)g^{p-2}tp + rp^2, \text{ con } r \in \mathbb{Z}.$$

Per Fermat $g^{p-1} \equiv 1 \pmod p$, ovvero $g^{p-1} = 1 + qp$. Quindi

$$(g+tp)^{p-1} = 1 + p\big(q + (p-1)t\,g^{p-2} + rp\big) = 1 + pu,$$

dove $u = q + (p-1)g^{p-2}t + rp$. Resta quindi da mostrare che esiste t tale che $p \nmid u$. Consideriamo

$$\left\{ q + (p-1)g^{p-2}t \pmod p \;\middle|\; t \in \mathbb{Z}/p\,\mathbb{Z} \right\}.$$

Da g radice primitiva $\pmod p$ e $p-1$ coprimo con p abbiamo

$$\big((p-1)g^{p-2}, p\big) = 1-$$

Ricordando che $a(\mathbb{Z}/p\,\mathbb{Z}) + b = \mathbb{Z}/p\,\mathbb{Z}$ se $(a,p) = 1$, avremo

$$\left\{ q + (p-1)g^{p-2}t \pmod p \;\middle|\; t \in \mathbb{Z}/p\,\mathbb{Z} \right\} = \mathbb{Z}/p\,\mathbb{Z},$$

ovvero esiste $t \in \mathbb{Z}$ cercato.
Dobbiamo mostrare che $g+tp$ è una radice primitiva $\pmod{p^\alpha}$. Per il binomio di Newton

$$\begin{aligned}(g+tp)^{p(p-1)} = (1+up)^p &= 1 + \binom{p}{1}up + \binom{p}{2}(up)^2 + \dots \\ &= 1 + up^2 + rp^3 = 1 + p^2(u+rp) \\ &= 1 + u_2p^2, \text{ con } p \nmid u_2.\end{aligned}$$

Analogamente

$$\begin{aligned}(g+tp)^{p^2(p-1)} = (1+u_2p^2)^p &= 1 + pu_2p^2 + rp^4 \\ &= 1 + p^3(u_2 + r, \pi) = 1 + u_3p^3, \text{ con } p \nmid u_3.\end{aligned}$$

lo si può verificare per induzione

In generale, avremo

$$(g+tp)^{p^{r-1}(p-1)} = 1 + u_rp^r, \text{ con } p \nmid u_r,$$

ovvero $(g+tp)^{\varphi(p^r)} \equiv 1 \pmod{p^r}$, che implica, per Fermat,

$$\operatorname{ord}_{p^r}(g+tp) \mid \varphi(p^r).$$

□

Esempio. Consideriamo $m = 125 = 5^3$, se prendiamo il suo IRR avremo

$$(\mathbb{Z}/p\,\mathbb{Z})^* = \{\,1,2,4,3\,\} = \{\,1,2,2^2,2^3\,\},$$

quindi 2 è una radice primitiva modulo 5. Proviamo a sollevarla ad una radice modulo 125 tramite il teorema.
Dobbiamo quindi trovare t tale che

$$(2+5t)^4 = 1+5u,$$

con $5 \nmid u$. Se $t = 0$ otteniamo

$$2^4 = 16 = 1+3\cdot 5,$$

con $5 \nmid 3$, per cui 2 è una radice primitiva modulo 5^α per ogni $\alpha \in \mathbb{N}$.

Osservazione. Supponiamo che $a \in (\mathbb{Z}/m\,\mathbb{Z})^*$, allora è ben noto che

$$\operatorname{ord}_m a^k = \frac{\operatorname{ord}_m a}{(k, \operatorname{ord}_m a)}.$$

Per cui, se $(k, \operatorname{ord}_m a) = 1$, si ha $\operatorname{ord}_m a^k = \operatorname{ord}_m a$. Quindi, se a è una radice primitiva $\pmod m$, allora

$$\left\{\, a^k \;\middle|\; 1 \leqslant k \leqslant \varphi(m), (k, \varphi(m)) = 1 \,\right\},$$

è l'insieme di tutte e sole le radici primitive.

Esempio. Si esibiscano tutte le radici primitive modulo 25.

Soluzione. $25 = 5^2$, quindi per il teorema di Gauss esisteranno radici primitive. Dall'esempio precedente sappiamo che 2 è una radice primitiva di 5^α. In particolare, per l'osservazione precedente, avremo precisamente $\varphi\big(\varphi(25)\big) = \varphi(20) = 8$ radici primitive $\pmod{25}$ del tipo 2^k con k minore di $\varphi(25)$ e coprime con $\varphi(25)$, ovvero

$$2, 2^3, 2^7, 2^9, 2^{11}, 2^{13}, 2^{17}, 2^{19}.$$

Esempio. Si esibiscano tutte le radici modulo 49.

Soluzione. $49 = 7^2$, consideriamo quindi 3 che è una radice primitiva modulo 7 e proviamo a sollevarla. Vogliamo t tale che

$$(3+7t)^6 = 1+7u,$$

con $7 \nmid u$. Se $t = 0$ abbiamo

$$3^6 = 729 = 1+728 = 1+7\cdot 104,$$

dove $7 \nmid 104$. Quindi 3 è una radice primitiva modulo 49. In particolare avremo $\varphi\big(\varphi(49)\big) = \varphi(42) = 12$ radici primitive $\pmod{49}$ del tipo 3^k, ovvero

$$3, 3^5, 3^{11}, 3^{13}, 3^{17}, 3^{19}, 3^{23}, 3^{25}, 3^{29}, 3^{31}, 3^{37}, 3^{41}.$$

Teorema 3.27 – Sollevamento di una radice primitiva modulo p^r

Sia p primo e sia g una radice primitiva dispari modulo p^r. Allora g è una radice primitiva modulo $2p^r$.

Dimostrazione. Supponiamo che $g^{\varphi(p^r)} \equiv 1 \pmod{p^r}$. Per ipotesi $g^{\varphi(p^r)}$ e 1 sono dispari, quindi $p^r \mid g^{\varphi(p^r)} - 1$ che è pari. Ma p^r è necessariamente dispari, per cui

$$2k\,p^r = g^{\varphi(p^r)} - 1,$$

ovvero

$$2p^r \mid g^{\varphi(p^r)} - 1 \iff g^{\varphi(p^r)} \equiv 1 \pmod{2p^r},$$

per cui $k = \operatorname{ord}_{2p^r} \mid \varphi(p^r)$.
Osserviamo che $p \neq 2$, per cui $\varphi(p^r) = \varphi(2p^r)$. Ora, per ragionamenti analoghi ai precedenti si ha

$$g^k \equiv 1 \pmod{2p^r} \implies g^k \equiv 1 \pmod{p^r},$$

ovvero $\varphi(p^r) = \operatorname{ord}_{p^r} g \mid k$. Quindi

$$\operatorname{ord}_{2p^r} g = \varphi(p^r) = \varphi(2p^r).$$

□

Teorema 3.28 – di Gauss

Preso $m \in \mathbb{N}$ esiste una radice primitiva modulo m se e soltanto se

$$m = 2, 4, p^\alpha, 2p^\alpha, \text{ con } p \geqslant 3.$$

⇐) *Dimostrazione.* Per $m = 2, 4$ la tesi è banalmente verificata rispettivamente da $1 \pmod 2$ e $3 \pmod 4$. Per i casi $m = p^\alpha, 2p^\alpha$ la dimostrazione segue dai risultati precedentemente visti in questo paragrafo.

⇒) Sia $m \in \mathbb{N}$ e consideriamo la sua fattorizzazione unica $m = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$. Sia

$$l = \left[\varphi(p_1^{\alpha_1}), \ldots, \varphi(p_s^{\alpha_s})\right],$$

il minimo comune multiplo delle funzioni di Eulero calcolate nei fattori primi. Per la moltiplicatività di φ avremo che $l \mid \varphi(m) = \varphi(p_1^{\alpha_1}), \ldots, \varphi(p_s^{\alpha_s})$. Vogliamo determinare quando vale $l = \varphi(m)$, ovvero

$$\left[(p_1 - 1)p_1^{\alpha_1 - 1}, \ldots, (p_s - 1)p_s^{\alpha_s - 1}\right] = (p_1 - 1)p_1^{\alpha_1 - 1} \cdot \ldots \cdot (p_s - 1)p_s^{\alpha_s - 1}$$

Sicuramente tale uguaglianza vale quando $m = p^\alpha$ con $p \geqslant 2$. D'altronde sarà certamente falsa se $m = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$ con $s \geqslant 2$ e $p_i \geqslant 3$, infatti in questo caso $p_i - 1$ è pari e quindi $l \mid \frac{\varphi(m)}{2}$.
Analogamente se $s \geqslant 2, p_1 = 2$ ma $\alpha_1 \geqslant 2$ si avrebbe $2 \mid (p_1 - 1)p_1^{\alpha_1 - 1}$ e nuovamente $l \mid \frac{\varphi(m)}{2}$.
In conclusione gli unici casi in cui vale l'uguaglianza sono per $m = p_1^{\alpha_1}$ con $p_1 \geqslant 2$ oppure $m = 2p_2^{\alpha_2}$ con $p_2 \geqslant 3$.
In tutti gli altri casi, preso $a \in \mathbb{Z}$ con $(a, m) = 1$ si avrebbe

$$a^l \equiv \left(a^{\varphi(p_j^{\alpha_j})}\right)^{\frac{l}{\varphi(p_j^{\alpha_j})}} \equiv 1 \pmod{p_j^{\alpha_j}},\ \forall\, j,$$

ovvero $a^l \equiv 1 \pmod m$. Quindi non potrà mai accadere che $\operatorname{ord}_m a = \varphi(m)$, poichè abbiamo dimostrato che

$$\operatorname{ord}_m a \mid l < \varphi(m).$$

Resta da dimostrare che non esistono radici primitive nel caso $m = 2^\alpha$ con $\alpha \geqslant 3$. Mostriamo per induzione su $k \geqslant 3$ che, preso $a \in \mathbb{Z}$ dispari con $(a, 2^k) = 1$ si ha

$$a^{\frac{1}{2}\varphi(2^k)} \equiv 1 \pmod{2^k},$$

ovvero che

$$\operatorname{ord}_{2^k} a \mid \frac{1}{2}\varphi(2^k) < \varphi(2^k).$$

Per $k = 3$ sappiamo già che $a^2 \equiv 1 \pmod 8$, supponiamo quindi che sia vero per ogni $u < k$, avremo quindi

$$a^{\frac{1}{2}\varphi(2^u)} \equiv 1 \pmod{2^u} \iff a^{2^{u-2}} = 1 + h\,2^u.$$

Mostriamolo quindi per k:

$$\begin{aligned} a^{\frac{1}{2}\varphi(2^k)} &= a^{2^{k-2}} = \left(a^{2^{k-3}}\right)^2 = \left(a^{\frac{1}{2}\varphi(2^{k-1})}\right)^2 && \text{applicando l'ipotesi induttiva} \\ &= \left(1 + h\,2^{k-1}\right)^2 = 1 + h\,2^k + h^2 2^{2k-2} \\ &= 1 + h\,2^k\left(1 + h\,2^{k-2}\right) && k \geqslant 3 \implies 2k - 2 > k \\ &= 1 + h'2^k, \end{aligned}$$

ovvero

$$a^{\frac{1}{2}\varphi(2^k)} \equiv 1 \pmod{2^k}. \qquad \square$$

Corollario. $(\mathbb{Z}/m\mathbb{Z})^*$ è ciclico se e soltanto se $m = 2, 4, p^\alpha, 2p^\alpha$, con $p \geqslant 3$.

4 RESIDUI QUADRATICI

4.1 INTRODUZIONE

Definizione 4.1 – Residuo quadratico

Sia $p \geqslant 3$ primo. $a \in \mathbb{Z}$ si definisce *residuo quadratico modulo* p se $p \nmid a$ e

$$x^2 \equiv a \pmod{p},$$

è risolubile.

Osservazione. Il caso $p \mid a$ viene escluso in quanto $x^2 \equiv a \equiv 0 \pmod{p}$ ammette come unica soluzione $x_0 = 0$ che risulta di scarso interesse.

Osservazione. Se $p = 2$, la congruenza $x^2 \equiv a \pmod{2}$ può sempre essere risolta e vale

$$x_0 = \begin{cases} 0 & \text{se } 2 \mid a \\ 1 & \text{se } 2 \nmid a \end{cases}$$

Osservazione. In generale se $p \geqslant 3$ avremo

$$N_{x^2-a} = \begin{cases} 0 \\ 1 \quad \text{se } p \mid a \\ 2 \end{cases}$$

dove il valore 2 viene assunto quando esiste $b \neq 0$ tale che $b^2 \equiv a \pmod{p}$, in tal caso infatti $p - b$ è un'altra soluzione.

Teorema 4.2 – Cardinalità dei residui quadratici modulo p

Sia $p \geqslant 3$, allora l'insieme dei residui quadratici modulo p

$$\mathcal{RQ}(p) = \{\, a \in \mathbb{Z}/p\mathbb{Z} \mid a \text{ residuo quadratico modulo } p \,\},$$

ha precisamente $\frac{p-1}{2}$ elementi, ciascuno dei quali è congruo ad uno dei seguenti

$$1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2,$$

i quali sono mutualmente incongrui.

Dimostrazione. Supponiamo che $i^2 \equiv j^2 \pmod{p}$ con $1 \leqslant i < j \leqslant \frac{p-1}{2}$, allora

$$p \mid i^2 - j^2 \iff p \mid (j-i)(j+i) \iff p \mid j-i \quad \text{oppure} \quad p \mid j+i,$$

ma entrambi i casi non possono accadere in quanto $j - i < \frac{p-1}{2}$ e $j + i < p - 1$. Quindi tutti gli interi della lista sono mutualmente incongrui.
Supponiamo che a sia un residuo quadratico modulo p, allora esiste $b \in \mathbb{Z}/p\mathbb{Z}$ tale che

$$a \equiv b^2 \pmod{p}, \qquad \text{con} \qquad 0 < b \leqslant \frac{p-1}{2} \quad \text{oppure} \quad \frac{p-1}{2} < b \leqslant p-1.$$

Se $0 < b < \frac{p-1}{2}$ abbiamo soddisfatto la tesi. Supponiamo quindi che $\frac{p-1}{2} < b \leqslant p-1$, posto $b' = p - b$ avremo

$$p - (p-1) \leqslant b < p - \left(\frac{p-1}{2}\right) \iff 1 \leqslant b' < \frac{p+1}{2},$$

ovvero $0 < b' \leqslant \frac{p-1}{2}$. Mostriamo infine che b' è un residuo quadratico modulo p:

$$b'^2 = (p-b)^2 \equiv (-b)^2 \equiv a \pmod{p}. \qquad \square$$

4.2 IL SIMBOLO DI LEGENDRE

Definizione 4.3 – Simbolo di Legendre

Sia $a \in \mathbb{Z}$ e sia $p \geqslant 3$ primo, definiamo *simbolo di Legendre* la seguente notazione

$$\left(\frac{a}{p}\right)_L = \begin{cases} 1 & \text{se } a \in \mathcal{RQ}(p) \\ 0 & \text{se } p \mid a \\ -1 & \text{se } p \notin \mathcal{RQ}(p) \end{cases}$$

Proprietà. Sia $a \in \mathbb{Z}$ e sia p un primo dispari, allora

$$1 + \left(\frac{a}{p}\right)_L = \begin{cases} 2 & \text{se } a \in \mathcal{RQ}(p) \\ 1 & \text{se } p \mid a \\ 0 & \text{se } a \notin \mathcal{RQ}(p) \end{cases} = N_{x^2-a}(p).$$

Teorema 4.4 – Criterio di Eulero

Sia $a \in \mathbb{Z}$ e sia p un primo dispari, allora

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)_L \pmod{p}.$$

Dimostrazione. Se a è un residuo quadratico allora $a \equiv b^2 \pmod{p}$, da cui

$$a^{\frac{p-1}{2}} \equiv b^{\frac{p-1}{2}2} \equiv b^{p-1} \equiv b^{\varphi(p)} \equiv 1 \equiv \left(\frac{a}{p}\right)_L \pmod{p}.$$

Se $p \mid a$ allora ovviamente

$$a^{\frac{p-1}{2}} \equiv 0 \equiv \left(\frac{a}{p}\right)_L \pmod{p}.$$

Supponiamo infine che a non sia un residuo quadratico.
In generale sappiamo che $x^{p-1} - 1 \equiv 0 \pmod{p}$ ha $p-1$ radici modulo p, ma

$$(x^{p-1} - 1) = (x^{\frac{p-1}{2}} - 1)(x^{\frac{p-1}{2}} + 1),$$

dove $x^{\frac{p-1}{2}} - 1$ ha $\frac{p-1}{2}$ radice che saranno necessariamente residui quadratici. Da ciò segue che ogni a che non è un residuo quadratico sarà radice di $x^{\frac{p-1}{2}} + 1 \pmod p$, ovvero

$$a^{\frac{p-1}{2}} \equiv -1 \equiv \left(\frac{c}{p}\right)_L \pmod p.$$

□

Corollario. Sia p un primo dispari, allora

$$\left(\frac{-1}{p}\right)_L = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{se } p \equiv 1 \pmod 4 \\ -1 & \text{se } p \equiv 3 \pmod 4 \end{cases}$$

Dimostrazione. Dal teorema sappiamo che

$$\left(\frac{-1}{p}\right)_L \equiv (-1)^{\frac{p-1}{2}} \pmod p \implies p \mid (-1)^{\frac{p-1}{2}} - \left(\frac{-1}{p}\right)_L,$$

ma $(-1)^{\frac{p-1}{2}} - \left(\frac{-1}{p}\right)_L$ è una differenza tra segni e può pertanto assumere solo i valori $-2, 0, 2$. Per ipotesi p è un primo dispari quindi $p \nmid 2, -2$, da cui

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

□

Inoltre vale

$$\left(\frac{-1}{p}\right)_L = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{se } p \equiv 1 \pmod 4 \\ -1 & \text{se } p \equiv 3 \pmod 4 \end{cases}$$

poichè in modulo 4 si ha $p = 4k + \varepsilon$ con $0 \leqslant \varepsilon < 4$. Ma ε non può essere né 0 né 2, altrimenti si avrebbe $2, 4 \mid p$. Da ciò segue che ogni primo è del tipo $1+4k$ oppure $3+4k$, da cui

$$p = 1 + 4k \implies (-1)^{\frac{4k}{2}} = (-1)^{2k} = 1$$
$$p = 3 + 4k \implies (-1)^{\frac{2+4k}{2}} = (-1)(-1)^{2k} = -1.$$

Corollario. Sia p un primo dispari e siano $a, b \in \mathbb{Z}$, allora

$$\left(\frac{a\,b}{p}\right)_L = \left(\frac{a}{p}\right)_L \left(\frac{b}{p}\right)_L$$

