Università degli Studi di Parma
Facoltà di Scienze Matematiche, Fisiche e Naturali
Corso di Laurea in Matematica

Alessandro Zaccagnini

Lezioni di Teoria dei Numeri

A. A. 2002–2003

Il testo è stato composto per mezzo di un pacchetto di macro creato dall'Autore e basato su $\mathcal{AMS}$-TEX 2.1, © American Mathematical Society. La maggior parte delle figure sono state create per mezzo di Mathematica^{TM}, Wolfram Research Inc, o di MetaPost. L'ultima versione di questo testo è disponibile agli indirizzi

`http://www.math.unipr.it/~zaccagni/psfiles/lezioni/Lezioni.ps.gz`
`http://www.math.unipr.it/~zaccagni/psfiles/lezioni/Lezioni.pdf`

Una versione aggiornata dell'Errata per queste dispense si trova agli indirizzi

`http://www.math.unipr.it/~zaccagni/psfiles/lezioni/Errata2002.ps.gz`
`http://www.math.unipr.it/~zaccagni/psfiles/lezioni/Errata2002.pdf`

La data di questa versione è 13.6.2004.

Questa versione su Internet è a disposizione di chiunque, gratuitamente, per un qualsiasi valido scopo di istruzione, a patto che non se ne faccia commercio e che non venga modificata in alcun modo.

Si prega di inviare suggerimenti e critiche, e di segnalare eventuali errori di stampa all'indirizzo qui sotto.

Dr. Alessandro Zaccagnini
Dipartimento di Matematica
Università degli Studi di Parma
Via Massimo d'Azeglio, 85/A
43100 Parma, ITALIA
Tel. 0521 032302 – Telefax 0521 032350
`e-mail:` `alessandro.zaccagnini@unipr.it`
`pagina web:` `http://www.math.unipr.it/~zaccagni/home.html`

Capitolo 0. Simboli e Notazioni

Scriveremo $f \stackrel{\text{def}}{=} g$ per indicare l'uguaglianza per definizione. Dato un qualunque insieme finito $\mathcal{A}$, indicheremo con $|\mathcal{A}|$ la sua cardinalità. Le lettere d, i, j, k, m, n, q indicano di solito numeri interi (non necessariamente positivi), mentre la lettera p denota sempre un numero primo. Le lettere x, y, t indicano numeri reali.

Per convenzione $\mathbb{N}$ indica l'insieme degli interi non negativi, e quindi $0 \in \mathbb{N}$. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ e $\mathbb{C}$ hanno il significato consueto, mentre $\mathbb{F}_q$ indica il campo finito con q elementi (se q è una potenza di un primo). Indicheremo con $\mathbb{Z}_n$ l'insieme delle classi di resto modulo n, che ricordiamo costituire un anello commutativo con identità, e con $\mathbb{Z}_n^*$ l'insieme delle unità di $\mathbb{Z}_n$, cioè l'insieme dei suoi elementi invertibili.

Scriveremo $d \mid n$ quando d ed n sono interi ed esiste un altro intero q tale che $dq = n$. Osserviamo che con questa convenzione $d \mid 0$ per ogni $d \in \mathbb{Z}$, mentre $0 \mid n$ implica $n = 0$. Scriveremo $d \nmid n$ per negare questa relazione. Scriveremo anche $p^\alpha \parallel n$ (ma solo per numeri primi p) se α è la piú grande potenza di p che divide n, cioè se $p^\alpha \mid n$ ma $p^{\alpha+1} \nmid n$. Quando n, m sono numeri interi non entrambi nulli, indicheremo con (n, m) e con $[n, m]$ rispettivamente il massimo comun divisore ed il minimo comune multiplo di n ed m. Supporremo sempre $(n, m) > 0$ e $[n, m] > 0$, anche se n o m sono numeri negativi.

Scriveremo $\sum_{d|n}$ per indicare una somma estesa a tutti i divisori *positivi* d di n (anche quando n è un numero negativo). Scriveremo $\sum_{a \mod q}$ e $\sum^*_{a \mod q}$ rispettivamente per indicare una somma su tutte le classi di resto modulo q o su tutte le classi $a \mod q$ con $(a, q) = 1$ (quando queste somme sono ben definite). Le somme e i prodotti indicati con $\sum_{n \le x}$ oppure $\prod_{n \le x}$ sono estesi a tutti i numeri naturali nell'intervallo $[1, x]$. Quando la variabile è p è sottinteso che queste somme o prodotti sono estesi solo ai primi che soddisfano le condizioni richieste. Per convenzione, assegneremo il valore 0 alla somma vuota, ed il valore 1 al prodotto vuoto.

Con $[x] \stackrel{\text{def}}{=} \max\{n \in \mathbb{Z} : n \le x\}$ indichiamo la parte intera del numero reale x, e con $\{x\} \stackrel{\text{def}}{=} x - [x] \in [0, 1)$ la sua parte frazionaria. $\Re(z)$, $\Im(z)$ e $\overline{z}$ denotano rispettivamente parte reale, parte immaginaria e coniugato del numero complesso z. Indicheremo con i l'unità immaginaria, con $e(x)$ la funzione esponenziale complessa $e^{2\pi i x}$ (di solito quando x è un numero reale) e con $e_q(x)$ la funzione $e\big(x/q\big)$.

Useremo i simboli di Bachmann-Landau (o, $\mathcal{O}$), di Vinogradov ($\ll$, $\gg$) e di Hardy-Littlewood (Ω) con il seguente significato: siano f, g funzioni definite in un intorno di x_0, ma non necessariamente in x_0 (che può essere ∞). Se g è non negativa in un intorno di x_0 scriviamo $f(x) = \mathcal{O}(g(x))$ (oppure $f(x) \ll g(x)$) se

$$\limsup_{x \to x_0} \frac{|f(x)|}{g(x)} < +\infty,$$

cioè se esiste $C \in \mathbb{R}^+$ tale che per tutti gli x in un opportuno intorno di x_0 si ha

$$|f(x)| \le Cg(x).$$

Se la costante C non è uniforme, ma dipende dai parametri A, B, ... , scriveremo $f(x) = \mathcal{O}_{A,B,\dots}(g(x))$ oppure $f(x) \ll_{A,B,\dots} g(x)$. Scriviamo $f(x) \gg g(x)$ se f è positiva ed inoltre $g(x) \ll f(x)$. Scriviamo $f(x) = o(g(x))$ se

$$\lim_{x\to x_0} \frac{f(x)}{g(x)} = 0$$

ed $f(x) = \Omega\big(g(x)\big)$ se $f(x)$ non è $o(g(x))$, cioè se

$$\limsup_{x\to x_0} \frac{|f(x)|}{g(x)} > 0.$$

Scriveremo $f(x) = \Omega_-\big(g(x)\big)$ oppure $f(x) = \Omega_+\big(g(x)\big)$ per indicare, rispettivamente,

$$\liminf_{x\to x_0} \frac{f(x)}{g(x)} < 0 \qquad \text{e} \qquad \limsup_{x\to x_0} \frac{f(x)}{g(x)} > 0.$$

Con $f(x) = \Omega_\pm\big(g(x)\big)$ indichiamo che le due relazioni precedenti valgono simultaneamente. Scriveremo inoltre $f \sim g$ se

$$\lim_{x\to x_0} \frac{f(x)}{g(x)} = 1,$$

ed $f \asymp g$ per indicare che $g(x) \ll f(x) \ll g(x)$ quando $x \to x_0$.

Quando $c \in \mathbb{R}$, useremo l'abbreviazione

$$\int_{(c)} f(s)\,\mathrm{d}s \qquad \text{per} \qquad \int_{c-\mathrm{i}\infty}^{c+\mathrm{i}\infty} f(s)\,\mathrm{d}s,$$

cioè per l'integrale sulla retta verticale dei numeri complessi di parte reale c.

La definizione e le proprietà elementari di alcune funzioni speciali sono date nel testo: piú precisamente, la funzione ζ di Riemann è definita nel §2.7, la funzioni Γ e B di Eulero nell'Appendice A2.

Ringraziamenti. Desidero ringraziare quanti mi hanno segnalato errori, imprecisioni, miglioramenti e nuovi riferimenti bibliografici. Fra questi, in particolare G. Molteni, G. Rossi e C. Viola.

Nota. Per quanto possibile queste dispense sono autocontenute. Solo qualche risultato è
𝔈 1.2.3 stato citato ed utilizzato senza dimostrazione. Il simbolo nel margine rimanda all'Esercizio 3 del §1.2. I numeri fra parentesi quadrate si riferiscono ai testi citati nella Bibliografia; se preceduti da una A si tratta di articoli, da cercare nell'elenco apposito.

Capitolo 1. Risultati Elementari

§1.1. L'algoritmo di Euclide

Lemma 1.1.1 (Euclide). *Dati n, $m \in \mathbb{Z}$ si ha $\mathcal{A}(n,m) \stackrel{\text{def}}{=} \{an + bm : a, b \in \mathbb{Z}\} = d\mathbb{Z}$, l'insieme dei multipli interi di $d \stackrel{\text{def}}{=} (n,m)$, e dunque esistono λ, $\mu \in \mathbb{Z}$ tali che $d = \lambda n + \mu m$.*

𝔈 1.1.1–3 Dim.: È evidente che d divide ogni elemento di $\mathcal{A}$. Sia $\delta = \lambda n + \mu m$ il minimo elemento positivo di $\mathcal{A}$ (purché almeno uno fra n e m sia non nullo). Poiché $d \mid \delta$, resta da dimostrare che $\delta \mid d$. Consideriamo il resto r della divisione euclidea di n per δ (cioè l'intero r tale che $0 \le r < \delta$ ed inoltre esiste $q \in \mathbb{Z}$ tale che $n = q\delta + r$). È chiaro che $r \in \mathcal{A}$ (poiché $r = (1 - \lambda q)n - \mu q m$) e dunque $r = 0$ (poiché altrimenti esisterebbe un elemento positivo di $\mathcal{A}$ strettamente minore di δ), cioè $\delta \mid n$. Analogamente $\delta \mid m$, e quindi $\delta \mid d$. □

Definizione 1.1.2. *Un intero $n \ge 2$ si dice* primo *se $d \mid n$ implica $|d| = 1$ oppure $|d| = n$.*

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

Dim.: Se $p \nmid a$ allora $(a,p) = 1$ e per il Lemma 1.1.1 esistono interi λ e μ tali che $\lambda p + \mu a = 1$. Moltiplichiamo questa uguaglianza per b ed otteniamo $\lambda pb + \mu ab = b$. Poiché p ne divide il primo membro, deve dividere anche il secondo. □

Definizione 1.1.4. *Dato $n \in \mathbb{N}^*$ chiamiamo* forma canonica di n *la decomposizione*

$$n = \prod_{i=1}^{k} p_i^{\alpha_i}, \qquad \text{dove } p_i < p_j \text{ se } i < j,\ \alpha_i \in \mathbb{N}^* \text{ per } i = 1, \dots, k,$$

ed i p_i sono numeri primi. Se $n = 1$ il prodotto è vuoto.

Teorema 1.1.5 (Fattorizzazione Unica). *Ogni $n \in \mathbb{N}^*$ ha un'unica forma canonica.*

Dim.: Sia $n \ge 2$ il piú piccolo numero naturale con due forme canoniche diverse

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

con le convenzioni della definizione. Per il Corollario 1.1.3, se $p_1 \mid n$ allora p_1 è uno dei primi q_j, ed analogamente q_1 è uno dei primi p_i e dunque $p_1 = q_1$ (poiché entrambi sono uguali al piú piccolo fattore primo di n). Quindi anche il numero $n/p_1 = n/q_1 < n$ ha due forme canoniche distinte, contro la minimalità di n. □

Corollario 1.1.6. *Se $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ con p_i ed α_i come sopra, e $d \mid n$, allora esistono interi β_i con $0 \le \beta_i \le \alpha_i$ tali che $d = \prod_{i=1}^{k} p_i^{\beta_i}$.*

Teorema 1.1.7 (Euclide). *Esistono infiniti numeri primi.*

Dim.: Sia $\{p_1, \dots, p_n\}$ un qualunque insieme finito non vuoto di numeri primi. Il numero $N = p_1 \cdots p_n + 1 > 1$ non è divisibile per alcuno dei primi $p_1, \dots, p_n$. □

Corollario 1.1.8. *Sia p_n l'n-esimo numero primo. Si ha $p_n \le 2^{2^{n-1}}$.*

§1.2. Congruenze: i teoremi di Fermat, Eulero, Wilson e Gauss

Definizione 1.2.1. *Fissato $m \in \mathbb{Z}$, se $m \mid a - b$ diciamo che a* è congruo a b modulo m *e scriviamo $a \equiv b \mod m$. Se $m \in \mathbb{N}^*$ ed $x \in \mathbb{Z}$, si dice minimo residuo positivo di x modulo m l'intero a tale che $a \in \{0, \dots, m-1\}$ ed $x \equiv a \mod m$, e lo si indica con $x \mod m$.*

Osservazione 1.2.2. *La relazione di congruenza è una relazione di equivalenza. Indichiamo con $\mathbb{Z}_m$ l'insieme quoziente. Inoltre, per ogni $c \in \mathbb{Z}$ si ha*

$$a \equiv b \mod m \quad \Longrightarrow \quad a + c \equiv b + c \mod m \quad e \quad ac \equiv bc \mod m,$$
$$ac \equiv bc \mod m \quad \Longrightarrow \quad a \equiv b \mod \frac{m}{(m,c)},$$

l'ultima delle quali segue dal Lemma 1.1.1, poiché questo implica che se $(\alpha, \beta) = 1$ allora esiste $\alpha^{-1} \mod \beta$. Dunque, $\mathbb{Z}_m$ è un anello commutativo con identità, che è un campo se
𝔈 1.2.1 *e solo se m è primo. $\mathbb{Z}_m^*$ è l'insieme degli elementi invertibili di $\mathbb{Z}_m$.*

Corollario 1.2.3. *Dato $a \in \mathbb{Z}_q^*$, l'applicazione $f_a \colon \mathbb{Z}_q^* \to \mathbb{Z}_q^*$ definita da $f_a(x) \stackrel{\text{def}}{=} ax \mod q$ è una biiezione.*

Teorema 1.2.4 (Teorema Cinese del Resto). *Se n_1, $n_2 \in \mathbb{Z}^*$ ed $(n_1, n_2) = 1$, il sistema seguente ha un'unica soluzione $\mod n_1 n_2$:*

$$\begin{cases} x \equiv a_1 \mod n_1, \\ x \equiv a_2 \mod n_2. \end{cases}$$

Dim.: Sia $\mathcal{A} \stackrel{\text{def}}{=} \{a_1 + bn_1 \colon b = 0, \dots, n_2 - 1\}$. È evidente che tutti gli elementi di $\mathcal{A}$ soddisfano la prima congruenza, e vogliamo dimostrare che sono tutti distinti modulo n_2. Supponiamo per assurdo che $a_1 + b_1 n_1 \equiv a_1 + b_2 n_1 \mod n_2$, per due valori distinti b_1, $b_2 \in \{0, \dots, n_2 - 1\}$. Per l'Osservazione 1.2.2 abbiamo $b_1 n_1 \equiv b_2 n_1 \mod n_2$, da cui $b_1 \equiv b_2 \mod n_2$, poiché $(n_1, n_2) = 1$. Ma questo è assurdo, perché $0 < |b_1 - b_2| < n_2$. □

Teorema 1.2.5 (Fermat). *Se p è un numero primo, allora qualunque sia $a \in \mathbb{Z}$ si ha*

$$a^p \equiv a \mod p.$$

DIM.: Se $p \mid a$ la tesi è evidente. Se $p \nmid a$ è sufficiente dimostrare che $a^{p-1} \equiv 1 \mod p$. Per il Corollario 1.2.3 l'insieme $\mathcal{A} \stackrel{\text{def}}{=} \{na \mod p : n = 1, \dots, p-1\}$ ha tutti gli elementi distinti e quindi, per il principio dei cassetti, $\mathcal{A} = \{1, \dots, p-1\}$. Dunque

$$(p-1)! \equiv (p-1)!\, a^{p-1} \mod p,$$

e la tesi segue immediatamente osservando che $\big(p, (p-1)!\big) = 1$. □

𝔈 1.2.2–3 Il Teorema di Fermat dà una condizione necessaria ma non sufficiente per la primalità: per esempio $2^{340} \equiv 1 \mod 341$ come si può vedere facilmente dato che $2^{10} = 1024 \equiv 1 \mod 341$, ma $341 = 11 \cdot 31$ (si osservi che $2^5 \equiv -1 \mod 11$ e $2^5 \equiv 1 \mod 31$), oppure $3^{90} \equiv 1 \mod 91$ poiché $3^6 \equiv 1 \mod 7$ e $3^3 \equiv 1 \mod 13$, ma $91 = 7 \cdot 13$. Ancor piú semplicemente, $4^{14} \equiv 1 \mod 15$, poiché $4^{14} = 16^7 \equiv 1^7 \mod 15$. In effetti vale il seguente

TEOREMA 1.2.6 (CIPOLLA). *Fissato un intero $a \geq 2$, esistono infiniti numeri composti m tali che $a^{m-1} \equiv 1 \mod m$, detti* pseudoprimi *in base a.*

DIM.: Sia p un numero primo tale che $p \nmid a\big(a^2-1\big)$. Osserviamo che p è necessariamente dispari e consideriamo il numero intero

$$m \stackrel{\text{def}}{=} \frac{a^{2p}-1}{a^2-1} = \frac{a^p-1}{a-1}\frac{a^p+1}{a+1} = \big(a^{p-1}+a^{p-2}\cdots+a+1\big)\big(a^{p-1}-a^{p-2}+\cdots-a+1\big). \quad (1.2.1)$$

Per ipotesi a^2-1 è invertibile modulo p, e quindi per il Teorema di Fermat $m \equiv 1 \mod p$. Inoltre, ciascuno dei due fattori a destra nella (1.2.1) è dispari, poiché contiene un numero dispari di addendi ed $a^{2j} + a^{2j-1} = a^{2j-1}(a+1)$ è pari. Quindi $m \equiv 1 \mod 2p$ ed $a^{2p} = 1 + m(a^2-1) \equiv 1 \mod m$. Infine $m - 1 = 2pr$ per qualche intero r da cui $a^{m-1} \equiv \big(a^{2p}\big)^r \equiv 1 \mod m$. Il Teorema è dimostrato poiché possiamo scegliere p ad arbitrio, purché $p \nmid a(a^2-1)$. □

Vi sono interi n che non sono primi ma per i quali $a^{n-1} \equiv 1 \mod n$ per ogni $a \in \mathbb{Z}$ tale che $(a, n) = 1$. Questi sono detti *numeri di Carmichael* ed è stato dimostrato recentemente
𝔈 1.2.4–5 che sono infiniti. I piú piccoli sono 561, 1105 e 1729.

TEOREMA 1.2.7 (WILSON). *Se p è un numero primo allora si ha*

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

𝔈 1.2.6 DIM.: Ricordiamo che $\mathbb{Z}_p$ è un campo. Quindi, l'equazione $x^2 = 1$ ha al piú 2 soluzioni (che naturalmente sono ± 1) e cioè se $x \in \mathbb{Z}_p \setminus \{0, 1, -1\}$ allora $x \not\equiv x^{-1} \mod p$. Nel prodotto $(p-1)! \mod p$ possiamo associare ciascun fattore $\neq \pm 1$ al suo reciproco ottenendo

$$(p-1)! \equiv 1 \cdot (-1) \cdot 1^{(p-3)/2} \equiv -1 \mod p.$$

Alternativamente, per il Teorema di Fermat 1.2.5, il polinomio $x^{p-1} - 1$ ha come radici $x = 1, \dots, p-1$ (tutti gli elementi non nulli di $\mathbb{Z}_p$) e quindi si ha la fattorizzazione

$$x^{p-1} - 1 = \prod_{n=1}^{p-1} (x - n). \quad (1.2.2)$$

𝔈 1.2.7 Il Teorema di Wilson segue ponendo $x = 0$ in questa identità. □

𝔈 1.2.8 Osserviamo che se $n \geq 6$ non è primo allora $(n-2)! \equiv 0 \mod n$ e quindi il Teorema di Wilson dà una condizione necessaria e sufficiente affinché n sia primo, che non può essere usata come criterio di primalità efficiente poiché richiede essenzialmente n moltiplicazioni.

Osservazione 1.2.8. *I Teoremi di Fermat e Wilson permettono di dare un'espressione esplicita per* $a^{-1} \mod p$ *se* $p \nmid a$*: infatti* $a^{-1} \equiv a^{p-2} \equiv \big((p-2)!/a\big) \mod p$.

Osservazione 1.2.9. *Per* $p \geq 3$ *poniamo* $x \stackrel{\text{def}}{=} 1 \cdot 2 \cdots \frac{1}{2}(p-1)$, $y = \frac{1}{2}(p+1) \cdots (p-1)$ *in modo tale che* $xy = (p-1)!$. *Poiché per ogni fattore* n *in* x *c'è il fattore* $p - n \equiv -n \mod p$ *in* y, *si ha* $x \equiv y(-1)^{(p-1)/2} \mod p$, *e quindi* $x^2 \equiv -1 \mod p$ *se* $p \equiv 1 \mod 4$ *ed* $x^2 \equiv 1 \mod p$ *se* $p \equiv 3 \mod 4$.

Teorema 1.2.10 (Eulero). *Se* n, $a \in \mathbb{Z}$ *ed* $(n, a) = 1$, *allora*

$$a^{\varphi(n)} \equiv 1 \mod n, \qquad \text{dove} \qquad \varphi(n) \stackrel{\text{def}}{=} \big|\mathbb{Z}_n^*\big|.$$

Dim.: È una conseguenza immediata del Corollario 1.2.3. □

Osservazione 1.2.11. *Nella seguente uguaglianza gli insiemi a destra sono mutuamente disgiunti: le frazioni a destra si ottengono da quelle a sinistra riducendole ai minimi termini.*

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

Lemma 1.2.12. *Per ogni* $n \geq 1$ *si ha* $\sum_{d \mid n} \varphi(d) = n$.

Dim.: La cardinalità dell'insieme a sinistra nell'Osservazione 1.2.11 è n, e quella di ciascuno degli insiemi a destra è $\varphi(d)$, per definizione. □

Definizione 1.2.13. *Diciamo che l'*ordine *di* $g \in \mathbb{Z}_n^*$ *è* r *se* r *è il minimo intero positivo tale che* $g^r \equiv 1 \mod n$. *Diciamo che* g *è una* radice primitiva modulo n *se il suo ordine è* $\varphi(n)$, *cioè se* g *genera* $\mathbb{Z}_n^*$.

𝔈 1.2.9

Lemma 1.2.14. *Se* r *è l'ordine di* $a \in \mathbb{Z}_n^*$, *allora* $a^m \equiv 1 \mod n$ *se e solo se* $r \mid m$.

Dim.: Sia $d \stackrel{\text{def}}{=} (r, m)$; per il Lemma 1.1.1 esistono λ, $\mu \in \mathbb{Z}$ tali che $d = \lambda r + \mu m$, e quindi $a^d \equiv a^{\lambda r + \mu m} \equiv 1 \mod n$ e per la minimalità di r questo è possibile solo se $d = r$. □

Teorema 1.2.15 (Gauss). *Per ogni primo* p, $\mathbb{Z}_p^*$ *è un gruppo ciclico di ordine* $p - 1$.

Dim.: Sia $h_d(x) \stackrel{\text{def}}{=} x^d - 1$: osserviamo che $h_d \mid h_{p-1}$ in $\mathbb{Z}[x]$ quando $d \mid p-1$. Inoltre, per la fattorizzazione (1.2.2) valida in $\mathbb{Z}_p$, h_d ha esattamente d soluzioni (evidentemente tutte distinte) in $\mathbb{Z}_p$: infatti, poiché $\mathbb{Z}_p$ è un campo, h_d ha al piú d soluzioni, e h_{p-1}/h_d al piú $p - 1 - d$, ma il loro prodotto h_{p-1} ne ha esattamente $p - 1$, e quindi i due polinomi h_d ed h_{p-1}/h_d devono avere d e $p - 1 - d$ radici rispettivamente.

𝔈 1.2.6

Sia $n_p(d)$ il numero delle soluzioni dell'equazione $h_d(x) \equiv 0 \mod p$ che hanno ordine d. Dimostreremo che $n_p(d) = \varphi(d)$ per $d \mid p-1$. Per $d = 1$ questo è ovvio e supponiamo aver dimostrato la tesi per ogni $\delta \mid d$ con $\delta < d$. Per il Lemma 1.2.14 ogni soluzione di $h_d(x) \equiv 0 \mod p$ ha ordine $\delta \mid d$ e quindi per il Lemma 1.2.12

$$d = \sum_{\delta \mid d} n_p(\delta) = \sum_{\delta \mid d,\, \delta < d} \varphi(\delta) + n_p(d) = \big(d - \varphi(d)\big) + n_p(d),$$

da cui la tesi segue immediatamente. In particolare, $n_p(p-1) = \varphi(p-1) \geq 1$, e dunque il gruppo $\mathbb{Z}_p^*$ risulta essere ciclico, e con $\varphi(p-1)$ generatori. □

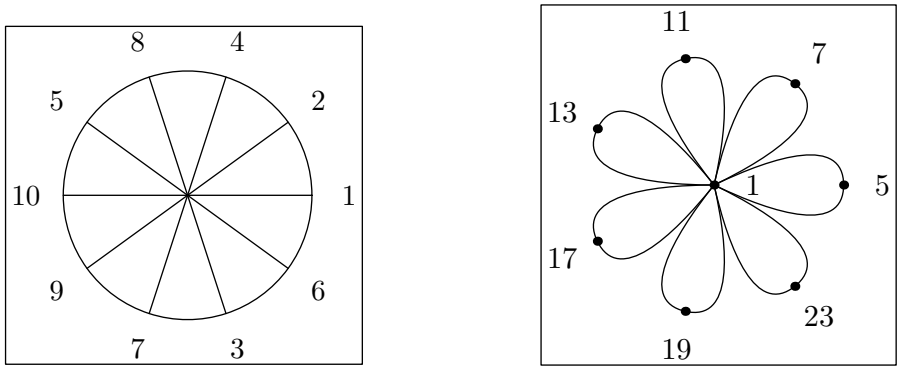


Figura 1.1. *Struttura di* $(\mathbb{Z}/11\mathbb{Z})^*$ *e di* $(\mathbb{Z}/24\mathbb{Z})^*$*. Gli archi connettono le potenze successive dello stesso elemento: nel caso a sinistra le potenze di* 2 *(che è un generatore di* $\mathbb{Z}_{11}^*$*), nel caso a destra, poiché ogni elemento di* $\mathbb{Z}_{24}^*$ *soddisfa* $x^2 \equiv 1 \mod 24$*, le potenze successive di* $x \neq 1$ *sono* $1, x, 1, x, \ldots$

Equazione	Soluzioni	di cui primitive
$x \equiv 1 \mod 11$	$x = 1$	1
$x^2 \equiv 1 \mod 11$	$x = 1, 10$	10
$x^5 \equiv 1 \mod 11$	$x = 1, 3, 4, 5, 9$	3, 4, 5, 9
$x^{10} \equiv 1 \mod 11$	$x = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10$	2, 6, 7, 8

Tavola 1.2. *Dimostrazione del Teorema di Gauss per* $p = 11$*.*

TEOREMA 1.2.16. *Se* p *è un primo dispari allora* $\mathbb{Z}_{p^\alpha}^*$ *è ciclico per ogni* $\alpha \geq 1$*, mentre* $\mathbb{Z}_{2^{\alpha+2}}^* \simeq \mathbb{Z}_2 \times \mathbb{Z}_{2^\alpha}$ *per ogni* $\alpha \geq 0$*.*

DIM.: Il Teorema 1.2.15 garantisce l'esistenza di una radice primitiva $g_1 \mod p$. Inoltre un semplice calcolo mostra che $g_1^{p-1} \not\equiv (g_1 + p)^{p-1} \mod p^2$ e quindi esiste $g_2 \in \mathbb{Z}_{p^2}^*$ tale che $g_2^{p-1} \not\equiv 1 \mod p^2$. Sia r l'ordine di $g_2 \mod p^2$: per il Lemma 1.2.14 si ha $r \mid \varphi(p^2) = p(p-1)$ e poiché $g_1 \equiv g_2 \mod p$ e g_1 ha ordine $p-1 \mod p$, $p-1 \mid r$. Ma $r \neq p-1$ e quindi $r = p(p-1)$, cioè g_2 è una radice primitiva $\mod p^2$. Dunque $g_2^{p-1} = 1 + k_1 p$ con $p \nmid k_1$ e, per induzione, $g_2^{(p-1)p^{\alpha-1}} = 1 + k_\alpha p^\alpha$ dove $p \nmid k_\alpha$. Lo stesso ragionamento di sopra mostra che g_2 è una radice primitiva $\mod p^\alpha$, poiché, per induzione $g_2^{(p-1)p^{\alpha-2}} \not\equiv 1 \mod p^\alpha$ e quindi l'ordine di $g_2 \mod p^\alpha$ è $(p-1)p^{\alpha-1}$. □

§1.3. TERNE PITAGORICHE

DEFINIZIONE 1.3.1. *Chiamiamo* terna pitagorica *ogni terna di interi* $(a, b, c) \in \mathbb{Z}^3$ *tali che* $a^2 + b^2 = c^2$*. Inoltre diremo che la terna pitagorica è* primitiva *se* $(a, b) = (a, c) = (b, c) = 1$*.*

TEOREMA 1.3.2 (DIOFANTO). *Se* (a, b, c) *è una terna pitagorica primitiva, allora esistono* $n, m \in \mathbb{Z}$ *tali che* $(n, m) = 1$*,* $n \not\equiv m \mod 2$ *ed inoltre*

$$\begin{cases} a = 2mn, \\ b = m^2 - n^2, \\ c = m^2 + n^2. \end{cases} \tag{1.3.1}$$

Viceversa, dati n, $m \in \mathbb{Z}$ tali che $(n,m)=1$, $n \not\equiv m \mod 2$, gli interi (a,b,c) definiti dalla (1.3.1) *formano una terna pitagorica primitiva.*

Dim.: Daremo due dimostrazioni diverse di questo Teorema. La prima è sostanzialmente quella di originale di Diofanto di Alessandria (III sec. d. C.). Osserviamo che c è necessariamente dispari: infatti, se a e b fossero entrambi dispari, diciamo $a=2n+1$, $b=2m+1$, allora $a^2+b^2=4(n^2+n+m^2+m)+2=c^2$, e quindi $c^2 \equiv 2 \mod 4$, che è impossibile. Dunque possiamo supporre che a sia pari e b dispari e scriviamo $a=2a_0$, con $a_0 \in \mathbb{Z}$.