Dimostrazione. Dal teorema sappiamo

$$\left(\frac{a\,b}{p}\right)_L \equiv (a\,b)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)_L \left(\frac{b}{p}\right)_L \pmod p,$$

quindi applicando lo stesso ragionamento mostrato nel corollario precedente avremo

$$\left(\frac{a\,b}{p}\right)_L \equiv \left(\frac{a}{p}\right)_L \left(\frac{b}{p}\right)_L \pmod p \implies \left(\frac{a\,b}{p}\right)_L = \left(\frac{a}{p}\right)_L \left(\frac{b}{p}\right)_L.$$

□

Teorema 4.5 – Lemma di Gauss

Siano $a \in \mathbb{Z}$ e $p \geqslant 3$ primo con $p \nmid a$. Definito $S = \left[1, \frac{p-1}{2}\right]$, poniamo

$$S_1 = \left\{ x \in S \;\middle|\; \frac{p}{2} < ax \pmod p < p \right\}.$$

Allora

$$\left(\frac{a}{p}\right)_L = (-1)^{\#S_1}.$$

Dimostrazione. Dal criterio di Eulero

$$\prod_{x\in S} ax = a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \equiv \left(\frac{a}{p}\right)_L \left(\frac{p-1}{2}\right)! \pmod p$$

Definiamo $r_x = ax \pmod p$, da cui

$$\prod_{x\in S} ax \equiv \prod_{x\in S_1} r_x \prod_{x\in S_2} ax \pmod p,$$

dove $S_2 = S - S_1 = \left\{ x \in S \;\middle|\; 0 \leqslant ax \pmod p < \frac{p}{2} \right\}$. Inoltre $\frac{p}{2} < r_x < p \implies 0 < p - r_x < \frac{p}{2}$, quindi

$$\prod_{x\in S_1} r_x \prod_{x\in S_2} ax \equiv (-1)^{\#S_1} \prod_{x\in S_1} (p - r_x) \prod_{x\in S_2} ax \pmod p,$$

con $x \in S_1 \implies 1 \leqslant p - ax \pmod p < \frac{p}{2}$ e $x \in S_2 \implies 1 \leqslant ax < \frac{p}{2}$. Inoltre se consideriamo

$$S_1 = \{\alpha_1, \ldots, \alpha_m\} \qquad \text{e} \qquad S_2 = \{\beta_1, \ldots, \beta_l\},$$

allora $\{\alpha_i\}, \{\beta_j\}$ sono tutti distinti e vale $p - \alpha_i \neq \beta_j$, $\forall\, i, j$. Infatti se valesse $\alpha_i + \beta_j = p$ si avrebbe

$$ax + ay \equiv 0 \pmod p \iff p \mid a(x+y) \overset{p\nmid a}{\implies} p \mid x + y,$$

ma ciò è assurdo in quanto $x + y \in [1, p-1]$. Quindi $\#S_1 + \#S_2 = \#S = \frac{p-1}{2}$, da cui

$$\left(\frac{a}{p}\right)_L \left(\frac{p-1}{2}\right)! \equiv_p (-1)^{\#S_1} \prod_{x\in S_1} (p - r_x) \prod_{x\in S_2} ax = (-1)^{\#S_1} \left(\frac{p-1}{2}\right)!$$

ovvero

$$\left(\frac{a}{p}\right)_L \left(\frac{p-1}{2}\right)! \equiv (-1)^{\#S_1} \left(\frac{p-1}{2}\right)! \pmod p \iff \left(\frac{a}{p}\right)_L \equiv (-1)^{\#S-1} \pmod p$$
$$\iff \left(\frac{a}{p}\right)_L = (-1)^{\#S_1},$$

in quanto entrambi segni. □

Osservazione. Se $a > 0$ avremo

$$\begin{aligned}\frac{p}{2} < ax \pmod p < p &\iff \frac{p}{2} < ax - p\left[\frac{ax}{p}\right] < p \\ &\iff \frac{1}{2} < \frac{ax}{p} - \left[\frac{ax}{p}\right] < 1 \\ &\iff \frac{1}{2} < \left\{\frac{ax}{p}\right\} < 1.\end{aligned}$$

Corollario. Sia p un primo dispari, allora

$$\left(\frac{2}{p}\right)_L = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{se } p \equiv \pm 1 \pmod 8 \\ -1 & \text{se } p \equiv \pm 3 \pmod 8 \end{cases}$$

Dimostrazione. Consideriamo la notazione del lemma di Gauss. Sia quindi $a = 2$, affermo che

$$S_1 = \left\{ x \in S \;\middle|\; \frac{p}{2} < 2x \pmod p < p \right\} = \left\{ x \in S \;\middle|\; \frac{p}{4} < x < \frac{p}{2} \right\}.$$

Infatti se $2x \in \left(\frac{p}{2}, p\right)$ allora $2x \pmod p = 2x$. Viceversa

$$1 \leqslant x \leqslant \frac{p-1}{2} \implies 2 \leqslant 2x \leqslant p-1 \implies 2x \pmod p = 2x.$$

Per cui

$$\#S_1 = \left[\frac{p}{2}\right] - \left[\frac{p}{4}\right] = \begin{cases} 4k - 2k & \text{se } p \equiv 1 \pmod 8 \\ 3 + 4k - 1 - 2k & \text{se } p \equiv 7 \pmod 8 \\ 1 + 4k - 2k & \text{se } p \equiv 3 \pmod 8 \\ 2 + 4k - 1 - 2k & \text{se } p \equiv 5 \pmod 8 \end{cases}$$

ovvero, per il lemma di Gauss

$$\left(\frac{2}{p}\right)_L = (-1)^{\left[\frac{p}{2}\right] - \left[\frac{p}{4}\right]} = \begin{cases} 1 & \text{se } p \equiv \pm 1 \pmod 8 \\ -1 & \text{se } p \equiv \pm 3 \pmod 8 \end{cases}$$

□

Lemma 4.6. Sia $a \in \mathbb{N}$ e sia $p \geqslant 3$ primo con $p \nmid a$. Allora

$$\left(\frac{a}{p}\right)_L = (-1)^n \qquad \text{con } n = \sum_{x=1}^{\frac{p-1}{2}} \left[\frac{2ax}{p}\right].$$

Dimostrazione. Ricordiamo che per il lemma di Gauss

$$\left(\frac{a}{p}\right)_L = (-1)^m \qquad \text{con } m = \#\left\{ x \in \mathbb{N} \;\middle|\; 1 \leqslant x < \frac{p}{2}, ax \pmod p > \frac{p}{2} \right\}.$$

Ora $ax \pmod p = ax - p\left[\frac{ax}{p}\right]$. Inoltre per la condizione

$$\left\{ x \in \mathbb{N} \;\middle|\; 1 \leqslant x < \frac{p}{2}, ax \pmod p > \frac{p}{2} \right\},$$

avremo

$$1 < \frac{ax \pmod p}{p/2} = \frac{ax - p\left[\frac{ax}{p}\right]}{p/2} < 2 \iff 1 < \frac{2ax}{p} - 2\left[\frac{ax}{p}\right] < 2.$$

Quindi, per ogni $1 \leqslant y \leqslant \frac{p-1}{2}$, si ha

$$\left[\frac{2ay}{p} - 2\left[\frac{ay}{p}\right]\right] = \begin{cases} 1 & \text{se } y \text{ è tale che } ay \pmod p > \frac{p}{2} \\ 0 & \text{se } y \text{ è tale che } ay \pmod p < \frac{p}{2} \end{cases}$$

ovvero

$$\sum_{y=1}^{\frac{p-1}{2}} \left[\frac{2ay}{p} - 2\left[\frac{ay}{p}\right]\right] = m.$$

D'altronde $[\alpha + n] = [\alpha] + n$. Quindi

$$\sum_{y=1}^{\frac{p-1}{2}} \left[\frac{2ay}{p} - 2\left[\frac{ay}{p}\right]\right] = \sum_{y=1}^{\frac{p-1}{2}} \left[\frac{2ay}{p}\right] - 2\sum_{y=1}^{\frac{p-1}{2}} \left[\frac{ay}{p}\right] = n - 2k,$$

ovvero $(-1)^m = (-1)^{n-2k} = (-1)^n$. Da cui segue la tesi per il lemma di Gauss. □

Lemma 4.7. Sia $a \in \mathbb{Z}$ dispari e sia $p \geqslant 3$ primo tale che $p \nmid a$. Allora

$$\left(\frac{a}{p}\right)_L = (-1)^{\lambda(a,p)} \qquad \text{con } \lambda(a,p) = \sum_{x=1}^{\frac{p-1}{2}} \left[\frac{ax}{p}\right].$$

Dimostrazione. Per le proprietà precedentemente dimostrate

$$\begin{aligned} \left(\frac{\frac{1}{2}(a+p)}{p}\right)_L &= \overbrace{\left(\frac{4}{p}\right)_L}^{=1}\left(\frac{\frac{1}{2}(a+p)}{p}\right)_L = \left(\frac{2a+2p}{p}\right)_L \\ &= \left(\frac{2a+2p \pmod p}{p}\right)_L = \left(\frac{2a}{p}\right)_L \\ &= \left(\frac{2}{p}\right)_L \left(\frac{a}{p}\right)_L \end{aligned}$$

Sfruttando il lemma precedente

$$\left(\frac{\frac{1}{2}(a+p)}{p}\right)_L = (-1)^n \qquad \text{con } n = \sum_{x=1}^{\frac{p-1}{2}} \left[\frac{ax+px}{p}\right].$$

Inoltre

$$\begin{aligned} n &= \sum_{x=1}^{\frac{p-1}{2}} \left[\frac{ax+px}{p}\right] = \sum_{x=1}^{\frac{p-1}{2}} \left[\frac{ax}{p}\right] + x && \textit{sfruttando la somma id Gauss} \\ &= \sum_{x=1}^{\frac{p-1}{2}} \left[\frac{ax}{p}\right] + \frac{1}{2}\frac{p-1}{2}\left(\frac{p-1}{2}+1\right) \\ &= \sum_{x=1}^{\frac{p-1}{2}} \left[\frac{ax}{p}\right] + \frac{p^2-1}{8} = \lambda(a,p) + \frac{p^2-1}{8}. \end{aligned}$$

Da cui

$$\left(\frac{2}{p}\right)_L \left(\frac{a}{p}\right)_L = (-1)^{\lambda(a,p)}(-1)^{\frac{p^2-1}{8}} \iff \left(\frac{a}{p}\right)_L = (-1)^{\lambda(a,p)}.$$

□

Teorema 4.8 – Legge della reciprocità quadratica

Siano p, q primi dispari distinti, allora

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

Dimostrazione. Per il lemma precedente

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

Quindi la dimostrazione si riduce a provare

$$(-1)^{\lambda(p,q)+\lambda(q,p)} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}.$$

Per definizione

$$\lambda(p,q) = \sum_{1\leqslant x<\frac{p}{2}} \left[\frac{qx}{p}\right] = \sum_{1\leqslant x<\frac{p}{2}} \sum_{1\leqslant y<\frac{qx}{p}} 1 = \sum_{1\leqslant y<\frac{q}{2}} \sum_{\frac{yp}{q}<x\leqslant\frac{p-1}{2}} 1.$$

Analogamente

$$\lambda(q,p) = \sum_{1\leqslant y<\frac{q}{2}} \left[\frac{px}{1}\right] = \sum_{1\leqslant y<\frac{q}{2}} \sum_{1\leqslant x<\frac{yp}{q}} 1.$$

Per cui

$$\begin{aligned}\lambda(p,q)+\lambda(q,p) &= \sum_{1\leqslant y<\frac{q}{2}} \left(\sum_{\frac{yp}{q}<x\leqslant\frac{p-1}{2}} 1 + \sum_{1\leqslant x<\frac{yp}{q}} 1 \right) = \sum_{1\leqslant y<\frac{q}{2}} \sum_{1\leqslant x<\frac{p-1}{2}} 1 \\ &= \sum_{1\leqslant y<\frac{q}{2}} = \frac{p-1}{2}\frac{q-1}{2}.\end{aligned}$$

□

4.3 IL SIMBOLO DI JACOBI

Definizione 4.9 – Simbolo di Jacobi

Sia $a \in \mathbb{Z}$ e sia $m \in \mathbb{Z}$ dispari. Definiamo *simbolo di Jacobi* come

$$\left(\frac{a}{m}\right)_J = \left(\frac{a}{p_1}\right)_L^{\alpha_1} \cdot \ldots \cdot \left(\frac{a}{p_s}\right)_L^{\alpha_s},$$

dove $m = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$.

Osservazione. In generale se $m = p$ primo vale

$$\left(\frac{a}{p}\right)_J = \left(\frac{a}{p}\right)_L.$$

Notazione. Per l'osservazione precedente non distingueremo più il simbolo di Legendre dai simboli di Jacobi. Utilizzeremo invece il simbolo più generale

$$\left(\frac{a}{m}\right)$$

Proprietà 4.10. Sia $m \in \mathbb{Z}$ dispari. Allora

$$\left(\frac{1}{m}\right) = 1$$

Dimostrazione. Ricordiamo che se p primo dispari vale

$$\left(\frac{1}{p}\right) = 1.$$

Quindi per definizione

$$\left(\frac{1}{m}\right) = \prod_p \left(\frac{1}{p}\right)^{\nu_p(m)} = \prod_p 1^{\nu_p(m)} = 1.$$ □

Proprietà 4.11. Sia $a \in \mathbb{Z}$ e sia $m \in \mathbb{Z}$ dispari. Allora

$$\left(\frac{a}{m}\right) = \left(\frac{a \pmod m}{m}\right).$$

Dimostrazione. Sappiamo $a = a \pmod m + k\,m$, per cui

$$\left(\frac{a}{m}\right) = \prod_p \left(\frac{a}{p}\right)^{\nu_p(m)} = \prod_p \left(\frac{a \pmod m + k\,m}{p}\right)^{\nu_p(m)}.$$

In generale se $\nu_p(m) \geqslant 1$ avremo $p \mid m$, ovvero $k\,m \equiv 0 \pmod p$. Da cui

$$\left(\frac{a}{m}\right) = \prod_p \left(\frac{a \pmod m}{m}\right)^{\nu_p(m)} = \left(\frac{a \pmod m}{m}\right).$$ □

Proprietà 4.12. Siano $a, b \in \mathbb{Z}$ e sia $m \in \mathbb{Z}$ dispari. Allora

$$\left(\frac{a\,b}{m}\right) = \left(\frac{a}{m}\right)\left(\frac{b}{m}\right).$$

Dimostrazione. Applicando la definizione e le proprietà del simbolo di Legendre

$$\left(\frac{a\,b}{m}\right) = \prod_p \left(\frac{a\,b}{p}\right)^{\nu_p(m)} = \prod_p \left(\frac{a}{p}\right)^{\nu_p(m)} \prod_p \left(\frac{b}{p}\right)^{\nu_p(m)} = \left(\frac{a}{m}\right)\left(\frac{b}{m}\right).$$ □

Lemma 4.13. La funzione

$$\chi_4(m) = \begin{cases} (-1)^{\frac{m-1}{2}} & \text{se } 2 \nmid m \\ 0 & \text{se } 2 \mid m \end{cases}$$

è totalmente moltiplicativa.

Dimostrazione. Siano $n, m \in \mathbb{N}$ e supponiamo che $2 \mid n\,m$. Per definizione $\chi_4(n\,m) = 0$, ma $2 \mid n\,m \implies 2 \mid n$ oppure $2 \mid m$. Quindi $\chi_4(n) = 0$ oppure $\chi_4(m) = 0$.
Supponiamo ora $2 \nmid n, m$, avremo

$$\chi_4(m)\chi_4(n)\chi_4(m\,n)^{-1} = (-1)^{\frac{m-1}{2}+\frac{n-1}{2}-\frac{m\,n-1}{2}} = (-1)^{-\frac{(m-1)(n-1)}{2}},$$

ma m, n sono dispari, quindi $m-1, n-1$ sono pari. Ovvero

$$\frac{(m-1)(n-1)}{2} \text{ pari} \implies (-1)^{-\frac{(m-1)(n-1)}{2}} = 1.$$

□

Lemma 4.14. La funzione

$$\chi_8(m) = \begin{cases} (-1)^{\frac{m^2-1}{8}} & \text{se } 2 \nmid m \\ 0 & \text{se } 2 \mid m \end{cases}$$

è totalmente moltiplicativa.