Poniamo $\alpha \stackrel{\text{def}}{=} \frac{1}{2}(c+b)$, $\beta \stackrel{\text{def}}{=} \frac{1}{2}(c-b)$, osservando che α, $\beta \in \mathbb{Z}$ poiché $b \equiv c \equiv 1 \mod 2$. Quindi $a_0^2 = \alpha\beta$. Inoltre, se $d \stackrel{\text{def}}{=} (\alpha,\beta)$, allora $d \mid \alpha \pm \beta$ e quindi $d \mid \alpha+\beta=c$ ed anche $d \mid \alpha-\beta=b$ da cui $d=1$. Ma questo implica che α e β siano quadrati perfetti, cioè esistono n, $m \in \mathbb{Z}$ tali che

$$\alpha = m^2 \qquad \text{e} \qquad \beta = n^2.$$

Da queste ricaviamo immediatamente $b=m^2-n^2$, $c=m^2+n^2$, $a=2mn$. Questo dimostra che qualunque sia la terna pitagorica primitiva (a,b,c) esistono due interi n, m tali che $(n,m)=1$, $n \not\equiv m \mod 2$ ed inoltre vale la (1.3.1). Lo svantaggio di questa costruzione è che dipende dalla particolare forma della relazione fra i numeri a, b e c.

La seconda dimostrazione che diamo si adatta bene ad un gran numero di casi simili. Cambiamo prospettiva: poniamo $x \stackrel{\text{def}}{=} \frac{a}{c}$, $y \stackrel{\text{def}}{=} \frac{b}{c}$ (dove supponiamo tacitamente che $c \neq 0$, ma è chiaro che se $c=0$ allora si ha anche $a=b=0$) e risolviamo l'equazione $x^2+y^2=1$ in numeri razionali x, y, cioè cerchiamo i punti a coordinate razionali sulla circonferenza unitaria $\gamma \stackrel{\text{def}}{=} \{(x,y) \in \mathbb{R}^2 : x^2+y^2=1\}$. Fissiamo $t \in \mathbb{Q}$ e tracciamo la retta $r(t)$ passante per il punto $P=(-1,0)$ (che appartiene a γ) e per il punto $Q(t)=(0,t)$ (vedi Figura 1.3). Questa retta interseca γ in P ed in un altro punto $R(t)$, le cui coordinate soddisfano

$$\begin{cases} x^2+y^2=1, \\ y=t(x+1). \end{cases}$$

Questo sistema si risolve facilmente, tenendo presente il fatto che ne conosciamo già una soluzione (e cioè $P=(-1,0)$). Le coordinate del punto $R(t)$ sono

$$R(t) = \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2} \right) \tag{1.3.2}$$

Facendo riferimento alla Figura 1.3, se chiamiamo α l'angolo $\widehat{AOR}$ dove $A=(1,0)$, per un noto teorema di geometria elementare l'angolo $\widehat{APR}$ vale $\frac{1}{2}\alpha$ ed inoltre, per definizione, $t = \operatorname{tg}\left(\frac{1}{2}\alpha\right)$, $x = \cos\alpha$, $y = \sin\alpha$. Dunque le (1.3.2) sono le "formule razionali" per esprimere le funzioni trigonometriche in termini della tangente dell'angolo metà, di cui abbiamo dato una dimostrazione alternativa a quella classica. Notiamo per inciso che le (1.3.2) rappresentano le equazioni parametriche di $\gamma \setminus \{P\}$. Si osservi infine che, ponendo $t=\frac{n}{m}$ nella (1.3.2), si riottengono le formule (1.3.1). Inoltre, questo procedimento può essere invertito: se $Q \neq P$ è un qualsiasi punto di γ, tracciando la retta per P e Q, si trova che questa interseca l'asse delle ordinate in un punto che ha ordinata razionale. Infatti, se $Q=(x_0,y_0)$, la retta per P e Q taglia l'asse delle y nel punto di coordinate $\left(0, \frac{y_0}{x_0+1}\right)$. □

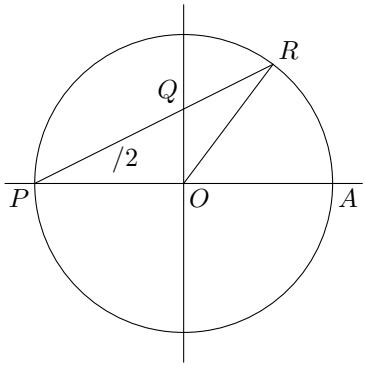


Figura 1.3. *Come parametrizzare i punti della circonferenza unitaria.*

Piú in generale, consideriamo una conica di equazione $ax^2 + bxy + cy^2 + dx + ey + f = 0$ con i coefficienti interi e supponiamo che la conica sia irriducibile sui numeri reali, cioè che il polinomio a primo membro non si spezzi nel prodotto di due polinomi di primo grado a coefficienti reali. Inoltre, supponiamo di avere un punto $P = (x_0, y_0)$ a coordinate razionali che giace su questa conica. Scelta arbitrariamente una retta del piano che non passa per P, con equazione a coefficienti razionali, possiamo scegliere su questa retta un punto $Q = (x_1, y_1)$ con entrambe le coordinate razionali, e considerare la retta passante per P e Q e l'ulteriore punto di intersezione R con la conica. In questo modo otteniamo un'infinità di punti a coordinate entrambe razionali che giacciono sulla conica data, a partire da uno solo: il motivo è che dobbiamo risolvere equazioni di secondo grado a coefficienti razionali, di cui conosciamo già una soluzione razionale. Le operazioni necessarie a determinare la seconda soluzione sono tutte razionali, come abbiamo visto sopra in un caso particolare, e quindi necessariamente anche la seconda soluzione è razionale.

§1.4. Somme di due e tre quadrati

Lemma 1.4.1 (Hurwitz). *Dati $\xi \in \mathbb{R} \setminus \mathbb{Q}$ ed $N \in \mathbb{N}^*$, esistono $m \in \mathbb{Z}$, $q \in \mathbb{Z}^*$ tali che*

$$|q| \le N \qquad e \qquad \left|\xi - \frac{m}{q}\right| < \frac{1}{|q|(N+1)}.$$

Dim.: Consideriamo gli $N+1$ numeri $\{n\xi\}$, dove $n = 0, \dots, N$. Osserviamo che nessuno di questi numeri è 1, e sono tutti distinti, poiché $\xi \notin \mathbb{Q}$. Deve esistere un qualche intervallo del tipo $\left[\frac{x}{N+1}, \frac{x+1}{N+1}\right]$ nel quale cadono due di questi numeri, dato che $(N+1)^{-1}$ è la loro distanza media. Diciamo che $\{a\xi\}$ e $\{b\xi\}$ hanno questa proprietà, cioè

$$0 < \{b\xi\} - \{a\xi\} < \frac{1}{N+1}.$$

Abbiamo dunque le equazioni

$$\begin{gathered} \{b\xi\} = b\xi - [b\xi] \\ \{a\xi\} = a\xi - [a\xi] \\ \hline \{b\xi\} - \{a\xi\} = (b-a)\xi - [b\xi] + [a\xi] \end{gathered}$$

Il risultato cercato segue ponendo $m \stackrel{\text{def}}{=} [b\xi] - [a\xi]$ e $q \stackrel{\text{def}}{=} b - a$. □

LEMMA 1.4.2. *Siano $\xi \in \mathbb{Q}$ ed $N \in \mathbb{N}^*$ tali che $\xi = \frac{a}{b}$ con a, $b \in \mathbb{Z}$, $(a,b) = 1$, ed $N < b$. Esistono $m \in \mathbb{Z}$, $q \in \mathbb{N}^*$ tali che $(m,q) = 1$, $q \le N$ e*

$$\left| \xi - \frac{m}{q} \right| \le \frac{1}{q(N+1)}.$$

DIM.: La dimostrazione è analoga a quella del Lemma di Hurwitz 1.4.1. □

TEOREMA 1.4.3. *Siano n, $a \in \mathbb{N}$ tali che $n \mid a^2 + 1$. Allora esistono s, $t \in \mathbb{N}$ tali che $n = s^2 + t^2$ e $(s,t) = 1$.*

DIM.: Possiamo evidentemente supporre $n \ge 2$. Sia $N \stackrel{\text{def}}{=} \left[\sqrt{n}\right] \le \sqrt{n} < n$. Poiché $(n,a) = 1$, per il Lemma precedente esistono m, $q \in \mathbb{N}$ con $q \le N$ ed $(m,q) = 1$, tali che

$$\left| \frac{a}{n} - \frac{m}{q} \right| \le \frac{1}{q(N+1)}, \qquad \text{da cui} \qquad |aq - mn| \le \frac{n}{N+1} < \sqrt{n}.$$

Vogliamo verificare che $n = (aq - mn)^2 + q^2$. Per cominciare $n \mid (aq - mn)^2 + q^2$, poiché quest'ultima espressione può essere scritta nella forma $q^2(a^2+1) + n(nm^2 - 2amq)$. Inoltre $1 \le q \le N$ e $|aq - mn| < \sqrt{n}$. Quindi $1 \le (aq - mn)^2 + q^2 < n + N^2 < 2n$. Questo basta per dimostrare quanto voluto.

Osserviamo che $(aq - mn, q) = (q, mn) = (q, n)$. Poiché $n = q^2(a^2+1) + n(nm^2 - 2amq)$, si ha $1 = q^2 \frac{a^2+1}{n} + (nm^2 - 2amq)$ e quindi $1 = q\left(q\frac{a^2+1}{n} - 2am\right) + nm^2$. Dal Lemma 1.1.1 segue immediatamente $(q,n) = 1$. □

COROLLARIO 1.4.4. *Siano n, a, $b \in \mathbb{N}$ tali che $n \mid a^2 + b^2$ e $(a,b) = 1$. Allora esistono s, $t \in \mathbb{N}$ tali che $n = s^2 + t^2$ e $(s,t) = 1$.*

DIM.: Osserviamo che, grazie alla relazione

$$(a^2 + b^2)(c^2 + d^2) = (ac \pm bd)^2 + (ad \mp bc)^2, \tag{1.4.1}$$

basta scegliere c e d in modo che $ac - bd = 1$. Dunque $n \mid (a^2 + b^2)(c^2 + d^2) = 1 + e^2$, dove $e = ad + bc$. Ora la tesi segue dal Teorema 1.4.3. □

LEMMA 1.4.5. *Se p è un numero primo $p \equiv 1 \mod 4$, allora esistono m, $x \in \mathbb{N}$ tali che $0 < m < p$ e $x^2 + 1 = mp$.*

DIM.: L'equazione $x^2 \equiv -1 \mod p$ ha soluzione, poiché $\mathbb{Z}_p^*$ è un gruppo ciclico con $p - 1$ elementi per il Teorema 1.2.15. Per esempio, per il Teorema di Fermat 1.2.5, possiamo scegliere $x \equiv g^{(p-1)/4} \mod p$, dove g è un generatore di $\mathbb{Z}_p^*$, e piú precisamente, per l'Osservazione 1.2.9, possiamo prendere $x \equiv \left(\frac{1}{2}(p-1)\right)! \mod p$. Poiché i quadrati degli interi 1, 2, ... , $\frac{1}{2}(p-1)$ sono tutti distinti modulo p, deve esistere un tale x che soddisfa $1 \le x \le \frac{1}{2}(p-1) < \frac{1}{2}p$, e quindi $x^2 + 1 < \frac{1}{4}p^2 + 1 < p^2$, e la tesi segue. □

Osservazione 1.4.6 (Fermat). *Per il Corollario* 1.4.4 *ed il Lemma* 1.4.5, *se p è un numero primo $\equiv 1 \mod 4$ allora esistono a, $b \in \mathbb{Z}$ tali che $p = a^2 + b^2$.*

Lemma 1.4.7. *Se p è primo esistono m, x, $y \in \mathbb{N}$ tali che $0 < m < p$ e $x^2 + y^2 + 1 = mp$.*

Dim.: Se $p = 2$ la tesi è ovvia. Altrimenti consideriamo gli insiemi

$$\mathcal{A} \stackrel{\text{def}}{=} \left\{ x^2 \mod p : 0 \le x \le \frac{1}{2}(p-1) \right\} \quad \text{e} \quad \mathcal{B} \stackrel{\text{def}}{=} \left\{ -1 - y^2 \mod p : 0 \le y \le \frac{1}{2}(p-1) \right\}.$$

Per quanto detto sopra, x distinti danno elementi distinti di $\mathcal{A}$, e y distinti danno elementi distinti di $\mathcal{B}$. In altre parole $|\mathcal{A}| = |\mathcal{B}| = \frac{1}{2}(p+1)$. Questo implica che esiste $t \in \mathcal{A} \cap \mathcal{B}$, cioè esistono x ed y tali che $x^2 \equiv -1 - y^2 \mod p$. Per le scelte fatte sopra si ha $x^2 + y^2 + 1 < p^2$, e la tesi segue anche in questo caso. □

Quindi per il Lemma 1.4.5, se $p \equiv 1 \mod 4$ possiamo scegliere $y = 0$ nel Lemma 1.4.7.

Definizione 1.4.8. *Se $n = x^2 + y^2$ con x, $y \in \mathbb{N}$, $(x, y) = 1$, la coppia (x, y) si dice* rappresentazione primitiva *di n.*

𝔈 1.4.1 Lemma 1.4.9. *Se esiste $p \mid n$ con $p \equiv -1 \mod 4$, n non ha rappresentazioni primitive.*

Dim.: Supponiamo che $n = a^2 + b^2$. Se $a \not\equiv 0 \mod p$, poniamo $x \stackrel{\text{def}}{=} -ba^{-1}$, dove a^{-1} è l'inverso di a in $\mathbb{Z}_p$. Evidentemente $x^2 \equiv -1 \mod p$ e per il Teorema di Fermat 1.2.5 abbiamo anche $x^{p-1} \equiv 1 \mod p$. Poiché $p - 1 = 4m + 2$ per qualche $m \in \mathbb{N}$ si ha

$$1 \equiv x^{p-1} = x^{4m+2} \equiv \left(x^2\right)^{2m+1} \equiv -1 \mod p,$$

che è assurdo. Quindi $p \mid a$ da cui segue $p \mid b$. In altre parole, se $n = a^2 + b^2$ ed esiste $p \equiv -1 \mod 4$ tale che $p \mid n$, esistono anche α, $\beta \in \mathbb{Z}$ tali che $n = p^2\left(\alpha^2 + \beta^2\right)$. □

Teorema 1.4.10. *L'equazione $n = x_1^2 + x_2^2$ è risolubile in interi x_1, x_2 se e soltanto se il numero naturale n è divisibile per potenze pari di primi $p \equiv 3 \mod 4$. Inoltre esiste una rappresentazione primitiva di n se e solo se $n \equiv 1, 2 \mod 4$ e tutti i fattori primi dispari di n sono $\equiv 1 \mod 4$.*

Dim.: Grazie alla relazione (1.4.1) è sufficiente dimostrare che sono risolubili le equazioni $2 = x_1^2 + x_2^2$, $p = x_1^2 + x_2^2$ per ogni $p \equiv 1 \mod 4$, e dimostrare che se $p \equiv 3 \mod 4$ e $p \mid a^2 + b^2$ allora esiste un numero pari $\alpha \ge 2$ tale che $p^\alpha \parallel a$, $p^\alpha \parallel b$. La prima affermazione è banale, mentre la terza segue utilizzando iterativamente il Lemma 1.4.9. La seconda segue dall'Osservazione 1.4.6. □

Teorema 1.4.11 (Gauss). *L'equazione $n = x_1^2 + x_2^2 + x_3^2$ è risolubile in interi x_1, x_2, x_3 se e soltanto se il numero naturale n non è della forma $4^m(8k + 7)$ per m, $k \in \mathbb{N}$.*

Dim.: Osserviamo che $x^2 \equiv 0$, 1, o 4 modulo 8, e quindi $x_1^2 + x_2^2 + x_3^2 \not\equiv 7 \mod 8$. Questo dimostra il caso $m = 0$. Se n è un numero naturale della forma $4^m(8k + 7)$ con $m > 0$, e si avesse $n = x_1^2 + x_2^2 + x_3^2$, dovremmo avere che i numeri x_1, x_2 ed x_3 sono tutti pari, o ce ne sono esattamente due dispari. Ma in quest'ultimo caso avremmo $x_1^2 + x_2^2 + x_3^2 \equiv 0 + 1 + 1 \mod 8$ oppure $x_1^2 + x_2^2 + x_3^2 \equiv 4 + 1 + 1 \mod 8$, il che è assurdo. Quindi i tre numeri x_1, x_2 ed x_3 sono tutti pari. Poniamo $y_i \stackrel{\text{def}}{=} \frac{1}{2}x_i$ per $i = 1, 2, 3$. Avremmo $\frac{1}{4}n = y_1^2 + y_2^2 + y_3^2$ con $\frac{1}{4}n = 4^{m-1}(8k + 7)$, il che è impossibile per ipotesi induttiva. □

§1.5. Il teorema dei quattro quadrati

Teorema 1.5.1 (Lagrange). *L'equazione $n = x_1^2 + x_2^2 + x_3^2 + x_4^2$ è risolubile in interi x_1, x_2, x_3, x_4 qualunque sia il numero naturale n.*

Dim.: Osserviamo che vale la formula

$$\begin{aligned}(a^2+b^2+c^2+d^2)(\alpha^2+\beta^2+\gamma^2+\delta^2)&\\ =(a\alpha+b\beta+c\gamma+d\delta)^2+(a\beta-b\alpha+c\delta-d\gamma)^2+&\\ (a\gamma-b\delta-c\alpha+d\beta)^2+(a\delta+b\gamma-c\beta-d\alpha)^2&\end{aligned} \tag{1.5.1}$$

(dovuta a Fermat). Questa formula esprime la relazione $N(\xi)N(\eta) = N(\xi\eta)$ dove $\xi = a + bi + cj + dk$ ed $\eta = \alpha + \beta i + \gamma j + \delta k$ sono due quaternioni a coefficienti reali, ed N è la norma, cioè $N(\xi) = (a^2+b^2+c^2+d^2)^{1/2}$.

Per la (1.5.1) è sufficiente dimostrare che ogni numero primo è somma di quattro quadrati. Poiché $2 = 1^2 + 1^2 + 0^2 + 0^2$, possiamo supporre che il primo p in questione sia dispari. Per il Lemma 1.4.7 esistono x, $y \in \mathbb{N}$ tali che $1 + x^2 + y^2 = mp$, per qualche m intero, $m \in (0, p)$. Poniamo $m_0 \stackrel{\text{def}}{=} \min\{m \in \mathbb{N}^* : mp = x^2 + y^2 + z^2 + t^2$ per opportuni x, y, z, $t \in \mathbb{Z}\}$. La nostra tesi equivale a $m_0 = 1$, ed abbiamo già osservato che $m_0 < p$. Se m_0 fosse pari, a meno di riordinamenti avremmo $x \equiv y \mod 2$ e $z \equiv t \mod 2$, da cui

$$\frac{1}{2}m_0 p = \left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2 + \left(\frac{z+t}{2}\right)^2 + \left(\frac{z-t}{2}\right)^2,$$

contrariamente all'ipotesi di minimalità di m_0. Ora supponiamo per assurdo che $m_0 \geq 3$, e scriviamo $x = x_1 m_0 + x_2$, dove $|x_2| < \frac{1}{2}m_0$, ed analogamente per y, z e t. Quindi abbiamo

$$m_0 p = \big(x_1^2+y_1^2+z_1^2+t_1^2\big)m_0^2 + 2m_0\big(x_1x_2+y_1y_2+z_1z_2+t_1t_2\big) + \big(x_2^2+y_2^2+z_2^2+t_2^2\big). \tag{1.5.2}$$

Ma $0 < x_2^2 + y_2^2 + z_2^2 + t_2^2 < m_0^2$ ed $m_0 \mid x_2^2 + y_2^2 + z_2^2 + t_2^2$ per la (1.5.2), e quindi esiste un intero $m_1 \in [1, m_0)$ tale che

$$x_2^2 + y_2^2 + z_2^2 + t_2^2 = m_1 m_0.$$

Moltiplichiamo quest'ultima uguaglianza membro a membro per $x^2 + y^2 + z^2 + t^2 = m_0 p$, ed usiamo l'identità (1.5.1), ottenendo, per opportuni interi α, β, γ e δ,

$$\alpha^2 + \beta^2 + \gamma^2 + \delta^2 = m_0^2 m_1 p.$$

Vogliamo dimostrare che $\alpha \equiv \beta \equiv \gamma \equiv \delta \equiv 0 \mod m_0$. Infatti, sempre dalla (1.5.1), abbiamo $\alpha = xx_2 + yy_2 + zz_2 + tt_2 \equiv x_2^2 + y_2^2 + z_2^2 + t_2^2 \equiv 0 \mod m_0$, ed analogamente per β, γ e δ. Dunque

$$\left(\frac{\alpha}{m_0}\right)^2 + \left(\frac{\beta}{m_0}\right)^2 + \left(\frac{\gamma}{m_0}\right)^2 + \left(\frac{\delta}{m_0}\right)^2 = m_1 p,$$

in contrasto con la minimalità di m_0. In definitiva $m_0 = 1$, come si voleva. □

§1.6. La legge di reciprocità quadratica

Definizione 1.6.1: Simbolo di Legendre. *Sia p un numero primo, ed a un intero qualsiasi. Poniamo*

$$\left(\frac{a}{p}\right) \stackrel{\text{def}}{=} \begin{cases} 1 & \text{se } p \nmid a \text{ e l'equazione } x^2 \equiv a \mod p \text{ è risolubile.} \\ 0 & \text{se } p \mid a. \\ -1 & \text{se } p \nmid a \text{ e l'equazione } x^2 \equiv a \mod p \text{ non è risolubile.} \end{cases}$$

Per comodità tipografica, nel testo scriviamo il simbolo di Legendre nella forma $\big(a \mid p\big)$. Diremo che a è un residuo quadratico modulo p *se $\big(a \mid p\big) = 1$ e che a è un* non residuo quadratico *se $\big(a \mid p\big) = -1$.*

Lemma 1.6.2. *Per $p \geq 3$ ci sono esattamente $\frac{1}{2}(p-1)$ residui quadratici modulo p, ed esattamente $\frac{1}{2}(p-1)$ non residui quadratici modulo p.*

Dim.: Il sottogruppo dei quadrati di $\mathbb{Z}_p^*$ ha indice 2. □

Lemma 1.6.3. *Il simbolo di Legendre è completamente moltiplicativo nel primo argomento: in altre parole, qualunque siano a, $b \in \mathbb{Z}$ si ha:*

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Dim.: Se $p \mid ab$ entrambi i membri sono nulli. Se $\big(a \mid p\big) = \big(b \mid p\big) = 1$ è ovvio che l'equazione $x^2 \equiv ab \mod p$ abbia soluzione. Se invece, per esempio, $\big(a \mid p\big) = 1$ e $\big(b \mid p\big) = -1$, sia y una soluzione di $y^2 \equiv a \mod p$. L'equazione $x^2 \equiv ab \mod p$ diventa $\big(xy^{-1}\big)^2 \equiv b \mod p$, che quindi non ha soluzione. Resta il caso in cui $\big(a \mid p\big) = \big(b \mid p\big) = -1$. Per quanto appena visto, posto $f\colon \mathbb{Z}_p^* \to \mathbb{Z}_p^*$, $f(x) = ax \mod p$ si ha $f(R) = N$ dove $R \stackrel{\text{def}}{=} \{x \in \mathbb{Z}_p^*\colon \big(x \mid p\big) = 1\}$, $N \stackrel{\text{def}}{=} \{x \in \mathbb{Z}_p^*\colon \big(x \mid p\big) = -1\}$, e quindi, per il Corollario 1.2.3, $f(N) = R$. Dunque ab è un residuo quadratico. □

Teorema 1.6.4 (Gauss). *Se p e q sono primi dispari distinti, allora*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}, \qquad \textit{mentre} \qquad \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

Dim.: Avremo bisogno di un certo numero di osservazioni.

1. Se $\xi \in \mathbb{C}$ è una radice n-esima dell'unità diversa da 1, allora

$$\sum_{r=1}^{n-1} \xi^r = \frac{\xi - \xi^n}{1-\xi} = -1.$$

2. Se x, $y \in \mathbb{F}_{q^a}$, dove q è un numero primo e $d \geq 1$, allora

$$(x+y)^q \equiv x^q + y^q \mod q.$$

𝔈 1.6.1 Infatti tutti i coefficienti binomiali $\binom{q}{n}$ con $1 \le n \le q-1$ sono divisibili per q.

3. Se f è una funzione aritmetica periodica con periodo q (cioè se i suoi valori dipendono solo dalla classe di resto modulo q), e se $(q,m)=1$, allora

$$\sum_{h \mod q} f(hm) = \sum_{r \mod q} f(r),$$

perché per il Corollario 1.2.3 l'applicazione $h \mapsto hm \mod q$ è una biiezione.

4. Se $nm \equiv 1 \mod q$ allora $\big(n \mid q\big) = \big(m \mid q\big)$. Infatti, se x è una soluzione dell'equazione $x^2 \equiv n \mod q$, allora x^{-1} è una soluzione dell'equazione $y^2 \equiv m \mod q$.
5. Per il Lemma 1.6.2 (nella notazione del Lemma 1.6.3) si ha

$$\sum_{m \mod q} \left(\frac{m}{q}\right) = |R| - |N| = 0.$$

6. Si ha $\big(-1 \mid q\big) = (-1)^{(q-1)/2}$ per i Lemmi 1.4.5 e 1.4.9.

𝔈 1.6.2 7. Se $q \nmid n$ allora $\big(n \mid q\big) \equiv n^{(q-1)/2} \mod q$ per il Teorema di Fermat 1.2.5.

Consideriamo ora la somma di Gauss $\tau = \tau(q)$ definita da

$$\tau \stackrel{\text{def}}{=} \sum_{m \mod q} \left(\frac{m}{q}\right) e_q(m).$$

Per le osservazioni fatte sopra si ha

$$\begin{aligned}\left(\frac{n}{q}\right)^2 \tau^2 = \left(\frac{n^{-1}}{q}\right)^2 \tau^2 &= \sum_{m_1,\, m_2 \mod q} \left(\frac{n^{-1}m_1}{q}\right)\left(\frac{n^{-1}m_2}{q}\right) e_q(m_1+m_2) \\ &= \sum_{h_1,\, h_2 \mod q} \left(\frac{h_1}{q}\right)\left(\frac{h_2}{q}\right) e_q\big(n(h_1+h_2)\big).\end{aligned}$$

Ora sommiamo questa relazione su tutti i valori di $n \in \mathbb{Z}_q^*$:

$$\begin{aligned}\tau^2 \sum_{n=1}^{q-1} \left(\frac{n}{q}\right)^2 &= \sum_{h_1,\, h_2 \mod q} \left(\frac{h_1}{q}\right)\left(\frac{h_2}{q}\right) \sum_{n=1}^{q-1} e_q\big(n(h_1+h_2)\big) \\ &= \sum_{h_1,\, h_2 \mod q} \left(\frac{h_1}{q}\right)\left(\frac{h_2}{q}\right) \begin{cases} -1 & \text{se } h_1+h_2 \not\equiv 0 \mod q, \\ q-1 & \text{se } h_1+h_2 \equiv 0 \mod q. \end{cases}\end{aligned}$$

Quindi

$$(q-1)\tau^2 = q \sum_{h \mod q} \left(\frac{-h^2}{q}\right) - \sum_{h_1,\, h_2 \mod q} \left(\frac{h_1 h_2}{q}\right) = q \sum_{h=1}^{q-1} \left(\frac{-1}{q}\right) - \Big(\sum_{h \mod q} \left(\frac{h}{q}\right)\Big)^2$$

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

In definitiva abbiamo dimostrato che $\tau^2 = q\big(-1 \mid q\big)$ e in particolare, $\tau \neq 0$. Vogliamo ora dimostrare che $\tau^p = \tau\big(p \mid q\big)$. Per fare questo, scegliamo d in modo che nel campo $\mathbb{F}_{p^d}$ il polinomio $x^q - 1$ si spezzi in fattori lineari. Per quanto osservato sopra

$$\tau^p = \sum_{m \mod q} \left(\frac{m}{q}\right)^p e_q(pm) = \sum_{h \mod q} \left(\frac{hp^{-1}}{q}\right) e_q(h) = \left(\frac{p}{q}\right) \sum_{h \mod q} \left(\frac{h}{q}\right) e_q(h) = \left(\frac{p}{q}\right)\tau.$$

Quindi abbiamo che $\tau^{p-1} = \big(p \mid q\big)$. Sostituendo il valore di τ^2 trovato sopra, si ha

$$\left(\frac{p}{q}\right) \equiv \big(\tau^2\big)^{(p-1)/2} \equiv q^{(p-1)/2}\left(\frac{-1}{q}\right)^{(p-1)/2} \equiv \left(\frac{q}{p}\right)(-1)^{(p-1)(q-1)/4},$$

dove tutte le congruenze sono modulo p. Ma sia il primo che l'ultimo termine sono numeri interi di valore assoluto 1, e quindi queste congruenze implicano l'uguaglianza richiesta.

𝔈 1.6.3 Per la dimostrazione nel caso $q = 2$ si vedano gli Esercizi. □

Osservazione 1.6.5. *La legge di reciprocità quadratica permette di determinare facilmente se la congruenza $x^2 \equiv a \mod p$ è risolubile.*

Per esempio, si voglia determinare se la congruenza $x^2 \equiv 42 \mod 47$ ha soluzione. Si può procedere come segue:

$$\left(\frac{42}{47}\right) = \left(\frac{2}{47}\right)\left(\frac{3}{47}\right)\left(\frac{7}{47}\right) = (-1)\left(\frac{47}{3}\right)\cdot(-1)\left(\frac{47}{7}\right) = \left(\frac{2}{3}\right)\left(\frac{5}{7}\right) = -\left(\frac{7}{5}\right) = -\left(\frac{2}{5}\right) = 1,$$

oppure, piú semplicemente, $\big(42 \mid 47\big) = \big(-5 \mid 47\big)$. Non c'è un metodo diretto altrettanto efficiente per determinare esplicitamente una soluzione. Con qualche calcolo si dimostra che le soluzioni sono $x \equiv \pm 18 \mod 47$.

§1.7. Formule per i numeri primi

Usando il Teorema di Wilson 1.2.7, è possibile scrivere una "formula" per l'n-esimo numero primo, ed una formula esatta per $\pi(x)$, il numero dei numeri primi $\leq x$. Naturalmente,

𝔈 1.2.8 queste formule non sono utilizzabili nella pratica, perché richiedono troppi calcoli. Abbiamo già osservato sopra che se $k \geq 6$ non è un numero primo allora $k \mid (k-2)!$, mentre per il Teorema di Wilson, se p è primo allora $(p-2)! \equiv 1 \mod p$. Quindi, per $x \geq 5$,

$$\pi(x) = 2 + \sum_{5 \leq k \leq x} k\left\{\frac{(k-2)!}{k}\right\},$$

dove $\{x\}$ indica la parte frazionaria di x. Ora definiamo $f(x,y) \stackrel{\text{def}}{=} 1$ se $x > y$, ed $f(x,y) \stackrel{\text{def}}{=} 0$ se $x \leq y$. Per il Corollario 1.1.8 possiamo scrivere

$$p_n = 1 + \sum_{d=1}^{2^{2^n}} f\big(n, \pi(d)\big),$$

dove p_n denota l'n-esimo numero primo, e $\pi(d)$ si calcola usando la formula precedente.

Teorema 1.7.1. *Se $f \in \mathbb{Z}[x]$ assume valore primo per ogni intero, allora f è costante.*

Dim.: Sia $f \in \mathbb{Z}[x]$ un polinomio che assume solo valori primi e sia $p \stackrel{\text{def}}{=} f(1)$. Si ha ovviamente $f(1+np) \equiv f(1) \equiv 0 \mod p$ per ogni $n \in \mathbb{Z}$. Dunque $p \mid f(1+np)$ per ogni $n \in \mathbb{Z}$ e quindi $f(1+np) = \pm p$ poiché deve essere un numero primo, ma questo è assurdo se f non è costante, perché allora $|f(1+np)|$ dovrebbe tendere a $+\infty$ quando $n \to \infty$. □

Teorema 1.7.2 (Schur). *Sia $f \in \mathbb{Z}[x]$ un polinomio non costante. L'insieme $\mathfrak{P}_f \stackrel{\text{def}}{=} \{p$: esiste $n \in \mathbb{N}$ tale che $f(n) \neq 0$ e $p \mid f(n)\}$ è infinito.*

Dim.: Per assurdo, sia $\mathfrak{P}_f = \{p_1, \dots, p_k\}$. Se $f(x) = a_r x^r + \cdots + a_0$ con $a_r \neq 0$, poniamo $U(x) \stackrel{\text{def}}{=} \{m \leq x : m \in f(\mathbb{N})\}$; si ha $|U(x)| \sim \left(\frac{x}{|a_r|}\right)^{1/r}$ per $x \to +\infty$. Invece, posto $V(x) \stackrel{\text{def}}{=} \{m \leq x : p \mid m \Rightarrow p \in \mathfrak{P}_f\}$, si ha $m \in V(x)$ se e solo se esistono $\alpha_1, \dots, \alpha_k \in \mathbb{N}$ tali che $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ e quindi $\log m = \alpha_1 \log p_1 + \cdots + \alpha_k \log p_k \leq \log x$. In altre parole $|V(x)| \sim \int \cdots \int_T \mathrm{d}x_1 \cdots \mathrm{d}x_k$ dove $T \stackrel{\text{def}}{=} \{(x_1, \dots, x_k) \in \mathbb{R}^k : x_i \geq 0,\ x_1 \log p_1 + \cdots + x_k \log p_k \leq \log x\}$, e quindi $|V(x)| \sim c(\log x)^k$, dove $c = \left(k! \log p_1 \cdots \log p_k\right)^{-1}$, in contraddizione con il fatto che $U(x) \subseteq V(x)$. □

Evidentemente non è necessario conoscere esattamente $|V(x)|$: è sufficiente osservare che da $\log m = \alpha_1 \log p_1 + \cdots + \alpha_k \log p_k \leq \log x$ segue che $\alpha_i \leq 1 + \left[\frac{\log x}{\log p_i}\right]$ e quindi $|V(x)| \leq \prod_i \left(1 + \frac{\log x}{\log p_i}\right) = \mathcal{O}_{p_1,\dots,p_k}\left((\log x)^k\right)$.

Teorema 1.7.3. *Esistono infiniti primi nelle progressioni aritmetiche $4n+1$ e $4n-1$.*

Dim.: Supponiamo che esistano solo un numero finito di primi $p_i \equiv 1 \mod 4$. Poniamo $N \stackrel{\text{def}}{=} (2p_1 \cdots p_k)^2 + 1$. Se q è un fattore primo di N, per il Corollario 1.4.4 si ha $q = s^2 + t^2$ per opportuni s, $t \in \mathbb{N}$, e quindi $q \equiv 1 \mod 4$. Se esistessero solo un numero finito di numeri primi $p_i \equiv -1 \mod 4$, posto $N \stackrel{\text{def}}{=} 4p_1 \cdots p_k - 1$, si avrebbe $N \equiv -1 \mod 4$, ed evidentemente non è possibile che tutti i fattori primi di N siano congrui a 1 mod 4. □

Questa dimostrazione può essere facilmente modificata per dare il seguente risultato: qualunque sia $q \geq 3$, i numeri primi non sono definitivamente $\equiv 1 \bmod q$. Esiste una dimostrazione elementare del fatto che dato $q \geq 2$ ci sono infiniti numeri primi $\equiv 1 \bmod q$ che qui non daremo perché nel Capitolo 5 otterremo un risultato molto piú preciso.

Teorema 1.7.4. *Se il numero $2^m + 1$ è primo, allora $m = 2^n$ per qualche intero n.*

Definizione 1.7.5. *Per $n \in \mathbb{N}$ si chiama n-esimo* numero di Fermat *il numero $F_n \stackrel{\text{def}}{=} 2^{2^n} + 1$. Per $n \in \mathbb{N}^*$ si chiama n-esimo* numero di Mersenne *il numero $M_n \stackrel{\text{def}}{=} 2^n - 1$.*

Teorema 1.7.6. *Se il numero M_n è primo, allora n è primo.*

Fermat congetturò che tutti i numeri F_n fossero primi, ma questo è vero solo per $n = 0,$
𝔈 1.7.2–7 $\dots, 4$, e falso per $n = 5, \dots, 32$. Mersenne dette una lista di numeri primi p per i quali M_p è primo, ma questa lista contiene vari errori ed omissioni.

Capitolo 2. Algoritmi Fondamentali e Crittografia

In questo capitolo presenteremo alcuni degli algoritmi fondamentali della Teoria dei Numeri, e qualche loro applicazione alla crittografia moderna. Scriveremo $\leftarrow$ per indicare l'*assegnazione*, cioè per dire che alla variabile a sinistra viene dato il valore dell'espressione a destra: quindi $A \leftarrow A^2$ significa che dobbiamo calcolare A^2 ed assegnare questo valore alla variabile A.

§2.1. L'algoritmo di Euclide

Abbiamo visto nel Lemma 1.1.1 che è possibile esprimere il massimo comun divisore d di due interi n ed m come combinazione lineare a coefficienti interi $d = \lambda n + \mu m$, ed abbiamo osservato che questo è rilevante per il calcolo dell'inverso moltiplicativo nel gruppo $\mathbb{Z}_n^*$.

𝔈 1.1.1–3 Possiamo supporre $0 < m < n$; poniamo $r_{-1} \leftarrow n$, $r_0 \leftarrow m$, $k \leftarrow 0$. Poi ripetiamo iterativamente i due passi:

1. se $r_k = 0$ allora $r_{k-1} = (n, m)$; l'algoritmo termina;
2. si divide r_{k-1} per r_k trovando due interi q_{k+1} ed r_{k+1} (quoziente e resto) con la proprietà
$$r_{k-1} = q_{k+1} r_k + r_{k+1} \qquad \text{e} \qquad 0 \le r_{k+1} < r_k.$$
Si pone $k \leftarrow k + 1$. Si torna al passo 1.

L'algoritmo deve terminare poiché la successione dei resti è monotona, strettamente decrescente ed assume valori in $\mathbb{N}$. Questo non dà subito anche (n, m) come combinazione lineare di n ed m, ma possiamo costruire due successioni a_k e b_k che risolvono il problema. Poniamo per definizione

$$a_{-1} \stackrel{\text{def}}{=} 1, \quad b_{-1} \stackrel{\text{def}}{=} 0, \quad a_0 \stackrel{\text{def}}{=} 0, \quad b_0 \stackrel{\text{def}}{=} 1.$$

Ad ogni passo con $k > 0$ si calcolano a_k e b_k mediante

$$a_k \stackrel{\text{def}}{=} a_{k-2} - q_k a_{k-1}, \qquad b_k \stackrel{\text{def}}{=} b_{k-2} - q_k b_{k-1}, \tag{2.1.1}$$

(la regola è la stessa, ma le successioni hanno valori iniziali differenti). Queste due successioni hanno la proprietà (di facile verifica) che

$$r_k = a_k n + b_k m \qquad \text{per ogni } k > 0$$

ed in particolare, se $r_{K+1} = 0$, per $k = K$ e quindi

$$r_K = (n, m) = a_K n + b_K m.$$

La Tavola 2.1 fornisce un esempio pratico di applicazione dell'algoritmo. Si può dimostrare

𝔈 2.1.1–2 che il numero di moltiplicazioni o divisioni necessarie per l'esecuzione è $\mathcal{O}(\log m)$.

k		q_k	r_k	a_k	b_k	cosicché
-1			43	1	0	
0			35	0	1	
1	$43 = 1 \cdot 35 + 8$	1	8	1	-1	$8 = 1 \cdot 43 + (-1) \cdot 35$
2	$35 = 4 \cdot 8 + 3$	4	3	-4	5	$3 = (-4) \cdot 43 + 5 \cdot 35$
3	$8 = 2 \cdot 3 + 2$	2	2	9	-11	$2 = 9 \cdot 43 + (-11) \cdot 35$
4	$3 = 1 \cdot 2 + 1$	1	1	-13	16	$1 = (-13) \cdot 43 + 16 \cdot 35$
5	$2 = 2 \cdot 1 + 0$	2	0			

Tavola 2.1. *L'algoritmo inizia dalla riga con $k = 1$: le prime due righe servono per completare lo schema. A sinistra eseguiamo l'algoritmo di Euclide su $(n, m) = (43, 35)$ ed usiamo i coefficienti q_k ed r_k per le operazioni a destra, mediante le formule* (2.1.1)*. Per chiarezza, q_k ed r_k sono scritti in colonne separate.*

§2.2. Il crivello di Eratostene

Eratostene (II sec. a. C.) inventò il cosiddetto crivello (cioè setaccio) che permette di determinare in modo piuttosto efficiente i numeri primi nell'intervallo $[1, N]$ purché N non sia troppo grande. Illustriamo il funzionamento del crivello per $N = 144$: lasciamo da parte il numero 1, e cancelliamo dallo schema riprodotto nella Tavola 2.2 tutti i multipli di 2 a partire da $2^2 = 4$. Poi guardiamo qual è il piú piccolo numero non cancellato, 3, e procediamo come prima, partendo da $3^2 = 9$. Ripetiamo queste operazioni con 5, a partire da $5^2 = 25$, poi con 7, partendo da $7^2 = 49$, ed infine con 11, partendo da $11^2 = 121$. A questo punto possiamo fermarci, poiché il primo numero non ancora cancellato è 13, e $13^2 = 169$ che è fuori dalla nostra tavola: questa mostra dunque 1 e tutti i numeri primi fino a 144. Le righe aiutano a cancellare i multipli dello stesso numero primo. Il Teorema 4.3.4 implica che il numero di passi per eseguire il crivello di Eratostene sui numeri interi in $[1, N]$ è $\mathcal{O}(N \log\log N)$, mentre, evidentemente, l'occupazione di memoria è $\mathcal{O}(N)$.

§2.3. Criteri di primalità

Osserviamo che non è necessario conoscere esplicitamente i fattori di n per dimostrare che è composto. Il Teorema di Fermat 1.2.5 fornisce una condizione necessaria ma non sufficiente per la primalità, come abbiamo visto nel Capitolo 1, che non richiede il calcolo degli eventuali fattori di n. Alcuni criteri di primalità si basano su varianti del Teorema di Fermat, e richiedono la conoscenza della fattorizzazione completa di $n-1$; altri, che qui non descriveremo, necessitano della fattorizzazione di $n+1$, per altri ancora è sufficiente una fattorizzazione parziale di $n \pm 1$. Il Teorema di Wilson 1.2.7 dà una condizione necessaria e sufficiente per la primalità, ma non è efficiente. Il Teorema 1.2.6 e l'esistenza di infiniti numeri di Carmichael rendono necessarî i criteri di primalità come quello di Lucas.

Teorema 2.3.1 (Lucas, Inverso del Teorema di Fermat). *Se $a^d \not\equiv 1 \mod n$ per ogni $d \mid n-1$ tale che $d < n-1$ ed inoltre $a^{n-1} \equiv 1 \mod n$, allora n è primo.*

Dim.: a ha ordine $n-1$ in $\mathbb{Z}_n^*$, e quindi $n-1 \mid \varphi(n) \leq n-1$ da cui $\varphi(n) = n-1$, cioè n è primo. □

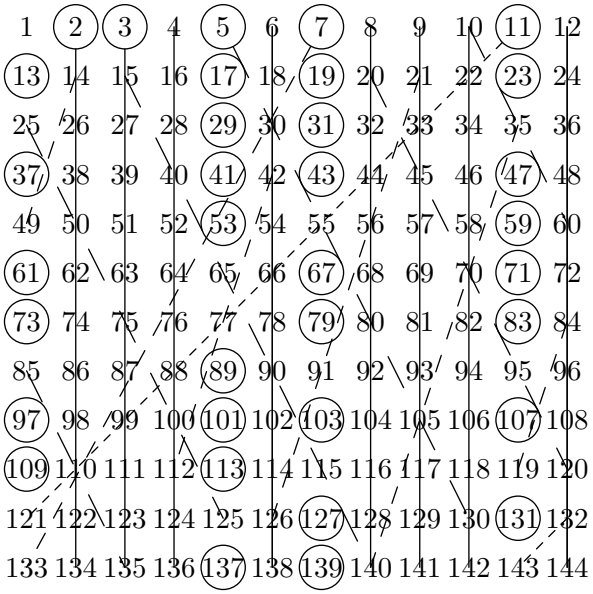


Tavola 2.2. *Il crivello di Eratostene.*

LEMMA 2.3.2. *Per $n \in \mathbb{N}^*$ dispari, con $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ sia $\lambda(n) \stackrel{\text{def}}{=} \left[\varphi\left(p_1^{\alpha_1}\right), \ldots, \varphi\left(p_k^{\alpha_k}\right)\right]$. $\lambda(n)$ è il massimo ordine possibile degli elementi di $\mathbb{Z}_n^*$.*

DIM.: Poiché $\mathbb{Z}_{p_i^{\alpha_i}}^*$ è ciclico per il Teorema 1.2.16, ha un elemento x_i di ordine $\varphi\left(p_i^{\alpha_i}\right)$. L'elemento $x \in \mathbb{Z}_n^*$ che è $\equiv x_i \mod p_i^{\alpha_i}$ per $i = 1, \ldots, k$ ha dunque ordine $\lambda(n)$. Il viceversa è ovvio. □

COROLLARIO 2.3.3. *Il numero composto dispari n è di Carmichael se e solo se $\lambda(n) \mid n-1$.*

TEOREMA 2.3.4 (CRITERIO DI KORSELT). *L'intero n è di Carmichael se e solo se è composto, libero da quadrati e $p-1 \mid n-1$ per ogni $p \mid n$. Dunque n è dispari ed $\omega(n) \geq 3$.*

DIM.: Se n è di Carmichael evidentemente soddisfa la condizione data poiché per ogni $p^\alpha \parallel n$ possiamo scegliere $a \in \mathbb{Z}_{p^\alpha}^*$ di ordine massimo $= p^{\alpha-1}(p-1)$. Questo numero deve dividere $n-1$, e ciò è possibile solo se $\alpha = 1$. Viceversa, se $p-1 \mid n-1$ per ogni $p \mid n$, allora $a^{n-1} \equiv 1 \mod p$ ed il risultato segue dal Teorema Cinese del Resto. Infine se $n = pq$ è di Carmichael con $p < q$ da $q-1 \mid pq-1 = p(q-1)+p-1$ ricaviamo $q-1 \mid p-1$, assurdo, mentre se $n = 2r$ con $r > 1$ dispari e $p \mid r$ allora $p-1 \nmid n-1$ poiché $2 \nmid n-1$. □

È importante osservare che nell'agosto del 2002, Agrawal, Kayal e Saxena [A1] hanno trovato un rivoluzionario criterio di primalità sostanzialmente elementare, che è impossibile però riassumere in questa sede. Si veda anche l'appendice di Pomerance [A7].

§2.4. ALGORITMI DI FATTORIZZAZIONE

> Problema, numeros primos a compositis dignoscendi, hosque in factores suos primos resolvendi, ad gravissima ac utilissima totius arithmeticæ pertinere, et geometrarum tum veterum tum recentiorum industriam ac sagacitatem occupavisse, tam notum est, ut de hac re copiose loqui superfluum foret ... Prætereaque scientiæ dignitas requirere videtur, ut omnia subsidia ad solutionem problematis tam elegantis ac celebris sedulo excolantur.
>
> K. F. Gauss, *Disquisitiones Arithmeticae*, 1801, Art. 329.

Divisione per tentativi. Si può dimostrare che un numero intero $N \geq 2$ è primo verificando direttamente la definizione, cioè verificando che nessuna delle divisioni di N per gli interi $2 \leq m \leq N-1$ è esatta. Poiché se $N = mr$ uno fra m ed r è necessariamente $\leq \sqrt{N}$, è sufficiente effettuare $\mathcal{O}\big(N^{1/2}\big)$ divisioni. Inoltre, avendo una lista dei numeri primi $\leq \sqrt{N}$ è sufficiente provare a dividere N per ciascuno di questi numeri primi, ma in ogni caso il numero delle divisioni necessarie non è significativamente piú piccolo di $\sqrt{N}$.

Fattorizzazione "alla Fermat" (Algoritmo di Lehman). Il metodo della divisione per tentativi ha certamente il vantaggio dell'estrema semplicità, ma anche l'enorme svantaggio che può richiedere quasi $\sqrt{N}$ operazioni per scomporre in fattori dei numeri N che hanno esattamente 2 fattori primi molto vicini fra loro, come per esempio $N = 3992003 = 1997 \cdot 1999$. In questo caso è piú efficiente un altro metodo, basato su una semplice osservazione: se riusciamo a trovare x ed $y \in \mathbb{N}$ tali che $N + y^2 = x^2$, allora $N = x^2 - y^2 = (x-y)\cdot(x+y)$ e quindi N è scomposto in due fattori. Naturalmente $x-y$ ed $x+y$ non sono necessariamente primi, ed è anche possibile che $x-y$ sia proprio uguale ad 1, rendendo questa scomposizione poco interessante. In ogni modo, questa osservazione suggerisce di calcolare $N + y^2$ per alcuni valori (relativamente piccoli) di y, e di verificare se $N + y^2$ risulti essere un quadrato perfetto (osserviamo che l'algoritmo di Newton per il calcolo della radice quadrata è molto piú efficiente e piú semplice da implementare di quello insegnato di solito nelle scuole medie, visto soprattutto che qui ci interessa soltanto di sapere se $\sqrt{N+y^2} \in \mathbb{N}$). Applicato all'esempio precedente, questo metodo funziona immediatamente: per $y = 1$ troviamo che $N + 1 = 1998^2$ e quindi N ha la fattorizzazione data. Naturalmente non è possibile sapere *a priori* che le cose funzioneranno meglio con questo metodo piuttosto che con l'altro, ma è possibile "mescolarli" per ottenere un metodo di fattorizzazione piú efficiente di ciascuno dei due. In pratica si procede come segue: posto $R \stackrel{\text{def}}{=} N^{1/3}$, applichiamo la divisione per tentativi, con $m = 2$ e tutti gli interi dispari $\leq R$. Questo richiede $\mathcal{O}(R)$ divisioni. Se nessuna delle divisioni è esatta, allora N è primo oppure N è il prodotto pq di due numeri primi che soddisfano $R < p \leq q < N/R = R^2$. Si può dimostrare che se N non è primo è possibile trovare x, y e $k \in \mathbb{N}$ tali che

$$\begin{cases} x^2 - y^2 = 4kN & \text{dove } 1 \leq k \leq R \\ 0 \leq x - \sqrt{4kN} \leq \sqrt{\frac{N}{k}}(4R)^{-1} & \\ p = \min\big((x+y, N), (x-y, N)\big). & \end{cases}$$

Per determinare x, y e k, procediamo di nuovo per tentativi, verificando se, fissato k, esiste un valore intero di x compreso fra $x_0 \stackrel{\text{def}}{=} \lceil \sqrt{4kN} \rceil$ ed $x_1 \stackrel{\text{def}}{=} \big[\sqrt{4kN} + \sqrt{N/k}/4R\big]$ per il quale $x^2 - 4kN$ sia un quadrato perfetto. Si dimostra che anche questa parte del calcolo richiede al massimo $\mathcal{O}(R)$ operazioni, e quindi il costo totale dell'algoritmo è $\mathcal{O}(R) = \mathcal{O}\big(N^{1/3}\big)$. Senza entrare nei dettagli, se $N = pq$ con $R < p \leq q < R^2$ ed esistono r, $s \in \mathbb{N}^*$ tali che $\frac{p}{q} \approx \frac{r}{s}$ allora il numero $pqrs = (ps)(rq)$ ha due fattori quasi uguali ed è relativamente facile determinarli con il metodo visto sopra. Evidentemente, questo dà un buon algoritmo di fattorizzazione se si può dimostrare che esistono r ed s piú piccoli di p: questo segue dal Lemma 1.4.2. Osserviamo che la moltiplicazione per $4k$ con k relativamente piccolo serve per numeri del tipo $N = 3 \cdot 103 \cdot 311$, in cui la parte di divisioni per tentativi rende

(paradossalmente) piú difficile l'applicazione dell'idea di Fermat, poiché N ha due fattori relativamente vicini (309 e 311), mentre $\frac{1}{3}N$ no.

> Can the reader say what two numbers multiplied together will produce the number 8 616 460 799? I think it is unlikely that anyone but myself will ever know.
>
> William S. Jevons, "The Principles of Science, A Treatise on Logic and Scientific Method," 1877.

Qui $R = \lfloor N^{1/3} \rfloor = 2050$, e si vede facilmente che $N = 8\,616\,460\,799$ non ha fattori primi $\leq R$. Per $k = 210$ si trova $4kN = 2690321^2 - 109^2 = x^2 - y^2$ da cui $N = p \cdot q$ dove

$$\begin{cases} p = (2690321 + 109, N) = 89681, \\ q = (2690321 - 109, N) = 96079. \end{cases}$$

Il metodo funziona bene perché y è relativamente piccolo. Si noti che

$$\begin{cases} 2690321 + 109 = 30 \cdot 89681, \\ 2690321 - 109 = 28 \cdot 96079, \end{cases} \qquad 4k = 30 \cdot 28, \qquad \frac{q}{p} \approx \frac{30}{28} = \frac{15}{14}.$$

Questo algoritmo richiede circa 410 iterazioni per trovare un valore di k (oltre a circa 1000 iterazioni della divisione per tentativi), mentre la divisione per tentativi ne richiede circa 44840. In questo caso particolare, la ricerca diretta di x ed y tali che $x^2 - y^2 = N$ è ancora
𝔈 2.4.1 piú efficiente: richiede solo 56 iterazioni.

Il crivello quadratico. Gli algoritmi che descriveremo si basano tutti sullo stesso schema, che ha la sua origine nelle idee esposte qui sopra: l'obiettivo è quello di determinare una congruenza non banale $X^2 \equiv Y^2 \mod N$, dove N è il numero da scomporre in fattori. Si calcola poi $d \stackrel{\text{def}}{=} (X - Y, N)$ che è un fattore di N: se $1 < d < N$, allora abbiamo scomposto N nel prodotto di due fattori, non necessariamente primi, ma comunque piú piccoli di N. Di solito, ci si assicura preliminarmente che N non abbia fattori primi molto piccoli.

Lo schema di cui parliamo, dovuto a Kraitchik, si può riassumere come segue:

1. determinazione di congruenze $A_i \equiv B_i \mod N$ con $A_i \neq B_i$;
2. determinazione della scomposizione in fattori primi (parziale o completa) dei numeri A_i, B_i per un sottoinsieme delle congruenze ottenute sopra;
3. determinazione di un sottoinsieme $\mathcal{S}$ delle congruenze ottenute nel punto 2 tale che

$$\prod_{i \in \mathcal{S}} A_i \equiv X^2 \mod N; \qquad \prod_{i \in \mathcal{S}} B_i \equiv Y^2 \mod N;$$

4. calcolo di $(X - Y, N)$ per ottenere un fattore di N.

Dei molti algoritmi che appartengono a questa famiglia, parleremo solamente del *crivello quadratico* di Carl Pomerance. L'idea è di costruire una "base di fattori" $\mathcal{B}$ costituita da un opportuno insieme di numeri primi piccoli, ed un insieme di numeri relativamente piccoli che permettano di individuare le congruenze necessarie al punto 2. Si veda la Tavola 2.3 per un esempio. Piú precisamente, poniamo

$$Q(A) \stackrel{\text{def}}{=} \left(A + \lfloor N^{1/2} \rfloor\right)^2 - N.$$

A	$Q(A)$	Fattorizzazione	$\underline{v}(A)$	$\underline{v}(A) \mod 2$
1	200	$2^3 \cdot 5^2$	$(3,2,0,0)$	$(1,0,0,0)$
3	608	$2^5 \cdot 19$	$(5,0,0,1)$	$(1,0,0,1)$
5	1024	2^{10}	$(10,0,0,0)$	$(0,0,0,0)$
6	1235	$5 \cdot 13 \cdot 19$	$(0,1,1,1)$	$(0,1,1,1)$
19	4160	$2^6 \cdot 5 \cdot 13$	$(6,1,1,0)$	$(0,1,1,0)$
41	9880	$2^3 \cdot 5 \cdot 13 \cdot 19$	$(3,1,1,1)$	$(1,1,1,1)$
51	12800	$2^9 \cdot 5^2$	$(9,2,0,0)$	$(1,0,0,0)$

Tavola 2.3. *Implementazione del crivello quadratico per la fattorizzazione di* $10001 = 73 \cdot 137$. *Qui scegliamo come base di fattori l'insieme* $\mathcal{B} \stackrel{\text{def}}{=} \{2, 5, 13, 19\}$. *Nella Tavola sono riportati i valori di* A *per cui* $Q(A)$ *si fattorizza completamente in* $\mathcal{B}$, *il valore di* $Q(A)$, *i vettori* $\underline{v}(A)$ *corrispondenti, e gli stessi vettori modulo* 2. *Si osservi che i vettori negli insiemi* $\{\underline{v}(1), \underline{v}(51)\}$, $\{\underline{v}(3), \underline{v}(6), \underline{v}(19), \underline{v}(51)\}$, $\{\underline{v}(5)\}$, $\{\underline{v}(6), \underline{v}(41), \underline{v}(51)\}$, $\{\underline{v}(1), \underline{v}(3), \underline{v}(6), \underline{v}(19)\}$, $\{\underline{v}(1), \underline{v}(6), \underline{v}(41)\}$, $\{\underline{v}(3), \underline{v}(19), \underline{v}(41)\}$, *sono linearmente dipendenti* $\mod 2$, *ma solo i primi 4 portano alla scoperta di un fattore non banale di* 10001.

Osserviamo che per ogni A si ha $Q(A) \equiv \big(A + \big[N^{1/2}\big]\big)^2 \mod N$. L'insieme $\mathcal{B}$ è costituito dal numero primo 2 e dai numeri primi dispari piccoli p tali che $\big(N \mid p\big) = 1$, cioè dai primi piccoli per cui l'equazione $Q(A) \equiv 0 \mod p$ ha soluzione. Poiché per A piccolo $Q(A) \approx 2A\sqrt{N}$ è relativamente piccolo, si può sperare di riuscire a scomporre in fattori primi *tutti appartenenti a* $\mathcal{B}$ numerosi valori $Q(A)$. Posto $k \stackrel{\text{def}}{=} |\mathcal{B}|$, per ogni intero A_j per cui $Q(A_j)$ si fattorizza completamente su $\mathcal{B}$, diciamo $Q(A_j) = \prod_{p \in \mathcal{B}} p^{\alpha_{p,j}}$, costruiamo il vettore $\underline{v}(A_j) \in \mathbb{N}^k$ che ha come componenti gli esponenti $\alpha_{p,j}$, e poi riduciamo queste componenti modulo 2, ottenendo i vettori $\underline{v}_2(A_j)$. Una semplice applicazione dell'algebra lineare su $\mathbb{Z}_2$ ci permette di concludere che $k+1$ di questi vettori ridotti sono certamente linearmente dipendenti su $\mathbb{Z}_2$. È importante notare che una relazione di dipendenza lineare su $\mathbb{Z}_2$ significa semplicemente che $\underline{v}_2(A'_1) + \cdots + \underline{v}_2(A'_m) \equiv \underline{0} \mod 2$ (i coefficienti della relazione di dipendenza lineare possono essere solo 0 o 1); una volta determinato un insieme $\mathcal{I}$ di indici tale che $\{\underline{v}_2\big(A_j\big) : j \in \mathcal{I}\}$ sia linearmente dipendente su $\mathbb{Z}_2$, abbiamo trovato la combinazione di congruenze cercata. Infatti, per quanto osservato sopra, si ha

$$\prod_{j \in \mathcal{I}} \big(A_j + \big[N^{1/2}\big]\big)^2 \equiv \prod_{j \in \mathcal{I}} Q(A_j) \equiv \prod_{p \in \mathcal{B}} p^{\Sigma_{j \in \mathcal{I}} \alpha_{p,j}} \mod N$$

e, per costruzione, ciascuno degli esponenti a destra è pari. A questo punto si può passare alla quarta fase del programma, il calcolo del massimo comun divisore d. Si osservi che se $d = 1$ oppure $d = N$, è sufficiente cercare un'ulteriore fattorizzazione di qualche nuovo $Q(A)$, e ripetere il passo 3. Nelle realizzazioni pratiche vi sono numerosi accorgimenti per migliorare l'efficienza dell'algoritmo: per esempio è possibile evitare l'operazione di divisione per tentativi (costosa dal punto di vista computazionale), risolvendo preliminarmente l'equazione $Q(A) \equiv 0 \mod p$ per ogni $p \in \mathcal{B}$. Gli algoritmi di questa famiglia hanno una complessità che è (euristicamente) stimata in una una potenza fissata di $L(N) \stackrel{\text{def}}{=} \exp\big((\log N \log\log N)^{1/2}\big)$.

§2.5. Radici primitive

Il Teorema 1.2.15 implica che per ogni p primo esiste $g \in \mathbb{Z}_p^*$ che ha ordine esattamente $p-1$, cioè esiste una radice primitiva $\bmod p$, ed anzi, ne esistono $\varphi(p-1)$. Daremo un algoritmo per determinare una radice primitiva dovuto a Gauss: si sceglie un qualsiasi intero $a_1 \in \mathbb{Z}_p^*$ (naturalmente non conviene scegliere una potenza perfetta), e si calcolano i valori a_1, $a_1^2 \bmod p$, $a_1^3 \bmod p$, ... Sia r_1 l'ordine di $a_1 \bmod p$. Se $r_1 = p-1$ allora a_1 è una radice primitiva $\bmod p$ ed abbiamo finito; in caso contrario sia $b_1 \in \mathbb{Z}_p^* \setminus \{a_1, a_1^2 \bmod p, \ldots, a_1^{r_1} \bmod p\}$, di ordine s_1. Se $s_1 = p-1$ allora b_1 è una radice primitiva $\bmod p$ ed abbiamo finito; altrimenti poniamo $v_1 \stackrel{\text{def}}{=} [r_1, s_1]$. Possiamo scrivere $v_1 = n_1 m_1$ con $(n_1, m_1) = 1$, $n_1 \mid r_1$, $m_1 \mid s_1$. Se poniamo $a_2 \stackrel{\text{def}}{=} a_1^{v_1/n_1} b_1^{v_1/m_1}$, si può verificare che l'ordine r_2 di a_2 è $> \max(r_1, s_1)$, ed abbiamo trovato un intero che ha ordine piú grande di a_1. Evidentemente, l'algoritmo termina in un numero finito di passi.