Dimostrazione. Analoga alla dimostrazione precedente. □

Proprietà 4.15. Sia $m \in \mathbb{Z}$ dispari. Allora

$$\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}} = \begin{cases} 1 & \text{se } p \equiv 1 \pmod 4 \\ -1 & \text{se } p \equiv 3 \pmod 4 \end{cases}.$$

Dimostrazione. Dalla definizione e per la totale moltiplicatività di χ_4,

$$\begin{aligned} \left(\frac{-1}{m}\right) &= \prod_p \left(\frac{-1}{p}\right)^{\nu_p(m)} = \prod_p \left((-1)^{\frac{p-1}{2}}\right)^{\nu_p(m)} \\ &= \prod_p \chi_4(p)^{\nu_p(m)} = \chi_4\left(\prod_p p^{\nu_p(m)}\right) \\ &= \chi_4(m) = (-1)^{\frac{m-1}{2}}. \end{aligned}$$

□

Proprietà 4.16. Sia $m \in \mathbb{Z}$ dispari. Allora

$$\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}} = \begin{cases} 1 & \text{se } p \equiv \pm 1 \pmod 8 \\ -1 & \text{se } p \equiv \pm 3 \pmod 8 \end{cases}.$$

Dimostrazione. Dalla definizione e per la totale moltiplicatività di χ_8,

$$\begin{aligned}\left(\frac{2}{m}\right) &= \prod_p \left(\frac{2}{p}\right)^{\nu_p(m)} = \prod_p \chi_8(p)^{\nu_p(m)} \\ &= \chi_8\left(\prod_p p^{\nu_p(m)}\right) = \xi_8(m) \\ &= (-1)^{\frac{m^2-1}{8}}.\end{aligned}$$

□

Proprietà 4.17. Siano $m, n \in \mathbb{Z}$ dispari. Allora

$$\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)(-1)^{\frac{m-1}{2}\frac{n-1}{2}}.$$

Dimostrazione. Se $(m,n) \neq 1$ allora

$$\left(\frac{n}{m}\right) = \left(\frac{m}{n}\right) = 0,$$

quindi la tesi è soddisfatta.
Supponiamo quindi $(m,n) = 1$, allora

$$\begin{aligned}\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) &= \prod_p \left(\frac{m}{p}\right)^{\nu_p(m)}\left(\frac{n}{p}\right)^{\nu_p(n)} = \prod_p\prod_q \left(\frac{q}{p}\right)^{\nu_p(m)\nu_q(n)}\left(\frac{q}{p}\right)^{\nu_p(n)\nu_q(m)} \\ &= \prod_{p,q}\left(\frac{q}{p}\right)^{\nu_p(m)\nu_q(n)}\prod_{p,q}\left(\frac{p}{q}\right)^{\nu_p(m)\nu_q(n)} = \prod_{p,q}\left[\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)\right]^{\nu_p(m)\nu_q(n)} \\ &= \prod_{p,q}\left[\left((-1)^{\frac{p-1}{1}}\right)^{\frac{q-1}{2}}\right]^{\nu_p(m)\nu_q(n)} = \prod_{p,q}\left(\chi_4(p)^{\frac{q-1}{2}}\right)^{\nu_p(m)\nu_q(n)} \\ &= \prod_q\left[\prod_p \chi_4(p)^{\nu_p(m)}\right]^{\nu_q(n)\frac{q-1}{2}} = \prod_q \chi_4(m)^{\nu_q(n)\frac{q-1}{2}} \\ &= \prod_q\left((-1)^{\frac{m-1}{2}\frac{q-1}{2}}\right)^{\nu_q(n)} = \left(\prod_q \chi_4(q)^{\nu_q(n)}\right)^{\frac{m-1}{2}} \\ &= \chi_4(n)^{\frac{m-1}{2}} = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}.\end{aligned}$$

□

Proposizione 4.18 – Algoritmo per il calcolo del simbolo di Jacobi

Siano $m, n \in \mathbb{N}$ con $2 \nmid n$, allora

$$\left(\frac{m}{n}\right) = \begin{cases} 0 & m = 0 \\ 1 & m = 1 \\ (-1)^{\frac{n^2-1}{8}}\left(\frac{m/2}{n}\right) & 2 \mid m \\ \left(\frac{m \pmod n}{n}\right) & 2 \nmid m, m \geqslant n \\ \left(\frac{n}{m}\right)(-1)^{\frac{n-1}{2}\frac{m-1}{2}} & 2 \nmid m, m < n \end{cases}$$

Dimostrazione. Segue immediatamente dalle proprietà precedenti. □

Esempio. Si calcoli il simbolo di Jacobi associato a $\left(\frac{3073}{2919}\right)$. Sfruttiamo l'algoritmo

$$\begin{aligned}\left(\frac{3073}{2919}\right) &= \left(\frac{3073 \pmod{2919}}{2919}\right) = \left(\frac{154}{2919}\right)\\ &= \left(\frac{2\cdot 77}{2919}\right) = \left(\frac{77}{2919}\right)\\ &= \left(\frac{2919}{77}\right)\\ &= \left(\frac{2919 \pmod{77}}{77}\right) = \left(\frac{70}{77}\right)\\ &= \left(\frac{2\cdot 35}{77}\right) = -\left(\frac{35}{77}\right)\\ &= -\left(\frac{77}{35}\right)\\ &= -\left(\frac{77 \pmod{35}}{35}\right) = -\left(\frac{7}{35}\right)\\ &= -\left(\frac{35}{7}\right)\\ &= -\left(\frac{35 \pmod{7}}{7}\right) = -\left(\frac{0}{7}\right)\\ &= 0.\end{aligned}$$

4.4 MINIMO RESIDUO NON QUADRATICO

Definizione 4.19 – Minimo residuo non quadratico

Sia $p \geqslant 3$ primo. Definiamo n_p come il più piccolo residuo non quadratico modulo p:

$$n_p = \min\left\{ a \in \mathbb{N} \;\middle|\; \left(\frac{a}{p}\right) = -1 \right\}.$$

Osservazione. Sicuramente $n_p \leqslant \frac{p}{2}+1$. Infatti i residui quadratici sono precisamente $\frac{p-1}{2}$, quindi dopo $\frac{p-1}{2}$ ne troveremo almeno uno.

Osservazione. Se $p \equiv 3 \pmod 8$ allora $n_p = 2$. Infatti

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = -1,$$

quando $p \equiv \pm 3 \pmod 8$.

Proposizione 4.20 – Lemma di Linnick

Sia $p \geqslant 3$ primo. Allora

$$\forall\, \varepsilon > 0, n_p \ll p^{\frac{1}{4}+\varepsilon}.$$

Dimostrazione. Non fornita. □

Osservazione. La congettura di Vinogradov (1919), afferma che

$$\forall\, \varepsilon > 0, n_p \ll p^{\varepsilon}.$$

Teorema 4.21 – Non limitatezza di n_p

Sia $p \geqslant 3$ primo. Allora

$$\limsup_{p \to +\infty} n_p = +\infty,$$

ovvero

$$\forall\, k \in \mathbb{N} \exists\, p \text{ primo } : n_p \geqslant k.$$

Dimostrazione. Il teorema di Dirichlet sui primi in progressione aritmetica, afferma che per ogni coppia $a, b \in \mathbb{Z}$ coprimi con $b > 1$, esistono infiniti primi p tali che $p \equiv a \pmod b$. Quindi esisterà p primo tale che $p \equiv 1 \pmod{8k!}$ per ogni $k \in \mathbb{N}$. In particolare

$$p \equiv 1 \pmod 8 \implies \left(\frac{2}{p}\right) = 1.$$

Ora, preso $l \geqslant 3$ primo con $l < k$, si ha $l \mid k!$. Da cui $p \equiv 1 \pmod l$ che implica

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

ricordiamo che $p \equiv 1 \pmod 8$

Sia ora $m < k$ con m non necessariamente primo. Avremo

$$\left(\frac{m}{p}\right) = \prod_l \left(\frac{l}{p}\right)^{\nu_l(m)} = \prod_l 1^{\nu_l(m)} = 1.$$

$\nu_l(m) \neq 0$ *se e soltanto se* $l \mid m < k$, *quindi* $l < k$

Quindi m è un residuo quadratico fintanto che è minore di k. In particolare il più piccolo residuo non quadratico è necessariamente maggiore di k, ovvero

$$n_p \geqslant k \implies \limsup_{p \to +\infty} = +\infty.$$

□

Esempio. Troviamo p primo tale che $n_p \geqslant 5$. Se $n_p \geqslant 5$ necessariamente

$$\left(\frac{1}{p}\right) = \left(\frac{2}{p}\right) = \left(\frac{3}{p}\right) = \left(\frac{4}{p}\right) = 1.$$

Dove

$$\left(\frac{1}{p}\right) = \left(\frac{4}{p}\right) = 1,$$

sono condizioni sempre verificate, mentre

$$\left(\frac{2}{p}\right) = 1 \iff (-1)^{\frac{p^2-1}{8}} = 1 \iff p \equiv \pm 1 \pmod 8,$$

e

$$\left(\frac{3}{p}\right) = 1 \iff \left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}\frac{3-1}{2}} = \begin{cases} (-1)^{\frac{p-1}{2}} & \text{se } p \equiv 1 \pmod 3 \\ -(-1)^{\frac{p-1}{2}} & \text{se } p \equiv 2 \pmod 3 \end{cases}$$
$$\iff \begin{cases} p \equiv 1 \pmod 3 \\ p \equiv 1 \pmod 4 \end{cases} \vee \begin{cases} p \equiv 2 \pmod 3 \\ p \equiv 3 \pmod 4 \end{cases}$$
$$\iff p \equiv 1 \pmod{12} \vee p \equiv -1 \pmod{12}.$$

Il problema si riduce quindi a quattro sistemi distinti

$$\begin{cases} p \equiv \pm 1 \pmod 8 \\ p \equiv \pm 1 \pmod{12} \end{cases}$$

Ora se $p \equiv \pm 1 \pmod 8$ in particolare $p \equiv \pm 1 \pmod 4$, quindi $p \not\equiv \mp 1 \pmod{12}$. I sistemi accettabili sono quindi

$$\begin{cases} p \equiv 1 \pmod 8 \\ p \equiv 1 \pmod{12} \end{cases} \vee \begin{cases} p \equiv -1 \pmod 8 \\ p \equiv -1 \pmod{12} \end{cases} \iff p \equiv \pm 1 \pmod{24}.$$

Da cui $p = 23$.

Teorema 4.22 – Limite superiore di n_p

Sia $p \geqslant 3$ primo. Allora

$$n_p < \frac{1}{2} + \sqrt{p + \frac{1}{4}}.$$

Dimostrazione. Sia $h = \left[\frac{p}{n_p}\right] + 1$, per definizione avremo

$$\frac{p}{n_p} < h < \frac{p}{n_p} + 1 \implies p < h n_p < p + n_p.$$

Ora $\left(\frac{h}{p}\right) = -1$, infatti

$$\left(\frac{n_p h - p}{p}\right) = 1,$$

in quanto $0 < n_p h - p < n_p$ dove n_p è il più piccolo residuo non quadratico modulo p. Ma

$$1 = \left(\frac{n_p h - p}{p}\right) = \left(\frac{n_p h}{p}\right) = \left(\frac{n_p}{p}\right)\left(\frac{h}{p}\right)$$
$$= -\left(\frac{h}{p}\right).$$

Per definizione di minimo, $\left(\frac{h}{p}\right) = -1$ ci dice $h \geqslant n_p$, ovvero

$$n_p^2 \leqslant p + n_p \implies n_p^2 - n_p - p \leqslant 0$$
$$\implies n_p \leqslant \frac{1}{2} + \frac{1}{2}\sqrt{1 + 4p}$$
$$\implies n_p < \frac{1}{2} + \sqrt{p + \frac{1}{4}}.$$

□

5 SOMME DI QUADRATI

5.1 INTRODUZIONE

Definizione 5.1 – Somma di quadrati

Diremo che $n \in \mathbb{N}$ è somma di quadrati se esistono $x_1, \ldots, x_k \in \mathbb{N}$ tali che

$$n = x_1^2 + \ldots + x_k^2.$$

Notazione. Indicheremo con $\square$ un quadrato perfetto. Ad esempio per dire che n è somma di k quadrati scriveremo $n = k\square$.

Teorema 5.2 – di Lagrange

Ogni $n \in \mathbb{N}$ è al più somma di quattro quadrati.

Dimostrazione. A pagina 86. □

Esempio. Mostriamo la scomposizione in somma di quadrati di alcuni interi:

$$2 = 1^2 + 1^2;$$
$$3 = 1^2 + 1^2 + 1^2;$$
$$4 = 2^2;$$
$$5 = 2^2 + 1^2;$$
$$6 = 2^2 + 1^2 + 1^2;$$
$$7 = 2^2 + 1^2 + 1^2 + 1^2.$$

Teorema 5.3 – di Legendre

Sia $n \in \mathbb{N}$. Allora n è la somma di tre quadrati se e soltanto se

$$n \neq 4^l(7 + 8k), l, k \in \mathbb{N}.$$

Dimostrazione. A pagina 88. □

Osservazione. Quando si dice che n è somma di tre quadrati si includono anche i naturali che sono somma di uno o due quadrati. A questi infatti è possibile sommare 0^2 per raggiungere i tre interi.

Teorema 5.4 – di Fermat

Sia $p \geqslant 3$ primo. Allora

$$p = 2\square \iff p \equiv 1 \pmod 4.$$

⇒) *Dimostrazione.* Supponiamo che p sia somma di due quadrati. Dal momento che p primo, certamente $p \not\equiv 0, 2 \pmod 4$. Inoltre, in generale, se $n \equiv 3 \pmod 4$, allora n non è somma di due quadrati. Infatti i quadrati modulo 4 sono 0 e 1, in quanto

$$\mathbb{Z}_4 = \{0, 1, 2, 3\} \implies (\mathbb{Z}_4)^2 = \{0, 1\}.$$

Quindi se fosse $n = x^2 + y^2$ si avrebbe

$$n \mod 4 = x^2 \mod 4 + y^2 \mod 4 \implies 3 = a^2 + b^2,$$

che è assurdo in quanto $a, b \in \{0, 1\}$. Per cui $p \equiv 1 \pmod 4$.

⇐) Supponiamo $p \equiv 1 \pmod 4$, in particolare $\left(\frac{-1}{p}\right) = 1$. Quindi esiste $x_0 \in \mathbb{Z}$ tale che $x_0^2 + 1^2 \equiv 0 \pmod p$. Inoltre x_0 possiamo sceglierlo nel sistema completo di residui

$$\left\{-\frac{p-1}{2}, \dots, \frac{p-1}{2}\right\}.$$

Per cui esiste $x_0 \in \mathbb{Z}$ tale che $|x_0| < \frac{p}{2}$ e $x_0^2 + 1^2 \equiv 0 \pmod p$. Ovvero esiste $m \in \mathbb{Z}$ tale che $mp = x_0^2 + 1^2$. Dove $m < p$ in quanto

$$mp = x_0^2 + 1^2 < \frac{p^2}{4} + 1^2 < p^2 \implies m < p.$$

La strategia a questo punto, sapendo che esiste $1 \leqslant m < p$ tale che $mp = 2\square$, è mostrare che se $m > 1$ esiste m_0 tale che $1 \leqslant m_0 < m$ e $m_0 p = 2\square$. Iterando il procedimento troveremo necessariamente $m_n = 1$ tale che $m_n p = 2\square$, ovvero $p = 2\square$.
Sia $mp = x^2 + y^2$ e siano $x_1, y_1 \in \mathbb{N}$ tali che

$$x_1 \equiv x \pmod m \qquad \text{e} \qquad y_1 \equiv y \pmod m.$$

In particolare posso prenderli tali che $|x_1| \leqslant \frac{m}{2}$ e $|y_1| \leqslant \frac{m}{2}$. Quindi

$$x_1^2 + y_1^2 \equiv x^2 + y^2 \equiv 0 \pmod m.$$

Pertanto esisterà $m_0 \in \mathbb{N}$ tale che $m_0 m = x_1^2 + y_1^2$. D'altronde

$$x_1^2 + y_1^2 \leqslant \left(\frac{m}{2}\right)^2 + \left(\frac{m}{2}\right)^2 = \frac{m^2}{2} \iff m_0 m \leqslant \frac{m^2}{2},$$

ovvero

$$m_0 m \leqslant \frac{m^2}{2} < m^2 \iff m_0 \leqslant \frac{m}{2} < m.$$

Inoltre $m_0 \neq 0$, poichè altrimenti $x_1^2 + y_1^2 = 0$, quindi

$$x_1 = y_1 = 0 \implies m \mid x, y \implies m^2 \mid x^2 + y^2,$$

ma ciò è assurdo poichè altrimenti $m \mid p$ che contraddice $1 < m < p$ con p primo.
Quindi abbiamo trovato m_0 tale che $1 \leqslant m_0 < m$ e $m_0 m = x_1^2 + y_1^2$.
Osserviamo che se $n_1 = 2\square = a_1^2 + b_1^2$ e $n_2 = 2\square = a_2^2 + b_2^2$, si ha

$$n_1 n_2 = (a_1^2 + b_1^2)(a_2^2 + b_2^2) = (a_1 b_2 - a_2 b_1)^2 + (a_1 a_2 + b_1 b_2)^2 = 2\square.$$

Quindi, dal momento che $m_0 m$ e mp sono entrambi $2\square$, troviamo

$$m_0 m \cdot mp = 2\square = (x_1 y - y_1 x)^2 + (x_1 x + y_1 y)^2,$$

ovvero

$$m_0 p = \left(\frac{x_1 y - y_1 x}{m}\right)^2 + \left(\frac{x_1 x + y_1 y}{m}\right)^2 = 2\square.$$

Da cui, iterando, giungo alla tesi. □

Osservazione. L'implicazione $p \equiv 1 \pmod 4 \implies p = \square + \square$ può essere dimostrata in maniera alternativa. Si usa il fatto che se $p \equiv 1 \pmod 4$ allora esiste $x \in \mathbb{Z}$ tale che $x^2 + 1 \equiv 0 \pmod p$

Esempio. Consideriamo $13, 17$ entrambi primi congrui ad 1 modulo 4. Avremo

$$13 = 3^2 + 2^2 \qquad \text{e} \qquad 17 = 4^2 + 1^2.$$

Teorema 5.5 – Naturali somma di due quadrati

Sia $n \in \mathbb{N}$ e supponiamo $n = 2^r p_1^{r_1} \cdot \ldots \cdot p_t^{r_t} q_1^{u_1} \cdot \ldots \cdot q_s^{u_s}$, dove

$$p_j \equiv 1 \pmod 4 \qquad \text{e} \qquad q_i \equiv 3 \pmod 4.$$

Allora $n = 2\square$ se e soltanto se $u_1, \ldots, u_s$ sono tutti pari.

Dimostrazione. Per il teorema precedente $p_j \equiv 1 \pmod 4 \implies p_j = 2\square$. Abbiamo già osservato nella dimostrazione precedente che il prodotto si somme di due quadrati è una somma di due quadrati, quindi $p_1^{r_1} \cdot \ldots \cdot p_t^{r_t} = 2\square$. ⇐)

D'altronde u_i pari ci dice che $q_i^{u_i} = \left(q_i^{\frac{u_i}{2}}\right)^2 + 0^2$, quindi nuovamente $q_1^{u_1} \cdot \ldots \cdot q_s^{u_s}$ è somma di due quadrati in quanto prodotto di somme di due quadrati. Pertanto $n = 2\square$.

Supponiamo per assurdo che esista u_i tale che $2 \nmid u_i$. Dal momento che $n = x^2 + y^2$ avremo $x^2 + y^2 \equiv 0 \pmod{q_i}$. Se fosse $q_i \nmid y$ allora esisterebbe il suo inverso moltiplicativo $y^* : y\,y^* \equiv 1 \pmod{q_i}$. Quindi ⇒)

$$x^2 + y^2 \equiv_{q_i} 0 \iff (x\,y^*)^2 + (y\,y^*)^2 \equiv_{q_i} 0 \iff (x\,y^*)^2 \equiv -1 \pmod{q_i},$$

ovvero $\left(\frac{-1}{q_i}\right) = 1$, ma ciò non può accadere in quanto $q_1 \equiv 3 \pmod 4$. Quindi $q_i \mid y \implies q_i \mid x$. Per cui

$$n = (q_i x')^2 + (q_i y')^2 \implies \frac{n}{q_i^2} = x'^2 + y'^2.$$

Ricordiamo che $u_i \geqslant 3$, per cui ripetendo il ragionamento su $\frac{n}{q_i^2}$ otteniamo $u_i - 3 \geqslant 3$. Ripetendo il procedimento un numero sufficiente di volte si giunge inevitabilmente ad una contraddizione. □

5.2 SOMMA DI DUE QUADRATI

Definizione 5.6 – Funzione enumerativa della somma di due quadrati

Definiamo una funzione aritmetica S che associ ad ogni naturali il numero di modi in cui può essere scomposto come somma di due quadrati,

$$S(n) = \#\left\{ (a, b) \in \mathbb{Z}^2 \;\middle|\; a^2 + b^2 = n \right\}.$$

Esempio. $S(2) = 4$, infatti $2 = 1^2 + 1^2, (-1)^2 + 1^2, 1^2 + (-1)^2, (-1)^2 + (-1)^2$. Analogamente $S(3) = 0$ e $S(5) = 8$.