Siano $p = 41$, $a_1 = 2$. Le potenze di a_1, ridotte $\bmod p$, sono nell'ordine 2, 4, 8, 16, 32, 23, 5, 10, 20, 40, 39, 37, 33, 25, 9, 18, 36, 31, 21, 1, e quindi $r_1 = 20$. Possiamo prendere $b_1 = 3$, le cui potenze successive sono 3, 9, 27, 40, 38, 32, 14, 1, e quindi $s_1 = 8$. Dunque $v_1 = [20, 8] = 40$, $n_1 = 5$, $m_1 = 8$, $a_2 = 2^4 \cdot 3 \bmod p = 7$, e l'ordine di $7 \bmod p$ è 40.

Dato il numero primo $p = 65537 = F_4 = 2^{16}+1$ si può prendere $g = 75$. Non è necessario calcolare esplicitamente tutte le potenze g^n per $n = 1, \ldots, p-1$ per dimostrare che 75 è una radice primitiva $\bmod p$; poiché $p-1$ è una potenza di 2 e l'ordine di 75 deve dividere $p-1$, deve essere a sua volta una potenza di 2 ed è quindi sufficiente verificare che $75^n \not\equiv 1 \bmod p$ quando n è una potenza di 2 minore di $p-1$. In effetti, poiché $p-1$ è una potenza di 2, è sufficiente dimostrare che 75 non è un quadrato $\bmod p$, ed infatti

$$\left(\frac{75}{65537}\right) = \left(\frac{3}{65537}\right) = \left(\frac{65537}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

𝔈 1.7.3 In generale, se $p = F_n$ è primo, allora h è un generatore di $\mathbb{Z}_p^*$ se e solo se $\big(h \mid p\big) = -1$.

§2.6. Logaritmo discreto

Illustriamo il funzionamento dell'algoritmo per il calcolo del logaritmo discreto per mezzo di un esempio. Prima però è opportuno mettere in guardia i lettori che conoscono l'Analisi Matematica: per calcolare con una certa approssimazione il logaritmo di un numero reale positivo si sfruttano proprietà quali continuità, derivabilità, convessità e monotonia delle funzioni esponenziale e logaritmo. Qui invece il concetto di monotonia (che si basa sulle disuguaglianze) non ha alcun senso, né, evidentemente, ne possono avere continuità e derivabilità, ed inoltre il logaritmo discreto in $\mathbb{Z}_p^*$ è un elemento di $\mathbb{Z}_{(p-1)}$ e sarà determinato esattamente, senza approssimazioni. Si tratta quindi di un problema di natura essenzialmente diversa da quello con lo stesso nome che conosciamo dall'Analisi.

Poiché 3 è un generatore di $\mathbb{Z}_{31}^*$, vogliamo trovare il *logaritmo discreto* di 7 in base 3, cioè l'elemento x di $\mathbb{Z}_{30}$ tale che $3^x \equiv 7 \bmod 31$. Il calcolo comprende due parti.

Precomputazione. Si calcolano i numeri $r_{j,p} \equiv 3^{30j/p} \bmod 31$ per tutti i fattori primi

p di 30, e per $j = 0, 1, \dots, p-1$. Questo ci dà la tabella

$$\begin{array}{lllll} r_{0,2} = 1 & r_{1,2} = -1 & & & \\ r_{0,3} = 1 & r_{1,3} = -6 & r_{2,3} = 5 & & \\ r_{0,5} = 1 & r_{1,5} = 16 & r_{2,5} = 8 & r_{3,5} = 4 & r_{4,5} = 2 \end{array}$$

Osserviamo che $r_{j,p}^p \equiv 1 \mod 31$: poiché 3 genera $\mathbb{Z}_{31}^*$, i numeri $r_{j,p}$ sono tutte e sole le radici p-esime di 1.

Il logaritmo discreto. Se $3^x \equiv 7 \mod 31$ ed $x = a + 2a'$ con $a \in \{0, 1\}$, allora

$$3^{15x} = 3^{15a+30a'} \equiv 3^{15a} \equiv 7^{15} \equiv 1 \mod 31.$$

Ora notiamo che $(7^{15})^2 \equiv 7^{30} \equiv 1 \mod 31$, cioè 7^{15} è una delle due radici quadrate di 1 calcolate sopra, ed in effetti l'ultima congruenza rivela che $7^{15} = r_{0,2}$. Poiché $3^0 \equiv 1 \mod 31$, mentre $3^{15} \equiv -1 \mod 31$, concludiamo che $a = 0$, cioè che $x \equiv 0 \mod 2$. Analogamente, se $x = b + 3b'$ con $b \in \{0, 1, 2\}$, allora

$$3^{10x} = 3^{10b+30b'} \equiv 3^{10b} \equiv 7^{10} \equiv -6 \mod 31,$$

da cui $b = 1$ cioè $x \equiv 1 \mod 3$. Infine, se $x = c + 5c'$ con $c \in \{0, 1, 2, 3, 4\}$ allora

$$3^{6x} = 3^{6c+30c'} \equiv 3^{6c} \equiv 7^6 \equiv 4 \mod 31,$$

da cui $c = 3$ cioè $x \equiv 3 \mod 5$. Troviamo cosí il sistema di congruenze

$$\begin{cases} x \equiv 0 \mod 2 \\ x \equiv 1 \mod 3 \\ x \equiv 3 \mod 5 \end{cases} \qquad \text{da cui} \qquad x \equiv 28 \mod 30$$

per il Teorema Cinese del Resto. Un algoritmo simile (ma piú complicato) funziona quando l'ordine del gruppo è divisibile per potenze di un primo piú grandi di 1. Concludiamo osservando che per eseguire questi calcoli in $\mathbb{Z}_p^*$ è necessario conoscere la completa scomposizione in fattori primi di $p-1$.

§2.7. Numeri pseudocasuali

Qualche volta, per simulare numericamente dei fenomeni casuali, può sorgere la necessità di costruire una sequenza di numeri "casuali," cioè una successione di numeri il cui comportamento sia per quanto possibile imprevedibile. Naturalmente, qualunque successione generata da un calcolatore non può essere casuale in senso stretto: quindi, ciò che cerchiamo realmente è una successione di numeri, che chiameremo *pseudocasuali*, per i quali sia pressoché impossibile prevedere un termine conoscendo i precedenti. Un buon metodo per generare numeri pseudocasuali è legato al Teorema 1.2.15: dato un numero primo p ed una radice primitiva g di $\mathbb{Z}_p^*$, consideriamo la successione $a\colon \mathbb{N} \to [0,1)$ definita da $a_n \stackrel{\text{def}}{=} \big((g^n \bmod p) - 1\big)(p-1)^{-1}$. Il difetto principale è che la successione di numeri cosí ottenuta è periodica con periodo $p-1$. Naturalmente, tanto piú grande è p tanto piú lungo è il periodo ed inoltre tanto meglio sono distribuiti i numeri a_n nell'intervallo $[0,1)$, che sono le frazioni $\frac{0}{p-1}, \frac{1}{p-1}, \frac{2}{p-1}, \dots, \frac{p-2}{p-1}$, in un altro ordine naturalmente, e quindi la loro distanza è $\frac{1}{p-1}$. Si osservi infine che non è necessario calcolare ogni volta *ex novo* la potenza: è sufficiente memorizzare $g^n \mod p$ e poi calcolare $g^{n+1} \equiv g^n \cdot g \mod p$.

§2.8. Applicazioni alla crittografia

Le idee esposte in questo Capitolo sono state utilizzate per costruire dei sistemi crittografici detti a "chiave pubblica" che sono di importanza fondamentale per lo sviluppo delle comunicazioni su rete e del commercio elettronico. Prima di parlare della crittografia moderna, però, ricordiamo brevemente le origini della crittografia "tradizionale": il primo ad utilizzare un sistema crittografico sarebbe stato Giulio Cesare.

Per fissare il linguaggio una volta per tutte, ricordiamo che il problema fondamentale della crittografia è la trasmissione di informazioni che devono essere comprese solo dal destinatario, ed anche se intercettate, restare incomprensibili a terze persone. Fissiamo dunque un insieme di *messaggi* $\mathfrak{M}$: solitamente $\mathfrak{M} = \mathbb{Z}_N$ dove $N \in \mathbb{N}$ è molto grande (tipicamente al giorno d'oggi $N \approx 2^{512} \approx 10^{154}$). In altre parole, per noi un messaggio è un elemento di $\mathbb{Z}_N$. Nella pratica, si dovrà preliminarmente trasformare ogni testo alfanumerico in uno o piú messaggi di questo tipo. Le *funzioni crittografiche* che consideriamo sono biiezioni $f\colon \mathfrak{M} \to \mathfrak{M}$. Nelle applicazioni pratiche queste funzioni dipendono da uno o piú parametri, parte dei quali sono tenuti segreti da ciascun utente del sistema, mentre altri possono essere resi pubblici.

Nel metodo di Cesare si prende $\mathfrak{M} = \mathbb{Z}_{26}$ (per esempio) e l'applicazione $f_a\colon \mathfrak{M} \to \mathfrak{M}$ definita da $f_a(x) = (x+a) \mod 26$: in sostanza è una traslazione dell'alfabeto, considerato come disposto attorno ad una circonferenza. Qui c'è un unico parametro a: per decifrare il destinatario calcola f_{-a} e ritrova il messaggio originale. La debolezza di questo metodo è che il parametro a può assumere solo 25 valori diversi, e quindi non è difficile decifrare un messaggio anche senza conoscere a: è sufficiente tentare i valori di a in successione.

Solo nel XV secolo, per motivi politico-diplomatici, sono stati studiati altri metodi crittografici: i piú semplici fra questi sono dati dalle cifre monoalfabetiche, nelle quali f è data da un'opportuna permutazione dell'alfabeto, di solito scelta a partire da una *parola chiave* che deve rimanere segreta. In questo caso, evidentemente, si hanno a disposizione 26! possibili permutazioni dell'alfabeto (un netto miglioramento rispetto al metodo di Cesare) ma lo stesso il sistema crittografico è debole, e cede facilmente ad un'*analisi di frequenza*. In effetti, nella lingua italiana alcune vocali tendono ad essere molto piú frequenti delle altre lettere, ed un calcolo delle frequenze relative (anche di testi piuttosto corti) le rivela facilmente. Inoltre, sempre per l'italiano, è possibile sfruttare il fatto che quasi tutte le parole terminano con una vocale. Per una divertente descrizione delle debolezze delle cifre monoalfabetiche si veda il racconto *Lo scarabeo d'oro*, di Edgar Allan Poe.

Un'importante invenzione del XV secolo sono le cifre periodiche, cioè cifre del tipo $f(a_1, \ldots, a_k) = (f_1(a_1), \ldots, f_k(a_k))$: in pratica, il messaggio viene suddiviso in blocchi di k lettere, e a ciascuna lettera viene applicato un *diverso* metodo crittografico. Anche queste cifre, tuttavia, hanno la stessa debolezza della cifra monoalfabetica, perché le lettere che occupano posizioni che distano di un multiplo di k sono state cifrate con lo stesso alfabeto, e si può di nuovo utilizzare un'analisi di frequenza.

Piú difficili da attaccare, invece, sono le cifre in cui il blocco di k lettere viene considerato come un'unità e cifrato come tale. In ogni caso, a parte l'interesse storico, queste cifre sono state abbandonate perché non offrono garanzie di sicurezza né di velocità di cifratura/decifratura. A questi difetti, si deve aggiungere il fatto che i soggetti che vogliono comunicare devono quasi sempre concordare le *chiavi* (in un linguaggio piú matematico, i

parametri) dei sistemi crittografici, e questo, per definizione, non può avvenire per mezzo di un canale di trasmissione dei dati non sicuro. Questo spiega il successo dei moderni sistemi di crittografia, in cui i parametri del sistema crittografico sono resi pubblici. Come questa affermazione, apparentemente paradossale, possa essere realizzata nella pratica è l'argomento del prossimo paragrafo. Sorprendentemente, la matematica necessaria è nota fin dai tempi di Eulero.

Crittosistemi a chiave pubblica: RSA. L'idea chiave del sistema detto RSA (da Rivest, Shamir ed Adleman) è molto semplice: l'utente che chiameremo A sceglie due numeri primi grandi p e q, calcola una volta per tutte $n = p \cdot q$, $\varphi(n) = (p-1)(q-1) = n - p - q + 1$ e sceglie un intero e tale che $\big(e, \varphi(n)\big) = 1$. Infine, determina $d \in \mathbb{Z}_n^*$ tale che $e \cdot d \equiv 1 \mod \varphi(n)$. A rende nota la coppia (n, e) ma deve tenere segreti p, q e d. L'insieme dei messaggi è $\mathfrak{M} \stackrel{\text{def}}{=} \mathbb{Z}_n$. Chi voglia inviare un messaggio $M \in \mathfrak{M}$ ad A calcola $C = f(M) \stackrel{\text{def}}{=} M^e \mod n$ e lo trasmette. Per leggere il messaggio originale, A calcola $f^{-1}(C) \stackrel{\text{def}}{=} C^d \mod n$: infatti $C^d \equiv \big(M^e\big)^d \equiv M^{ed} \equiv M \mod n$ per il Teorema di Eulero 1.2.10. La sicurezza di questo sistema dipende in modo essenziale dalla difficoltà di scomporre n nei suoi fattori primi. La conoscenza di p e q permette di determinare d se è
𝔈 2.8.1 noto e e quindi di leggere i messaggi destinati all'utente A.

Firma digitale. Un altro problema di fondamentale importanza nella comunicazione fra soggetti distanti è la certificazione dell'identità. In altre parole, ogni utente di un crittosistema ha bisogno non solo di sapere che i messaggi a lui destinati non possono essere decifrati da altri, ma anche che chi scrive sia realmente chi dice di essere. Supponiamo dunque che l'utente A, con chiave pubblica (n_A, e_A) e funzione crittografica f_A voglia convincere della propria identità l'utente B, con chiave pubblica (n_B, e_B) e funzione crittografica f_B. Per raggiungere questo scopo, l'utente A sceglie una "firma digitale" s_A che rende pubblica: in pratica A sceglie $s_A \in \mathbb{Z}_{n_A}$. Per convincere B della propria identità invia una forma crittografata della firma, e precisamente

$$m_A \stackrel{\text{def}}{=} f_B\big(f_A^{-1}(s_A)\big) \quad \text{se } n_A < n_B; \qquad m_A \stackrel{\text{def}}{=} f_A^{-1}\big(f_B(s_A)\big) \quad \text{se } n_A > n_B,$$

dove f_A^{-1} ed f_B sono definite come nel sottoparagrafo precedente a partire da (n_A, e_A) e (n_B, e_B) rispettivamente. Per assicurarsi dell'identità di A, B calcola

$$f_A\big(f_B^{-1}(m_A)\big) \quad \text{se } n_A < n_B; \qquad f_B^{-1}\big(f_A(m_A)\big) \quad \text{se } n_A > n_B.$$

Tutto questo funziona perché solo A può eseguire f_A^{-1}, e solo B può eseguire f_B^{-1}.

Il crittosistema di Massey–Omura. Anche in questo caso ciascun utente del crittosistema sceglie e rende nota una parte dei parametri della propria funzione crittografica, ma non tutti. Tutti gli utenti decidono di utilizzare lo stesso numero primo grande p. Nel caso piú semplice, l'utente A sceglie $e_A \in \mathbb{Z}_p^*$ e ne calcola l'inverso $d_A \equiv e_A^{-1} \mod p-1$. L'utente B sceglie analogamente e_B e d_B in modo che $e_B d_B \equiv 1 \mod p-1$. Per spedire il messaggio $M \in \mathbb{Z}_p$ all'utente B, A calcola $C = f_A(M) \stackrel{\text{def}}{=} M^{e_A} \mod p$. B calcola $D = f_B(C) \stackrel{\text{def}}{=} C^{e_B} \mod p = M^{e_A e_B} \mod p$ e spedisce questo numero ad A, che a sua volta calcola $E = f_A^{-1}(D) \stackrel{\text{def}}{=} D^{d_A} \mod p = M^{e_B} \mod p$ e spedisce questo numero a B. A

Testo				M	$C = M^e \mod n$
M	Y	␣	M	346482	888745
I	S	T	R	232787	1201313
E	S	S	’	124768	1174612
␣	E	Y	E	787324	636449
S	␣	A	R	512117	227442
E	␣	N	O	134504	1999438
T	H	I	N	519553	483208
G	␣	L	I	188438	983073
K	E	␣	T	274489	1326351
H	E	␣	S	193488	151797
U	N	.	␣	552539	1507154

Tavola 2.4. *Codifica del messaggio “*MY␣MISTRESS’␣EYES␣ARE␣NOTHING␣LIKE␣THE␣SUN.␣*” per mezzo dell’alfabeto “*ABCDEFGHIJKLMNOPQRSTUVWXYZ,.’␣*” Il testo viene convertito in un equivalente numerico M come segue: la stringa* ABCD *viene letta come il numero in base 30* $\mathtt{A}\cdot 30^3+\mathtt{B}\cdot 30^2+\mathtt{C}\cdot 30+\mathtt{D}$*, e poi ad* A *viene assegnato il valore 0, a* B *il valore 1, e cosí via, dove* ␣ *sta per lo spazio ed ha equivalente numerico 29. Inoltre sono stati scelti i seguenti valori dei parametri:* $p = 1069$*,* $q = 1973$*,* $n = pq = 2109137$*,* $\varphi(n) = 2106096$*,* $e = 10001$*,* $d \equiv e^{-1} \mod \varphi(n) = 40433$*. (La frase citata è il primo verso del Sonetto 130 di W. Shakespeare).*

questo punto B calcola $f_B^{-1}(E) \stackrel{\text{def}}{=} E^{d_B} \mod p = M \mod p$ e quindi può leggere il messaggio originale. Si deve però osservare che è necessario utilizzare anche un sistema di firma digitale, perché altrimenti un terzo utilizzatore potrebbe fingere di essere B e leggere i messaggi relativi.

§2.9. Calcolo di prodotti e potenze modulo N

Parliamo ora brevemente di due algoritmi che, pur non essendo a stretto rigore relativi alla Teoria dei Numeri, sono nondimeno essenziali per realizzare quanto presentato sopra.

L’algoritmo del prodotto. L’algoritmo del prodotto $m \cdot n$ è illustrato nella Tavola 2.5: si assegnano i valori iniziali $S \leftarrow 0$, $A \leftarrow m$, $B \leftarrow n$. Ad ogni passo si determinano q ed r (quoziente e resto della divisione di A per 2) in modo che $A = 2 \cdot q + r$, con $r \in \{0, 1\}$. Se $r = 1$ poniamo $S \leftarrow S + B$. Infine poniamo $A \leftarrow q$, $B \leftarrow 2 \cdot B$. Se $q = 0$ l’algoritmo termina ed S vale $m \cdot n$. Non è difficile dimostrare che al termine di ogni ciclo si ha sempre $m \cdot n = S + A \cdot B$. Questo algoritmo è particolarmente utile quando si devono fare calcoli modulo un numero molto grande N: facendo seguire ad ogni operazione di somma o prodotto il calcolo del resto $\mod N$, si può fare in modo che tutti i risultati parziali del calcolo siano $\leq 2N$. Inoltre, se invece di prendere il minimo resto positivo, si prende il minimo resto in valore assoluto (cioè, se quando il resto $r \in \left[\frac{1}{2}N, N\right]$ si sceglie $r' \stackrel{\text{def}}{=} r - N \in \left[-\frac{1}{2}N, 0\right]$), tutti i risultati parziali dei calcoli sono, in valore assoluto, $\leq N$.

L’algoritmo delle potenze. Un algoritmo analogo permette il calcolo delle potenze in modo molto efficiente. L’idea di base è molto semplice: per calcolare a^m, dove $m \in \mathbb{N}^*$, scriviamo a^m come un prodotto di potenze con base a il cui esponente sia una potenza di 2. Per esempio, se $m = 11$ allora $a^{11} = a^8 \cdot a^2 \cdot a$. Per trovare gli esponenti è sufficiente scrivere il

q	r	S	A	B
		0	27	41
13	1	$0+41=41$	13	82
6	1	$41+82=123$	6	164
3	0	123	3	328
1	1	$123+328=451$	1	656
0	1	$451+656=1107$	0	1312

Tavola 2.5. *Calcolo del prodotto* $27\cdot 41$. *Nella prima riga vengono assegnati ad* S, A *ed* B *i rispettivi valori iniziali. Dalla seconda riga in avanti i calcoli sono eseguiti da sinistra a destra secondo le regole date nel testo. Si osservi che alla fine di ogni ciclo si ha sempre* $m\cdot n = S + A\cdot B$.

q	r	P	M	A
		1	11	a
5	1	$1\cdot a = a$	5	a^2
2	1	$a\cdot a^2 = a^3$	2	a^4
1	0	a^3	1	a^8
0	1	$a^3\cdot a^8 = a^{11}$	0	

Tavola 2.6. *Calcolo della potenza* a^{11}. *Nella prima riga vengono assegnati a* P, M *ed* A *i rispettivi valori iniziali. Dalla seconda riga in avanti i calcoli sono eseguiti da sinistra a destra secondo le regole date nel testo. Si osservi che alla fine di ogni ciclo si ha sempre* $a^{11} = P\cdot A^M$.

numero m in binario: in questo caso $11_{10} = 1011_2$. Il vantaggio è che ciascun termine della successione a, a^2, a^4, a^8, $\dots$, si ottiene dal precedente mediante un elevamento al quadrato. Quindi, per determinare a^{11} basta calcolare a^2, a^4, a^8 (tre elevamenti al quadrato) e poi moltiplicare a per a^2 per a^8, per un totale di 5 moltiplicazioni, invece delle 10 necessarie per eseguire il calcolo nel modo consueto. Il numero totale delle moltiplicazioni è $\mathcal{O}(\log m)$.

In pratica non è neppure necessario scrivere m in binario, ed è possibile procedere come nella Tavola 2.6: iniziamo col porre $P\leftarrow 1$, $M\leftarrow m$, $A\leftarrow a$. Come sopra, calcoliamo q ed r rispettivamente quoziente e resto della divisione euclidea di M per 2. Se $r=1$ poniamo $P\leftarrow P\cdot A$. Infine poniamo $A\leftarrow A^2$, $M\leftarrow q$ e ricominciamo da capo se $M>0$; se invece $M=0$ allora $P=a^m$ ed il calcolo termina. Osserviamo infine che per calcolare potenze modulo N è sufficiente far seguire ad ogni operazione di prodotto (incluso il calcolo di A^2) la divisione euclidea del risultato per N ed in questo modo non compaiono mai numeri piú grandi di N^2. Usando invece l'algoritmo del prodotto con gli accorgimenti indicati qui sopra, si può fare in modo che tutti i risultati parziali siano $\le N$ in valore assoluto.

Capitolo 3. Funzioni Aritmetiche

§3.1. Definizioni e prime proprietà

Definizione 3.1.1. *Si dice* funzione aritmetica *una qualsiasi applicazione* $f\colon \mathbb{N}^* \to \mathbb{C}$. *Per* $n \in \mathbb{N}^*$, $\beta \in \mathbb{C}$ *e* $k \in \mathbb{N}^*$ *consideriamo le funzioni aritmetiche elementari*

$$N_\beta(n) \stackrel{\text{def}}{=} n^\beta \qquad \varphi(n) \stackrel{\text{def}}{=} \left|\mathbb{Z}_n^*\right|$$

$$\sigma_\beta(n) \stackrel{\text{def}}{=} \sum_{d|n} d^\beta \qquad d(n) \stackrel{\text{def}}{=} \sigma_0(n) = \sum_{d|n} 1 = \left|\{d \in \mathbb{N}^*\colon d \mid n\}\right|$$

$$\omega(n) \stackrel{\text{def}}{=} \sum_{p|n} 1 \qquad \Omega(n) \stackrel{\text{def}}{=} \sum_{p^\alpha \| n} \alpha$$

$$L(n) \stackrel{\text{def}}{=} \log n \qquad r_k(n) \stackrel{\text{def}}{=} \left|\{(x_1, \dots, x_k) \in \mathbb{Z}^k\colon n = x_1^2 + \cdots + x_k^2\}\right|$$

$$I(n) \stackrel{\text{def}}{=} \left[\frac{1}{n}\right] = \begin{cases} 1 & \text{se } n = 1 \\ 0 & \text{se } n > 1 \end{cases} \qquad \Lambda(n) \stackrel{\text{def}}{=} \begin{cases} \log p & \text{se } \exists p, \exists m \in \mathbb{N}^* \text{ tali che } n = p^m \\ 0 & \text{altrimenti.} \end{cases}$$

Definizione 3.1.2. *Date due funzioni aritmetiche* f *e* g *chiamiamo* prodotto di convoluzione o di Dirichlet *di* f *e* g *la funzione aritmetica* h *definita dalla relazione*

$$h(n) \stackrel{\text{def}}{=} (f * g)(n) \stackrel{\text{def}}{=} \sum_{d|n} f(d)\, g\left(\frac{n}{d}\right) = \sum_{d_1 d_2 = n} f(d_1) g(d_2).$$

Definizione 3.1.3. *Una funzione aritmetica* f *si dice* moltiplicativa *se* $f(1) = 1$ *e per ogni* n, $m \in \mathbb{N}^*$ *con* $(n, m) = 1$ *si ha* $f(nm) = f(n)f(m)$. *Se questo vale per ogni* n, $m \in \mathbb{N}^*$, f *si dice* completamente moltiplicativa. *Indicheremo con* $\mathfrak{M}$ *ed* $\mathfrak{M}^*$ *rispettivamente l'insieme delle funzioni moltiplicative e quello delle funzioni completamente moltiplicative.*

Per esempio, le funzioni φ, d, $\sigma_k \in \mathfrak{M}$, I, $N_\beta \in \mathfrak{M}^*$, cosí come $\left(\cdot \mid p\right)$ è completamente moltiplicativa per ogni primo p fissato, mentre Λ, ω, Ω ed L non sono moltiplicative (ma, ovviamente, $e^\omega \in \mathfrak{M}$, mentre $e^L = N_1$, $e^\Omega \in \mathfrak{M}^*$).

𝔈 3.1.1

𝔈 3.1.2

TEOREMA 3.1.4. *Se f, $g \in \mathfrak{M}$ allora anche $f * g \in \mathfrak{M}$.*

DIM.: Sia $h = f * g$ e siano n, $m \in \mathbb{N}^*$ tali che $(n,m) = 1$. Osserviamo che se $d \mid nm$, sono univocamente determinati d_1, $d_2 \in \mathbb{N}^*$ tali che $d_1 \mid n$, $d_2 \mid m$ e $d_1 d_2 = d$. Inoltre, ovviamente, $(d_1, d_2) = 1$. Quindi

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

□

𝔈 3.1.3 Osserviamo però che se f, $g \in \mathfrak{M}^*$, non è detto che $f * g \in \mathfrak{M}^*$, come $d = N_0 * N_0$.

LEMMA 3.1.5. *Sia $f \in \mathfrak{M}$. Valgono le seguenti relazioni:*

$$\text{se} \qquad n = \prod_{i=1}^{k} p_i^{\alpha_i} \quad \text{allora} \quad f(n) = \prod_{i=1}^{k} f\big(p_i^{\alpha_i}\big) \quad \text{e} \quad \sum_{d \mid n} f(d) = \prod_{i=1}^{k} \sum_{j=0}^{\alpha_i} f\big(p_i^j\big).$$

DIM.: La prima segue immediatamente dalla definizione di moltiplicatività, mentre nella seconda entrambi i membri sono uguali ad $(f * N_0)(n)$, per il Teorema 3.1.4. □

TEOREMA 3.1.6. *L'insieme delle funzioni aritmetiche con l'operazione $*$ è un anello commutativo con identità I. Gli elementi invertibili sono le funzioni aritmetiche f tali che $f(1) \neq 0$, e per queste la funzione inversa (che indichiamo con f^{-1}) soddisfa*

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

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

DIM.: La proprietà commutativa ed il fatto che I sia l'identità seguono immediatamente dalla definizione. Per dimostrare la proprietà associativa, osserviamo che

$$\begin{aligned} \big((f * g) * h\big)(n) &= \sum_{d_1 d_2 = n} (f * g)(d_1) h(d_2) = \sum_{d_1 d_2 = n} \sum_{\delta_1 \delta_2 = d_1} f(\delta_1) g(\delta_2) h(d_2) \\ &= \sum_{\delta_1 \delta_2 \delta_3 = n} f(\delta_1) g(\delta_2) h(\delta_3) = \big(f * (g * h)\big)(n). \end{aligned}$$

Ora vogliamo dimostrare che se $f(1) \neq 0$ allora esiste una funzione aritmetica tale che $f * f^{-1} = f^{-1} * f = I$. Poiché vogliamo avere $\big(f * f^{-1}\big)(1) = 1$, deve necessariamente essere $f^{-1}(1) = 1/f(1)$. Ora supponiamo per induzione che f^{-1} sia univocamente determinata per $1 \leq k < n$. Poiché vogliamo risolvere $\big(f * f^{-1}\big)(n) = 0$, si deve avere

$$\sum_{d \mid n} f\left(\frac{n}{d}\right) f^{-1}(d) = 0 \quad \Rightarrow \quad f(1) f^{-1}(n) = -\sum_{d \mid n,\, d<n} f\left(\frac{n}{d}\right) f^{-1}(d), \tag{3.1.1}$$

come si voleva. Dunque se $f \in \mathfrak{M}$ allora $f(1) = f^{-1}(1) = 1$. Scegliamo ora due interi n, m primi fra loro tali che $nm > 1$, e supponiamo di aver dimostrato che $f^{-1}(ab) = f^{-1}(a)f^{-1}(b)$ per tutti gli interi a, b tali che $(a,b) = 1$ ed $ab < nm$. Per la (3.1.1), procedendo come nella dimostrazione del Teorema 3.1.4, si ha

$$\begin{aligned} f^{-1}(nm) &= -\sum_{\substack{d|nm \\ d<nm}} f\left(\frac{nm}{d}\right) f^{-1}(d) = -\sum_{\substack{d_1|n\ d_2|m \\ d_1 d_2<nm}}\sum f\left(\frac{n}{d_1}\right) f\left(\frac{m}{d_2}\right) f^{-1}(d_1)f^{-1}(d_2) \\ &= -\sum_{d_1|n} f\left(\frac{n}{d_1}\right) f^{-1}(d_1) \sum_{d_2|m} f\left(\frac{m}{d_2}\right) f^{-1}(d_2) + f^{-1}(n)f^{-1}(m) \\ &= -I(n)I(m) + f^{-1}(n)f^{-1}(m) = f^{-1}(n)f^{-1}(m). \end{aligned}$$

□

Corollario 3.1.7. *Se f, $f * g \in \mathfrak{M}$, allora anche $g \in \mathfrak{M}$.*

Dim.: $g = f^{-1} * (f * g)$ è prodotto di funzioni moltiplicative. □

Definizione 3.1.8. *Si dice* funzione μ di Möbius *la funzione aritmetica $\mu \in \mathfrak{M}$ data da:*

$$\text{se} \quad n = \prod_{i=1}^{k} p_i^{\alpha_i} \quad \text{allora} \quad \mu(n) \stackrel{\text{def}}{=} \begin{cases} 1 & \text{se } n = 1, \\ 0 & \text{se } \alpha_i \geq 2 \text{ per qualche } i \in \{1, \dots, k\}, \\ (-1)^k & \text{se } \alpha_i = 1 \text{ per ogni } i \in \{1, \dots, k\}. \end{cases}$$

𝔈 3.1.4 Teorema 3.1.9. *Si ha $N_0 * \mu = I$, cioè $\mu = N_0^{-1}$.*

Dim.: L'uguaglianza desiderata vale quando n è potenza di un numero primo: se $\alpha \geq 1$

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

poiché tutti gli eventuali altri addendi sono nulli. La tesi segue dal Lemma 3.1.5. □

Corollario 3.1.10. *Se $f \in \mathfrak{M}^*$, allora $f^{-1} = \mu f$.*

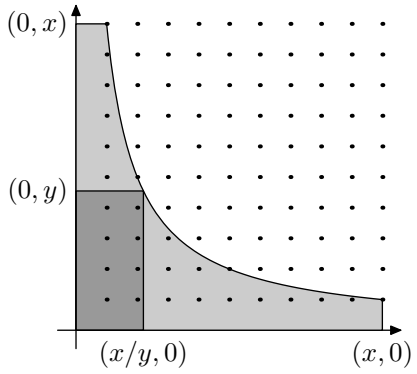
Dim.: A causa della completa moltiplicatività, per $\alpha \geq 1$ si ha

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

□

Corollario 3.1.11 (Prima formula di inversione di Möbius). *Se f e g sono funzioni aritmetiche allora $f = g * \mu$ se e solo se $g = f * N_0$.*

Dim.: Partendo da $f = g * \mu$, moltiplichiamo ambo i membri per N_0, ottenendo $f * N_0 = (g * \mu) * N_0 = g * (\mu * N_0) = g * I = g$, e viceversa. □



Al punto di coordinate (h,k) con $h,\ k\in\mathbb{N}^*$ si associ $f(h)g(k)$ che è un addendo della somma per $n=hk$, $d=h$. Le tre quantità a secondo membro nel Teorema 3.1.13 sono le $\Sigma f(h)g(k)$ estese rispettivamente agli insiemi
$\{1\le k\le y,\ 1\le hk\le x\}$,
$\{1\le h\le x/y,\ 1\le hk\le x\}$,
$\{1\le h\le x/y,\ 1\le k\le y\}$.