Definizione 5.7 – Numero di interi scomponibili come somma di due quadrati

Definiamo una funzione aritmetica K che ci fornisca il numero di interi, minori di un dato T, che possono essere scritti come somma di due quadrati,

$$K(T) = \#\{\, n \in \mathbb{N} \mid n \leqslant T, n = \square + \square \,\}.$$

Esempio. $K(5) = 4$, infatti $1, 2, 4$ e 5 possono essere scritti come somma di due quadrati.
Analogamente $K(10) = 7, K(20) = 12$.

Definizione 5.8 – Densità naturale

Sia $S \subseteq \mathbb{N}$. Definiamo la *densità naturale* δ_S di S come

$$\delta_S = \lim_{T \to +\infty} \frac{\#(S \cap [1, T])}{\#(\mathbb{N} \cap [1, T])}.$$

Osservazione. Esistono insiemi che non ammettono densità naturale. Un esempio è costituito dall'insieme

$$A = \bigcup_{n=0}^{+\infty} \{2^{2n}, \dots, 2^{2n+1} - 1\}.$$

Infatti se definiamo $T(n) = \#(A \cap [1, n])$, avremo che

$$T(k) = \frac{2^{2n+2} - 1}{3}, \ \forall\, k \in [2^{2n+1} - 1, 2^{2n+2} - 1],$$

ma questo ci mostra immediatamente che il limite della densità naturale non può esistere in quanto

$$\limsup_{n \to +\infty} \frac{T(n)}{n} = \lim_{n \to +\infty} \frac{1 + 2^2 + 2^4 + \dots + 2^{2n}}{2^{2n+1} - 1} = \lim_{n \to +\infty} \frac{2^{2m+2} - 1}{3(2^{2m+1} - 1)} = \frac{2}{3}$$
$$\liminf_{n \to +\infty} \frac{T(n)}{n} = \lim_{n \to +\infty} \frac{1 + 2^2 + 2^4 + \dots + 2^{2n}}{2^{2n+2} - 1} = \lim_{n \to +\infty} \frac{2^{2m+2} - 1}{3(2^{2m+2} - 1)} = \frac{1}{3}.$$

Teorema 5.9 – di Landau

Vale la seguente stima asintotica

$$K(T) \sim c \frac{T}{\sqrt{\ln T}}.$$

Dimostrazione. Non fornita. □

Corollario. L'insieme degli interi che possono essere scritti come somma di due quadrati hanno densità nulla.

Dimostrazione. Dal teorema abbiamo

$$\delta_{2\square} = \lim_{T\to+\infty} \frac{K(T)}{T+o(1)} = \lim_{T\to+\infty} \frac{c\frac{T}{\sqrt{\ln T}}}{T} = 0.$$

□

Teorema 5.10 – Lemma delle gabbie e dei piccioni

Sia $x \in \mathbb{Z}$ tale che $x^2+1 \equiv 0 \pmod p$, con p primo. Allora esistono $a, b \in \mathbb{Z}$ tali che

$$0 < |a|, |b| < \sqrt{p} \qquad \text{e} \qquad a\,x \equiv b \pmod p.$$

Dimostrazione. Definiamo il seguente insieme

$$S = \{\, u\,x - v \mid u, v \in \mathbb{Z}, 0 \leqslant u, v \leqslant \sqrt{p}\,\}.$$

Avremo $[\sqrt{p}]+1$ scelte sia per u che per v. Quindi S ha $\left([\sqrt{p}]+1\right)^2 > p$ coppie (u,v) distinte.
D'altronde se consideriamo il resto modulo p di $u\,x - v$ avremo p possibili resti.
Ora, dal momento che il numero delle coppie (u,v) è maggiore del numero di resti, avremo necessariamente che

$$\exists\, (u_1,v_1),(u_2,v_2) : u_1 x - v_1 \equiv u_2 x - v_2 \pmod p.$$

Se definiamo $a = u_1 - u_2$ e $b = v_1 - v_2$ abbiamo che $a\,x \equiv b \pmod p$. Resta da verificare che $0 < |a|, |b| < \sqrt{p}$. Ma

$$|a| = |u_1 - u_2| < \sqrt{p} \qquad \text{e} \qquad |b| = |v_1 - v_2| < \sqrt{p},$$

quindi la seconda disuguaglianza è verificata. Se per assurdo $b = 0$ si avrebbe $a\,x \equiv 0 \pmod p$; d'altronde $x^2 \equiv -1 \pmod p$, per cui $p \nmid x$ e di conseguenza $p \mid a \implies a = 0$ in quanto $a < \sqrt{p}$.
Per cui $a = 0, b = 0 \implies u_1 = u_2$ e $v_1 = v_2$ che è ovviamente assurdo per la nostra scelta iniziale. Analogamente si mostra che $a = 0 \implies b = 0$ che porta alla stessa contraddizione. □

Corollario. Sia $x \in \mathbb{Z}$ tale che $x^2+1 \equiv 0 \pmod p$, con p primo. Allora esistono $a, b \in \mathbb{Z}$ tali che $a^2 + b^2 = p$.

Dimostrazione. Per il teorema esistono $a, b \in \mathbb{Z}$ tali che

$$0 < |a|, |b| < \sqrt{p} \qquad \text{e} \qquad a\,x \equiv b \pmod p.$$

Quindi

$$a^2 + b^2 \equiv_p a^2 + (a\,x)^2 = a^2(1+x^2) \equiv 0 \pmod p.$$

Dunque $p \mid a^2 + b^2$, ovvero $a^2 + b^2 = k\,p$. D'altronde $0 < a^2 + b^2 < 2p$, per cui $a^2 + b^2 = p$. □

Osservazione. Tramite questo risultato possiamo dimostrare in maniera alternativa, e molto utile per gli esercizi, che se $p \equiv 1 \pmod 4$ allora $p = \square + \square$. Useremo proprio il fatto che se $p \equiv 1 \pmod 4$ allora esiste $x \in \mathbb{Z}$ tale che $x^2 + 1 \equiv 0 \pmod p$.

Infatti se prendiamo $x = \left(\frac{p-1}{2}\right)!$, avremo

$$\begin{aligned} x^2 &= \prod_{r=1}^{\frac{p-1}{2}} r^2 = \underbrace{(-1)^{\frac{p-1}{2}}}_{=1} \prod_{r=1}^{\frac{p-1}{2}} r^2 = \prod_{r=1}^{\frac{p-1}{2}} r(-r) \equiv \prod_{r=1}^{\frac{p-1}{2}} r \prod_{r=1}^{\frac{p-1}{2}} (p-r) \pmod p \\ &= \left(1 \cdot 2 \cdot \ldots \cdot \left(\frac{p-1}{2}\right)\right)\left((p-1)(p-2) \cdot \ldots \cdot \left(\frac{p-1}{2}+1\right)\right) \\ &= (p-1)! \equiv -1 \pmod p, \end{aligned}$$

dove l'ultima equivalenza è dovuta al teorema di Wilson, dimostrato a pagina 55.

Teorema 5.11 – Generalizzazione del lemma delle gabbie e dei piccioni

Sia $n \in \mathbb{N}, n > 1$. Allora per ogni $x \in \mathbb{Z}$ tale che $x^2+1 \equiv 0 \pmod n$, esiste un'unica coppia $(a, b) \in \mathbb{N}^2$ tale che

$$(a, b) = 1; \qquad n = a^2 + b^2 \qquad \text{e} \qquad a\,x \equiv b \pmod n.$$

Dimostrazione. Definiamo nuovamente

$$S = \{\, u\,x - v \mid u, v \in \mathbb{Z}, 0 \leqslant u, v \leqslant \sqrt{p}\,\}.$$

Sfruttando argomenti del tutto analoghi a quelli usati nel lemma precedente si può dimostrare che esistono $a, b \in \mathbb{Z}$ tali che $a\,x \equiv b \pmod n$ e $n = a^2 + b^2$.
Mostriamo che $a, b \in \mathbb{N}$, assumendo, senza perdita di generalità, che $a > 0$. Se $b > 0$ non c'è nulla da dimostrare, supponiamo quindi che $b < 0$ e deifiniamo $a' = -b$ e $b' = a$. Avremo quindi $a', b' \in \mathbb{N}, a'^2 + b'^2 = n$ e

$$a'x = -b\,x \equiv_n -x\,a\,x = (-x^2)a \equiv_n a = b'.$$

A meno di effettuare tali variazioni, resta da dimostrare che $(a', b') = 1$ e che non vi sono ulteriori coppie. Se scriviamo $b = a\,x + k\,n$ otteniamo

$$\begin{aligned} n = a^2 + b^2 &= a^2 + (a\,x + k\,n)^2 = a^2 + a^2x^2 + k\,n\,a\,x + k\,n\,a\,x + k^2n^2 \\ &= a^2(x^2+1) + k\,n\,a\,x + k\,n(a\,x + k\,n) = a^2\,l\,n + k\,n\,a\,x + k\,n\,b \\ &= (a(a\,l\,n + x\,k) + k\,b)n. \end{aligned}$$

Da cui

$$\begin{aligned} a^2 + b^2 = n &\iff (a(a\,l\,n + x\,k) + k\,b)n = n \iff a(a\,l\,n + x\,k) + k\,b = 1 \\ &\iff a\,\alpha + b\,\beta = 1, \end{aligned}$$

ovvero $(a, b) = 1$.
Supponiamo infine che (A, B) sia una seconda coppia che soddisfa il teorema, per cui

$$\begin{aligned} &(A, B) = 1 && (a, b) = 1 \\ &A^2 + B^2 = n && a^2 + b^2 = n \\ &A\,x \equiv B \pmod n && a\,x \equiv b \pmod n \end{aligned}$$

In particolare $n^2 = (a\,A + b\,B)^2 + (a\,B - b\,A)^2$, dove

$$a\,A + b\,B \equiv a\,A + a\,A\,x^2 = a\,A(1 + x^2) \equiv 0 \pmod n \implies a\,A + b\,B = k\,n.$$

L'unica possibilità è che $a\,A + b\,B = n$ e $a\,B - b\,a = 0$, da cui

$$a\,B = A\,b \implies \begin{matrix} a \mid A\,b \implies a \mid A \\ A \mid a\,B \implies A \mid a \end{matrix} \implies a = A.$$

e analogamente $b = B$. □

Lemma 5.12. Sia $a x^2 + b x + c = 0 \pmod p$, $p \geqslant 3$ primo, una congruenza di secondo grado e sia $D = b^2 - 4ac$ il discriminante. Allora la congruenza ammette soluzioni se e soltanto se D è un residuo quadratico modulo p.

Dimostrazione. Applichiamo gli stessi passaggi che si effettuano nel caso di equazioni reali

$$\begin{aligned} a x^2 + b x + c \equiv_p 0 &\iff 4a^2x^2 + 4ab x + 4ac \equiv_p 0 \\ &\iff 4a^2x^2 + 4ab x + b^2 \equiv_p b^2 - 4ac \\ &\iff (2ax + b)^2 \equiv_p b^2 - 4ac. \end{aligned}$$

A questo punto si tratta di risolvere il sistema

$$\begin{cases} y^2 \equiv D \pmod p \\ 2ax + b \equiv \bar y \pmod p \end{cases}$$

dove $\bar y$ è una soluzione della prima congruenza. Osserviamo che la seconda congruenza è sempre risolubile a meno che $p \mid a$, il quale è però un caso banale. Pertanto abbiamo una soluzione quando $y^2 \equiv D \pmod p$, ovvero quando D è un residuo quadratico modulo p. □

Esempio. Dimostriamo che

$$p \equiv 1 \pmod 3 \iff \exists\, x, y \in \mathbb{Z} : p = x^2 + xy + y^2.$$

Consideriamo l'uguaglianza $p = x^2 + xy + y^2$ modulo 3 ⇐)

$$p = x^2 + xy + y^2 \equiv_3 x^2 - 2xy + y^2 = (x-y)^2.$$

Ora se $n \in \mathbb{Z}_3$ si ha che $n^2 \in \{0, 1\}$, per cui

$$p \equiv_3 (x-y)^2 \in \{0, 1\}.$$

D'altronde p primo ci dice che $p \not\equiv 0 \pmod 3$, da cui $p \equiv 1 \pmod 3$.
Consideriamo la congruenza associata $T^2+T+1 \equiv_p 0$ e supponiamo che α sia una sua soluzione. Tale soluzione esiste per il lemma precedente, in quanto il discriminante è -3 e abbiamo ⇒)

$$\left(\frac{-3}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{3-1}{2}\frac{p-1}{2}}\left(\frac{p}{3}\right) = \left(\frac{p}{3}\right) = \left(\frac{p \pmod 3}{3}\right) = \left(\frac{1}{3}\right) = 1.$$

Ora utilizzando argomenti analoghi al lemma delle gabbie e dei piccioni, avremo che esistono $a, b \in \mathbb{Z}$ tali che

$$0 < |a|, |b| < \sqrt{p} \qquad \text{e} \qquad a\alpha \equiv b \pmod p.$$

Da cui

$$a^2 + ab + b^2 \equiv a(1 + \alpha + \alpha^2) \equiv 0 \pmod p,$$

in quanto α è soluzione della congruenza $T^2 + T + 1 \equiv_p 0$. Inoltre

$$0 \underbrace{<}_{\Delta<0} a^2 + ab + b^2 < 3p \implies a^2 + ab + b^2 = \begin{cases} p \\ 2p \end{cases}$$

Ora se per assurdo $a^2 + ab + b^2 = 2p$, dal momento che $p \equiv 1 \pmod 3$, si avrebbe

$$(a-b)^2 \equiv 2 \pmod 3,$$

che è assurdo per quanto mostrato nella prima parte dell'esercizio. Per cui $a^2 + ab + b^2 = p$.

Teorema 5.13 – Ulteriori proprietà

Consideriamo le seguenti funzioni enumerative

- $T(n) = \#\left\{ x \in \mathbb{Z}_n \;\middle|\; x^2 \equiv -1 \pmod{n} \right\}$;
- $R^+(n) = \#\left\{ (a,b) \in \mathbb{N}^2 \;\middle|\; (a,b) = 1, a^2 + b^2 = n \right\}$;
- $R(n) = \#\left\{ (a,b) \in \mathbb{Z}^2 \;\middle|\; (a,b) = 1, a^2 + b^2 = n \right\}$.

Allora

$$T(n) = R^+(n), n > 1 \qquad \text{e} \qquad R(n) = 4R^+(n), \forall\, n.$$

Dimostrazione. Posto $n > 1$, mostriamo che vi è una corrispondenza biunivoca fra

$$\left\{ x \in \mathbb{Z}_n \;\middle|\; x^2 \equiv -1 \pmod{n} \right\} \qquad \text{e} \qquad \left\{ (a,b) \in \mathbb{N}^2 \;\middle|\; (a,b) = 1, a^2 + b^2 = n \right\}.$$

Se x soddisfa $x^2 + 1 \equiv 0 \pmod{n}$ abbiamo già mostrato che esiste un'unica coppia $(a,b) \in \mathbb{N}^2$ che soddisfa le proprietà cercate.
Viceversa supponiamo che $(a,b) \in \mathbb{N}^2$ soddisfino

$$a^2 + b^2 = n \qquad \text{e} \qquad (a,b) = 1.$$

Ora se $(a,n) = d > 1$ allora $d \mid a^2, n$, in particolare $d \mid b^2 = n - a^2$, per cui $d \mid (a^2, b^2)$, ma ciò è assurdo in quanto $(a,b) = 1 \implies (a^2,b^2) = 1$. Quindi $(a,n) = 1 \implies ax \equiv b \pmod{n}$ è risolubile e ammette un'unica soluzione. Mandiamo quindi (a,b) in tale soluzione x, avremo

$$n = a^2 + b^2 \implies 0 \equiv a^2 + b^2 = a^2(x^2+1) \pmod{n},$$

d'altronde $(a,n) = 1$, quindi $x^2 \equiv -1 \pmod{n}$.
Dimostriamo infine che $R(n) = 4R^+(n)$. Sia $(a,b) \in \mathbb{N}^2$ tale che $(a,b) = 1$ e $a^2 + b^2 = n$. Se $a, b \neq 0$ posso considerare le coppie

$$(a,b), \qquad (-a,b), \qquad (a,-b), \qquad (-a,-b).$$

Se invece $ab = 0$ allora $a = 0$ oppure $b = 0$. Supponiamo che $a = 0$, ma abbiamo già osservato che $(a,n) = 1$, quindi $n = 1$, che il caso escluso per ipotesi. □

Osservazione. $T(n)$ è moltiplicativa, infatti già sappiamo che se $f \in \mathbb{Z}[x]$,

$$N_f(n) = \#\{ x \in \mathbb{Z}_n \mid f(x) \equiv 0 \pmod{n} \},$$

è moltiplicativa.

Proposizione 5.14 – Calcolo della funzione $T(n)$

Preso $n \in \mathbb{N}$, sia $T(n)$ il numero delle soluzione di $x^2 + 1 \equiv 0 \pmod{n}$. Allora

$$T(n) = \begin{cases} 0 & \text{se } 4 \mid n \text{ oppure se } q \mid n \text{ con } q \equiv_4 3 \text{ primo} \\ 2^{\omega_o(n)} & \text{altrimenti} \end{cases}$$

dove $\omega_o(n)$ è il numero di primi dispari che dividono n.

Dimostrazione. Chiaramente il risultato è valido per $T(1) = 1$, per cui assumiamo $n > 1$. Abbiamo già osservato che T è una funzione moltiplicativa. Quindi se consideriamo la

scomposizione di n come

$$n = 2^r p_1^{r_1} \cdot \ldots \cdot p_t^{r_t} q_1^{u_1} \cdot \ldots \cdot q_s^{u_s},$$

dove p_j, q_i sono primi tali che $p_j \equiv 1 \pmod 4$ e $u_i \equiv 3 \pmod 4$, allora

$$T(n) = T(2^r)T(p_1^{r_1}) \cdot \ldots \cdot T(P_t^{r_t})T(u_1^{q_1}) \cdot \ldots \cdot T(u_s^{q_s}).$$

Si verifica facilmente che $T(2) = 1$. D'altronde $x^2 + 1 \equiv 0 \pmod 4$ non ha soluzioni e pertanto $T(2^r) = 0$ per $r \geqslant 2$. Segue che $T(n) = 0$ se $4 \mid n$.
Supponiamo adesso che q sia un primo tale che $q \equiv 3 \pmod 4$, ne segue che -1 non è un residuo quadratico modulo q, quindi $T(q^s) = 0$ per $s \geqslant 1$. In particolare $T(n) = 0$ se $q \mid n$.
Resta da dimostrare che se $p \equiv 1 \pmod 4$ primo, allora $T(p^r) = 2$ per ogni $r \geqslant 1$. Sappiamo che se $p \equiv 1 \pmod 4$ allora $x^2 + 1 \equiv 0 \pmod p$ ammette soluzione, pertanto $T(p) = 2$. Ora se α è tale che $\alpha^2 + 1 \equiv 0 \pmod p$ allora $2\alpha \not\equiv 0 \pmod p$, quindi, per il teorema del sollevamento ogni soluzione si solleva a p^2 in modo unico. Iterando questo procedimento si mostra proprio quanto richiesto. □

il teorema del sollevamento viene trattato nell'esercizio 7 del secondo foglio di esercizi

Teorema 5.15 – Calcolo della funzione $S(n)$

Consideriamo la funzione enumerativa della somma di due quadrati definita come

$$S(n) = \#\left\{ (a, b) \in \mathbb{Z}^2 \;\middle|\; a^2 + b^2 = n \right\}.$$

Allora

$$S(n) = 4 \sum_{d^2 \mid n} T\left(\frac{n}{d^2}\right).$$

Dimostrazione. Per definizione

$$S(n) = \sum_{\substack{(a,b)\in\mathbb{Z}^2 \\ a^2+b^2=n}} 1 = \sum_{d\in\mathbb{N}} \sum_{\substack{(a,b)\in\mathbb{Z}^2 \\ d=(|a|,|b|) \\ a^2+b^2=n}} 1.$$

Ora se $d = (|a|, |b|)$ allora $d^2 \mid a^2 + b^2 = n$. Quindi se scriviamo $a = d\,a_1$ e $b = d\,b_1$ otteniamo

$$a_1^2 + b_1^2 = \frac{n}{d^2}.$$

Da cui

$$\begin{aligned} S(n) &= \sum_{d^2\mid n} \sum_{\substack{(a,b)\in\mathbb{Z}^2 \\ d=(|a|,|b|) \\ a^2+b^2=n}} 1 = \sum_{d^2\mid n} \sum_{\substack{(a_1,b_1)\in\mathbb{Z}^2 \\ (|a_1|,|b_1|)=1 \\ a_1^2+b_1^2=n/d^2}} 1 = \sum_{d^2\mid n} R\left(\frac{n}{d^2}\right) \\ &= 4 \sum_{d^2\mid n} T\left(\frac{n}{d^2}\right). \end{aligned}$$

□

Teorema 5.16 – Scrittura alternativa di $S(n)$

Consideriamo la funzione enumerativa della somma di due quadrati definita come

$$S(n) = \#\left\{ (a,b) \in \mathbb{Z}^2 \mid a^2 + b^2 = n \right\}.$$

Allora

$$S(n) = 4 \sum_{m \mid n} \chi_4(m), \qquad \text{dove } \chi_4(m) = \begin{cases} 0 & 2 \mid m \\ (-1)^{\frac{m-1}{2}} & 2 \nmid m \end{cases}$$

Dimostrazione. Sappiamo che χ_4 è una funzione totalmente moltiplicativa, da cui

$$\omega(n) = \sum_{m \mid n} \chi_4(m),$$

è moltiplicativa. In particolare

$$\omega(p^\alpha) = \sum_{m \mid p^\alpha} \chi_4(m) = \sum_{\beta=0}^{\alpha} \chi_4(p^\beta) = \chi_4(1) + \chi_4(p) + \ldots + \chi_4(p^\alpha)$$
$$= \begin{cases} 1 & p = 2 \\ \alpha + 1 & p \equiv 1 \pmod 4 \\ 1 & p \equiv 3 \pmod 4, \alpha \text{ pari} \\ 0 & p \equiv 3 \pmod 4, \alpha \text{ dispari} \end{cases}$$

Ora, anche

$$\frac{S(n)}{4} = \sum_{d^2 \mid n} T\left(\frac{n}{d^2}\right),$$

è moltiplicativa, quindi ci basta calcolare $S(p^\alpha)/4$:

$$\frac{S(p^\alpha)}{4} = \sum_{d^2 \mid p^\alpha} T\left(\frac{p^\alpha}{d^2}\right) = \begin{cases} T(p^\alpha) + T(p^{\alpha-2}) + \ldots + T(1) & \text{se } \alpha \text{ pari} \\ T(p^\alpha) + T(p^{\alpha-2}) + \ldots + T(p) & \text{se } \alpha \text{ dispari} \end{cases}$$

Sappiamo che

$$T(p^\alpha) = \begin{cases} 1 & \text{se } p^\alpha = 2 \\ 0 & \text{se } 4 \mid p^\alpha \text{ oppure } p \equiv 3 \pmod 4 \\ 2 & \text{se } p \equiv 1 \pmod 4 \end{cases}$$

Da cui

$$\frac{S(p^\alpha)}{4} = \begin{cases} 1 & \text{se } \alpha \text{ pari, } p = 2 \\ 1 + 2\frac{\alpha}{2} & \text{se } \alpha \text{ pari, } p \equiv 1 \pmod 4 \\ 1 & \text{se } \alpha \text{ pari, } p \equiv 3 \pmod 4 \\ 1 & \text{se } \alpha \text{ dispari, } p = 2 \\ 2\frac{\alpha+1}{2} & \text{se } \alpha \text{ dispari, } p \equiv 1 \pmod 4 \\ 0 & \text{se } \alpha \text{ dispari, } p \equiv 3 \pmod 4 \end{cases}$$
$$= \begin{cases} 1 & \text{se } p = 2 \text{ oppure } p \equiv 3 \pmod 4 \text{ con } \alpha \text{ pari} \\ 0 & \text{se } p \equiv 3 \pmod 4 \text{ con } \alpha \text{ dispari} \\ \alpha + 1 & \text{se } p \equiv 1 \pmod 4 \end{cases}$$

Dal momento che i risultati coincidono la tesi è verificata. □

Osservazione. Dalla dimostrazione si può ricavare l'andamento medio si $S(n)$:

$$\frac{1}{T}\sum_{n\leqslant T} S(n) = \frac{4}{T}\sum_{n\leqslant T}\sum_{m\mid n}\chi_4(m) = \frac{4}{T}\sum_{m\leqslant T}\chi_4(m)\left[\frac{T}{m}\right].$$

Teorema 5.17 – Stima asintotica della somma di $S(n)$

Consideriamo la funzione enumerativa della somma di due quadrati definita come

$$S(n) = \#\left\{(a,b)\in\mathbb{Z}^2 \;\middle|\; a^2+b^2 = n\right\}.$$

Allora

$$\sum_{n\leqslant T} S(n) = \pi T + O(\sqrt{T}), T\to+\infty.$$

Dimostrazione. Sfruttiamo nuovamente il metodo dell'iperbole di Dirichlet (vedi teorema 2.15):

$$\begin{aligned}\sum_{n\leqslant T} S(n) &= 4\sum_{n\leqslant T}\sum_{m\mid n}\chi_4(m) = 4\sum_{\substack{a,b\in\mathbb{N}\\ ab\leqslant T}}\chi_4(a)\\ &= \sum_{a\leqslant\sqrt{T}}\chi_4(a)\sum_{b\leqslant T/a}1 + \sum_{b\leqslant\sqrt{T}}\sum_{\sqrt{T}\leqslant a\leqslant T/b}\chi_4(a)\\ &= 4\sum_{a\leqslant\sqrt{T}}\chi_4(a)\left[\frac{T}{a}\right] + O(\sqrt{T}) = 4T\sum_{a\leqslant\sqrt{T}}\frac{\chi_4(a)}{a} + O(\sqrt{T}).\end{aligned}$$

la seconda somma del secondo addendo corrisponde a $1-1+1-\ldots\leqslant 1$

Posto $\alpha = \sum \frac{\chi_4(n)}{n}$ otteniamo

$$4\alpha T + O\left(T\sum_{a>\sqrt{T}}\frac{\chi_4(a)}{a}\right) + O(\sqrt{T}) = 4\alpha T + O(\sqrt{T}).$$

Ora

$$\chi_4(2k) = 0 \implies \sum_{n=1}^{+\infty}\frac{\chi_4(n)}{n} = \sum_{k=0}^{+\infty}\frac{(-1)^k}{2k+1}.$$

Inoltre da

$$\sum_{a=0}^{t} y^a = \frac{1-y^{t+1}}{1-y},$$

posto $y = -x^2$, otteniamo

$$\sum_{n=0}^{k-1}(-1)^n x^{2n} = \frac{1-x^{2k}}{1+x^2} \implies \sum_{n=0}^{k-1}(-1)^n x^{2n} + \frac{x^{2k}}{1+x^2} = \frac{1}{1+x^2}.$$

Da cui

$$\frac{\pi}{4} = \int_0^1\frac{dx}{1+x^2} = \sum_{n=0}^{k-1}(-1)^n\int_0^1 x^{2n}\,dx + \int_0^1\frac{x^{2k}}{1+x^2}\,dx,$$

ovvero

$$\frac{\pi}{4} = \sum_{n=0}^{k-1}\frac{(-1)^n}{2n+1} + \int_0^1\frac{x^{2k}}{x^2+1}\,dx \leqslant \sum_{n=0}^{k-1}\frac{(-1)^n}{2n+1} + \int_0^1 x^{2k}\,dx = \sum_{n=0}^{k-1}\frac{(-1)^n}{2n+1} + \frac{1}{2k+1}.$$

Riepilogando

$$\sum_{n=0}^{k-1} \frac{(-1)^n}{2n+1} = \frac{\pi}{4} + O\left(\frac{1}{k}\right),$$

da cui

$$4T \sum_{a \leqslant \sqrt{T}} \frac{\chi_4(a)}{a} + O(\sqrt{T}) = \pi + O(\sqrt{T}).$$

5.3 SOMMA DI QUATTRO QUADRATI

Lemma 5.18 (Identità di Eulero)**.** Siano $n_1, n_2 \in \mathbb{N}$ tali che $n_1 = 4\square$ e $n_2 = 4\square$. Allora

$$n_1 n_2 = 4\square$$

Dimostrazione. Supponiamo che

$$n_1 = x_1^2 + x_2^2 + x_3^2 + x_4^2 \qquad \text{e} \qquad n_2 = y_1^2 + y_2^2 + y_3^2 + y_4^2.$$

Allora è sufficiente verificare la seguente uguaglianza per ottenere la tesi

$$\begin{aligned}(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) &= (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 \\ &+ (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2 + (x_1y_3 - x_3y_1 - x_2y_4 + x_4y_2)^2 \\ &+ (x_1y_4 - x_4y_1 - x_3y_2 + x_2y_3)^2.\end{aligned}$$

Teorema 5.19 – di Lagrange

Ogni $n \in \mathbb{N}$ è al più somma di quattro quadrati.

Dimostrazione. Per l'identità di Eulero ci basta dimostrare che per ogni p primo si abbia $p = 4\square$.
Per $p = 2$ la tesi è verificata in quanto $2 = 1^2 + 1^2 + 0^2 + 0^2$.
Supponiamo che $p \equiv 1 \pmod 4$, allora per il teorema di Fermat $p = x^2 + y^2$. Quindi anche in questo caso la tesi è verificata per $p = x^2 + y^2 + 0^2 + 0^2$.
Resta da verificare il caso q primo con $q \equiv 3 \pmod 4$. Certamente

$$q \equiv 3 \pmod 4 \implies \left(\frac{-1}{q}\right) = -1.$$

Definiamo

$$a = \min\left\{ x \in \mathbb{N} \;\middle|\; \left(\frac{x+1}{q}\right) = -1 \right\}.$$

In particolare avremo

$$\left(\frac{a}{q}\right) = 1 \qquad \text{e} \qquad \left(\frac{a+1}{q}\right) = -1.$$

Da cui

$$\left(\frac{-a-1}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{a+1}{q}\right) = 1.$$

Quindi abbiamo che $a \equiv x^2 \pmod q$ e $-a-1 \equiv y^2 \pmod q$. Naturalmente posso scegliere $|x|, |y| < \frac{q}{2}$ ed ottenere

$$x^2 + y^2 + 1 = m\,q,$$

dove $m \geqslant 1$ e $m < q$. Quest'ultima perchè

$$x^2 + y^2 + 1 \leqslant \frac{q^2}{4} + \frac{q^2}{4} + 1 = \frac{q^2}{2} + 1,$$

da cui

$$m\,q \leqslant \frac{q^2}{2} + 1 \iff m < \frac{q}{2} + \frac{1}{q} < q.$$

Quindi abbiamo verificato che se $q \equiv 3 \pmod 4$ allora esiste $1 \leqslant m < q$ tale che $m\,q = x_1^2 + x_2^2 + x_3^2 + x_4^2$.
Vogliamo mostrare che il minimo con tale proprietà è proprio $m = 1$.
Osserviamo che se fosse m pari si avrebbe che il numero di j tali che x_j è pari è $0, 2$ oppure 4. In ogni caso possiamo concludere, a meno di riordinare gli indici, che

$$x_1 \equiv x_2 \pmod 2 \qquad \text{e} \qquad x_3 \equiv x_4 \pmod 2.$$

Da cui

$$\frac{m}{2}q = \left(\frac{x_1 + x_2}{2}\right)^2 + \left(\frac{x_1 - x_2}{2}\right)^2 + \left(\frac{x_3 + x_4}{2}\right)^2 + \left(\frac{x_3 - x_4}{2}\right)^2.$$

Da ciò deduco che al posto di m posso prendere $m/2$, questa è una contraddizione se assumiamo che m è il minimo.
Possiamo quindi supporre m dispari. Per ogni $j = 1, 2, 3, 4$ consideriamo y_j tali che

$$y_j \equiv x_j \pmod m \qquad \text{e} \qquad |y_j| < \frac{m}{2},$$

dove $|y_j| \neq m/2$ in quanto m è dispari.
Avremo quindi

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv 0 \pmod m \implies y_1^2 + y_2^2 + y_3^2 + y_4^2 = m_0 m,$$

dove $m_0 \neq 0$ poiché altrimenti si avrebbe

$$y_j = 0, \forall\, j \implies x_j \equiv 0 \pmod m \implies q\,m = k\,m^2 \iff q = k\,m \implies m \mid q,$$

che è assurdo in quanto $1 < m < q$ con q primo. D'altronde $m_0 < m$, infatti

$$m_0 m = y_1^2 + y_2^2 + y_3^2 + y_4^2 < 4\frac{m^2}{4} = m^2 \implies m_0 < m.$$

Riassumendo sappiamo che

$$m\,q = x_1^2 + x_2^2 + x_3^2 + x_4^2, \qquad \text{con } 1 \leqslant m < q \text{ dispari},$$

e che

$$m\,m_0 = y_1^2 + y_2^2 + y_3^2 + y_4^2, \qquad \text{con } 1 \leqslant m_0 < m \text{ e } x_j \equiv y_j \pmod m.$$

Quindi, per l'identità di Eulero

$$m^2 q\,m_0 = 4\square = \underbrace{\square}_{\equiv 0 \pmod m} + \underbrace{\square}_{\equiv 0 \pmod m} + \underbrace{\square}_{\equiv 0 \pmod m} + \underbrace{\square}_{\equiv 0 \pmod m},$$

da cui

$$q\,m_0 = \frac{\square}{m^2} + \frac{\square}{m^2} + \frac{\square}{m^2} + \frac{\square}{m^2},$$

ovvero $m_0 q = z_1^2 + z_2^2 + z_3^2 + z_4^2$, con $m_0 < m$, che è una contraddizione se assumiamo che m è minimo. □

5.4 SOMMA DI TRE QUADRATI

Teorema 5.20 – di Legendre

Sia $n \in \mathbb{N}$. Allora n è la somma di tre quadrati se e soltanto se

$$n \neq 4^l(7+8k), l, k \in \mathbb{N}.$$

$\Rightarrow$) *Dimostrazione.* Se $x \in \mathbb{Z}_8$ allora $x^2 \in \{0,1,4\}$. Osserviamo che non c'è modo di ottenere 7 come somma di 3 elementi tra $\{0,1,4\}$. Per cui

$$7+8k \neq 3\square.$$

Quindi la tesi è vera per $l=0$. Procediamo ora per induzione su l. Supponiamo quindi che non esistano interi della forma

$$4^l(7+8k) = \square+\square+\square.$$

Dimostriamolo per $l+1$. Supponiamo per assurdo che esistano $x_1, x_2, x_3 \in \mathbb{Z}$ tali che

$$4^{l+1}(7+8k) = x_1^2+x_2^2+x_3^2.$$

Osserviamo che modulo 4 si ha $x^2 \equiv 0$ se x è pari e $x^2 \equiv 1$ se, viceversa, x è dispari. Quindi

$$x_1^2+x_2^2+x_3^2 = 4^{l+1}(7+8k) \equiv 0 \pmod 4,$$

ci dice che x_1, x_2, x_3 sono tutti pari, da cui

$$4^l(7+8k) = \left(\frac{x_1}{2}\right)^2+\left(\frac{x_2}{2}\right)^2+\left(\frac{x_3}{2}\right)^2,$$

che è assurdo per ipotesi induttiva. □

6 TEORIA ELEMENTARE DEI NUMERI PRIMI

6.1 RIVISITAZIONE DEL TEOREMA DI EUCLIDE

Nella prima parte del corso abbiamo dimostrato il teorema di Euclide sull'infinitezza dei numeri primi. In questo paragrafo amplieremo questo risultato.

Teorema 6.1 – Serie dei reciproci dei primi

La serie

$$\sum_{p} \frac{1}{p}.$$

è divergente.