Figura 3.1. *Dimostrazione del Teorema* 3.1.13.

TEOREMA 3.1.12 (SECONDA FORMULA DI INVERSIONE DI MÖBIUS). *Se $h\in\mathfrak{M}$, allora*

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

DIM.: Infatti si ha

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

𝔈 3.1.5 L'implicazione inversa si dimostra scambiando f e g. □

TEOREMA 3.1.13 (METODO DELL'IPERBOLE DI DIRICHLET). *Siano f e g funzioni aritmetiche e poniamo*

$$F(x)\stackrel{\text{def}}{=}\sum_{n\le x}f(n)\qquad e\qquad G(x)\stackrel{\text{def}}{=}\sum_{n\le x}g(n).$$

Per ogni $y\in[1,x]$ si ha

$$\sum_{n\le x}f*g(n)=\sum_{n\le y}F\left(\frac{x}{n}\right)g(n)+\sum_{n\le x/y}f(n)G\left(\frac{x}{n}\right)-F\left(\frac{x}{y}\right)G(y).$$

In particolare, scegliendo $y=x$ ed $y=1$ rispettivamente, si ha

$$\sum_{n\le x}f*g(n)=\sum_{n\le x}F\left(\frac{x}{n}\right)g(n)=\sum_{n\le x}f(n)G\left(\frac{x}{n}\right).$$

DIM.: Infatti

$$\begin{aligned}\sum_{1\le n\le x}f*g(n)&=\sum_{1\le n\le x}\sum_{hk=n}f(h)g(k)=\sum_{1\le k\le y}g(k)\sum_{1\le h\le x/k}f(h)+\sum_{y<k\le x}\sum_{1\le h\le x/k}f(h)g(k)\\&=\sum_{1\le k\le y}F\left(\frac{x}{k}\right)g(k)+\sum_{1\le h\le x/y}\sum_{y<k\le x/h}f(h)g(k)\\&=\sum_{1\le k\le y}F\left(\frac{x}{k}\right)g(k)+\sum_{1\le h\le x/y}f(h)\left(G\left(\frac{x}{h}\right)-G(y)\right)\\&=\sum_{1\le k\le y}F\left(\frac{x}{k}\right)g(k)+\sum_{1\le h\le x/y}f(h)G\left(\frac{x}{h}\right)-F\left(\frac{x}{y}\right)G(y).\end{aligned}$$

□

§3.2. Le funzioni r_2, d, σ_k, φ, Λ e c_q

Teorema 3.2.1. *La funzione r_2 non è moltiplicativa. Inoltre, si ha*

$$\liminf_{n\to\infty} r_2(n) = 0 \qquad e \qquad \limsup_{n\to\infty} r_2(n) = +\infty.$$

Dim.: $r_2 \notin \mathfrak{M}$ poiché $r_2(1) = 4$, $(1 = 0^2 + (\pm1)^2 = (\pm1)^2 + 0^2)$, ma osserviamo che $\frac14 r_2$ lo è: cfr Teorema 5.5.1. La seconda affermazione segue dal fatto che $r_2(4n+3) = 0$ per ogni $n \in \mathbb{N}$, poiché $x^2 \equiv 0,\ 1 \bmod 4$, e dunque $x^2 + y^2 \equiv 0,\ 1,\ 2 \bmod 4$.

Dimostreremo la terza provando che se $p \equiv 1 \mod 4$, allora $r_2\big(p^\alpha\big) \geq 4\alpha + 4$. Questo è certamente vero per $\alpha = 0$, dato che $1 = 0^2 + (\pm1)^2 = (\pm1)^2 + 0^2$. Ricordiamo inoltre che, per il Teorema 1.4.9, esistono $a,\ b \in \mathbb{N}^*$ tali che $p = a^2 + b^2$ e $p \nmid ab$. Supponiamo dunque che per ogni numero naturale $\beta \leq \alpha+1$ si abbia $r_2\big(p^\beta\big) \geq 4(\beta+1)$ e che inoltre se $\beta \geq 1$ almeno una di queste rappresentazioni sia primitiva. Per dimostrare che $r_2\big(p^{\alpha+2}\big) \geq 4\alpha + 12$, moltiplichiamo le rappresentazioni $a_i^2 + b_i^2$ di p^α per p^2, in modo che $(pa_i)^2 + (pb_i)^2$ siano rappresentazioni distinte (non primitive) di $p^{\alpha+2}$. Inoltre, sempre per ipotesi induttiva, $p^{\alpha+1}$ ha almeno una rappresentazione primitiva, diciamo $c^2 + d^2$, con $p \nmid cd$. Usando la formula (1.4.1), possiamo costruire le rappresentazioni $p^{\alpha+2} = (ac \pm bd)^2 + (ad \mp bc)^2$. Resta da dimostrare che almeno una di queste è primitiva: ma se entrambe non lo fossero, allora $p \mid ac + bd$ e $p \mid ac - bd$, da cui $p \mid 2ac$ e $p \mid 2bd$, il che è assurdo perché avevamo supposto che $p \nmid 2abcd$. Questa rappresentazione primitiva, per simmetrie e cambiamenti di segno, ne fornisce 8, distinte fra loro e da tutte quelle contate prima, perché non primitive. In totale, quindi $r_2\big(p^{\alpha+2}\big) \geq r_2\big(p^\alpha\big) + 8 \geq 4\alpha + 12$, per induzione. □

𝔈 3.2.1–2

Teorema 3.2.2 (Gauss). *Per $x \to \infty$ si ha*

$$R_2(x) \stackrel{\text{def}}{=} \sum_{n\leq x} r_2(n) = \pi x + \mathcal{O}\Big(x^{1/2}\Big).$$

Dim.: A ciascuna coppia di interi (a, b) associamo in modo univoco il quadrato $Q(a, b)$ di vertici $\big(a - \frac12, b - \frac12\big)$, $\big(a + \frac12, b - \frac12\big)$, $\big(a + \frac12, b + \frac12\big)$, $\big(a - \frac12, b + \frac12\big)$. In altre parole $Q(a, b)$ è il quadrato di centro (a, b) con lati di lunghezza 1 e paralleli agli assi coordinati. In questo modo, posto per brevità

$$U(x) \stackrel{\text{def}}{=} \bigcup_{\substack{a,b\in\mathbb{Z}\\ a^2+b^2\leq x}} Q(a, b), \qquad \text{si ha} \qquad R_2(x) = \sum_{\substack{a,b\in\mathbb{Z}\\ a^2+b^2\leq x}} 1 = \iint_{U(x)} \mathrm{d}u\,\mathrm{d}v.$$

Consideriamo i cerchi C_1 e C_2 di centro l'origine e raggio $R_1 = \sqrt{x} - \sqrt{2}$ ed $R_2 = \sqrt{x} + \sqrt{2}$, rispettivamente. È chiaro che $C_1 \subseteq U(x) \subseteq C_2$, e quindi $\pi R_1^2 \leq \iint_{U(x)} \mathrm{d}u\,\mathrm{d}v \leq \pi R_2^2$. Ma $\pi R^2 = \pi x + \mathcal{O}\big(x^{1/2}\big)$ sia per $R = R_1$ che per $R = R_2$, ed il risultato voluto segue. □

𝔈 3.2.3

Teorema 3.2.3 (Landau). *Per $x \to +\infty$ si ha*

$$R_2'(x) \stackrel{\text{def}}{=} |\{n \leq x \colon r_2(n) \geq 1\}| \sim \frac{x}{(K \log x)^{1/2}} \quad \textit{dove} \quad K \stackrel{\text{def}}{=} 2 \prod_{p\equiv 3 \bmod 4} \left(1 - \frac{1}{p^2}\right).$$

𝔈 3.2.4 Si vedano anche il Teorema 5.5.1 e il Capitolo 6. A questo punto è opportuno leggere le Appendici 1 e 4.

TEOREMA 3.2.4. *La funzione $d \in \mathfrak{M}$, e $d(p^\alpha) = \alpha + 1$. Inoltre*

$$\liminf_{n\to\infty} d(n) = 2 \qquad \text{e per ogni } \Delta \in \mathbb{R} \text{ si ha} \quad \limsup_{n\to\infty} \frac{d(n)}{(\log n)^\Delta} = +\infty.$$

In altre parole $d(n) = \Omega_+\big((\log n)^\Delta\big)$.

DIM.: Per la moltiplicatività è sufficiente osservare che per definizione $d = N_0 * N_0$. Inoltre $d \mid p^\alpha$ se e solo se $d = p^\beta$ con $\beta \in \{0, \dots, \alpha\}$. L'affermazione sul minimo limite segue dal fatto che $d(p) = 2$ per ogni numero primo p e che $d(n) \geq 2$ per ogni $n \geq 2$.

Infine, dato $\Delta \in \mathbb{R}^+$, sia $k \in \mathbb{N}$ tale che $k - 1 \leq \Delta < k$, p_i l'i-esimo numero primo ed $n \stackrel{\text{def}}{=} p_1 \cdots p_k$. Per quanto già dimostrato, $d(n^m) = (m+1)^k > m^k$, e quindi

$$\frac{d(n^m)}{\big(\log(n^m)\big)^k} > \left\{ \frac{m}{m \log(p_1 \cdots p_k)} \right\}^k = c(k),$$

𝔈 3.2.6 dove $c(k) > 0$ è una costante che dipende solo da k. Poniamo $\delta \stackrel{\text{def}}{=} k - \Delta > 0$. Dunque

$$d(n^m) > c(k)\big(\log(n^m)\big)^{\Delta+\delta} \qquad \text{da cui} \qquad \frac{d(n^m)}{\big(\log(n^m)\big)^\Delta} > c(k)\big(\log(n^m)\big)^\delta.$$

□

TEOREMA 3.2.5 (DIRICHLET). *Sia γ la costante di Eulero. Per $x \to +\infty$ si ha*

$$D(x) \stackrel{\text{def}}{=} \sum_{n\leq x} d(n) = x \log x + (2\gamma - 1)x + \mathcal{O}\Big(x^{1/2}\Big).$$

𝔈 3.2.8 DIM.: Segue dal Teorema 3.1.13 con $y = x^{1/2}$ e dal Teorema A.4.1 nel caso $k = -1$. □

TEOREMA 3.2.6. *Si ha $\sigma_k \in \mathfrak{M}$ per ogni $k \in \mathbb{C}$. Inoltre, per $k \neq 0$,*

$$\sigma_k(n) = \prod_{p^\alpha \| n} \frac{p^{k(\alpha+1)} - 1}{p^k - 1}.$$

DIM.: Basta osservare che $\sigma_k = N_0 * N_k$ e che per $k \neq 0$

$$\sigma_k(p^\alpha) = \sum_{\beta=0}^{\alpha} p^{k\beta} = \frac{p^{k(\alpha+1)} - 1}{p^k - 1},$$

𝔈 3.2.9 ed il risultato segue dal Lemma 3.1.5. □

Osservazione 3.2.7 (Eulero). *Se esistessero un numero finito di primi $p_1, \dots, p_r$, posto $M \stackrel{\text{def}}{=} p_1 \cdots p_r$, si avrebbe $\varphi(M) = 1$, dato che ogni intero > 1 dovrebbe essere divisibile per un fattore di M, ma per $M \geq 3$ si ha $\varphi(M) \geq 2$, poiché $(1, M) = (M - 1, M) = 1$.*

Teorema 3.2.8. *La funzione $\varphi \in \mathfrak{M}$, e $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$. Inoltre $\varphi = N_1 * \mu$,*

$$\limsup_{n\to\infty} \frac{\varphi(n)}{n} = 1 \qquad e \qquad \frac{\varphi(n)}{n} = \prod_{p|n} \left(1 - \frac{1}{p}\right).$$

Dim.: Per dimostrare che $\varphi \in \mathfrak{M}$ siano n, $m \in \mathbb{N}^*$ primi fra loro. Facciamo vedere che esiste una biiezione $f\colon \mathbb{Z}_n^* \times \mathbb{Z}_m^* \to \mathbb{Z}_{nm}^*$. Se $(a, b) \in \mathbb{Z}_n^* \times \mathbb{Z}_m^*$ poniamo $f(a, b) \stackrel{\text{def}}{=} am + bn \mod nm$. È chiaro che f è iniettiva: se $am + bn \equiv \alpha m + \beta n \mod nm$ allora $bn \equiv \beta n \mod m$ e quindi $b \equiv \beta \mod m$, ed allo stesso modo $a \equiv \alpha \mod n$. Per dimostrare che f è suriettiva, ricordiamo che per il Lemma 1.1.1 esistono λ, $\mu \in \mathbb{Z}$ tali che $\lambda n + \mu m = 1$: se $r \in \mathbb{Z}_{nm}^*$, si vede subito che $f(r\mu, r\lambda) = r$.

Per determinare $\varphi(p^\alpha)$ contiamo quanti interi $\in [1, p^\alpha]$ sono primi con p^α, cioè con p: gli interi non primi con p sono tutti e soli quelli divisibili per p e nell'intervallo in questione ce ne sono esattamente $p^{\alpha-1}$. Per dimostrare che $\varphi = N_1 * \mu$ osserviamo che N_1, $\mu \in \mathfrak{M}$, e quindi dobbiamo verificare quest'uguaglianza quando $n = p^\alpha$. In questo caso abbiamo

$$(N_1 * \mu)(p^\alpha) = \sum_{\beta=0}^{\alpha} p^\beta \mu(p^{\alpha-\beta}) = p^\alpha - p^{\alpha-1} = \varphi(p^\alpha),$$

dato che tutti gli eventuali altri addendi sono nulli. Osserviamo che abbiamo già dimostrato la relazione equivalente $N_1 = \varphi * N_0$ nel Lemma 1.2.12. L'affermazione sul massimo limite segue dal fatto che $\varphi(p) = p - 1$ per ogni primo p, e che $\varphi(n) \leq n$ per ogni intero $n \in \mathbb{N}^*$.
𝔈 3.2.10–12 L'ultima affermazione è una riscrittura delle proprietà appena dimostrate. □

Lemma 3.2.9. *Si ha $\Lambda = L * \mu$ o, equivalentemente, $L = \Lambda * N_0$.*

Dim.: Le due relazioni sono evidentemente equivalenti in virtú della prima formula di inversione di Möbius 3.1.11. Inoltre, se $n = \prod_{i=1}^k p_i^{\alpha_i}$, si ha

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

poiché Λ è diversa da 0 solo sulle potenze dei numeri primi. □

Corollario 3.2.10. *Si ha*

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

Dim.: Infatti, dato che $I(n) \log n = 0$ per ogni $n \in \mathbb{N}^*$, si ha

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

□

Teorema 3.2.11 (Ramanujan). *La funzione di Ramanujan $c_q(n)$ definita qui sotto è una funzione moltiplicativa di q e si ha*

$$c_q(n) \stackrel{\text{def}}{=} \sum_{h=1}^{q}{}^{*} e\big(\tfrac{hn}{q}\big) = \mu\left(\frac{q}{(q,n)}\right) \frac{\varphi(q)}{\varphi\left(q/(q,n)\right)}.$$

Dim.: Siano $q_1, q_2 \in \mathbb{N}^*$ tali che $(q_1, q_2) = 1$. Per il Teorema 1.2.4 si ha $\mathbb{Z}^*_{q_1 q_2} \simeq \{a_2 q_1 + a_1 q_2 \bmod q_1 q_2 \colon a_1 \in \mathbb{Z}^*_{q_1},\ a_2 \in \mathbb{Z}^*_{q_2}\}$. Dunque

$$c_{q_1 q_2}(n) = \sum_{a_1=1}^{q_1}{}^{*} \sum_{a_2=1}^{q_2}{}^{*} e\big(\tfrac{a_1 n}{q_1} + \tfrac{a_2 n}{q_2}\big) = c_{q_1}(n) c_{q_2}(n),$$

cioè $c_q \in \mathfrak{M}$. Per l'Osservazione 1.2.11 si ha

$$f_n(q) \stackrel{\text{def}}{=} \sum_{h=1}^{q} e\big(\tfrac{hn}{q}\big) = \sum_{d|q} \sum_{a=1}^{d}{}^{*} e\big(\tfrac{an}{d}\big) = \sum_{d|q} c_d(n).$$

Inoltre $f_n(q) = 0$ se $q \nmid n$ ed $f_n(q) = q$ se $q \mid n$. Per la Prima Formula di Möbius 3.1.11

$$c_q(n) = \sum_{d|q} \mu\left(\frac{q}{d}\right) \sum_{a=1}^{d} e\big(\tfrac{an}{d}\big) = \sum_{d|q,\, d|n} \mu\left(\frac{q}{d}\right) d.$$

Prendiamo $q = p^\alpha$ dove p è primo, $\alpha \geq 1$, e $p^\beta = (q, n)$, con $0 \leq \beta \leq \alpha$. La tesi è ora

$$\sum_{\gamma=0}^{\beta} \mu\big(p^{\alpha-\gamma}\big) p^\gamma = \mu\big(p^{\alpha-\beta}\big) \frac{\varphi\big(p^\alpha\big)}{\varphi\big(p^{\alpha-\beta}\big)}$$

e questo si vede facilmente distinguendo vari casi: se $\alpha \geq \beta + 2$ entrambe le espressioni valgono 0. Se $\alpha = \beta + 1$ entrambe valgono $-p^{\alpha-1}$ e se $\alpha = \beta$ valgono $\varphi\big(p^\alpha\big)$. □

§3.3. Il prodotto di Eulero

Teorema 3.3.1 (Prodotto di Eulero). *Sia $f \in \mathfrak{M}$ una funzione aritmetica moltiplicativa tale che $\sum_{n\geq 1} f(n)$ sia assolutamente convergente. Vale l'identità*

$$\sum_{n\geq 1} f(n) = \prod_p \Big(1 + f(p) + f\big(p^2\big) + f\big(p^3\big) + \cdots\Big),$$

dove il prodotto è esteso a tutti i primi ed è assolutamente convergente. Inoltre se $f \in \mathfrak{M}^*$

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

DIM.: Si ha $f(1) = 1$ poiché f è moltiplicativa. Poniamo

$$S \overset{\text{def}}{=} \sum_{n\geq 1} f(n) \qquad \text{e} \qquad P(x) \overset{\text{def}}{=} \prod_{p\leq x} \Big(1 + f(p) + f\big(p^2\big) + f\big(p^3\big) + \cdots\Big).$$

Poiché P è prodotto di un numero finito di serie assolutamente convergenti, possiamo moltiplicarle fra loro e riordinare i termini. Posto $\mathcal{A}(x) \overset{\text{def}}{=} \{n \in \mathbb{N}^* : p \mid n \Rightarrow p \leq x\}$, si ha

$$P(x) = \sum_{n\in\mathcal{A}(x)} f(n) \qquad \text{e quindi} \qquad S - P(x) = \sum_{n\notin\mathcal{A}(x)} f(n).$$

È chiaro che ogni n contato in quest'ultima somma è $> x$ e dunque

$$\Big|S - P(x)\Big| \leq \sum_{n\notin\mathcal{A}(x)} \big|f(n)\big| \leq \sum_{n>x} \big|f(n)\big|.$$

La prima parte della tesi segue per $x \to +\infty$. Il prodotto converge assolutamente poiché

$$\left|\sum_p \Big(f(p) + f\big(p^2\big) + f\big(p^3\big) + \cdots\Big)\right| \leq \sum_p \Big(|f(p)| + |f\big(p^2\big)| + |f\big(p^3\big)| + \cdots\Big) \leq \sum_{n\geq 1} |f(n)|.$$

Se poi $f \in \mathfrak{M}^*$, allora $f\big(p^n\big) = f(p)^n$ ed inoltre, per l'ultima disuguaglianza, $|f(p)| < 1$, altrimenti $|f(p)|+|f(p)|^2+\cdots$ divergerebbe. L'ultima affermazione segue immediatamente.

Diamo anche una dimostrazione alternativa della prima parte: per la convergenza assoluta possiamo raggruppare tutti gli interi che sono divisibili per la stessa potenza di 2:

$$\sum_{n\geq 1} f(n) = \sum_{\nu\geq 0} \sum_{\substack{n\geq 1 \\ 2^\nu \| n}} f(n) = \sum_{\nu\geq 0} f\big(2^\nu\big) \sum_{\substack{m\geq 1 \\ 2\nmid m}} f(m).$$

Analogamente, nell'ultima somma a destra raggruppiamo tutti gli interi che sono divisibili per la stessa potenza di 3:

$$\sum_{n\geq 1} f(n) = \Big(\sum_{\nu\geq 0} f\big(2^\nu\big)\Big) \sum_{\nu\geq 0} \sum_{\substack{n\geq 1 \\ 2\nmid n,\, 3^\nu \| n}} f(n) = \Big(\sum_{\nu\geq 0} f\big(2^\nu\big)\Big)\Big(\sum_{\nu\geq 0} f\big(3^\nu\big)\Big) \sum_{\substack{m\geq 1 \\ (2\cdot 3, m)=1}} f(m).$$

Iterando lo stesso ragionamento per i primi k numeri primi $p_1 = 2, \ldots, p_k$, si ha

$$\sum_{n\geq 1} f(n) = \Big(\prod_{j=1}^{k} \sum_{\nu\geq 0} f\big(p_j^\nu\big)\Big) \sum_{\substack{m\geq 1 \\ p\mid m \Rightarrow p > p_k}} f(m). \tag{3.3.1}$$

Evidentemente

$$\Big|\sum_{\substack{m\geq 1 \\ p\mid m \Rightarrow p > p_k}} f(m) - 1\Big| \leq \sum_{n > p_k} |f(n)| \tag{3.3.2}$$

da cui, sempre per la convergenza assoluta, si ha la tesi poiché

$$\lim_{k\to+\infty} \sum_{\substack{m\geq 1\\ p|m\Rightarrow p>p_k}} f(m) = 1. \tag{3.3.3}$$

In generale, la (3.3.1) e la (3.3.3) mostrano che la serie dell'enunciato può annullarsi solo se si annulla uno dei fattori. Può essere interessante notare che le due dimostrazioni proposte privilegiano diversamente le strutture additiva e moltiplicativa dei numeri naturali: nella prima si dimostra che $S - P(x) = o(1)$, nella seconda che $S = P(x)\big(1 + o(1)\big)$, dove $P(x) \stackrel{\text{def}}{=} \prod_{p\leq x}(1 + f(p) + f(p^2) + \cdots)$. □

§3.4. Serie di Dirichlet formali

Vogliamo brevemente motivare l'introduzione del prodotto di Dirichlet: per questo parliamo delle serie di Dirichlet formali associate a successioni di numeri complessi. Naturalmente è possibile studiare questo genere di funzioni utilizzando le tecniche dell'analisi complessa, ma qui parliamo solo dell'aspetto formale che può essere utilizzato per introdurre le funzioni aritmetiche (alcune relazioni risultano in effetti piú facili da comprendere), ma vedremo nel Capitolo 7 che le serie di Dirichlet sono molto piú utili nello studio dei numeri primi se introdotte nel loro appropriato contesto analitico.

Definizione 3.4.1. *Data una qualsiasi successione $(a_n)_{n\in\mathbb{N}^*}$ a valori in $\mathbb{C}$, definiamo la* serie di Dirichlet formale *associata mediante*

$$f(s) \stackrel{\text{def}}{=} \sum_{n\geq 1} \frac{a_n}{n^s}. \tag{3.4.1}$$

La serie di Dirichlet formale associata alla funzione aritmetica I è $F_I(s) = 1$, la funzione che vale costantemente 1, mentre la serie di Dirichlet formale associata alla funzione N_0 è detta funzione zeta di Riemann e si indica con $\zeta(s)$ (cfr Capitolo 7): in altre parole, tutti i coefficienti nella serie di Dirichlet per la funzione ζ sono uguali ad 1. Date due successioni (a_n) e (b_n) si riconosce senza difficoltà che, dette f e g le serie di Dirichlet formali associate, si ha

$$f(s)g(s) = \sum_{n\geq 1} \frac{(a*b)(n)}{n^s}.$$

Infatti, raggruppando i termini con lo stesso valore del denominatore e trascurando le questioni di convergenza,

$$f(s)g(s) = \sum_{n\geq 1}\sum_{m\geq 1} \frac{a_n b_m}{(nm)^s} = \sum_{d\geq 1}\sum_{\substack{n\geq 1,\, m\geq 1\\ nm=d}} \frac{a_n b_m}{(nm)^s} = \sum_{d\geq 1} \frac{1}{d^s} \sum_{\substack{n\geq 1,\, m\geq 1\\ nm=d}} a_n b_m,$$

che è la tesi. In questo nuovo contesto, la maggior parte dei risultati del §3.1 sono del tutto evidenti: il fatto che il prodotto di Dirichlet commuti e sia associativo è immediato. I Teoremi 3.1.9 e 3.2.4 sono equivalenti (almeno in parte) alle uguaglianze

$$\sum_{n\geq 1} \frac{\mu(n)}{n^s} = \frac{1}{\zeta(s)}, \qquad \sum_{n\geq 1} \frac{d(n)}{n^s} = \zeta(s)^2 \qquad \text{e} \qquad \zeta(s)^k = \sum_{n\geq 1} \frac{d_k(n)}{n^s},$$

dove $d_k(n)$ indica il numero dei modi in cui n può essere scritto come prodotto di k fattori e cioè $d_k = N_0 * \cdots * N_0$, con k fattori. Queste ultime possono essere facilmente giustificate in modo rigoroso per $\sigma = \Re(s) > 1$ sfruttando la convergenza totale delle serie in questione nei semipiani $\Re(s) \geq 1+\delta$, per ogni δ positivo fissato (cfr il Teorema 7.1.2). È semplice verificare la prima formula di inversione di Möbius 3.1.11: infatti

$$f(s) = g(s) \cdot \frac{1}{\zeta(s)} \qquad \text{se e solo se} \qquad g(s) = f(s)\zeta(s),$$

cioè $f = g * \mu$ se e solo se $g = f * N_0$. Inoltre il Lemma 3.2.9 equivale a

$$-\frac{\zeta'}{\zeta}(s) = \big(-\zeta'(s)\big)\frac{1}{\zeta(s)} \quad \text{dato che} \quad -\frac{\zeta'}{\zeta}(s) = \sum_{n\geq 1} \frac{\Lambda(n)}{n^s} \quad \text{e} \quad \zeta'(s) = -\sum_{n\geq 1} \frac{\log n}{n^s}.$$

Ci limitiamo ad osservare che affinché la serie a destra della (3.4.1) converga in qualche insieme è necessario e
𝔈 3.4.1 sufficiente che $a_n = \mathcal{O}(n^c)$ per qualche $c \in\mathbb{R}$ fissato, e che la conoscenza di opportune proprietà analitiche della funzione f permette di determinare una formula asintotica per $\sum_{n\leq x} a_n$.

Capitolo 4. Distribuzione dei Numeri Primi

§4.1. Risultati elementari

Definizione 4.1.1. *Per $x \geq 1$ poniamo*

$$\pi(x) \stackrel{\text{def}}{=} \sum_{p \leq x} 1 = |\{p \leq x\}|, \qquad \theta(x) \stackrel{\text{def}}{=} \sum_{p \leq x} \log p, \qquad \psi(x) \stackrel{\text{def}}{=} \sum_{n \leq x} \Lambda(n).$$

𝔈 4.1.1 *Queste ultime sono dette* funzioni di Chebyshev.

Osserviamo che il Corollario 1.1.8 implica che tutte queste funzioni divergono per $x \to \infty$, ed anche che $\limsup \pi(x)(\log\log x)^{-1} > 0$, ma, per esempio, $\pi(1000) = 168$, mentre $\log\log 1000 < 2$. Vogliamo ottenere informazioni piú precise: il nostro obiettivo non è tanto quello di ottenere una formula esatta per π, θ o ψ (cfr §1.7), quanto una formula che ci permetta di approssimare ciascuna di queste funzioni con una funzione "semplice" piú un resto sufficientemente piccolo. Formule di varia natura sono state congetturate da Legendre, Gauss, Riemann: si consulti l'Appendice "Distribuzione dei Numeri Primi" per un confronto numerico fra le varie approssimazioni proposte.