Dimostrazione. Per ogni $X \geqslant 2$ reale, consideriamo

$$P_X = \prod_{p \leqslant X} \left(1 - \frac{1}{p}\right)^{-1},$$

da cui, passando al logaritmo,

$$\ln P_X = -\sum_{p \leqslant X} \ln\left(1 - \frac{1}{p}\right).$$

Ricordiamo che l'espansione di Taylor di $-\ln(1-t)$ è

$$-\ln(1-t) = \sum_{n=1}^{\infty} \frac{t^n}{n}, \qquad \text{per } |t| < 1.$$

Nel nostro caso $1/p$ ha modulo chiaramente minore di 1, quindi

$$\begin{aligned} \ln P_X = -\sum_{p \leqslant X} \ln\left(1 - \frac{1}{p}\right) &= \sum_{p \leqslant X} \sum_{h=1}^{\infty} \frac{1}{h\, p^h} \\ &= \sum_{p \leqslant X} \frac{1}{p} + \sum_{p \leqslant X} \sum_{h=2}^{\infty} \frac{1}{h\, p^h}. \end{aligned}$$

Definiamo

$$S_1 = \sum_{p \leqslant X} \frac{1}{p} \qquad \text{e} \qquad S_2 = \sum_{p \leqslant X} \sum_{h=2}^{\infty} \frac{1}{h\, p^h}.$$

Noi vorremmo dimostrare che $S_1 \to \infty$ per $X \to \infty$. Per farlo mostreremo che S_2 è limitata e che P_X diverge. Infatti

$$0 \leqslant \sum_{h=2}^{\infty} \frac{1}{h\, p^h} \leqslant \sum_{h=2}^{\infty} \frac{1}{p^h} = \sum_{h=0}^{\infty} \frac{1}{p^h} - 1 - \frac{1}{p} = \frac{1}{p(p-1)},$$

da cui

$$0 \leqslant S_2 \leqslant \sum_p \frac{1}{p(p-1)} \leqslant \sum_{n=2}^{\infty} \frac{1}{n(n-1)} = 1,$$

dove l'ultima serie è 1 in quanto

$$\sum_{n=2}^{\infty} \frac{1}{n(n-1)} = \sum_{n=2}^{\infty} \left(\frac{1}{n-1} - \frac{1}{n} \right) = 1 - \frac{1}{2} + \frac{1}{2} - \frac{1}{3} + \frac{1}{3} - \ldots = 1.$$

Per cui $0 \leqslant S_2 \leqslant 1$. D'altronde, per $X \to \infty$, avremo

$$P_X = \prod_{p \leqslant X} \left(1 - \frac{1}{p}\right)^{-1} = \prod_{p \leqslant X} \sum_{h=0}^{\infty} \frac{1}{p^h} = \sum_{\substack{h \in \mathbb{N} \\ \max\{p \text{ primo} : p \mid h\} \leqslant X}}$$

$$\geqslant \sum_{h \leqslant X} \frac{1}{h} \to +\infty.$$

Da cui la tesi. □

Osservazione. Questo risultato ci prova che i primi non sono un sottoinsieme "rarefatto" dei naturali. A differenza, ad esempio, delle potenze di due.

Osservazione. Il matematico Viggo Brun, dimostrò che la serie dei reciproci dei numeri primi gemelli

$$\sum_{\substack{p \text{ primo} \\ p+2 \text{ primo}}} \frac{1}{p}.$$

converge.

6.2 FUNZIONE DI VON MANGOLDT

Nel capitolo 1 abbiamo parlato della funzione $\pi(X)$, che denota il numero di primi nell'intervallo $[2, X]$. Sappiamo che Hadamard e de la Vallée Poussin hanno dimostrato nel 1896 il teorema dei numeri primi

$$\pi(X) \sim \frac{X}{\ln X}.$$

Negli anni '50 il teorema fu ridimostrato con metodi elementari da Selberg ed Erdős.

Prima di questa dimostrazione si pensava che questo teorema fosse "trascendente", ossia che non fosse dimostrabile senza l'utilizzo di analisi complessa. Intorno al 1850, il matematico Chebičev dimostrò che esistono $C_1, C_2 \in \mathbb{R}$ tali che

$$C_1 \frac{X}{\ln X} \leqslant \pi(X) \leqslant C_2 \frac{X}{\ln X}, \qquad \text{con } 0 < C_1 < 1 < C_2 < 2.$$

In questo paragrafo introdurremo una funzione che ci sarà utile per dimostrare questo risultato.

Definizione 6.2 – Funzione di von Mangoldt

Si definisce *funzione di von Mangoldt* la seguente funzione aritmetica

$$\Lambda \colon \mathbb{N} \to \mathbb{C}, \Lambda(n) = \begin{cases} \ln p & \text{se } n = p^\alpha \text{ con } p \text{ primo} \\ 0 & \text{altrimenti} \end{cases}$$

Teorema 6.3 – Trasformata di Dirichlet di Λ

La trasformata di Dirichlet di Λ è

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

Dimostrazione. Sia $n = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$. Osserviamo che ogni divisore di n che non sia del tipo p^α contribuisce in maniera nulla alla somma in questione. Quindi

$$\begin{aligned}\sum_{d|n} \Lambda(d) &= \sum_{j=1}^{s} \sum_{\beta=1}^{\alpha_j} \Lambda(p_j^\beta) = \sum_{j=1}^{s} \sum_{\beta=1}^{\alpha_j} \ln p_j \\ &= \sum_{j=1}^{s} \ln p_j \sum_{\beta=1}^{\alpha_j} 1 = \sum_{j=1}^{s} \alpha_j \ln p_j = \ln\left(\prod_{j=1}^{s} p_j^{\alpha_j}\right) \\ &= \ln n.\end{aligned}$$

□

Osservazione. Ricordiamo che se

$$\zeta_f(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s},$$

allora $\zeta_f(s)\zeta_g(s) = \zeta_{f*g}(s)$.
Quindi, sapendo che $\Lambda * 1(n) = \ln n$, avremo

$$\zeta_{\Lambda*1}(s) = \zeta_{\ln n}(s) \iff \zeta_\Lambda(s)\zeta(s) = \zeta_{\ln n}(s),$$

da cui

$$\left(\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}\right) \zeta(s) = \sum_{n=1}^{\infty} \frac{\ln n}{n^s} = -\zeta'(s).$$

Teorema 6.4 – Stima asintotica di una somma di Λ

Vale la seguente stima

$$\sum_{n \leqslant X} \Lambda(n) \left[\frac{X}{n}\right] = X \ln X - X + O(\ln X), \qquad \text{per } X \to +\infty.$$

Dimostrazione. Applichiamo la formula delle somme parziali, trattata a pagina 98, alle somme di $\ln n$:

$$\begin{aligned}\sum_{n \leqslant X} \ln n &= [X] \ln X - \int_1^X \frac{[u]}{u}\, du = X \ln X + O(\ln X) - \int_1^X du + O\left(\int_1^X \frac{1}{u}\, du\right) \\ &= X \ln X - X + O(\ln X).\end{aligned}$$

ricordiamo che $[X] = X - \{X\} = X + O(1)$

Per il teorema precedente $\ln n = \Lambda * 1$, da cui

$$\begin{aligned}\sum_{n \leqslant X} \ln n &= \sum_{n \leqslant X} \sum_{d|n} \Lambda(d) = \sum_{d \leqslant X} \Lambda(d) \sum_{\substack{n \leqslant X \\ d|n}} 1 \\ &= \sum_{d \leqslant X} \Lambda(d) \left[\frac{X}{d}\right].\end{aligned}$$

□

6.3 TEOREMA DI CHEBIČEV

Teorema 6.5 – Valore medio di Λ

Esistono $C_3, C_4 \in \mathbb{R}$ tali che

$$\sum_{n\leqslant X} \Lambda(n) \geqslant \frac{1}{2} X \ln 2, \qquad \text{per } x \geqslant C_3$$

e

$$\sum_{\frac{X}{2}\leqslant n<X} \Lambda(n) \leqslant C_4 X, \qquad \text{per ogni } x \geqslant 0.$$

Dimostrazione. Ricordando la stima del teorema precedente avremo

$$\begin{aligned}\sum_{m\leqslant X} \Lambda(m)\left(\left[\frac{X}{m}\right]-2\left[\frac{X}{2m}\right]\right) &= \sum_{m\leqslant X}\Lambda(m)\left[\frac{X}{m}\right]-2\sum_{m\leqslant X}\Lambda(m)\left[\frac{X}{2m}\right]\\ &= X\ln X - X + O(\ln X) - 2\sum_{m\leqslant \frac{X}{2}}\Lambda(m)\left[\frac{X}{2m}\right]\\ &= X\ln X - X + O(\ln X) - 2\left(\frac{X}{2}\ln\frac{X}{2}-\frac{X}{2}+O\left(\ln\frac{X}{2}\right)\right)\\ &= X\ln 2 + O(\ln X).\end{aligned}$$

Osserviamo che per ogni $\alpha \in \mathbb{N}$ si ha

$$0 \leqslant [\alpha] - 2\left[\frac{\alpha}{2}\right] \leqslant 1,$$

infatti, dalla nota disuguaglianza $\alpha - 1 < [\alpha] \leqslant \alpha$, otteniamo

$$\begin{aligned}[\alpha]-2\left[\frac{\alpha}{2}\right] &\leqslant \alpha - 2\left[\frac{\alpha}{2}\right] < \alpha - 2\left(\frac{\alpha}{2}-1\right) = 2;\\ [\alpha]-2\left[\frac{\alpha}{2}\right] &\geqslant [\alpha] - 2\frac{\alpha}{2} > \alpha - 1 - 2\frac{\alpha}{2} = -1,\end{aligned}$$

da cui segue che il risultato in quanto le parti intere sono quantità discrete.
Per cui

$$\sum_{m\leqslant X}\Lambda(m) \geqslant \sum_{m\leqslant X}\Lambda(m)\left(\left[\frac{X}{2}\right]-2\left[\frac{X}{2m}\right]\right) = X\ln 2 + O(\ln X).$$

Quindi per $X \geqslant C_3$ si ha

$$\sum_{m\leqslant X}\Lambda(m) \geqslant \frac{1}{2}X\ln 2.$$

Resta da mostrare la seconda disuguaglianza. Chiaramente, per quanto mostrato prima,

$$\sum_{\frac{X}{2}<m\leqslant X}\Lambda(m) \geqslant \sum_{\frac{X}{2}<m\leqslant X}\Lambda(m)\left(\left[\frac{X}{m}\right]-2\frac{X}{2m}\right).$$

D'altronde per $m \in \left(\frac{X}{2}, X\right]$ avremo

$$\left[\frac{X}{m}\right] = 1 \qquad \text{e} \qquad \left[\frac{X}{2m}\right] = 0,$$

quindi in particolare

$$\begin{aligned}\sum_{\frac{X}{2}<m\leqslant X}\Lambda(m) &= \sum_{\frac{X}{2}<m\leqslant X}\Lambda(m)\left(\left[\frac{X}{m}\right]-2\frac{X}{2m}\right) \leqslant \sum_{m\leqslant X}\Lambda(m)\left(\left[\frac{X}{m}\right]-2\left[\frac{X}{2m}\right]\right)\\ &= X\ln 2 + O(\ln X),\end{aligned}$$

ovvero

$$\sum_{\frac{X}{2}<m\leqslant X} \Lambda(m) \leqslant X\ln 2 + C\ln X \leqslant C_4 X,\ \forall\ X > 0,$$

a patto di prendere C_4 molto grande. □

Teorema 6.6 – di Chebičev

Sia p la funzione enumerativa dei numeri primi, allora:

$$\exists\ C_1, C_2 \in \mathbb{R}^+ : C_1\frac{X}{\ln X} \leqslant \pi(X) \leqslant C_2\frac{X}{\ln X},$$

con $0 < C_1 < 1 < C_2$ e $X \geqslant 2$.

Dimostrazione. Per il teorema precedente

$$\begin{aligned}\frac{1}{2}X\ln 2 &\leqslant \sum_{m\leqslant X}\Lambda(m) = \sum_{\substack{p,k\in\mathbb{N}\\ p^k\leqslant X}} \ln p = \sum_{p\leqslant X}\ln p\cdot \#\left\{\, k\in\mathbb{N} \;\middle|\; p^k\leqslant X\,\right\}\\ &= \sum_{p\leqslant X}\ln p\left[\frac{\ln X}{\ln p}\right] \leqslant \sum_{p\leqslant X}\ln p\frac{\ln X}{\ln p} = \sum_{p\leqslant X}\ln X\\ &= \ln X\cdot\pi(X).\end{aligned}$$

la prima uguaglianza segue nel prendere tutti i valori per cui Λ è non nulla

Da cui

$$\pi(X) \geqslant \frac{1}{2}\ln 2\cdot\frac{X}{\ln X},\ \forall\ x \geqslant C_3.$$

Per la seconda disuguaglianza, sfruttiamo ancora il teorema precedente,

$$\sum_{\frac{X}{2^{j+1}}<m\leqslant\frac{X}{2^j}} \Lambda(m) \leqslant C_4\frac{X}{2^j},\ \forall\ x \geqslant 0,\ \forall\ j \geqslant 0.$$

Sia $k \in \mathbb{N}$ tale che $2^k \leqslant \sqrt{X} < 2^{k+1}$. Ne deduciamo che

$$\sum_{\sqrt{X}<m\leqslant X} \leqslant \sum_{j=0}^{k}\sum_{\frac{X}{2^{j+1}}<m\leqslant\frac{X}{2^j}} \Lambda(m).$$

Infatti

- per $j = 0$ si ha $m \in \left(\frac{X}{2}, X\right]$;
- per $j = 1$ si ha $m \in \left(\frac{X}{4}, \frac{X}{2}\right]$;
- ...
- per $j = k$ si ha $m \in \left(\frac{X}{2^{k+1}}, \frac{X}{2^k}\right]$.

D'altronde

$$\frac{X}{2^{k+1}} = \sqrt{X}\frac{\sqrt{X}}{2^{k+1}} < 1\cdot\sqrt{X} \implies (\sqrt{X}, X] \subseteq \left(\frac{X}{2^{k+1}}, X\right],$$

quindi la seconda somma contiene più addendi della prima, ed è pertanto più grande. Per cui applicando la disuguaglianza del teorema precedente

$$\sum_{\sqrt{X}<m\leqslant X} \Lambda(m) \leqslant C_4 X\sum_{j=0}^{k}\frac{1}{2^j} < 2C_4 X,$$

ovvero

$$\sum_{\sqrt{X}<m\leqslant X} \Lambda(m) \leqslant 2C_4 X,\ \forall\ X \geqslant 0.$$

Infine

$$\pi(X) = \sum_{p \leqslant X} 1 = \sum_{p \leqslant \sqrt{X}} 1 + \sum_{\sqrt{X} < p \leqslant X} 1 < \sqrt{X} + \sum_{\sqrt{X} < p \leqslant X} \frac{\ln p}{\ln \sqrt{X}}$$
$$= \sqrt{X} + \frac{2}{\ln X} \sum_{\sqrt{X} < p \leqslant X} \ln p \leqslant \sqrt{X} + \frac{2}{\ln X} \sum_{\sqrt{X} < p \leqslant X} \Lambda(m),$$

da cui

$$\pi(X) \leqslant \sqrt{X} + 4C_4 \frac{X}{\ln X} < C_5 \frac{X}{\ln X},$$

se C_5 è sufficientemente grande. □

6.4 TEOREMA DI MERTENS

Teorema 6.7 – di Mertens

Per $X \to +\infty$ vale

1. $\displaystyle\sum_{m \leqslant X} \frac{\Lambda(m)}{m} = \ln X + O(1).$
2. $\displaystyle\sum_{p \leqslant X} \frac{\ln p}{p} = \ln X + O(1).$
3. $\displaystyle\sum_{p \leqslant X} = \ln(\ln X) + A + O\left(\frac{1}{\ln X}\right).$

Dove A è la *costante di Mertens*.

7 ESERCIZI

7.1 PRIMO FOGLIO

Esercizio 7.1. Si calcoli il valore di

- $\mathrm{MCD}(5520, 3135)$,
- $\mathrm{MCD}(8736, 3135)$.

Soluzione. Applichiamo l'algoritmo di Euclide:

- Nel primo caso avremo

$$\begin{aligned} 5520 &= 1 \cdot 3135 + 2385 \\ 3135 &= 1 \cdot 2385 + 750 \\ 2385 &= 3 \cdot 750 + 75 \\ 135 &= 1 \cdot 75 + 60 \\ 75 &= 1 \cdot 60 + 15 \\ 60 &= 4 \cdot 15, \end{aligned}$$

  quindi $(5520, 3135) = 15$.

- Nel secondo

$$\begin{aligned} 8736 &= 2 \cdot 3135 + 2466 \\ 3135 &= 1 \cdot 2466 + 669 \\ 2466 &= 3 \cdot 669 + 459 \\ 669 &= 1 \cdot 459 + 210 \\ 459 &= 2 \cdot 210 + 39 \\ 210 &= 5 \cdot 39 + 15 \\ 30 &= 2 \cdot 15 + 9 \\ 15 &= 1 \cdot 9 + 6 \\ 9 &= 1 \cdot 6 + 3 \\ 6 &= 2 \cdot 4, \end{aligned}$$

  per cui $(8736, 3135) = 3$.

Esercizio 7.2. Si calcoli il valore di

- $\nu_2(70!)$,
- $\nu_5(125!)$,
- $\nu_7(130!)$.

Soluzione. Ricordiamo che, per il teorema 1.30, avremo

$$\nu_p(n!) = \sum_{k=1}^{+\infty} \left[\frac{n}{p^k} \right].$$

Applichiamolo quindi al nostro esercizio:

- Per il primo punto

$$\begin{aligned}\nu_2(70!) &= \sum_{k=1}^{+\infty}\left[\frac{70}{2^k}\right] = \left[\frac{70}{2}\right] + \left[\frac{70}{4}\right] + \left[\frac{70}{8}\right] + \left[\frac{70}{16}\right] + \left[\frac{70}{32}\right] + \left[\frac{70}{64}\right] \\ &= 35 + 17 + 8 + 4 + 2 + 1 = 67.\end{aligned}$$

- Per il secondo

$$\begin{aligned}\nu_5(125!) &= \sum_{k=1}^{+\infty}\left[\frac{125}{5^k}\right] = \left[\frac{125}{5}\right] + \left[\frac{125}{25}\right] + \left[\frac{125}{125}\right] \\ &= 25 + 5 + 1 = 31.\end{aligned}$$

- Infine per il terzo

$$\begin{aligned}\nu_7(130!) &= \sum_{k=1}^{+\infty}\left[\frac{130}{7^k}\right] = \left[\frac{130}{7}\right] + \left[\frac{130}{49}\right] \\ &= 18 + 2 = 20.\end{aligned}$$

Esercizio 7.3. Siano $a, b, c \in \mathbb{N}$, si dimostri che

- Se $a \mid n, b \mid n$ e $(a, b) = 1$, allora
$$a\,b \mid n.$$
- Se $a \mid b\,c$ e $(a, b) = 1$, allora
$$a \mid c.$$

Soluzione. Siano $a, b, c \in \mathbb{N}$.

- Per ipotesi $(a, b) = 1$, quindi, applicando l'identità di Bezout, avremo
$$1 = x\,a + y\,b \iff n = n\,x\,a + n\,y\,b,$$
ora, $a \mid n$ e $b \mid n$, per cui $a\,\alpha = n$ e $b\,\beta = n$, sostituendo nell'equazione precedente avremo
$$n = b\,\beta\,x\,a + a\,\alpha\,y\,b = a\,b(\beta x + \alpha y),$$
ovvero
$$a\,b \mid n.$$
- In modo del tutto analogo, poichè $(a, b) = 1$, avremo
$$1 = x\,a + y\,b \iff c = c\,x\,a + c\,y\,b,$$
ma $a \mid b\,c$, quindi $a\,\alpha = b\,c$, da cui
$$c = c\,x\,a + a\,\alpha\,y = a(c\,x + \alpha\,y),$$
ovvero
$$a \mid c.$$

Esercizio 7.4. Si dimostri che esistono infiniti primi p della forma $p = 4k - 1$.

Soluzione. Supponiamo per assurdo che $p_1 \cdot \ldots \cdot p_s$ siano tutti e soli i primi della forma $p = 4k - 1$. Consideriamo quindi $N = 4p_1 \cdot \ldots \cdot p_s - 1$. Osserviamo che N è della forma $4t - 1$ e che $(N, p_j) = 1$, rimane quindi da mostrare che N ammette un divisore primo della forma $4k - 1$.

Se condiseriamo un qualsiasi $n \in \mathbb{N}$, avremo, per la divisione col resto, che

$$n = q\,4 + r, \text{ con } r \in \{0,1,2,3\},$$

inoltre se n è dispari, come nel caso dei numeri primi distinti da 2, avremo $r = 1$ o $r = 3$. Ciò significa che i primi dispari sono tutti della forma $4k-1$ o $4k+1$. Ora, se N avesse tutti i fattori primi della forma $4k+1$, si avrebbe

$$N = l_1^{\alpha_1} \cdot \ldots \cdot l_t^{\alpha_t},$$

inoltre

$$(4k_1+1)(4k_2+1) = 4(k_1k_2 + k_1 + k_2) + 1 = 4h + 1,$$

per cui N sarebbe della forma $4z+1$. Ma ciò è assurdo per la scelta di N in quanto

$$4z + 1 = 4p_1 \cdot \ldots \cdot p_s - 1 \iff 4(z - p_1 \cdot \ldots \cdot p_s) = -2,$$

ovvero se e soltanto se $2 \mid 1$, che è assurdo.

Esercizio 7.5. Sia, per $k > 1$,

$$\zeta(k) = \sum_{n=1}^{+\infty} \frac{1}{n^k},$$

la funzione ζ di Riemann, si dimostri che

$$\sum_{n \leqslant X} \frac{1}{n^k} = \zeta(k) + O\left(\frac{1}{X^{k-1}}\right) \qquad \text{e che} \qquad \sum_{n \leqslant X} \frac{\mu(n)}{n^k} = \frac{1}{\zeta(k)} + O\left(\frac{1}{X^{k-1}}\right).$$

Soluzione. Chiaramente

$$\sum_{n \leqslant X} \frac{1}{n^k} = \zeta(k) + E(X),$$

con

$$|E(X)| = \sum_{n > X} \frac{1}{n^k} = \sum_{n \geqslant M} \frac{1}{n^k} \qquad M = [X] + 1$$
$$= \frac{1}{M^k} + \frac{1}{(M+1)^k} + \ldots$$

Applicando una disequazione integrale otteniamo

$$\int_M^{+\infty} \frac{dt}{t^k} \leqslant \sum_{n > X} \frac{1}{n^k} \leqslant \frac{1}{M^k} + \int_M^{+\infty} \frac{dt}{t^k},$$

ovvero

$$\sum_{n > X} \frac{1}{n^k} < \frac{1}{([X]+1)^k} + \frac{1}{k([X]+1)^{k-1}} < \frac{2}{k}\frac{1}{x^{k-1}} \ll \frac{1}{x^{k-1}}.$$

Per la seconda uguaglianza avremo

$$\sum_{n \leqslant X} \frac{\mu(k)}{n^k} = \frac{1}{\zeta(k)} + E(X),$$

dove

$$\begin{aligned} E(X) &= \left| \sum_{h > X} \frac{\mu(h)}{h^k} \right| \\ &\leqslant \sum_{h > X} \frac{\mu(h)}{h^k} \\ &\leqslant \sum_{h > X} \frac{1}{h^k} \ll \frac{1}{X^{k-1}}. \end{aligned}$$

Esercizio 7.6. Sia N un numero dispari perfetto, dimostrare che è della forma

$$N = p_1^{1+4k}\left(p_2^{\alpha_2}\cdot\ldots\cdot p_s^{\alpha_s}\right)^2, \text{ dove } p = 1+4h.$$

Soluzione. Scriviamo la generica fattorizzazione di N

$$N = p_1^{\alpha_1}\cdot\ldots\cdot p_s^{\alpha_s},$$

con $p_i > 2$ in quanto N è dispari. Ora N è perfetto, quindi

$$\sigma(N) = 2N = 2(1+2a) = 2+4a,$$

ma

$$\sigma(N) = \left(1+p_1+\ldots p_1^{\alpha_1}\right)\left(1+p_2+\ldots+p_2^{\alpha_2}\right)\cdot\ldots\cdot\left(1+p_s+\ldots+p_s^{\alpha_s}\right),$$

che è quindi pari ma non divisibile per 4. Ciò significa che esisterà un unico i tale che $\left(1+p_i+\ldots+p_i^{\alpha_i}\right)$ è pari ma non divisibile per 4, mentre, di conseguenza, tutti gli altri fattori di $\sigma(N)$ saranno dispari.

Assumiamo per semplicità che $i = 1$. Ora il generico $\left(1+p_j+\ldots+p_j^{\alpha_j}\right)$ dispari, sarà somma di α_j+1 elementi tutti necessariamente dispari in quanto, per ipotesi, $p_j > 2$. Avremo quindi, preso $j \geqslant 2$, che α_j+1 è dispari, ovvero

$$\alpha_j \text{ pari }, \forall\, j \geqslant 2.$$

Per la medesima ragione α_1 è necessariamente dispari. Riepilogando

$$N = p_1^{1+2\alpha_1}\left(p_2^{\alpha_2}\cdot\ldots\cdot p_s^{\alpha_s}\right)^2.$$

Resta da mostrare che non vi sono altre fattorizzazioni possibili, ma, per quanto detto finora,

$$2+4a = \sigma(N) = \left(1+p_1+\ldots+p_1^{2\alpha_1+1}\right)d,$$

dove d è dispari, mentre il primo fattore è primo ma non divisibile per 4. Quindi $p_1 = 4c+\varepsilon$ con $\varepsilon = \pm 1$, da cui

$$\begin{aligned} 2+4a = \sigma(N) &= \left(1+\varepsilon+4c+(\varepsilon+4c)^2+\ldots+(\varepsilon+4c)^{2\alpha_1+1}\right)d \\ &= \left(1+\varepsilon+\varepsilon^2+\ldots+\varepsilon^{2\alpha_1+1}+4D\right)d, \end{aligned}$$

dove, ancora una volta, avremo $1+\varepsilon+\varepsilon^2+\ldots+\varepsilon^{2\alpha_1+1}$ pari ma non divisibile per 4, quindi

$$\left(1+\varepsilon+\varepsilon^2+\ldots+\varepsilon^{2\alpha+1}\right) = \sum_{k=0}^{2\alpha_1+1}\varepsilon^k = \begin{cases} 2\alpha_1+2 & \varepsilon = 1 \\ \pm 1 & \varepsilon = -1 \end{cases}$$

Infine, l'unico modo per ottenere un numero pari ma non divisibile per 4, è che $\varepsilon = 1$ e α_1 sia pari, ovvero

$$N = p_1^{1+4k}\left(p_2^{\alpha_2}\cdot\ldots\cdot p_s^{\alpha_s}\right)^2, \text{ con } p_1 = 4c+1.$$

7.2 SECONDO FOGLIO

Esercizio 7.1 (Formula delle somme parziali)**.** Sia $(a_n)_{n\in\mathbb{N}}$ una successione di valori in $\mathbb{C}$ e sia $\varphi(x)$ una funzione di classe C^1. Si dimostri che

$$\sum_{1\leqslant n\leqslant x} a_n\varphi(n) = A(x)\varphi(x) - \int_1^x A(u)\varphi'(u)\,du, \qquad \text{con} \qquad A(x) = \sum_{1\leqslant n\leqslant x} a_n.$$

Soluzione. Suddividiamo l'integrale

$$A(x)\varphi(x) - \int_1^x A(u)\varphi'(u)\,du = A(x)\varphi(x) - \sum_{n=1}^{[x]-1} \int_n^{n+1} A(u)\varphi'(u)\,du - \int_{[x]}^x A(u)\varphi'(u)\,du.$$

Osserviamo che nell'intervallo $(n, n+1)$ avremo che $A(u) \equiv A(n)$, da cui

$$\begin{aligned}
&= A(x)\varphi(x) - \sum_{n=1}^{[x]-1} A(n)\ \varphi(u)|_n^{n+1} - A(x)\ \varphi(u)|_{[x]}^x \\
&= \cancel{A(x)\varphi(x)} - \sum_{n=1}^{[x]-1} A(n)\big(\varphi(n+1) - \varphi(n)\big) - \cancel{A(x)\varphi(x)} + A\big([x]\big)\varphi\big([x]\big) \\
&= -\sum_{n=1}^{[x]-1} \big(A(n+1) - a_{n+1}\big)\varphi(n+1) + \sum_{n=1}^{[x]-1} A(n)\varphi(n) + A\big([x]\big)\varphi\big([x]\big) \\
&= -\sum_{n=1}^{[x]-1} A(n+1)\varphi(n+1) + \sum_{n=1}^{[x]-1} a_{n+1}\varphi(n+1) + \sum_{n=1}^{[x]-1} A(n)\varphi(n) + A\big([x]\big)\varphi\big([x]\big) \\
&= \sum_{n=1}^{[x]-1} a_{n+1}\varphi(n+1) + A(1)\varphi(1) = \sum_{n=1}^{[x]} a_n\varphi(n).
\end{aligned}$$

Esercizio 7.2. Si trovino tutte le soluzioni di

$$5X \equiv 10 \pmod{35},$$

nell'intervallo $[-500, 500]$.

Soluzione. La congruenza ammette soluzioni se e soltanto se $(5, 35) \mid 10$, ma $(5, 35) = 5$, per cui le soluzioni esistono e sono precisamente 5. Quindi

$$5X \equiv 10 \pmod{35} \iff X \equiv 2 \pmod{7},$$

ovvero $X = 2 + 7k$ con $0 \leqslant k \leqslant 4$. Per cui le soluzioni modulo 35 sono

$$2, 9, 16, 23, 30.$$

In particolare le soluzioni intere nell'intervallo $[-500, 500]$ seguono da

$$-500 \leqslant 2 + 7k \leqslant 500 \iff \left[-\frac{502}{7}\right] + 1 \leqslant k \leqslant \left[\frac{498}{7}\right],$$

ovvero $-71 \leqslant k \leqslant 71$ che corrispondono precisamente a 143 soluzioni.

Esercizio 7.3. Calcolare tutte le radici primitive modulo 50

Soluzione. La strategia consiste nel trovare una radice primitiva modulo 5^α, per il teorema 3.27 essa sarà automaticamente una radice primitiva modulo $2\,5^\alpha$, infatti $50 = 2\,5^2$.

Possiamo osservare facilmente che 3 è una radice primitiva modulo 5, infatti

$$3^{\varphi(5)} = 3^4 \equiv 1 \pmod{5}.$$

Per sollevare 3 ad una radice modulo 5^α cerchiamo $t \in \mathbb{Z}$ tale che

$$(3 + 5t)^4 = 1 + 5u, \text{ con } 5 \nmid u.$$

Se $t = 0$ avremo

$$3^4 = 81 = 1 + 80 = 1 + 5\,16, \text{ con } 5 \nmid 16,$$

per cui 3 è una radice primitiva modulo 5^α, in particolare, essendo dispari, è una radice primitiva modulo $2\,5^\alpha$ e quindi anche modulo 50.

Tramite una radice primitiva conosciamo anche tutte le altre, esse saranno della forma 3^k con $\big(k, \varphi(50)\big) = 1$. Pertanto esisteranno precisamente $\varphi\big(\varphi(50)\big) = \varphi(20) = 8$ radici primitive modulo 50:

$$3^1, 3^3, 3^7, 3^9, 3^{11}, 3^{13}, 3^{17}, 3^{19},$$

ovvero

$$3, 13, 17, 23, 27, 33, 37, 47.$$

7.3 TERZO FOGLIO

Esercizio 7.1.a. Sia $p \neq 5$ primo tale che $p = x^2 + 5y^2$, con $x, y \in \mathbb{Z}$. Allora

$$p \equiv 1 \pmod{20} \qquad \text{oppure} \qquad p \equiv 9 \pmod{20}.$$

Soluzione. Supponiamo che esistano $x, y \in \mathbb{Z}$ tali che $p = x^2 + 5^y$, consideriamo tale uguaglianza modulo 4:

$$p = x^2 + 5y^2 \equiv x^2 + y^2 \pmod 4.$$

Ora se $n \in \mathbb{Z}_4$ allora $n^2 \in \{[0]_4, [1]_4\}$, per cui

$$x^2 + y^2 \in \{[0]_4, [1]_4, [2]_4\} \implies p \equiv 1 \pmod 4,$$

in quanto p primo implica $p \not\equiv 0, 2 \pmod 4$.

Analogamente consideriamo l'uguaglianza modulo 5:

$$p = x^2 + 5y^2 \equiv x^2 \pmod 5.$$

Se $n \in \mathbb{Z}_5$ allora $n^2 \in \{[0]_5, [1]_5, [4]_5\}$, per cui

$$p \equiv 1 \pmod 5 \qquad \text{oppure} \qquad p \equiv 4 \pmod 5,$$

in quanto, di nuovo, p primo implica $p \not\equiv 0 \pmod 5$.

Riepilogando se $p = x^2 + 5y^2$ allora

$$\begin{cases} p \equiv 1 \pmod 4 \\ p \equiv 1 \pmod 5 \end{cases} \qquad \text{oppure} \qquad \begin{cases} p \equiv 1 \pmod 4 \\ p \equiv 4 \pmod 5 \end{cases}$$

da cui si ottiene facilmente la tesi.

Esercizio 7.1.b. Si dimostri che per ogni $p \equiv 1, 9 \pmod{20}$ esiste $k \in \{1, 2, 3, 4, 5\}$ tale che

$$k\,p = x^2 + 5y^2.$$

Soluzione. Sia $\alpha \in \mathbb{Z}$ una soluzione di $x^2 + 5 \equiv 0 \pmod p$. Osserviamo che tale soluzione esiste se e solo se -5 è un residuo quadratico modulo p D'altronde $p \equiv 1, 9 \pmod{20}$ si ha $p \equiv 1 \pmod 4$, quindi

$$\left(\frac{-5}{p}\right) = \left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = \left(\frac{5}{p}\right) = \left(\frac{p \pmod 5}{5}\right) = 1.$$

Per il lemma delle gabbie e dei piccioni sappiamo che esistono $x, y \in \mathbb{Z}$ tali che

$$0 < |x|, |y| < \sqrt{p} \qquad \text{e} \qquad y\,\alpha \equiv x \pmod p.$$

Quindi

$$x^2 + 5y^2 \equiv_p y^2\alpha^2 + 5y^2 = y^2(\alpha^2 + 5) \equiv 0 \pmod p \implies x^2 + 5y^2 = k\,p.$$

Inoltre $0 < x^2 + 5y^2 < 6p$, quindi $k \in \{1, 2, 3, 4, 5\}$.

Esercizio 7.1.c. Dimostrare che se $x, y \in \mathbb{Z}$ allora $x^2 + 5y^2 \not\equiv 2, 3, 7, 18 \pmod{20}$. Dedurre inoltre che se p è primo con $p \equiv 1, 9 \pmod{20}$, allora

$$p = x^2 + 5y^2 \qquad \text{oppure} \qquad 4p = x^2 + 5y^2.$$

Soluzione. Abbiamo già mostrato negli esercizi precedenti che necessariamente

$$x^2 + 5y^2 \equiv 0, 1, 2 \pmod{4} \qquad \text{e} \qquad x^2 + 5y^2 \equiv 0, 1, 4 \pmod{5}.$$

Bisogna quindi risolvere tutti i possibili sistemi che queste condizioni inducono. Svolgendo i calcoli si ha che

$$x^2 + 5y^2 \equiv 0, 16, 4, 5, 1, 9, 10, 6, 14 \pmod{20},$$

che come ci aspettavamo non coincidono con $2, 3, 7, 18$.

Ora se $p \equiv 1 \pmod{20}$ e fosse $x^2 + 5y^2 = 2p, 3p$ allora

$$x^2 + 5y^2 \equiv 2, 3 \pmod{20},$$

che è assurdo per la parte precedente.

Analogamente se $p \equiv 9 \pmod{20}$ e $x^2 + 5y^2 = 2p, 3p$ allora

$$x^2 + 5y^2 \equiv 18, 7 \pmod{20},$$

che è nuovamente assurdo.

Osserviamo infine che se $x^2 + 5y^2 = 5p$ allora $5 \mid 5p, 5y^2 \implies 5 \mid x^2$. Quindi $x = 5x'$, da cui

$$25x'^2 + 5y^2 = 5p \implies 5x'^2 + y^2 = p,$$

che un caso già considerato.

Esercizio 7.1.d. Dimostrare che se $4 \mid x^2 + 5y^2$ allora $2 \mid (x, y)$. Dedurre che se p è primo si ha

$$p \equiv 1, 9 \pmod{20} \iff p = x^2 + 5y^2, x, y \in \mathbb{Z}.$$

Soluzione. Se per assurdo $2 \nmid (x, y)$ allora

$$x \equiv 1 \pmod{2} \qquad \text{oppure} \qquad y \equiv 1 \pmod{2} \qquad \text{oppure} \qquad x, y \equiv 1 \pmod{2}.$$

Nel primo caso si avrebbe $x^2 \equiv 1 \pmod{4}$ e $y \equiv 0 \pmod{4}$, quindi

$$x^2 + 5y^2 \equiv 1 \pmod{4},$$

che è assurdo in quanto $4 \mid x^2 + 5y^2$.

Nel secondo caso, analogamente, $y^2 \equiv 1 \pmod{4}$ e $x^2 \equiv 0 \pmod{4}$, quindi

$$x^2 + 5y^2 \equiv 5 \equiv 1 \pmod{4},$$

che è nuovamente assurdo.

Infine nell'ultimo caso, si avrebbe $x^2, y^2 \equiv 1 \pmod{4}$, da cui

$$x^2 + 5y^2 \equiv 6 \equiv 2 \pmod{4},$$

che è anch'esso assurdo.