Definizione 4.1.2. *Per $x \geq 2$ definiamo la funzione* logaritmo integrale *per mezzo della relazione*

$$\mathrm{li}(x) \stackrel{\text{def}}{=} \lim_{\varepsilon \to 0+} \Big\{ \int_{\varepsilon}^{1-\varepsilon} + \int_{1+\varepsilon}^{x} \Big\} \frac{\mathrm{d}t}{\log t}.$$

Teorema 4.1.3 (dei Numeri Primi, Hadamard, de la Vallée Poussin). *Esiste una costante $c > 0$ tale che per $x \to \infty$ si ha*

$$\pi(x) = \mathrm{li}(x) + \mathcal{O}\Big(x \exp\Big\{-c(\log x)^{3/5}(\log\log x)^{-1/5}\Big\}\Big).$$

Non daremo la dimostrazione di questo risultato (si vedano i Capitoli 7–18 del libro di Davenport [12] ed il Capitolo 7) in questa forma cosí forte. Ci limiteremo a dimostrare che
𝔈 4.1.2 $\pi(x) \sim \mathrm{li}(x) \sim x/\log x$ quando $x \to \infty$.

Congettura 4.1.4 (Riemann). *Per $x \to \infty$ si ha $\pi(x) = \mathrm{li}(x) + \mathcal{O}\big(x^{1/2}\log x\big)$.*

Nei prossimi paragrafi otterremo dei risultati approssimati sempre piú precisi.

Teorema 4.1.5 (Eulero). *La serie e il prodotto seguenti sono divergenti:*

$$\sum_p \frac{1}{p}, \qquad \prod_p \left(1-\frac{1}{p}\right).$$

Dim.: Sia $f \in \mathfrak{M}^*$ con $f(p) \stackrel{\text{def}}{=} p^{-1}$ se $p \le x$, $f(p) \stackrel{\text{def}}{=} 0$ se $p > x$. Poiché f è completamente moltiplicativa, per il Teorema 3.3.1 si ha

$$P(x) \stackrel{\text{def}}{=} \prod_{p\le x} \left(1-\frac{1}{p}\right)^{-1} = \sum_{n\in\mathcal{A}(x)} \frac{1}{n} \qquad \text{dove} \qquad \mathcal{A}(x) \stackrel{\text{def}}{=} \{n\in\mathbb{N}^*\colon p \mid n \Rightarrow p \le x\}.$$

Quindi $n \in \mathcal{A}(x)$ per ogni $n \le x$, e dunque, per il Teorema A.4.1 nel caso $k=-1$

$$P(x) \ge \sum_{n\le x} \frac{1}{n} = \log x + \gamma + \mathcal{O}\big(x^{-1}\big).$$

Inoltre per $0 \le y \le \frac12$ si ha $-\log(1-y) = y + \mathcal{O}\big(y^2\big)$, e quindi

$$\sum_{p\le x} \frac{1}{p} = -\sum_{p\le x} \log\left(1-\frac{1}{p}\right) + \mathcal{O}\left(\sum_{p\le x}\frac{1}{p^2}\right) = \log P(x) + \mathcal{O}(1) \ge \log\log x + \mathcal{O}(1),$$

che implica la tesi in una forma quantitativa piuttosto forte. □

Questa dimostrazione è importante perché lega un fatto analitico (la divergenza della serie armonica) ad una proprietà dei numeri primi.

§4.2. I teoremi di Chebyshev

Teorema 4.2.1. *Per i seguenti limiti si ha $\lambda_1 = \lambda_2 = \lambda_3$ e $\Lambda_1 = \Lambda_2 = \Lambda_3$.*

$$\lambda_1 \stackrel{\text{def}}{=} \liminf_{x\to\infty} \frac{\pi(x)\log x}{x}; \qquad \lambda_2 \stackrel{\text{def}}{=} \liminf_{x\to\infty} \frac{\theta(x)}{x}; \qquad \lambda_3 \stackrel{\text{def}}{=} \liminf_{x\to\infty} \frac{\psi(x)}{x};$$
$$\Lambda_1 \stackrel{\text{def}}{=} \limsup_{x\to\infty} \frac{\pi(x)\log x}{x}; \qquad \Lambda_2 \stackrel{\text{def}}{=} \limsup_{x\to\infty} \frac{\theta(x)}{x}; \qquad \Lambda_3 \stackrel{\text{def}}{=} \limsup_{x\to\infty} \frac{\psi(x)}{x}.$$

Dim.: Si ha banalmente $\theta(x) \le \psi(x)$ ed inoltre

$$\psi(x) = \sum_{n\le x} \Lambda(n) = \sum_{p^m\le x} \log p = \sum_{p\le x} \left[\frac{\log x}{\log p}\right] \log p \le \log x \sum_{p\le x} 1 = \pi(x)\log x.$$

Questo dimostra che $\lambda_2 \le \lambda_3 \le \lambda_1$ e che $\Lambda_2 \le \Lambda_3 \le \Lambda_1$. Inoltre per ogni $y \in (1,x]$ si ha

$$\theta(x) \ge \sum_{y<p\le x} \log p \ge \log y\big(\pi(x)-\pi(y)\big) \qquad \text{da cui} \qquad \pi(x) \le \frac{\theta(x)}{\log y} + \pi(y)$$

e quindi, ricordando che $\pi(y) \le y$,

$$\frac{\pi(x)\log x}{x} \le \frac{\theta(x)}{x}\frac{\log x}{\log y} + \frac{\pi(y)\log x}{x} \le \frac{\theta(x)}{x}\frac{\log x}{\log y} + \frac{y\log x}{x}.$$

Le disuguaglianze $\lambda_1 \le \lambda_2$ e $\Lambda_1 \le \Lambda_2$ seguono senz'altro scegliendo $y = x(\log x)^{-2}$. □

Chiameremo λ^* e Λ^* rispettivamente i valori comuni di questi limiti. Chebyshev fu il primo a dare disuguaglianze esplicite per λ^* e Λ^*, e dimostrò anche che se sono uguali (cioè se esiste il $\lim_{x\to\infty}\big(\pi(x)\log x\big)/x$) allora valgono entrambi 1.

TEOREMA 4.2.2 (CHEBYSHEV). *Si ha* $\log 2 \le \lambda^* \le \Lambda^* \le 2\log 2$.

DIM.: Consideriamo la successione

$$I_m \stackrel{\text{def}}{=} \int_0^1 x^m (1-x)^m \,\mathrm{d}x.$$

È chiaro che $0 < I_m \le 4^{-m}$, poiché la funzione integranda è positiva in $(0,1)$ ed ha un massimo in $x = \frac{1}{2}$. Inoltre, poiché la funzione integranda è un polinomio a coefficienti interi, $I_m \in \mathbb{Q}^+$, e i denominatori che compaiono nello sviluppo esplicito dell'integrale sono tutti $\le 2m+1$. Dunque $I_m \exp\psi(2m+1) \in \mathbb{N}^*$, e quindi $I_m \exp\psi(2m+1) \ge 1$. Da quest'ultima relazione ricaviamo

$$\psi(2m+1) \ge \log I_m^{-1} \ge 2m\log 2$$

da cui

$$\psi(2m+1) \ge (2m+1)\log 2 - \log 2,$$

e la prima disuguaglianza segue immediatamente, poiché $\psi(x) - \psi(x-2) \le \log(2x)$.

Per dimostrare la seconda disuguaglianza, consideriamo il coefficiente binomiale $M = \binom{2N+1}{N}$. Poiché M compare due volte nello sviluppo di $(1+1)^{2N+1}$, si ha $2M < 2^{2N+1}$ da cui $M < 2^{2N}$. Osserviamo che se $p \in (N+1, 2N+1]$ allora $p \mid M$, poiché divide il numeratore del coefficiente binomiale, ma non il denominatore. Questo ci permette di concludere che

$$\theta(2N+1) - \theta(N+1) \le \log M < 2N\log 2. \tag{4.2.1}$$

Supponiamo di aver dimostrato che $\theta(n) < 2n\log 2$ per $1 \le n \le n_0 - 1$, osservando che questa relazione è banale per $n = 1,\ 2$. Se n_0 è pari allora $\theta(n_0) = \theta(n_0-1) < 2(n_0-1)\log 2 < 2n_0\log 2$.

Se n_0 è dispari, $n_0 = 2N+1$ e quindi

$$\begin{aligned}\theta(n_0) = \theta(2N+1) &= \theta(2N+1) - \theta(N+1) + \theta(N+1)\\ &< 2N\log 2 + 2(N+1)\log 2 = 2n_0\log 2,\end{aligned}$$

per la (4.2.1) e per l'ipotesi induttiva, ed il Teorema segue. □

𝔈 4.2.1 Si può dimostrare facilmente, integrando $|k|$ volte per parti, che per $|k| \le m$ si ha

$$I_m = \frac{m!^2}{(m+k)!(m-k)!}\int_0^1 x^{m+k}(1-x)^{m-k}\mathrm{d}x. \tag{4.2.2}$$

Prendendo $k = m$ si ha $I_m = m!^2(2m+1)!^{-1}$, e dunque in effetti anche la dimostrazione della prima disuguaglianza dipende da considerazioni relative ad opportuni coefficienti binomiali. Inoltre, ripetendo la dimostrazione con il polinomio $p(x) \stackrel{\text{def}}{=} x^4(1-2x)^2(1-x)^4$

𝔈 4.2.2 si ottiene la limitazione $\lambda^* \ge \frac{1}{2}\log 5$, ed è possibile ottenere limitazioni ancora piú precise con altri polinomi. Osserviamo che la Formula di Stirling A.3.2 dà la relazione $I_m^{-1} = 2^{2m+1}m^{1/2}\pi^{-1/2}\big(1+\mathcal{O}\big(m^{-1}\big)\big)$, ma questa non dà informazioni piú precise. Infine si ha che $I_m = \mathrm{B}(m+1, m+1)$ dove B è la funzione Beta definita nell'Appendice A2, e la (4.2.2) segue immediatamente dalle proprietà indicate nell'Appendice.

§4.3. Le formule di Mertens

Teorema 4.3.1 (Prima Formula di Mertens). *Per $N \to \infty$ si ha*

$$\sum_{n\le N} \frac{\Lambda(n)}{n} = \log N + \mathcal{O}(1).$$

Dim.: Per la formula di Stirling A.3.2 abbiamo $\log N! = N\log N + \mathcal{O}(N)$. Inoltre

$$\log N! = \sum_{p^k\le N} \left[\frac{N}{p^k}\right] \log p = \sum_{n\le N} \left[\frac{N}{n}\right] \Lambda(n) = \sum_{n\le N} \frac{N\Lambda(n)}{n} + \mathcal{O}(\psi(N)) = \sum_{n\le N} \frac{N\Lambda(n)}{n} + \mathcal{O}(N),$$

per il Teorema 4.2.2; la tesi segue confrontando le due espressioni per $\log N!$. □

Teorema 4.3.2 (Seconda Formula di Mertens). *Per $N \to \infty$ si ha*

$$\sum_{p\le N} \frac{\log p}{p} = \log N + \mathcal{O}(1).$$

Dim.: Abbiamo

$$\sum_{n\le N} \frac{\Lambda(n)}{n} - \sum_{p\le N} \frac{\log p}{p} \le \sum_{p\le N} \left(\frac{\log p}{p^2} + \frac{\log p}{p^3} + \cdots\right) = \sum_{p\le N} \frac{\log p}{p(p-1)} \le \sum_{n\ge 2} \frac{\log n}{n(n-1)}$$

e la tesi segue dalla prima formula di Mertens 4.3.1. □

Teorema 4.3.3 (Terza Formula di Mertens). *Per $x \to \infty$ si ha*

$$\int_1^x \frac{\psi(t)}{t^2}\mathrm{d}t = \log x + \mathcal{O}(1).$$

Dim.: Per la formula di sommazione parziale A.1.1 si ha

$$\sum_{n\le x} \frac{\Lambda(n)}{n} = \frac{\psi(x)}{x} + \int_1^x \frac{\psi(t)}{t^2}\mathrm{d}t,$$

e il risultato voluto segue dai Teoremi 4.2.2 e 4.3.2. □

Teorema 4.3.4 (Formula di Mertens per i primi). *Esiste una costante $B \in \mathbb{R}$ tale che per $x \to \infty$ si ha*

$$\sum_{p\le x} \frac{1}{p} = \log\log x + B + \mathcal{O}\big((\log x)^{-1}\big).$$

Dim.: Dalla seconda formula di Mertens 4.3.2, $\sum_{p\le x} \frac{\log p}{p} = \log x + R(x)$ dove $R(x) = \mathcal{O}(1)$. Quindi otteniamo per sommazione parziale

$$\begin{aligned}
\sum_{p\le x} \frac{1}{p} &= \frac{1}{\log x} \sum_{p\le x} \frac{\log p}{p} + \int_2^x \sum_{p\le t} \frac{\log p}{p} \frac{\mathrm{d}t}{t(\log t)^2} = 1 + \mathcal{O}\left(\frac{1}{\log x}\right) + \int_2^x \frac{\log t + R(t)}{t(\log t)^2}\mathrm{d}t \\
&= 1 + \mathcal{O}\big((\log x)^{-1}\big) + \log\log x - \log\log 2 + \int_2^\infty \frac{R(t)}{t(\log t)^2}\mathrm{d}t + \mathcal{O}\left(\int_x^\infty \frac{\mathrm{d}t}{t(\log t)^2}\right) \\
&= \log\log x + 1 - \log\log 2 + \int_2^\infty \frac{R(t)}{t(\log t)^2}\mathrm{d}t + \mathcal{O}\big((\log x)^{-1}\big),
\end{aligned}$$

dove l'integrale improprio converge poiché $R(x) = \mathcal{O}(1)$. □

Corollario 4.3.5 (Chebyshev). *Se esiste il*

$$\lim_{x\to\infty} \frac{\pi(x)\log x}{x},$$

questo limite vale 1. *In altre parole, nella notazione del Teorema* 4.2.2, *si ha* $\lambda^* \le 1 \le \Lambda^*$.

Dim.: Sia L il limite nell'enunciato. Per la formula di sommazione parziale, si ha

$$\sum_{p\le x}\frac{1}{p} = \frac{\pi(x)}{x} + \int_2^x \frac{\pi(t)}{t^2}\mathrm{d}t = o(1) + \big(1+o(1)\big)\int_2^x \frac{L\,\mathrm{d}t}{t\log t} = \big(L+o(1)\big)\log\log x,$$

e la tesi segue dal Teorema 4.3.4. □

Una dimostrazione simile permette di ottenere lo stesso risultato direttamente dalla terza
𝔈 4.3.4 formula di Mertens 4.3.3.

Teorema 4.3.6 (Mertens). *Per* $x\to\infty$ *si ha*

$$\prod_{p\le x}\left(1-\frac{1}{p}\right) = \frac{e^{-\gamma}}{\log x} + \mathcal{O}\left(\frac{1}{(\log x)^2}\right),$$

dove γ *è la costante di Eulero.*

Dim.: Non è difficile mostrare questo risultato con una costante positiva (non esplicita) k al posto di $e^{-\gamma}$. Infatti, dal Teorema 4.3.4 si ha

$$\begin{aligned}\log\prod_{p\le x}\left(1-\frac{1}{p}\right) &= -\sum_{p\le x}\sum_{m\ge1}\frac{1}{mp^m} = -\sum_{p\le x}\frac{1}{p} - \sum_p\sum_{m\ge2}\frac{1}{mp^m} + \mathcal{O}\left(\sum_{p>x}\sum_{m\ge2}\frac{1}{mp^m}\right)\\ &= -\log\log x + C + \mathcal{O}\big((\log x)^{-1}\big).\end{aligned}$$

Per ottenere il risultato completo è necessario conoscere le proprietà delle funzioni zeta di Riemann e Gamma di Eulero: si vedano i riferimenti bibliografici. □

§4.4. Le formule di Selberg

Per dimostrare le formule di Selberg useremo una variante della seconda formula di inversione di Möbius 3.1.12.

Lemma 4.4.1 (Iseki–Tatuzawa). *Sia* $F\colon[1,+\infty)\to\mathbb{C}$ *una funzione qualsiasi e*

$$G(x) \stackrel{\text{def}}{=} \sum_{n\le x} F\left(\frac{x}{n}\right)\log x,$$

allora

$$F(x)\log x + \sum_{n\le x} F\left(\frac{x}{n}\right)\Lambda(n) = \sum_{n\le x}\mu(n)G\left(\frac{x}{n}\right).$$

Dim.: Infatti abbiamo

$$\begin{aligned}\sum_{n\le x}\mu(n)G\left(\frac{x}{n}\right) &= \sum_{n\le x}\mu(n)\sum_{nm\le x}F\left(\frac{x}{nm}\right)\log\frac{x}{n} = \sum_{d\le x}F\left(\frac{x}{d}\right)\sum_{n|d}\mu(n)\log\frac{x}{n}\\ &= \sum_{d\le x}F\left(\frac{x}{d}\right)\sum_{n|d}\mu(n)\big(\log x - \log n\big) = F(x)\log x + \sum_{d\le x}F\left(\frac{x}{d}\right)\Lambda(d),\end{aligned}$$

per il Teorema 3.1.9 ed il Corollario 3.2.10. □

Teorema 4.4.2 (Selberg). *Per $x \to \infty$ si hanno le seguenti relazioni equivalenti*

$$\sum_{n\le x} \Lambda(n)\log n + \sum_{nm\le x} \Lambda(n)\,\Lambda(m) = 2x\log x + \mathcal{O}(x),$$

$$\psi(x)\log x + \sum_{n\le x} \psi\left(\frac{x}{n}\right)\Lambda(n) = 2x\log x + \mathcal{O}(x).$$

Dim.: Per sommazione parziale

$$\sum_{n\le x} \Lambda(n)\log n = \psi(x)\log x - \int_1^x \frac{\psi(t)}{t}\mathrm{d}t = \psi(x)\log x + \mathcal{O}(x)$$

dal Teorema 4.2.2, ed inoltre

$$\sum_{nm\le x} \Lambda(n)\,\Lambda(m) = \sum_{n\le x}\Lambda(n) \sum_{m\le x/n} \Lambda(m) = \sum_{n\le x} \psi\left(\frac{x}{n}\right)\Lambda(n).$$

Dimostriamo dunque la seconda relazione: poniamo $F(x) = \psi(x) - x + \gamma + 1$ nel Lemma di Iseki–Tatuzawa 4.4.1, ed otteniamo

$$G(x) = \sum_{n\le x} \left\{\psi\left(\frac{x}{n}\right) - \frac{x}{n} + \gamma + 1\right\}\log x.$$

Ma dalla Formula di Stirling A.3.2 e dal Lemma 3.2.9 (oppure dal Metodo dell'Iperbole 3.1.13 con $f = \Lambda$, $F(x) = \psi(x)$, $g = N_0$, $G(x) = [x]$, $y = x$) otteniamo

$$\sum_{n\le x} \psi\left(\frac{x}{n}\right) = \sum_{n\le x}\sum_{nm\le x} \Lambda(m) = \sum_{d\le x}\sum_{m\mid d}\Lambda(m) = \sum_{d\le x} \log d = x\log x - x + \mathcal{O}(\log x).$$

Inoltre dal Lemma A.4.1 con $k = -1$ otteniamo

$$\sum_{n\le x} \frac{x}{n}\log x = x\log^2 x + \gamma x\log x + \mathcal{O}(\log x),$$

e quindi, in definitiva, $G(x) = \mathcal{O}\big(\log^2 x\big)$. Per il Lemma A.4.4 con $k = 2$ ed il Lemma 4.4.1, abbiamo

$$\left|\sum_{n\le x} \mu(n) G\left(\frac{x}{n}\right)\right| \le \sum_{n\le x} \left|G\left(\frac{x}{n}\right)\right| = \mathcal{O}(x).$$

Questo porta alla formula

$$F(x)\log x + \sum_{n\le x} F\left(\frac{x}{n}\right)\Lambda(n) = \mathcal{O}(x), \tag{4.4.1}$$

e si ottiene il risultato voluto ricordando che, per il Teorema 4.2.2, si ha $\psi(x) = \mathcal{O}(x)$. □

Le Formule di Selberg 4.4.2 sono alla base della dimostrazione elementare del Teorema dei Numeri Primi 4.1.3. La parola "elementare" non deve trarre in inganno: si tratta di una dimostrazione che non fa uso della teoria delle funzioni di una variabile complessa, ma è probabilmente meno chiara di quest'ultima, poiché il procedimento di "estrazione" delle informazioni presenti nelle formule di Selberg in media è piuttosto oscuro. Una semplice ma importante conseguenza è il seguente

COROLLARIO 4.4.3. *Siano λ^* e Λ^* i valori comuni dei limiti nel Teorema 4.2.1. Si ha $\lambda^* + \Lambda^* = 2$.*

DIM.: Per definizione, fissato $\varepsilon > 0$ è possibile trovare $x_0 = x_0(\varepsilon)$ tale che $(\lambda^* - \varepsilon)x \leq \psi(x) \leq (\Lambda^* + \varepsilon)x$ per ogni $x \geq x_0$. Inoltre, per il Teorema 4.2.2, esiste una costante assoluta C tale che $\psi(x) \leq Cx$ per ogni $x \geq 1$. Dividiamo la seconda formula di Selberg per $x \log x$, e separiamo nella somma i termini con $n \leq \frac{x}{x_0}$ dagli altri, ottenendo

$$\frac{\psi(x)}{x} + \frac{1}{x \log x} \sum_{1 \leq n \leq x/x_0} \psi\left(\frac{x}{n}\right) \Lambda(n) + \frac{1}{x \log x} \sum_{x/x_0 < n \leq x} \psi\left(\frac{x}{n}\right) \Lambda(n) = 2 + o(1). \quad (4.4.2)$$

Per stimare la prima somma usiamo la Prima Formula di Mertens 4.3.1:

$$\sum_{1 \leq n \leq x/x_0} \psi\left(\frac{x}{n}\right) \Lambda(n) \geq \sum_{1 \leq n \leq x/x_0} (\lambda^* - \varepsilon) \frac{x}{n} \Lambda(n) = \big(\lambda^* - \varepsilon + o(1)\big) x \log x.$$

Nella seconda abbiamo

$$\begin{aligned} \sum_{x/x_0 < n \leq x} \psi\left(\frac{x}{n}\right) \Lambda(n) &\leq \sum_{x/x_0 < n \leq x} C \frac{x}{n} \Lambda(n) = Cx \left(\log x + \mathcal{O}(1) - \log \frac{x}{x_0} + \mathcal{O}(1) \right) \\ &= Cx\big(\log x_0 + \mathcal{O}(1)\big) = o(x \log x). \end{aligned}$$

Sostituendo in (4.4.2) otteniamo

$$\frac{\psi(x)}{x} + \lambda^* - \varepsilon + o(1) \leq 2 + o(1),$$

e quindi per $x \geq x_0$ si ha

$$\frac{\psi(x)}{x} \leq 2 - \lambda^* + \varepsilon + o(1).$$

Passando al massimo limite, ed osservando che questa relazione deve valere per ogni $\varepsilon > 0$, si deduce immediatamente che $\Lambda^* + \lambda^* \leq 2$. L'altra disuguaglianza si dimostra in modo simile. Osserviamo che questo risultato implica il Corollario 4.3.5. □

Ricaviamo ora un'importante conseguenza delle formule di Selberg: posto $R(x) \stackrel{\text{def}}{=} \psi(x) - x$ (cosicché il Teorema dei Numeri Primi è equivalente all'affermazione $R(x) = o(x)$ quando $x \to \infty$), sostituendo otteniamo

$$x \log x + R(x) \log x + \sum_{n \leq x} \left(\frac{x}{n} + R\left(\frac{x}{n}\right) \right) \Lambda(n) = 2x \log x + \mathcal{O}(x).$$

Ricordando la Prima Formula di Mertens 4.3.1 e semplificando, si ottiene

$$R(x) \log x + \sum_{n \leq x} \Lambda(n) R\left(\frac{x}{n}\right) = \mathcal{O}(x). \quad (4.4.3)$$

Questa formula è equivalente alla (4.4.1) e sta alla base della dimostrazione che segue, che spezzeremo in vari Lemmi.

§4.5. Dimostrazione del teorema dei numeri primi

Lemma 4.5.1. *Si ha*

$$\big|R(x)\big|\log^2 x \le \sum_{n\le x} a_n \left|R\left(\frac{x}{n}\right)\right| + \mathcal{O}(x\log x),$$

dove

$$a_n \stackrel{\text{def}}{=} \Lambda(n)\log n + \sum_{hk=n}\Lambda(h)\Lambda(k), \qquad \sum_{n\le x} a_n = 2x\log x + \mathcal{O}(x).$$

Dim.: Sostituiamo x/m al posto di x nella (4.4.3) ed otteniamo

$$R\left(\frac{x}{m}\right)\log\frac{x}{m} + \sum_{n\le x/m}\Lambda(n)R\left(\frac{x}{mn}\right) = \mathcal{O}\Big(\frac{x}{m}\Big),$$

e quindi si ha

$$\log x\left\{R(x)\log x + \sum_{n\le x}\Lambda(n)R\left(\frac{x}{n}\right)\right\} - \sum_{m\le x}\Lambda(m)\left\{R\left(\frac{x}{m}\right)\log\frac{x}{m} + \sum_{n\le x/m}\Lambda(n)R\left(\frac{x}{mn}\right)\right\}$$
$$= \mathcal{O}(x\log x) + \mathcal{O}\left(x\sum_{m\le x}\frac{\Lambda(m)}{m}\right) = \mathcal{O}(x\log x),$$

per la prima formula di Mertens 4.3.1. Dunque

$$R(x)\log^2 x = -\sum_{n\le x}\Lambda(n)R\left(\frac{x}{n}\right)\log n + \sum_{mn\le x}\Lambda(n)\Lambda(m)R\left(\frac{x}{nm}\right) + \mathcal{O}(x\log x),$$

ed il Lemma segue immediatamente prendendo il valore assoluto. □

Lemma 4.5.2. *Si ha*

$$\sum_{n\le x} a_n\left|R\left(\frac{x}{n}\right)\right| = 2\int_1^x \left|R\left(\frac{x}{t}\right)\right|\log t\,\mathrm{d}t + \mathcal{O}(x\log x).$$

Dim.: Procediamo in due passi: prima approssimiamo la somma a sinistra con una nuova somma di forma simile in cui però a_n è rimpiazzato dal suo valor medio, che è $2\log n$ per il Lemma 4.5.1. Poi approssimiamo quest'ultima somma con l'integrale desiderato.

Osserviamo che, posto $F(t) \stackrel{\text{def}}{=} t + \psi(t)$, F risulta essere una funzione monotona strettamente crescente, e quindi se $0 \le t_0 \le t_1$ si ha

$$\begin{aligned}\big||R(t_1)| - |R(t_0)|\big| \le \big|R(t_1) - R(t_0)\big| &= \big|\psi(t_1) - \psi(t_0) - t_1 + t_0\big| \\ &\le \psi(t_1) - \psi(t_0) + t_1 - t_0 = F(t_1) - F(t_0). \qquad (4.5.1)\end{aligned}$$

Inoltre $F(t) = \mathcal{O}(t)$ per il Lemma 4.2.2 e quindi

$$\sum_{n\le x-1} n\left\{F\left(\frac{x}{n}\right) - F\left(\frac{x}{n+1}\right)\right\} = \sum_{n\le x} F\left(\frac{x}{n}\right) - [x]F\left(\frac{x}{[x]}\right)$$
$$= \mathcal{O}\left(x\sum_{n\le x}\frac{1}{n}\right) + \mathcal{O}(x) = \mathcal{O}(x\log x), \tag{4.5.2}$$

per il Lemma A.4.1 con $k = -1$. Ora poniamo

$$c_1 \stackrel{\text{def}}{=} 0, \qquad c_n \stackrel{\text{def}}{=} a_n - 2\int_{n-1}^{n}\log t\,\mathrm{d}t, \qquad \varphi(n) \stackrel{\text{def}}{=} \left|R\left(\frac{x}{n}\right)\right|,$$

e si ha quindi, integrando per parti, dalla prima formula di Selberg

$$C(x) \stackrel{\text{def}}{=} \sum_{n\le x} c_n = \mathcal{O}(x).$$

Usando la sommazione parziale A.1.1 con $\lambda_n = n$ ed $N = [x]$, dalla (4.5.1) otteniamo

$$\sum_{n\le x} c_n f(n) = \sum_{n\le x} a_n\left|R\left(\frac{x}{n}\right)\right| - 2\sum_{2\le n\le x}\left|R\left(\frac{x}{n}\right)\right|\int_{n-1}^{n}\log t\,\mathrm{d}t$$
$$= \sum_{n\le x-1} C(n)\left\{\left|R\left(\frac{x}{n}\right)\right| - \left|R\left(\frac{x}{n+1}\right)\right|\right\} + C(x)\left|R\left(\frac{x}{[x]}\right)\right|$$
$$= \mathcal{O}\left(\sum_{n\le x-1} n\left\{F\left(\frac{x}{n}\right) - F\left(\frac{x}{n+1}\right)\right\}\right) + \mathcal{O}(x) = \mathcal{O}(x\log x), \tag{4.5.3}$$

per la (4.5.2). Infine

$$\left|\left|R\left(\frac{x}{n}\right)\right|\int_{n-1}^{n}\log t\,\mathrm{d}t - \int_{n-1}^{n}\left|R\left(\frac{x}{t}\right)\right|\log t\,\mathrm{d}t\right| \le \int_{n-1}^{n}\left|\left|R\left(\frac{x}{n}\right)\right| - \left|R\left(\frac{x}{t}\right)\right|\right|\log t\,\mathrm{d}t$$
$$\le \int_{n-1}^{n}\left\{F\left(\frac{x}{t}\right) - F\left(\frac{x}{n}\right)\right\}\log t\,\mathrm{d}t \le (n-1)\left\{F\left(\frac{x}{n-1}\right) - F\left(\frac{x}{n}\right)\right\}. \tag{4.5.4}$$

Quindi dalle (4.5.2)-(4.5.4) otteniamo

$$\sum_{2\le n\le x}\left|R\left(\frac{x}{n}\right)\right|\int_{n-1}^{n}\log t\,\mathrm{d}t - \int_{1}^{x}\left|R\left(\frac{x}{t}\right)\right|\log t\,\mathrm{d}t$$
$$= \mathcal{O}\left(\sum_{2\le n\le x}(n-1)\left\{F\left(\frac{x}{n-1}\right) - F\left(\frac{x}{n}\right)\right\}\right) + \mathcal{O}(x\log x) = \mathcal{O}(x\log x).$$

Questo conclude la dimostrazione del Lemma. □

LEMMA 4.5.3. *Posto* $V(\xi) \stackrel{\text{def}}{=} e^{-\xi}R\big(e^{\xi}\big) = e^{-\xi}\psi\big(e^{\xi}\big) - 1$, *si ha*

$$\xi^2\big|V(\xi)\big| \le 2\int_0^{\xi}\int_0^{\zeta}\big|V(\eta)\big|\,\mathrm{d}\eta\,\mathrm{d}\zeta + \mathcal{O}(\xi).$$

DIM.: Combinando i risultati dei Lemmi 4.5.1-4.5.2 si ha

$$|R(x)|\log^2 x \le 2\int_1^x \left|R\left(\frac{x}{t}\right)\right|\log t\,\mathrm{d}t + \mathcal{O}(x\log x). \tag{4.5.5}$$

Usando la sostituzione dell'enunciato con $x = e^{\xi}$ e $t = xe^{-\eta}$ si ottiene

$$\begin{aligned}\int_1^x \left|R\left(\frac{x}{t}\right)\right|\log t\,\mathrm{d}t &= x\int_0^{\xi}\big|V(\eta)\big|(\xi-\eta)\,\mathrm{d}\eta \\ &= x\int_0^{\xi}\big|V(\eta)\big|\int_{\eta}^{\xi}\mathrm{d}\zeta\,\mathrm{d}\eta = x\int_0^{\xi}\int_0^{\zeta}\big|V(\eta)\big|\,\mathrm{d}\eta\,\mathrm{d}\zeta.\end{aligned}$$

La disuguaglianza voluta segue sostituendo nella (4.5.5) e dividendo per x. □

LEMMA 4.5.4. *Vale la disuguaglianza* $\alpha \le \beta$, *dove*

$$\alpha \stackrel{\text{def}}{=} \limsup_{\xi\to+\infty}\big|V(\xi)\big| \qquad e \qquad \beta \stackrel{\text{def}}{=} \limsup_{\xi\to+\infty}\frac{1}{\xi}\int_0^{\xi}\big|V(\eta)\big|\,\mathrm{d}\eta.$$

DIM.: È chiaro che α e β esistono finiti, poiché $\psi(x) = \mathcal{O}(x)$. Inoltre, per $\xi \to \infty$ si ha

$$\int_0^{\xi}\big|V(\eta)\big|\,\mathrm{d}\eta \le \big(\beta + o(1)\big)\xi$$

e quindi per il Lemma precedente 4.5.3

$$\xi^2\big|V(\xi)\big| \le 2\int_0^{\xi}\big(\beta + o(1)\big)\zeta\,\mathrm{d}\zeta + \mathcal{O}(\xi) = \beta\xi^2 + o\big(\xi^2\big),$$

da cui $\big|V(\xi)\big| \le \beta + o(1)$. Passando al massimo limite si ottiene la tesi. □

Osserviamo che la definizione di α e β implica immediatamente $\beta \le \alpha$, e quindi potremmo proseguire scrivendo $\alpha = \beta$.

LEMMA 4.5.5. *Esiste una costante assoluta* $A > 0$ *tale che per ogni* ξ_1, $\xi_2 \in \mathbb{R}^+$ *si ha*

$$\left|\int_{\xi_1}^{\xi_2} V(\eta)\,\mathrm{d}\eta\right| \le A.$$

DIM.: Basta osservare che

$$\left|\int_{\xi_1}^{\xi_2} V(\eta)\,\mathrm{d}\eta\right| = \left|\int_{\xi_1}^{\xi_2}\big(e^{-\eta}\psi\big(e^{\eta}\big) - 1\big)\,\mathrm{d}\eta\right| = \left|\int_{\exp\xi_1}^{\exp\xi_2}\frac{\psi(t)-t}{t^2}\mathrm{d}t\right| = \mathcal{O}(1),$$

per la Terza Formula di Mertens 4.3.3. □

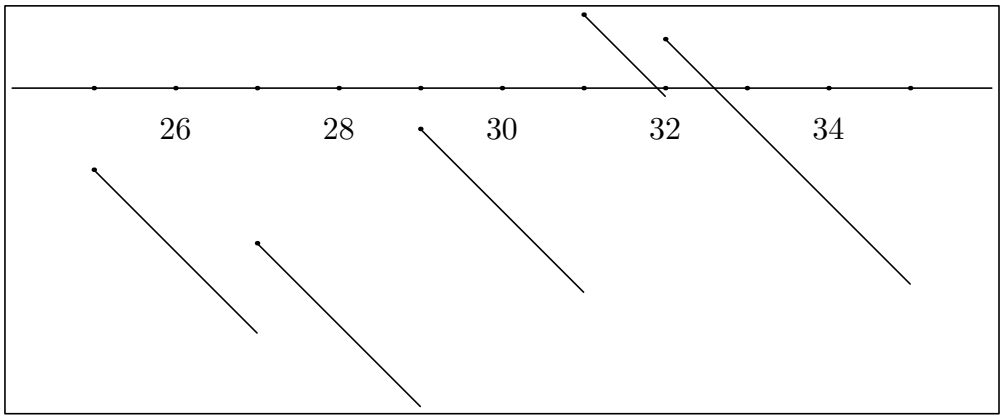


Figura 4.1. *Il grafico di $\psi(x) - x$ per $x \in [25, 35]$. Il grafico di $V(\xi)$ si può ricavare da questo mediante un cambiamento di variabile, ma il comportamento qualitativo è lo stesso.*

LEMMA 4.5.6. *Se $\eta_0 > 0$ e $V(\eta_0) = 0$ allora*

$$\int_0^\alpha \big|V(\eta_0 + \tau)\big| \, \mathrm{d}\tau \leq \frac{1}{2}\alpha^2 + \mathcal{O}\big(\eta_0^{-1}\big).$$

DIM.: Riscriviamo la seconda formula di Selberg 4.4.2 nella forma

$$\psi(x) \log x + \sum_{nm \leq x} \Lambda(n)\Lambda(m) = 2x \log x + \mathcal{O}(x),$$

e la usiamo due volte, con $x = x_0$ e con $x = x_1$ dove $1 \leq x_0 \leq x_1$, sottraendo i risultati:

$$\psi(x_1) \log x_1 - \psi(x_0) \log x_0 + \sum_{x_0 < mn \leq x_1} \Lambda(n)\Lambda(n) = 2x_1 \log x_1 - 2x_0 \log x_0 + \mathcal{O}(x_1).$$

La somma su n ed m è positiva e quindi

$$0 \leq \psi(x_1) \log x_1 - \psi(x_0) \log x_0 \leq 2x_1 \log x_1 - 2x_0 \log x_0 + \mathcal{O}(x_1)$$

da cui deduciamo immediatamente

$$\big|R(x_1) \log x_1 - R(x_0) \log x_0\big| \leq x_1 \log x_1 - x_0 \log x_0 + \mathcal{O}(x_1),$$

e quindi, dividendo per $x_1 \log x_1$ e scrivendo $\xi_i = \log x_i$ per $i = 0$, 1, si ha

$$\left|V(\xi_1) - V(\xi_0)\frac{\xi_0 e^{\xi_0}}{\xi_1 e^{\xi_1}}\right| \leq 1 - \frac{\xi_0 e^{\xi_0}}{\xi_1 e^{\xi_1}} + \mathcal{O}\big({\xi_0}^{-1}\big).$$

Scegliamo $\xi_0 = \eta_0$ e $\xi_1 = \eta_0 + \tau$, in modo che $R(x_0) = V(\xi_0) = 0$. Poiché $\tau \in [0, \alpha]$ si ha

$$|V(\eta_0 + \tau)| \leq 1 - \left(\frac{\eta_0}{\eta_0 + \tau}\right) e^{-\tau} + \mathcal{O}\big(\eta_0^{-1}\big) = 1 - e^{-\tau} + \mathcal{O}\big(\eta_0^{-1}\big) \leq \tau + \mathcal{O}\big(\eta_0^{-1}\big).$$

Quindi si ha

$$\int_0^\alpha \big|V(\eta_0 + \tau)\big| \, \mathrm{d}\tau \leq \int_0^\alpha \big(\tau + \mathcal{O}\big(\eta_0^{-1}\big)\big) \, \mathrm{d}\tau = \frac{1}{2}\alpha^2 + \mathcal{O}\big(\eta_0^{-1}\big),$$

che è la tesi. □

Per concludere dobbiamo dimostrare che $\alpha = 0$. Nel prossimo ed ultimo Lemma supporremo per assurdo che $\alpha > 0$, trovando che $\beta < \alpha$, in contrasto con il Lemma 4.5.4.

LEMMA 4.5.7. $\alpha = 0$.

DIM.: Detta A la costante nel Lemma 4.5.5, se $\alpha > 0$ poniamo

$$\delta \stackrel{\text{def}}{=} \frac{3\alpha^2 + 4A}{2\alpha} > \alpha,$$

e studiamo il comportamento di V nell'intervallo $[\zeta, \zeta+\delta-\alpha]$, per ζ grande, con l'obiettivo di dimostrare che la media di V nell'intervallo $[\zeta, \zeta+\delta]$ è piú piccola di quello che dovrebbe essere. La funzione V è decrescente tranne che nei suoi punti di discontinuità, dove cresce. Quindi nel nostro intervallo o esiste η_0 tale che $V(\eta_0) = 0$, oppure V cambia segno al piú una volta. Infatti, V passa da valori positivi a negativi con continuità, decrescendo, ma può passare da valori negativi a positivi solo saltando. Si veda la Figura 4.1.

Primo caso. Per ζ sufficientemente grande, per il Lemma 4.5.6 possiamo scrivere

$$\begin{aligned}\int_\zeta^{\zeta+\delta} \bigl|V(\eta)\bigr| \,\mathrm{d}\eta &= \left\{\int_\zeta^{\eta_0} + \int_{\eta_0}^{\eta_0+\alpha} + \int_{\eta_0+\alpha}^{\zeta+\delta}\right\} \bigl|V(\eta)\bigr| \,\mathrm{d}\eta \\ &\le \alpha(\eta_0 - \zeta) + \frac{1}{2}\alpha^2 + \alpha(\zeta + \delta - \eta_0 - \alpha) + o(1) \\ &= \alpha\left(\delta - \frac{1}{2}\alpha\right) + o(1) = \alpha_1\delta + o(1),\end{aligned}$$

dove

$$\alpha_1 \stackrel{\text{def}}{=} \alpha\left(1 - \frac{\alpha}{2\delta}\right) < \alpha.$$

Secondo caso. Se V cambia segno una sola volta nell'intervallo $[\zeta, \zeta+\delta-\alpha]$, diciamo in $\eta = \eta_1$, si ha

$$\int_\zeta^{\zeta+\delta-\alpha} \bigl|V(\eta)\bigr| \,\mathrm{d}\eta = \left|\int_\zeta^{\eta_1} V(\eta) \,\mathrm{d}\eta\right| + \left|\int_{\eta_1}^{\zeta+\delta-\alpha} V(\eta) \,\mathrm{d}\eta\right| \le 2A,$$

per il Lemma 4.5.5. Se invece V non cambia segno, sempre per lo stesso Lemma,

$$\int_\zeta^{\zeta+\delta-\alpha} \bigl|V(\eta)\bigr| \,\mathrm{d}\eta = \left|\int_\zeta^{\zeta+\delta-\alpha} V(\eta) \,\mathrm{d}\eta\right| \le A.$$

In definitiva

$$\int_\zeta^{\zeta+\delta} \bigl|V(\eta)\bigr| \,\mathrm{d}\eta = \left\{\int_\zeta^{\zeta+\delta-\alpha} + \int_{\zeta+\delta-\alpha}^{\zeta+\delta}\right\} \bigl|V(\eta)\bigr| \,\mathrm{d}\eta \le 2A + \alpha^2 + o(1) = \alpha_2\delta + o(1),$$

dove

$$\alpha_2 \stackrel{\text{def}}{=} \frac{2A + \alpha^2}{\delta} = \alpha\left(1 - \frac{\alpha}{2\delta}\right) = \alpha_1.$$

In ogni caso, dunque, abbiamo

$$\int_{\zeta}^{\zeta+\delta} \big|V(\eta)\big|\,\mathrm{d}\eta \le \alpha_1\delta + o(1), \tag{4.5.6}$$

dove $o(1)$ indica una funzione infinitesima per $\zeta \to \infty$. Per ottenere l'assurdo desiderato, suddividiamo l'intervallo $[0,\xi]$ in sottointervalli di ampiezza δ, su ciascuno dei quali applichiamo la (4.5.6). Poniamo $M \stackrel{\text{def}}{=} [\xi/\delta]$. Si ha

$$\begin{aligned}\int_0^{\xi} \big|V(\eta)\big|\,\mathrm{d}\eta &= \sum_{k=0}^{M-1} \int_{k\delta}^{(k+1)\delta} \big|V(\eta)\big|\,\mathrm{d}\eta + \int_{M\delta}^{\xi} \big|V(\eta)\big|\,\mathrm{d}\eta \\ &\le \alpha_1 M\delta + o(M) + \mathcal{O}(1) = \alpha_1\xi + o(\xi).\end{aligned}$$

Ma questo implica immediatamente che $\beta \le \alpha_1 < \alpha$, in contraddizione con il Lemma 4.5.4. Dunque $\alpha = 0$, come si voleva. □

Questo dimostra il Teorema dei Numeri Primi nella forma $\psi(x) \sim x$, o nella forma e-
𝔈 4.5.1–2 quivalente $\pi(x) \sim x(\log x)^{-1}$. Per poter confrontare questo risultato con il Teorema 4.1.3, osserviamo che mediante integrazioni per parti ripetute è facile mostrare che per ogni $n \in \mathbb{N}$
𝔈 4.5.3 fissato si ha

$$\mathrm{li}(x) = \frac{x}{\log x}\sum_{k=0}^{n}\frac{k!}{(\log x)^k} + \mathcal{O}_n\left(\frac{x}{(\log x)^{n+2}}\right). \tag{4.5.7}$$

Quindi abbiamo dimostrato che $\mathrm{li}(x) \sim x(\log x)^{-1} \sim \pi(x)$. Nelle applicazioni, però, è estremamente importante avere informazioni piú precise sulla quantità $\pi(x) - \mathrm{li}(x)$. Si vedano i commenti nel Capitolo 7.

§4.6. Altri risultati su alcune funzioni aritmetiche

In questo paragrafo poniamo

$$P(x) \stackrel{\text{def}}{=} \prod_{p\le x} p = \exp\theta(x).$$

Teorema 4.6.1. *Si ha*

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

Dim.: Disponiamo i numeri primi $p_1, p_2, \ldots,$ in ordine crescente, poniamo $n_0 \stackrel{\text{def}}{=} 1$ e per $k \in \mathbb{N}^*$ definiamo $n_k \stackrel{\text{def}}{=} P(p_k) = \exp\big(\theta(p_k)\big)$. Qualunque sia $n \in \mathbb{N}^*$, esiste $k \in \mathbb{N}$ tale che $n \in [n_k, n_{k+1})$, poiché la successione $(n_k)_{k\in\mathbb{N}}$ è strettamente crescente e diverge a $+\infty$. Vogliamo dimostrare la disuguaglianza

$$\frac{\varphi(n)}{n} \ge \frac{\varphi(n_k)}{n_k},$$

cioè che gli n_k sono punti di minimo locale per questo rapporto. Siano q_1, q_2, $\dots$, q_r, i fattori primi di n, contati ciascuno una volta sola, e disposti in ordine crescente. La disuguaglianza di sopra è equivalente a

$$\prod_{j=1}^{r}\Big(1-\frac{1}{q_j}\Big)\geq\prod_{j=1}^{k}\Big(1-\frac{1}{p_j}\Big).$$

Osserviamo che $r\leq k$ (poiché n_{k+1} è il piú piccolo numero naturale m che soddisfa $\omega(m)\geq k+1$), e che si ha $q_j\geq p_j$ per $j=1,\dots,r$. Quindi

$$\prod_{j=1}^{r}\Big(1-\frac{1}{q_j}\Big)\geq\prod_{j=1}^{r}\Big(1-\frac{1}{p_j}\Big)\geq\prod_{j=1}^{k}\Big(1-\frac{1}{p_j}\Big),$$

come si voleva. Osserviamo che per il Teorema di Mertens 4.3.6,

$$\frac{\varphi(n_k)}{n_k}=\prod_{j=1}^{k}\Big(1-\frac{1}{p_j}\Big)=\prod_{p\leq p_k}\Big(1-\frac{1}{p}\Big)=\frac{e^{-\gamma}}{\log p_k}\big(1+o(1)\big),$$

e cioè $n_k^{-1}\varphi(n_k)\log p_k=e^{-\gamma}\big(1+o(1)\big)$. Resta da dimostrare che

$$\lim_{k\to\infty}\frac{\log p_k}{\log\log n_k}=1.$$

Per definizione di n_k abbiamo $\log n_k=\theta(p_k)$, e per le disuguaglianze di Chebyshev 4.2.2 si ha $c_1p_k\leq\theta(p_k)\leq c_2p_k$ per opportune costanti positive c_1 e c_2, da cui $\log\log n_k=\log\theta(p_k)=\log p_k+\mathcal{O}(1)$.

Mettendo insieme queste disuguaglianze, concludiamo che quando $n\to\infty$ si ha

$$\frac{\varphi(n)\log\log n}{n}\geq e^{-\gamma}\big(1+o(1)\big)\qquad\text{e inoltre}\qquad\lim_{k\to\infty}\frac{\varphi(n_k)\log\log n_k}{n_k}=e^{-\gamma},$$

che insieme danno la tesi. □

Teorema 4.6.2. *Si ha $1\leq\omega(n)\leq\Omega(n)$ per ogni $n\geq2$ ed inoltre*

$$\liminf_{n\to\infty}\omega(n)=\liminf_{n\to\infty}\Omega(n)=1,$$
$$\limsup_{n\to\infty}\frac{\omega(n)\log\log n}{\log n}=1,\qquad\limsup_{n\to\infty}\frac{\Omega(n)}{\log n}=\frac{1}{\log2}.$$

Dim.: Le prime affermazioni seguono immediatamente dalle definizioni. Per quanto riguarda l'ultima, poiché 2^k è il piú piccolo intero positivo per cui $\Omega(n)\geq k$, si ha $\dfrac{\Omega\big(2^k\big)}{\log2^k}=\dfrac{1}{\log2}$ ed inoltre $\dfrac{\Omega(n)}{\log n}\leq\dfrac{k}{\log n}\leq\dfrac{\Omega\big(2^k\big)}{\log2^k}=\dfrac{1}{\log2}$ per tutti gli $n\in\big[2^k,2^{k+1}\big)$. Per dimostrare

la penultima disuguaglianza useremo il Teorema dei Numeri Primi 4.1.3. È chiaro che il piú piccolo intero positivo n_k per cui $\omega(n_k) = k$ è $n = p_1 \cdots p_k$, dove p_i indica l'i-esimo numero primo. Dunque abbiamo

$$\omega\big(P(x)\big) = \pi(x) \sim \frac{x}{\log x}, \tag{4.6.1}$$

per il Teorema dei Numeri Primi 4.1.3. Ma $\log P(x) = \theta(x) \sim x$, sempre per lo stesso risultato, e quindi $\log\log P(x) \sim \log x$. Sostituendo nella (4.6.1) si ha

$$\omega\big(P(x)\big) \sim \frac{\log P(x)}{\log\log P(x)}.$$

Inoltre la funzione $\dfrac{\log n}{\log\log n}$ è crescente per n grande, e la disuguaglianza voluta segue, come sopra. □

Teorema 4.6.3. *Esistono costanti A, $B \in \mathbb{R}$ tali che per $x \to \infty$ si ha*

$$\sum_{n\le x} \omega(n) = x\log\log x + Ax + o(x), \quad \sum_{n\le x} \Omega(n) = x\log\log x + Bx + o(x).$$

Dim.: Per la Formula di Mertens per i primi 4.3.4 si ha

$$\begin{aligned}\sum_{n\le x} \omega(n) &= \sum_{p\le x} \sum_{\substack{n\le x\\ p\mid n}} 1 = \sum_{p\le x} \left[\frac{x}{p}\right] = \sum_{p\le x} \left(\frac{x}{p} + \mathcal{O}(1)\right)\\ &= x\big(\log\log x + A + o(1)\big) + \mathcal{O}(\pi(x)) = x\log\log x + Ax + o(x).\end{aligned}$$

L'altra relazione si dimostra in modo analogo, considerando $\sum_{n\le x}\big(\Omega(n) - \omega(n)\big)$. □

Definizione 4.6.4. *Diciamo che un numero $n \in \mathbb{N}^*$ è* libero da quadrati *se $d^2 \mid n \Rightarrow |d| = 1$, cioè se n non è divisibile per il quadrato di alcun numero primo. In termini della funzione di Möbius, questo è equivalente a dire che $\mu(n) \neq 0$, oppure che $|\mu(n)| = \mu^2(n) = 1$.*

Teorema 4.6.5. *Per $N \to \infty$ si ha*

$$Q(N) \stackrel{\text{def}}{=} \sum_{n\le N} \mu^2(n) = \frac{6}{\pi^2} N + \mathcal{O}\Big(N^{1/2}\Big).$$

Dim.: Per quanto visto sopra, abbiamo

$$\begin{aligned}\sum_{n\le N} \mu^2(n) &= \sum_{n\le N} \sum_{d^2\mid n} \mu(d) = \sum_{d\le N^{1/2}} \mu(d) \sum_{\substack{n\le N\\ d^2\mid n}} 1\\ &= \sum_{d\le N^{1/2}} \mu(d) \left[\frac{N}{d^2}\right] = N \sum_{d\le N^{1/2}} \frac{\mu(d)}{d^2} + \mathcal{O}\Big(N^{1/2}\Big).\end{aligned}$$

L'errore introdotto completando la somma a tutti i $d \ge 1$ è a sua volta $\mathcal{O}\big(N^{1/2}\big)$, e la somma infinita risultante vale $\zeta(2)^{-1}$. Il risultato voluto segue immediatamente. Si vedano
𝔈 4.6.1 il Teorema 7.1.2 e gli Esercizi. □

Teorema 4.6.6. *Per $N \to \infty$ si ha*

$$\sum_{n\le N} \frac{1}{\varphi(n)} = \frac{\zeta(2)\zeta(3)}{\zeta(6)} \log N + \mathcal{O}(1).$$

Dim.: Si verifica immediatamente che $\dfrac{N_1}{\varphi} = \dfrac{\mu^2}{\varphi} * N_0$. Il Metodo dell'Iperbole 3.1.13 con $y = x$ dà

$$\begin{aligned}\sum_{n\le N} \frac{n}{\varphi(n)} &= N \sum_{n\le N} \frac{\mu^2(n)}{n\varphi(n)} + \mathcal{O}\left(\sum_{n\le N} \frac{\mu^2(n)}{\varphi(n)} \right) \\ &= N \sum_{n\ge 1} \frac{\mu^2(n)}{n\varphi(n)} + \mathcal{O}\left(N \sum_{n>N} \frac{\mu^2(n)}{n\varphi(n)} + \sum_{n\le N} \frac{\mu^2(n)}{\varphi(n)} \right).\end{aligned}$$

Per il Teorema 4.6.1 i termini d'errore sono entrambi $\mathcal{O}\big((\log N)^2\big)$. Il Teorema 3.3.1 mostra che la serie vale $\prod_p \big(1 + (p^2 - p)^{-1}\big)$ e con un breve calcolo si trova che questo è $\zeta(2)\zeta(3)\zeta(6)^{-1}$. Il risultato cercato segue per sommazione parziale. □

Teorema 4.6.7 (Formula di Gandhi). *Sia p_n l'n-esimo numero primo e sia $P_n \stackrel{\text{def}}{=} p_1 \cdot p_2 \cdots p_n$. Allora per $n \ge 0$ si ha*

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

Dim.: Per $n = 0$ si ha $P_0 = 1$ e quindi la formula dà $p_1 = 2$. Supponiamo che $n \ge 1$. Si ha

$$S_n \stackrel{\text{def}}{=} \sum_{d\mid P_n} \frac{\mu(d)}{2^d - 1} = \sum_{k\ge 1} \sum_{d\mid P_n} \frac{\mu(d)}{2^{kd}} = \sum_{m\ge 1} \frac{1}{2^m} \sum_{\substack{d\mid m \\ d\mid P_n}} \mu(d) = \sum_{m\ge 1} \frac{1}{2^m} I\big((m, P_n)\big)$$

dove I è l'identità. Ma $(m, P_n) = 1$ se e solo se $m = 1$ oppure tutti i fattori primi di m superano p_n. Dunque

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

In particolare se $n \ge 1$

$$\begin{aligned} S_n &> \frac{1}{2} + \frac{1}{2^{p_{n+1}}} \\ S_n &< \frac{1}{2} + \frac{1}{2^{p_{n+1}}} \left(1 + \frac{1}{2^2} + \frac{1}{2^4} + \cdots \right) = \frac{1}{2} + \frac{4}{3 \cdot 2^{p_{n+1}}} \end{aligned}$$

poiché tutti i numeri primi tranne $p_1 = 2$ sono dispari. Da questo segue che

$$1 - \log_2 \Big(S_n - \frac{1}{2} \Big) \in \left(p_{n+1} + 1 - \log_2 \frac{4}{3}, p_{n+1} + 1 \right) = \left(p_{n+1} + \log_2 \frac{3}{2}, p_{n+1} + 1 \right)$$

$d=1$	0 . 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 ...
$d=2$	−0 . 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 0 1 ...
$d=3$	−0 . 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 0 0 1 ...
$d=5$	−0 . 0 0 0 0 1 0 0 0 0 1 0 0 0 0 1 0 0 0 0 1 0 0 0 0 1 0 0 0 0 1 ...
$d=6$	0 . 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 0 0 0 0 0 1 ...
$d=10$	0 . 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 1 ...
$d=15$	0 . 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 ...
$d=30$	−0 . 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 ...
$S_3 =$	0 . 1 0 0 0 0 0 1 0 0 0 1 0 1 0 0 0 1 0 1 0 0 0 1 0 0 0 0 0 1 0 ...

Figura 4.2. *La Formula di Gandhi "corrisponde" a fare un crivello con i fattori primi di P_n. Si veda il Principio di Inclusione–Esclusione* 6.1.2.

che implica la tesi. □

Nel Capitolo 2 abbiamo visto la descrizione di alcuni algoritmi: le stime dei loro tempi di esecuzione dipendono spesso dalla distribuzione degli interi con particolari vincoli moltiplicativi. Senza alcuna pretesa di completezza, parliamo brevemente della piú importante fra le funzioni enumeratrici degli interi suddetti. Poniamo

$$\Psi(x,y) \stackrel{\text{def}}{=} |\{n \le x \colon p \mid n \Rightarrow p \le y\}|.$$

L'obiettivo è il conteggio degli interi $n \le x$ che non hanno fattori primi "grandi," dove la grandezza dei fattori primi è misurata dal parametro y. Cominciamo con una semplice osservazione: per ogni $\sigma > 0$ si ha

$$\Psi(x,y) = \sum_{\substack{n \le x \\ p \mid n \Rightarrow p \le y}} 1 \le \sum_{\substack{n \le x \\ p \mid n \Rightarrow p \le y}} \left(\frac{x}{n}\right)^{\sigma} \le \sum_{\substack{n \ge 1 \\ p \mid n \Rightarrow p \le y}} \left(\frac{x}{n}\right)^{\sigma} = x^{\sigma} \prod_{p \le y} \bigl(1 - p^{-\sigma}\bigr)^{-1}. \tag{4.6.2}$$

È evidente che questa relazione è interessante solo per $\sigma < 1$, poiché per $\sigma \ge 1$ il secondo membro è $\ge x$: vogliamo dunque scegliere σ in modo "ottimale" per ottenere una buona maggiorazione. Osserviamo che per y *limitato* è possibile stimare direttamente $\Psi(x,y)$ con il metodo illustrato nella dimostrazione del Teorema di Schur 1.7.2, con il risultato che

$$\Psi(x,y) \sim \Bigl(\pi(y)! \prod_{p \le y} \log p\Bigr)^{-1} (\log x)^{\pi(y)}. \tag{4.6.3}$$

È possibile dimostrare un risultato simile quando y è "piccolo" rispetto ad x: in particolare, se $2 \le y \le \sqrt{\log x}$, prendiamo $\sigma = c(\log x)^{-1}$ dove $c > 0$ verrà scelta piú avanti. Quindi $p^{\sigma} = \exp\bigl(\sigma \log p\bigr) = 1 + \sigma \log p + \mathcal{O}\bigl(\sigma^2 \log^2 p\bigr)$ e la (4.6.2) dà

$$\begin{aligned}
\log \Psi(x,y) &\le c + \sum_{p \le y} \log \frac{p^{\sigma}}{p^{\sigma} - 1} = c + \sigma\theta(y) - \sum_{p \le y} \log\Bigl(\sigma \log p\bigl(1 + \mathcal{O}(\sigma \log p)\bigr)\Bigr) \\
&= c + \sigma\theta(y) - \pi(y) \log \sigma - \sum_{p \le y} \log\log p + \mathcal{O}(\sigma\theta(y)) \\
&= c - \pi(y) \log c + \pi(y) \log\log x - \sum_{p \le y} \log\log p + \mathcal{O}(\sigma y).
\end{aligned}$$

Si osservi ora che la funzione $g(t) = t - A\log t$ ha un minimo per $t = A$: scelto dunque $c = \pi(y)$ si ottiene

$$\Psi(x,y) \le \left(\frac{e}{\pi(y)}\right)^{\pi(y)} \Big(\prod_{p\le y}\log p\Big)^{-1} (\log x)^{\pi(y)} \left\{1 + \mathcal{O}\left(\frac{y^2}{\log x\log y}\right)\right\} \tag{4.6.4}$$

Per la formula di Stirling $n! \sim \sqrt{2\pi n}\big(\frac{n}{e}\big)^n$ e quindi la stima (4.6.4) non è molto piú debole della formula asintotica (4.6.3). È importante cercare di estendere questo tipo di stime anche al caso in cui y è piú grande: per esempio, prendendo $\sigma = 1 - (2\log y)^{-1}$ in (4.6.2) ed usando le Formule di Mertens e la stima $p^{1-\sigma} = 1 + \mathcal{O}((1-\sigma)\log p)$ si ottiene la maggiorazione universale, valida per $x \ge 1$, $y \ge 2$, $\Psi(x,y) \ll xe^{-u/2}\log y$, dove $u = (\log x)/\log y$.

§4.7. Considerazioni finali

Le formule di Mertens 4.3.2 e 4.3.4 ed il Teorema di Mertens 4.3.6 danno informazioni sulla "densità" dei numeri primi nella successione dei numeri naturali. Può essere un buon esercizio sulla sommazione parziale A.1.1 dimostrare le formule analoghe in cui somme e prodotti sono estesi a tutti i numeri naturali. L'analoga della 4.3.4 è ovviamente il Teorema
𝔈 4.7.1 A.4.1 con $k = -1$, mentre le altre due diventano rispettivamente

$$\begin{aligned} \sum_{n\le x}\frac{\log n}{n} &= \frac{1}{2}(\log x)^2 + \mathcal{O}(\log x),\\ \prod_{2\le n\le x}\left(1-\frac{1}{n}\right) &= \frac{1}{[x]} = \frac{1}{x} + \mathcal{O}\left(\frac{1}{x^2}\right). \end{aligned} \tag{4.7.1}$$

Inoltre è importante notare che il Teorema dei Numeri Primi nella forma (che non abbiamo dimostrato)

$$\pi(x) = \frac{x}{\log x} + \frac{x}{(\log x)^2} + \mathcal{O}\left(\frac{x}{(\log x)^3}\right), \tag{4.7.2}$$

permette di migliorare alcune delle formule di Mertens: per esempio per sommazione parziale possiamo ottenere

$$\theta(x) = \pi(x)\log x - \int_2^x \frac{\pi(t)}{t}\mathrm{d}t = x + \mathcal{O}\left(\frac{x}{(\log x)^2}\right), \tag{4.7.3}$$

e poi

$$\begin{aligned} \sum_{p\le x}\frac{\log p}{p} &= \frac{\theta(x)}{x} + \int_2^x \frac{\theta(t)}{t^2}\mathrm{d}t = 1 + \mathcal{O}\big((\log x)^{-2}\big) + \int_2^x \frac{\mathrm{d}t}{t} + \int_2^x \frac{\theta(t)-t}{t^2}\mathrm{d}t\\ &= \log x + c + o(1), \end{aligned} \tag{4.7.4}$$

per un'opportuna costante c, poiché l'ultimo integrale può essere esteso a tutta la semiretta $[2,+\infty)$ e risulta convergente. Si osservi infine che, sempre per sommazione parziale, è possibile dedurre la (4.7.2) dalla (4.7.3).