Dall'esercizio precedente sappiamo che

$$p \equiv 1, 9 \pmod{20} \iff p, 4p = x^2 + 5y^2, x, y \in \mathbb{Z}.$$

Ora se $2 \mid (x, y)$ allora $x = 2x'$ e $y = 2y'$, da cui

$$4p = x^2 + 5y^2 \implies 4p = 4x'^2 + 4 \cdot 5y'^2 \implies p = x'^2 + 5y'^2.$$

Esercizio 7.2. Siano $a, b \in \mathbb{N}$, si calcoli il numero di modi in cui è possibile esprimere

$$6^a 65^b$$

come somma di due quadrati.

Soluzione. Dobbiamo calcolare $S(6^a 65^b)$. Sappiamo che $S(n)/4$ è una funzione moltiplicativa e

$$\frac{S(p^\alpha)}{4} = \begin{cases} 1 & \text{se } p = 2 \text{ oppure } p \equiv 3 \pmod 4 \text{ con } \alpha \text{ pari} \\ 0 & \text{se } p \equiv 3 \pmod 4 \text{ con } \alpha \text{ dispari} \\ \alpha + 1 & \text{se } p \equiv 1 \pmod 4 \end{cases}$$

Da cui

$$\frac{S(6^a 65^b)}{4} = \frac{S(2^a)}{4}\frac{S(3^a)}{4}\frac{S(5^b)}{4}\frac{S(13^b)}{4}.$$

Ora se $2 \mid a$ allora $S(6^a 65^b) = 0$ in quanto

$$3 \equiv 3 \pmod 4 \implies \frac{S(3^a)}{4} = 0.$$

Se $2 \nmid a$ avremo

$$\frac{S(2^a)}{4} = 1, \frac{S(3^a)}{4} = 1, \frac{S(5^b)}{4} = b + 1, \frac{S(13^b)}{4} = b + 1.$$

Quindi

$$S(6^a 65^b) = \begin{cases} 0 & \text{se } 2 \mid a \\ 4(b+1)^2 & \text{se } 2 \nmid a \end{cases}$$

Esercizio 7.3. Sia $\alpha \in \mathbb{R}$ con $0 \leqslant \alpha \leqslant 1$. Allora esiste $S \subset \mathbb{N}$ tale che ha densità naturale

$$\delta_S = \alpha, \qquad \text{con } \delta_S = \lim_{T \to +\infty} \frac{\#(S \cap [1, T])}{\#(\mathbb{N} \cap [1, T])}.$$

Osservazione. Si suggerisce di considerare la successione $\{[\beta n]\}_{n \in \mathbb{N}}$ per un certo $\beta \in \mathbb{R}$.

Soluzione. Definiamo, per il suggerimento,

$$S = \{\, [\beta n] \mid n \in \mathbb{N} \,\} \cap \mathbb{N}, \qquad \text{con } \beta \in \mathbb{R} \text{ fissato.}$$

Avremo

$$\#(S \cap [1, T]) = \{\, n \in \mathbb{N} \mid 0 < [\beta n] \leqslant T \,\} = \{\, n \in \mathbb{N} \mid \{\beta n\} < \beta n \leqslant T + \{\beta n\} \,\},$$

da cui

Esercizio 7.4. Tramite la formula delle somme parziali si trovi una formula asintotica per

$$\sum_{n \leqslant T} \ln^3 n.$$

Dimostrazione. Ricordiamo che se $\{a_n\}_{n \in \mathbb{N}}$ è una successione a valori in $\mathbb{C}$ e $\varphi(x)$ è una

funzione di classe C^1, allora vale

$$\sum_{n\leqslant T} a_n \varphi(n) = A(T)\varphi(T) - \int_1^T A(u)\varphi'(u)\,du, \qquad \text{con } A(T) = \sum_{n\leqslant T} a_n.$$

Nel nostro caso abbiamo $a_n \equiv 1$ e $\varphi(x) = \ln^3 x$. Da cui

$$\sum_{n\leqslant T} \ln^3 n = [T]\ln^3(T) - 3\int_1^T \frac{[T]\ln^2(u)}{u}\,du.$$

Ricordando che $[T] = T - \{T\} = T + O(1)$, avremo

$$\sum_{n\leqslant T} \ln^3 n = T\ln^3(T) + O\big(\ln^3(T)\big) - 3\int_1^T \ln^2(u)\,du - O\left(\int_1^T 3\frac{\ln^2 u}{u}\,du\right).$$

D'altronde

$$\int_1^T 3\frac{\ln^2 u}{u}\,du = \ln^3 T,$$

da cui

$$\sum_{n\leqslant T} \ln^3 n = T\ln^3(T) - 3\int_1^T \ln^2(u)\,du + O\big(\ln^3(T)\big).$$

A questo punto possiamo scegliere se stimare l'integrale oppure se ottenere un'approssimazione migliore tramite lo sviluppo per parti. Nel primo caso avremo

$$\int_1^T \ln^2 u\,du \leqslant \ln^2 T \int_1^T du = (T-1)\ln^2 T = O\big(T\ln^2 T\big).$$

Nel secondo, tramite uno sviluppo per parti, otterremmo

$$-3\int_1^T \ln^2 u\,du = -3T\ln^2 T + 6T\ln T - 6T + 6.$$

Quindi

$$\sum_{n\leqslant T} \ln^3 n = T\ln^3 T - 3T\ln^2 T + 6T\ln T - 6T + 6 + O\big(\ln^3(T)\big).$$

□

Esercizio 7.5.a. Un intero positivo d si definisce divisore unitario di $n \in \mathbb{N}$ se $d \mid n$ e $(d, n/d) = 1$. Definiamo

$$d^*(n) = \#\{\, d \in N \mid d \text{ divisore unitario di } n \,\}.$$

Si dimostri che d^* è una funzione moltiplicativa.

Soluzione. Siano $n, m \in \mathbb{N}$ tali che $(n, m) = 1$. Vorremmo dimostrare che esiste una corrispondenza biunivoca

$$D^*(n) \times D^*(m) \leftrightarrow D^(n\,m).$$

Mandiamo $(d_1, d_2) \mapsto d_1 d_2$. Dobbiamo verificare che $d_1 d_2$ è un divisore di $n\,m$ e che $(d_1 d_2, n/d_1\; m/d_2) = 1$.

Chiaramente se $d_1 \mid n$ e $d_2 \mid m$ allora $d_1 d_2 \mid n\,m$.

Ora supponiamo che $l \mid d_1\, d_2$

Esercizio 7.5.b. Si trovi una formula per $d^*(p^\alpha)$ con p primo e $\alpha \geqslant 1$.
Dedurre inoltre che se n è privo di fattori quadratici si ha

$$d^*(n) = d(n).$$

Produrre infine un esempio per cui $d^*(n) \neq d(n)$.

Dimostrazione. Chiaramente i divisori unitari di p^α sono 1 e p^α stesso. Quindi $d^*(p^\alpha) = 2$.
Ora se $n = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$, sapendo che $d^*(p^\alpha) = 2$ e che d^* è moltiplicativa, si ha

$$d^*(n) = 2^s \qquad \text{e} \qquad d(n) = \prod_{j=1}^{s}(\alpha_j + 1),$$

dove la seconda formula è stata dimostrata nella proposizione a pagina 21.
Quindi

$$\prod_{j=1}^{s} 2 = \prod_{j=1}^{s}(\alpha_j + 1) \iff 2 = \alpha_j + 1 \iff \alpha_j = 1, \forall\, j.$$

Ovvero $n = p_1 \cdot \ldots \cdot p_s$ è privo di fattori quadratici.
Alla luce di questo fatto è semplice trovare un caso in cui $d^*(n) = d(n)$, ad esempio

$$d^*(4) = 2 \neq d(4) = 3.$$

□

Esercizio 7.5.c. Si consideri la funzione

$$\sigma_k^*(n) = \sum_{\substack{d \mid n \\ (d,\, n/d)=1}} d^k.$$

Si provi che σ_k^* è moltiplicativa per ogni $k \in \mathbb{Z}$.

Dimostrazione. Segue da d^* moltiplicativa. Infatti se ho $n, m \in \mathbb{Z}$ tali che $(n, m) = 1$, allora

$$\begin{aligned}\sigma_k^*(nm) &= \sum_{\substack{d \mid nm \\ d \text{ unitario}}} d^k = \sum_{\substack{d_1 \mid n \\ d_2 \mid m \\ d_1, d_2 \text{ unitari}}} (d_1 d_2)^k = \sum_{\substack{d_1 \mid n \\ d_1 \text{ unitario}}} d_1^k \sum_{\substack{d_2 \mid m \\ d_2 \text{ unitario}}} d_2^k \\ &= \sigma_k^*(n)\sigma_k^*(m).\end{aligned}$$

□

Esercizio 7.5.d. Si trovi una formula per $\sigma_k^*(p^\alpha)$ con p primo e $\alpha \geqslant 1$. Si calcoli infine $\sigma_{-3}^* * \mu(324)$.

Soluzione. Dal punto b possiamo dedurre facilmente che

$$\sigma_k^*(p^\alpha) = 1 + p^{k\,\alpha}.$$

Ora, per calcolare $\sigma_{-3}^* * \mu(324)$, ricordiamo che la convoluzione di funzioni moltiplicative è moltiplicativa. Quindi

$$\sigma_{-3}^* * \mu(324) = \sigma_{-3}^* * \mu(2^2)\sigma_{-3}^* * \mu(3^4),$$

dove

$$\sigma^*_{-3} * \mu(2^2) = \sum_{d|2^2} \sigma^*_{-3}\left(\frac{2^2}{d}\right)\mu(d) = \sigma^*_{-3}(2^2) - \sigma^*_{-3}(2) = \frac{1}{2^6} - \frac{1}{2^3},$$

e

$$\sigma^*_{-3} * \mu(3^4) = \sum_{d|3^4} \sigma^*_{-3}\left(\frac{3^4}{d}\right)\mu(d) = \sigma^*_{-3}(3^4) - \sigma^*_{-3}(3^3) = \frac{1}{3^{12}} - \frac{1}{3^9}.$$

Esercizio 7.6. Descrivere gli interi che non possono essere scritti come somma di tre quadrati e provare che esistono infiniti di tali interi.

Soluzione. Si veda il teorema di Legendre a pagina 88.

Avremo quindi che ogni intero della forma $7+8k$ non è somma di tre quadrati. Ovviamente esistono infiniti interi siffatti.

Esercizio 7.7. Siano $d, n, m \in \mathbb{Z}$. Si dimostri che se esistono $x, y, z, t \in \mathbb{Z}$ tali che

$$n = x^2 + d\,y^2 \qquad \text{e} \qquad m = z^2 + d\,t^2,$$

allora esistono $u, v \in \mathbb{Z}$ tali che $n\,m = u^2 + d\,v^2$.
Usare questo fatto per esprimere 5548 nella forma $Q^2 + 3P^2$.

Soluzione. In generale possiamo considerare

$$x^2 + d\,y^2 = (x + \sqrt{-d}y)(x - \sqrt{-d}y) = \alpha\,\bar{\alpha},$$
$$z^2 + d\,t^2 = (z + \sqrt{-d}t)(z - \sqrt{-d}t) = \beta\,\bar{\beta},$$

dove

$$\alpha\,\beta = (x\,z - d\,y\,t) + \sqrt{-d}(x\,t + y\,z).$$

Da cui

$$n\,m = \alpha\,\beta\,\bar{\alpha\beta} = |\alpha\,\beta|^2 = (x\,z - d\,y\,t)^2 + d(x\,t + y\,z)^2 = u^2 + d\,v^2.$$

Adesso troviamo $Q, P \in \mathbb{Z}$ tali che $5548 = Q^2 + 3P^2$. Osserviamo che $5548 = 4 \cdot 19 \cdot 73$, dove

$$4 = 1 + 3 \cdot 1 = |1 + \sqrt{-3}|^2,$$
$$19 = 16 + 3 \cdot 1 = |4 + \sqrt{-3}|^2,$$
$$73 = 25 + 3 \cdot 16 = |5 + 4\sqrt{-3}|^2.$$

Da cui

$$5548 = |(1 + \sqrt{-3})(4 + \sqrt{-3})(5 + 4\sqrt{-3})|^2 = |-55 + 29\sqrt{-3}|^2 = 55^2 + 3 \cdot 29^2.$$

Esercizio 7.8.a. Sia $k \in \mathbb{N}$. Preso $n \in \mathbb{N}$ definiamo la funzione totiente di Jordan $J_k(n)$ di n come una generalizzazione della funzione di Eulero,

$$J_k(n) = \#\left\{ (a_1, \ldots, a_k) \in \mathbb{N}^k \;\middle|\; a_1, \ldots, a_k \leqslant n, (n, a_1, \ldots, a_k) = 1 \right\}.$$

Si provi che la funzione di Jordan è moltiplicativa e che

$$J_k(n) = n^k \prod_{p|n}\left(1 - \frac{1}{p^k}\right).$$

Soluzione. La strategia consiste nel dimostrare che:

1. J_k è moltiplicativa;

2. vale $J_k(p^\alpha) = p^{k\alpha}(1 - 1/p^k)$.

Da ciò dedurremmo, preso $n = p_1^{\alpha_1} \cdot \ldots \cdot p_s^{\alpha_s}$, che

$$\begin{aligned} J_k(n) &= \prod_{j=1}^{s} J_k(p_j^{\alpha_j}) = \prod_{j=1}^{s} p_j^{k\alpha_j}\left(1 - \frac{1}{p_j^k}\right) = \prod_{j=1}^{s} p_j^{k\alpha_j} \prod_{j=1}^{s}\left(1 - \frac{1}{p_j^k}\right) \\ &= n^k \prod_{p \mid n}\left(1 - \frac{1}{p^k}\right). \end{aligned}$$

Definiamo $H_k(n) = \left\{ (a_1, \ldots, a_k) \in (\mathbb{Z}_n)^k \;\middle|\; (n, a_1, \ldots, a_k) = 1 \right\}$, vorremmo la seguente corrispondenza biunivoca

$$H_k(nm) \leftrightarrow H_k(n) \times H_k(m).$$

$\leftarrow$) Supponiamo che $(a_1, \ldots, a_k) \in H_k(n), (b_1, \ldots, b_k) \in H_k(m)$. Per ogni j sia γ_j l'unica soluzione di

$$\begin{cases} x \equiv a_j \pmod{n} \\ x \equiv b_j \pmod{m} \end{cases}$$

segue che $(\gamma_1, \ldots, \gamma_k) \in H_k(nm)$.

$\rightarrow$) Analogamente, se $(\gamma_1, \ldots, \gamma_k) \in H_k(nm)$, per ogni j è sufficiente prendere a_j, b_j tali che

$$a_j \equiv \gamma_j \pmod{n} \qquad \text{e} \qquad b_j \equiv \gamma_j \pmod{m}.$$

Dimostriamo infine che $J_k(p^\alpha) = p^{k\alpha}(1 - 1/p^k)$. Ora per ogni $(a_1, \ldots, a_k) \in \mathbb{N}^k$ e per ogni p primo, avremo

$$(p^\alpha, a_1, \ldots, a_k) \neq 1 \iff p \mid a_i, \forall\, i,$$

da cui

$$\begin{aligned} &\#\left\{ (a_1, \ldots, a_k) \in \mathbb{N}^k \;\middle|\; a_1, \ldots, a_k \leqslant p^a, p \mid a_1, \ldots, a_k \right\} \\ &\qquad = \#\{ (a_1, \ldots, a_k) \in \mathbb{Z}_{p^\alpha} \mid p \mid a_1, \ldots, a_k \}^k = (p^{\alpha-1})^k. \end{aligned}$$

Ora è chiaro che $H_k(p^\alpha)$ corrisponde al complementare dell'insieme di cui abbiamo appena calcolato la cardinalità. Quindi, dal momento che $|(\mathbb{Z}_{p^\alpha})^k| = p^{\alpha k}$, avremo

$$\begin{aligned} J_k(p^\alpha) &= p^{\alpha k} - \#\{ (a_1, \ldots, a_k) \in \mathbb{Z}_{p^\alpha} \mid p \mid a_1, \ldots, a_k \}^k \\ &= p^{\alpha k} - p^{(\alpha-1)k} = p^{\alpha k}\left(1 - \frac{1}{p^k}\right). \end{aligned}$$

Esercizio 7.8.b. Dimostrare che

$$\sum_{d \mid n} J_k(d) = n^k.$$

Soluzione. Osserviamo che tale somma è la convoluzione di J_k e la funzione unitaria. Sappiamo che la convoluzione di due funzioni moltiplicative è moltiplicativa. In particolare la funzione unitaria è banalmente moltiplicativa e J_k lo è per il punto precedente.

Quindi affinché la tesi sia valida è sufficiente verificarla per $n = p^\alpha$:

la formula per $J_k(p^i)$ viene dal punto precedente

$$\begin{aligned} \sum_{d \mid p^\alpha} J_k(d) &= \sum_{i=0}^{\alpha} J_k(p^i) = 1 + \sum_{i=i}^{\alpha} p^{ki}\left(1 - \frac{1}{p^k}\right) \\ &= 1 + \left(1 - \frac{1}{p^k}\right)\sum_{i=1}^{\alpha} p^{ki} = 1 + \left(1 - \frac{1}{p^k}\right) p^k \frac{p^{k\alpha} - 1}{p^k - 1} \\ &= p^{k\alpha}. \end{aligned}$$

Esercizio 7.8.c. Si verifichi l'identità

$$J_k(n) = \mu(n) * n^k.$$

Soluzione. Ricordiamo la prima formula di inversione di Möebius

$$g(n) = \sum_{d|n} f(d) \implies f(n) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right),$$

ovvero $g = f * 1 \implies f = \mu * g$.

Dal punto precedente sappiamo che $J_k * 1 = n^k$, quindi, applicando l'inversione di Möebius,

$$J_k = \mu * n^k.$$

Esercizio 7.8.d. Si verifichi l'identità

$$\sum_{n \geqslant 1} \frac{J_k(n)}{n^s} = \frac{\zeta(s-k)}{\zeta(s)}.$$

Soluzione. Abbiamo già osservato a pagina 40 che se

$$\zeta_f(s) = \sum_{n \geqslant 1} \frac{f(n)}{n^s},$$

allora $\zeta_f(s)\zeta_g(s) = \zeta_{f*g}(s)$.

Nel punto precedente abbiamo dimostrato che $J_k = \mu * n^k$, da cui

$$\begin{aligned} \sum_{n \geqslant 1} \frac{J_k(n)}{n^s} = \zeta_{J_k}(s) = \zeta_{\mu * n^k}(s) = \zeta_\mu(s)\zeta_{n^k}(s) \\ = \sum_{n \geqslant 1} \frac{\mu(n)}{n^s} \sum_{n \geqslant 1} \frac{n^k}{n^s} = \frac{\zeta(s-k)}{\zeta(s)}, \end{aligned}$$

dove il calcolo di $\zeta_\mu(s)$ è possibile verificarlo a pagina 33.

INDICE ANALITICO