È comunque importante sottolineare il fatto che il Teorema dei Numeri Primi nella forma che abbiamo dimostrato è *equivalente* alla (4.7.4).

Capitolo 5. Primi nelle Progressioni Aritmetiche

§5.1. Caratteri di un gruppo abeliano

Svilupperemo la teoria dei caratteri solo per la parte che ci interessa direttamente.

Definizione 5.1.1. *Sia G un gruppo abeliano. Diciamo che $\chi\colon G \to \mathbb{C}^*$ è un* carattere *di G se χ è un omomorfismo.*

Lemma 5.1.2. *Sia G un gruppo ciclico finito di ordine n, generato da un suo elemento g. G ha esattamente n caratteri, e per ogni carattere χ di G esiste un intero $k \in \{0, \dots, n-1\}$ tale che $\chi(g) = e^{2\pi i k/n}$.*

Dim.: Basta osservare che $\chi\big(g^n\big) = \chi(g)^n = 1$ dato che $g^n = 1$. □

Lemma 5.1.3. *Se $G = G_1 \times G_2$ è un gruppo abeliano, e G_1 ha n_1 caratteri, G_2 ha n_2 caratteri, allora G ha $n_1 n_2$ caratteri.*

Corollario 5.1.4. *Se G è un gruppo abeliano finito, allora G ha $|G|$ caratteri.*

Nel seguito denoteremo con $\widehat{G}$ l'insieme dei caratteri $\chi\colon G \to \mathbb{C}^*$. Osserviamo che $\widehat{G}$ risulta essere un gruppo abeliano se poniamo per definizione

$$\chi_1\chi_2(g) \stackrel{\text{def}}{=} \chi_1(g)\chi_2(g)$$
$$\chi^{-1}(g) \stackrel{\text{def}}{=} \chi(g)^{-1}$$

Se G è finito, allora $\chi^{-1}(g) = \overline{\chi}(g)$.

Lemma 5.1.5. *Se G è un gruppo ciclico di ordine n, allora $\widehat{G} \simeq G$.*

Dim.: Se G è generato da g e ξ è una radice n-esima primitiva dell'unità (cioè se $\xi \in \mathbb{C}$ soddisfa $\xi^n = 1$, ed inoltre $\xi^d \neq 1$ per ogni $d \in \{1, \dots, n-1\}$), basta porre $\chi_j(g) = \xi^j$. □

Corollario 5.1.6. *Se G è un gruppo abeliano finito allora $\widehat{G} \simeq G$.*

Dim.: G è prodotto diretto di sottogruppi ciclici. □

Definizione 5.1.7. *Il carattere $\chi_0: G \to \mathbb{C}^*$ tale che $\chi_0(g) = 1$ per ogni $g \in G$ si dice* carattere principale.

Teorema 5.1.8 (Relazioni di ortogonalità). *Se G è un gruppo abeliano finito di ordine n e χ_0 è il carattere principale, si ha*

$$\sum_{g\in G} \chi(g) = \begin{cases} n & \text{se } \chi = \chi_0, \\ 0 & \text{se } \chi \neq \chi_0; \end{cases} \qquad \sum_{\chi\in\widehat{G}} \chi(g) = \begin{cases} n & \text{se } g = 1, \\ 0 & \text{se } g \neq 1. \end{cases}$$

Dim.: Sia $S \stackrel{\text{def}}{=} \sum_{g\in G} \chi(g)$. Se $\chi \neq \chi_0$, esiste $g_1 \in G$ tale che $\chi(g_1) \neq 1$. Quindi

$$\chi(g_1)S = \chi(g_1) \sum_{g\in G} \chi(g) = \sum_{g\in G} \chi(gg_1) = \sum_{h\in G} \chi(h) = S,$$

e la tesi segue. Sia $S \stackrel{\text{def}}{=} \sum_{\chi\in\widehat{G}} \chi(g)$. Se $g \neq 1$, esiste $\chi_1 \in \widehat{G}$ tale che $\chi_1(g) \neq 1$. Quindi

$$\chi_1(g)S = \chi_1(g) \sum_{\chi\in\widehat{G}} \chi(g) = \sum_{\chi\in\widehat{G}} \chi_1\chi(g) = \sum_{\psi\in\widehat{G}} \psi(g) = S,$$

ed anche la seconda relazione segue immediatamente. □

Definizione 5.1.9. *Dato $q \in \mathbb{N}^*$, e dato $\chi \in \widehat{\mathbb{Z}_q^*}$, chiamiamo* carattere di Dirichlet modulo *q la funzione $f: \mathbb{Z} \to \mathbb{C}$ definita da*

$$f(n) \stackrel{\text{def}}{=} \begin{cases} 0 & \text{se } (n,q) > 1, \\ \chi(n) & \text{se } (n,q) = 1. \end{cases}$$

Con questa definizione, i caratteri di Dirichlet risultano essere funzioni completamente moltiplicative. Con abuso di linguaggio, useremo la lettera χ per indicare sia il carattere
𝔈 5.1.1–2 del gruppo $\mathbb{Z}_q^*$, sia la sua estensione a $\mathbb{Z}$. Si vedano le tabelle dopo la Bibliografia.

Definizione 5.1.10. *Si dice* carattere principale *modulo q il carattere di Dirichlet χ_0*

$$\chi_0(n) \stackrel{\text{def}}{=} \begin{cases} 1 & \text{se } (n,q) = 1, \\ 0 & \text{se } (n,q) > 1. \end{cases}$$

Osservazione 5.1.11. *Le relazioni di ortogonalità* 5.1.8 *permettono di scegliere la progressione aritmetica $n \equiv a \mod q$, purché $(a,q) = 1$: infatti, per ogni successione (α_n) si ha*

$$\sum_{\substack{n\le x \\ n\equiv a \bmod q}} \alpha_n = \frac{1}{\varphi(q)} \sum_{n\le x} \alpha_n \sum_{\chi \bmod q} \overline{\chi}(a)\chi(n) = \frac{1}{\varphi(q)} \sum_{\chi \bmod q} \overline{\chi}(a) \sum_{n\le x} \chi(n)\alpha_n,$$

dove la prima somma interna è su tutti i caratteri modulo q, poiché ciascun addendo della somma interna vale $\chi(na^{-1})$ e la somma vale dunque $\varphi(q)$ se $n \equiv a \mod q$ e 0 altrimenti.

§5.2. Caratteri e funzioni L di Dirichlet

Lemma 5.2.1. *Sia $\chi \mod q$ un carattere non principale, $\Re(\delta) > 0$, $\frac{3}{2} \le x \le y$. Si ha*

$$\sum_{x<n\le y} \frac{\chi(n)}{n^\delta} = \mathcal{O}_q\big(x^{-\delta}\big), \qquad \sum_{x<n\le y} \frac{\chi(n)\log n}{n^\delta} = \mathcal{O}_q\big(x^{-\delta}\log x\big).$$

Dim.: Per la formula di sommazione parziale A.1.1 e per le relazioni di ortogonalità 5.1.8

$$\begin{aligned}\sum_{x<n\le y} \frac{\chi(n)}{n^\delta} &= y^{-\delta} \sum_{x<n\le y} \chi(n) + \delta \int_x^y \sum_{x<n\le t} \chi(n) \frac{\mathrm{d}t}{t^{\delta+1}} \\ &= \mathcal{O}_q\big(y^{-\delta}\big) + \delta \int_x^y \frac{\mathcal{O}_q(1)}{t^{\delta+1}}\mathrm{d}t = \mathcal{O}_q\big(y^{-\delta}\big) + \mathcal{O}_q\big(x^{-\delta}\big) = \mathcal{O}_q\big(x^{-\delta}\big).\end{aligned}$$

La seconda disuguaglianza si dimostra in modo analogo. □

Definizione 5.2.2. *Dato un carattere $\chi \mod q$ definiamo la* funzione L di Dirichlet *$L(s,\chi)$ e la* funzione zeta di Riemann *$\zeta(s)$ per mezzo delle relazioni*

$$L(s,\chi) \stackrel{\text{def}}{=} \sum_{n\ge1} \frac{\chi(n)}{n^s}, \qquad \zeta(s) \stackrel{\text{def}}{=} \sum_{n\ge1} \frac{1}{n^s}.$$

Teorema 5.2.3. *Se $\chi \neq \chi_0$, la serie $L(s,\chi)$ converge per $\sigma = \Re(s) > 0$, e totalmente in $\sigma \ge \delta$ per ogni $\delta > 0$ fissato. Invece le serie $\zeta(s)$ ed $L(s,\chi_0)$ convergono per $\sigma = \Re(s) > 1$, e totalmente in $\sigma \ge 1+\delta$ per ogni $\delta > 0$ fissato.*

Dim.: La prima parte è una conseguenza immediata del Lemma 5.2.1 con $\delta \stackrel{\text{def}}{=} \sigma$. Se $\chi = \chi_0$ abbiamo

$$A(x) \stackrel{\text{def}}{=} \sum_{n\le x} \chi(n) = \frac{\varphi(q)}{q}x + \mathcal{O}_q(1),$$

e quindi, per la formula di sommazione parziale A.1.1 con $f(x) = x^{-s}$ ed $a(n) = \chi_0(n)$:

$$\sum_{n\le x} \frac{\chi(n)}{n^s} = A(x)x^{-s} + s\int_1^x \frac{A(t)}{t^{s+1}}\mathrm{d}t = \frac{\varphi(q)}{q}\left\{x^{1-s} + \mathcal{O}_q\big(x^{-\sigma}\big) + s\int_1^x \frac{t+\mathcal{O}_q(1)}{t^{s+1}}\mathrm{d}t\right\},$$

e l'integrale è convergente solo se $\sigma = \Re(s) \ge 1+\delta$. □

Osservazione 5.2.4. *Preso un carattere di Dirichlet $\chi \mod q$ ed il carattere principale $\chi_0 \mod q$, e posto $f(n) = \chi(n)n^{-s}$, $f(n) = \chi_0(n)n^{-s}$ rispettivamente, per il Prodotto di Eulero* 3.3.1, *per $\sigma > 1$ si hanno le rappresentazioni*

$$L(s,\chi) = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} \qquad \text{e} \qquad L(s,\chi_0) = \zeta(s)\prod_{p\mid q}\left(1-\frac{1}{p^s}\right).$$

Si osservi che la prima di queste uguaglianze vale solo in $\sigma > 1$ e non nel semipiano piú grande $\sigma > 0$ dove converge la serie che definisce L se $\chi \neq \chi_0$, poiché in $0 < \sigma \leq 1$ la convergenza non è assoluta.

Osservazione 5.2.5. *La derivata di $L(s,\chi)$ è*

$$L'(s,\chi) = -\sum_{n\geq 1} \frac{\chi(n)\log n}{n^s}.$$

La serie data converge totalmente in $\sigma \geq 1+\delta$ per ogni $\delta > 0$ fissato (per il Lemma 5.2.1) ed anche la serie per $L(s,\chi)$ converge totalmente nello stesso insieme, ed è per questo motivo che si può derivare termine a termine. Ad ogni modo, la serie risulta convergente per $\sigma > 0$ se $\chi \neq \chi_0$ per lo stesso Lemma.

In questo paragrafo vogliamo dimostrare che esistono infiniti primi in ogni progressione aritmetica $a + nq$ con $(a,q) = 1$. Per una motivazione di quanto segue, si legga il §7.6.

Lemma 5.2.6. *Sia χ un carattere reale non principale modulo q. Allora $L(1,\chi) \neq 0$.*

Dim.: Consideriamo la funzione aritmetica $F \stackrel{\text{def}}{=} \chi * N_0$. Per il Teorema 3.1.4, anche F è una funzione moltiplicativa e si vede molto facilmente che

$$F\big(p^k\big) = \begin{cases} k+1 & \text{se } \chi(p) = 1, \\ 1 & \text{se } \chi(p) = -1 \text{ e } k \text{ è pari}, \\ 0 & \text{se } \chi(p) = -1 \text{ e } k \text{ è dispari}, \\ 1 & \text{se } p \mid q \text{ (cioè se } \chi(p) = 0). \end{cases}$$

Dunque, in ogni caso

$$F(n) \geq \begin{cases} 1 & \text{se } n = m^2, \\ 0 & \text{altrimenti.} \end{cases}$$

Perciò

$$G(x) \stackrel{\text{def}}{=} \sum_{n\leq x} \frac{F(n)}{n^{1/2}} \geq \sum_{m^2\leq x} \frac{F\big(m^2\big)}{m} \geq \sum_{m\leq x^{1/2}} \frac{1}{m} \to +\infty$$

quando $x \to \infty$. Ma abbiamo anche

$$\begin{aligned} G(x) &= \sum_{n\leq x} \frac{1}{n^{1/2}} \sum_{d\mid n} \chi(d) = \sum_{hk\leq x} \frac{\chi(h)}{\big(hk\big)^{1/2}} \\ &= \sum_{h\leq x^{1/2}} \frac{\chi(h)}{h^{1/2}} \sum_{k\leq x/h} k^{-1/2} + \sum_{k<x^{1/2}} k^{-1/2} \sum_{x^{1/2}<h\leq x/k} \frac{\chi(h)}{h^{1/2}} = \Sigma_1 + \Sigma_2, \end{aligned}$$

diciamo. Stimiamo Σ_1 come segue: per i Lemmi A.4.1 e 5.2.1,

$$\begin{aligned} \Sigma_1 &= \sum_{h\leq x^{1/2}} \frac{\chi(h)}{h^{1/2}} \Big\{ 2\left(\frac{x}{h}\right)^{1/2} + C + \mathcal{O}\Big(\Big(\frac{h}{x}\Big)^{1/2}\Big)\Big\} = 2\sqrt{x} \sum_{h\leq x^{1/2}} \frac{\chi(h)}{h} + \mathcal{O}_q(1) \\ &= 2\sqrt{x}\Big\{\sum_{h\geq 1} - \sum_{h>x^{1/2}}\Big\}\frac{\chi(h)}{h} + \mathcal{O}_q(1) = 2\sqrt{x}L(1,\chi) + \mathcal{O}_q(1). \end{aligned}$$

Invece $\Sigma_2 = \mathcal{O}_q(1)$ direttamente dal Lemma 5.2.1. In definitiva $G(x) = 2\sqrt{x}L(1,\chi) + \mathcal{O}(1)$, e la tesi segue poiché $G(x) \to \infty$ quando $x \to \infty$. □

LEMMA 5.2.7. *Sia χ un carattere non principale modulo q. Allora si ha*

$$-L'(1,\chi)\sum_{n\le x}\frac{\mu(n)\chi(n)}{n}=\begin{cases}\mathcal{O}_q(1) & \text{se } L(1,\chi)\neq 0,\\ -\log x+\mathcal{O}_q(1) & \text{se } L(1,\chi)=0.\end{cases}$$

DIM.: Ponendo $g(x)\stackrel{\text{def}}{=}x$, $h(n)\stackrel{\text{def}}{=}\chi(n)$, ed

$$f(x)\stackrel{\text{def}}{=}\sum_{n\le x}\frac{x}{n}\chi(n)=xL(1,\chi)+\mathcal{O}_q(1)$$

nella seconda formula di inversione di Möbius 3.1.12, poiché $|\mu(n)\chi(n)|\le 1$, troviamo

$$\begin{aligned}x&=\sum_{n\le x}\mu(n)\chi(n)\left\{\frac{x}{n}L(1,\chi)+\mathcal{O}_q(1)\right\}=xL(1,\chi)\sum_{n\le x}\frac{\mu(n)\chi(n)}{n}+\mathcal{O}_q\left(\sum_{n\le x}|\mu(n)\chi(n)|\right)\\&=xL(1,\chi)\sum_{n\le x}\frac{\mu(n)\chi(n)}{n}+\mathcal{O}_q(x).\end{aligned}$$

Se $L(1,\chi)\neq 0$, dividendo membro a membro l'uguaglianza precedente per x ricaviamo

$$L(1,\chi)\sum_{n\le x}\frac{\mu(n)\chi(n)}{n}=\mathcal{O}_q(1),$$

e, moltiplicando ambo i membri per $-L'(1,\chi)/L(1,\chi)=\mathcal{O}_q(1)$, troviamo la tesi. Se invece $L(1,\chi)=0$, ancora per la seconda formula di Möbius con $g(x)\stackrel{\text{def}}{=}x\log x$, $h(n)\stackrel{\text{def}}{=}\chi(n)$,

$$\begin{aligned}f(x)\stackrel{\text{def}}{=}\sum_{n\le x}\frac{x}{n}\log\frac{x}{n}\chi(n)&=x\log x\sum_{n\le x}\frac{\chi(n)}{n}-x\sum_{n\le x}\frac{\chi(n)\log n}{n}\\&=x\log x\big(L(1,\chi)+\mathcal{O}_q\big(x^{-1}\big)\big)-x\big(-L'(1,\chi)+\mathcal{O}_q\big(x^{-1}\log x\big)\big)\\&=xL'(1,\chi)+\mathcal{O}_q(\log x),\end{aligned}$$

per il Lemma 5.2.1. Quindi, invertendo

$$\begin{aligned}x\log x&=\sum_{n\le x}\mu(n)\chi(n)\left\{\frac{x}{n}L'(1,\chi)+\mathcal{O}_q\Big(\log\frac{x}{n}\Big)\right\}\\&=xL'(1,\chi)\sum_{n\le x}\frac{\mu(n)\chi(n)}{n}+\mathcal{O}_q(x),\end{aligned}$$

per il Lemma A.4.4. La tesi si ottiene dividendo la relazione precedente per x. □

Si noti che quella nell'enunciato è la somma parziale della serie di $L(1,\chi)^{-1}$, per il Corollario 3.1.10. È quindi naturale attendersi che questa quantità sia limitata se $L(1,\chi)\neq 0$, ed illimitata in caso contrario.

LEMMA 5.2.8. *Sia χ un carattere non principale modulo q. Si ha*

$$\sum_{p\le x}\frac{\chi(p)\log p}{p}=\begin{cases}\mathcal{O}_q(1) & \text{se } L(1,\chi)\neq 0,\\ -\log x+\mathcal{O}_q(1) & \text{se } L(1,\chi)=0.\end{cases}$$

DIM.: Posto

$$R(x)\stackrel{\text{def}}{=}\sum_{n\le x}\frac{\chi(n)\Lambda(n)}{n}-\sum_{p\le x}\frac{\chi(p)\log p}{p},$$

si vede facilmente che

$$|R(x)|\le\sum_{n\ge 2}\frac{\log n}{n(n-1)}=\mathcal{O}(1).$$

Quindi, usando i Lemmi 3.2.9 e 5.2.1, si ha

$$\begin{aligned}\sum_{p\le x}\frac{\chi(p)\log p}{p}&=\sum_{n\le x}\frac{\chi(n)\Lambda(n)}{n}+\mathcal{O}(1)\\ &=\sum_{n\le x}\frac{\chi(n)}{n}\sum_{d\mid n}\mu(d)\log\frac{n}{d}+\mathcal{O}(1)=\sum_{hk\le x}\frac{\chi(h)\chi(k)}{hk}\mu(h)\log k+\mathcal{O}(1)\\ &=\sum_{h\le x}\frac{\mu(h)\chi(h)}{h}\sum_{k\le x/h}\frac{\chi(k)\log k}{k}+\mathcal{O}(1)\\ &=\sum_{h\le x}\frac{\mu(h)\chi(h)}{h}\left\{-L'(1,\chi)+\mathcal{O}_q\left(\frac{\log(x/h)}{x/h}\right)\right\}+\mathcal{O}(1)\\ &=-L'(1,\chi)\sum_{h\le x}\frac{\mu(h)\chi(h)}{h}+\mathcal{O}_q\left(\sum_{h\le x}\frac{\log(x/h)}{x}\right)+\mathcal{O}(1)\\ &=-L'(1,\chi)\sum_{h\le x}\frac{\mu(h)\chi(h)}{h}+\mathcal{O}_q(1)\end{aligned}$$

per il Lemma A.4.4. Quindi la tesi segue dal Lemma 5.2.7. □

LEMMA 5.2.9. *Se χ è un carattere non principale modulo q, allora $L(1,\chi)\neq 0$.*

DIM.: Poniamo $N\stackrel{\text{def}}{=}|\{\chi\neq\chi_0\colon L(1,\chi)=0\}|$. Allora, per ortogonalità abbiamo

$$\begin{aligned}\varphi(q)\sum_{\substack{p\le x\\ p\equiv 1 \bmod q}}\frac{\log p}{p}&=\sum_{\chi \bmod q}\sum_{p\le x}\frac{\chi(p)\log p}{p}=\sum_{\substack{p\le x\\ p\nmid q}}\frac{\log p}{p}+\sum_{\chi\neq\chi_0}\sum_{p\le x}\frac{\chi(p)\log p}{p}\\ &=\log x+\mathcal{O}_q(1)-N\log x+\mathcal{O}_q(1)=(1-N)\log x+\mathcal{O}_q(1),\end{aligned}$$

per i Lemmi 4.3.2 e 5.2.8. Poiché la somma di partenza è positiva, N deve essere 0 oppure 1, e quindi $N=0$ poiché deve essere pari. Infatti, per il Lemma 5.2.6, se χ è un carattere reale allora $L(1,\chi)\neq 0$, mentre se χ non è reale allora $L(\overline{s},\overline{\chi})=\overline{L(s,\chi)}$ e quindi o $L(1,\chi)=L(1,\overline{\chi})=0$, oppure sono entrambi non nulli. □

§5.3. Il teorema di Dirichlet

Teorema 5.3.1 (Dirichlet). *Dato $q \in \mathbb{N}^*$, sia $a \in \mathbb{Z}$ un intero tale che $(a,q)=1$. Allora esistono infiniti numeri primi $p \equiv a \mod q$. Piú precisamente per $x \to \infty$ si ha*

$$\sum_{\substack{p\le x\\ p\equiv a \bmod q}} \frac{\log p}{p} = \frac{1}{\varphi(q)}\log x + \mathcal{O}_{q,a}(1).$$

Dim.: Per i Lemmi 5.2.8 e 5.2.9, se $\chi \neq \chi_0$ si ha

$$\sum_{p\le x} \frac{\chi(p)\log p}{p} = \mathcal{O}_{q,\chi}(1).$$

Per ortogonalità,

$$\begin{aligned}\varphi(q) \sum_{\substack{p\le x\\ p\equiv a \bmod q}} \frac{\log p}{p} &= \sum_{\chi \bmod q} \overline{\chi}(a) \sum_{p\le x} \chi(p)\frac{\log p}{p}\\ &= \sum_{\substack{p\le x\\ p\nmid q}} \frac{\log p}{p} + \sum_{\substack{\chi \bmod q\\ \chi\neq\chi_0}} \sum_{p\le x} \chi\big(pa^{-1}\big)\frac{\log p}{p} = \log x + \mathcal{O}_{q,a}(1),\end{aligned}$$

(per la seconda formula di Mertens 4.3.2) che è la tesi. □

Per completezza riportiamo l'enunciato del Teorema dei Numeri Primi nelle Progressioni Aritmetiche, dimostrato per la prima volta da de la Vallée Poussin nel 1897, nella versione di Siegel & Walfisz. Per la dimostrazione rimandiamo ai Capitoli 8–22 del libro di Davenport [12]. Questo risultato può essere espresso in modo piú pittoresco dicendo che i numeri primi sono equidistribuiti nelle progressioni aritmetiche.

Teorema 5.3.2. *Fissato $A>0$, esiste una costante $C=C(A)>0$ tale che per $x\to\infty$ ed uniformemente per $q \le (\log x)^A$ e per $(a,q)=1$ si ha*

$$\pi(x;q,a) \stackrel{\text{def}}{=} \sum_{\substack{p\le x\\ p\equiv a \bmod q}} 1 = \frac{1}{\varphi(q)}\operatorname{li}(x) + \mathcal{O}_A\Big(x\exp\big(-C\sqrt{\log x}\big)\Big).$$

§5.4. La disuguaglianza di Pólya–Vinogradov

Definizione 5.4.1. *Sia χ un carattere modulo q, sia q_1 un multiplo di q e sia χ_0 il carattere principale modulo q_1. Il carattere χ^* modulo q_1 definito da $\chi^* \stackrel{\text{def}}{=} \chi_0\chi$ si dice* indotto *da χ. Un carattere modulo q che* non è *indotto da altri caratteri modulo qualche divisore di q si dice* carattere primitivo*.*

Con queste definizioni, i caratteri modulo q si suddividono in tre categorie: il carattere principale, i caratteri primitivi e quelli indotti da altri caratteri. È interessante notare che

tutti i caratteri diversi dal carattere principale modulo numeri primi sono primitivi. Si vedano le tabelle nell'Appendice "Caratteri di Dirichlet." Si può notare che il carattere $\chi_2 \bmod 8$ è indotto da $\chi_1 \bmod 4$, e che $\chi_6 \bmod 15$ è indotto da $\chi_1 \bmod 3$ mentre χ_2, χ_5 e $\chi_7 \bmod 15$ sono indotti rispettivamente da χ_2, χ_1 e $\chi_3 \bmod 5$. Infine $\chi_1 \bmod 24$ è indotto da $\chi_1 \bmod 3$, $\chi_2 \bmod 24$ è indotto da $\chi_1 \bmod 4$, χ_5 e χ_7 sono indotti rispettivamente da χ_1 e $\chi_3 \bmod 8$ e χ_4 è indotto da un carattere mod 12. Si noti che se $\chi \bmod q$ induce $\chi^* \bmod q_1$ allora la funzione $L(s,\chi)$ differisce dalla funzione $L(s,\chi^*)$ solo per un prodotto finito (eventualmente vuoto) sui fattori primi di q_1/q, come si vede dall'Osservazione 5.2.4. Vediamo subito un risultato che vale solo per i caratteri primitivi.

LEMMA 5.4.2. *Sia $\tau(\chi)$ la somma di Gauss*

$$\tau(\chi) \stackrel{\text{def}}{=} \sum_{h \bmod q} \chi(h) e_q(h).$$

Se χ è un carattere primitivo si ha $|\tau(\chi)| = q^{1/2}$.

DIM.: Scegliamo n tale che $(n,q) = 1$, moltiplichiamo la somma di Gauss per $\overline{\chi}(n)$ e ricordiamo la proprietà delle somme sui residui modulo q già usata nella dimostrazione della Legge di Reciprocità Quadratica 1.6.4:

$$\overline{\chi}(n)\tau(\chi) = \sum_{h \bmod q} \chi\big(hn^{-1}\big) e_q(h) = \sum_{h_1 \bmod q} \chi(h_1) e_q(nh_1). \tag{5.4.1}$$

𝔈 5.4.1 Si può dimostrare, ma noi non lo faremo, che questa relazione vale anche se $(n,q) > 1$, perché χ è primitivo. Quindi

$$|\overline{\chi}(n)|^2 |\tau(\chi)|^2 = \sum_{h_1,\, h_2} \sum_{\bmod q} \chi(h_1)\overline{\chi}(h_2) e_q\big(n(h_1 - h_2)\big).$$

Sommiamo quest'ultima relazione su tutti gli n modulo q, ed usiamo il fatto che conosciamo la somma dei primi termini di una progressione geometrica:

$$\begin{aligned}\varphi(q)|\tau(\chi)|^2 &= \sum_{h_1,\, h_2} \sum_{\bmod q} \chi(h_1)\overline{\chi}(h_2) \sum_{n \bmod q} e_q\big(n(h_1 - h_2)\big) \\ &= \sum_{h_1,\, h_2} \sum_{\bmod q} \chi(h_1)\overline{\chi}(h_2) \begin{cases} q & \text{se } h_1 \equiv h_2 \bmod q, \\ 0 & \text{altrimenti,} \end{cases} = q\varphi(q).\end{aligned}$$

Il Lemma segue immediatamente. □

Se $\chi \bmod q$ è un qualsiasi carattere non principale, la somma

$$\sum_{n \le x} \chi(n)$$

è limitata, poiché χ è una funzione periodica e la somma su q interi consecutivi vale 0 (cfr le relazioni di ortogonalità 5.1.8). Talvolta è utile avere informazioni piú precise, e queste ci sono fornite dal seguente

Teorema 5.4.3 (Disuguaglianza di Pólya–Vinogradov). *Sia $\chi \bmod q$ un carattere non principale. Si ha*

$$\sum_{n\le x} \chi(n) \ll q^{1/2}\log q.$$

Dim.: Ci limitiamo al caso di χ primitivo. Per la (5.4.1) si ha

$$\begin{aligned}\sum_{n\le x}\chi(n) &= \sum_{n\le x}\frac{1}{\tau(\overline{\chi})}\sum_{h \bmod q}\overline{\chi}(h)e_q(nh) = \frac{1}{\tau(\overline{\chi})}\sum_{h \bmod q}\overline{\chi}(h)\sum_{n\le x}e_q(nh)\\ &= \frac{1}{\tau(\overline{\chi})}\sum_{\substack{h \bmod q\\(h,q)=1}}\overline{\chi}(h)\frac{e_q(h)-e_q\big(h([x]+1)\big)}{1-e_q(h)}.\end{aligned}$$

Osserviamo che a causa della presenza del fattore $\overline{\chi}(h)$ possiamo aggiungere alla somma su $h \bmod q$ la condizione $(h,q)=1$, la quale implica che non c'è l'addendo corrispondente ad $h=q$ che farebbe annullare il denominatore. Passando al modulo ed utilizzando il Lemma precedente ed il fatto che se $u\in\mathbb{R}$ allora $|1-e(u)| = 2|\sin(\pi u)|$ otteniamo

$$\Big|\sum_{n\le x}\chi(n)\Big| \ll q^{-1/2}\sum_{h=1}^{q-1}\frac{1}{|\sin(h\pi/q)|}.$$

Usando il Lemma A.4.5 con $f(t) \stackrel{\text{def}}{=} \big(|\sin(\pi t)|\big)^{-1}$, $\delta \stackrel{\text{def}}{=} q^{-1}$ otteniamo

$$\sum_{h=1}^{q-1}\frac{1}{|\sin\big(h\pi/q\big)|} \le q\int_{1/(2q)}^{1-1/(2q)}\frac{\mathrm{d}t}{|\sin\pi t|} = 2q\int_{1/(2q)}^{1/2}\frac{\mathrm{d}t}{|\sin\pi t|}.$$

Ma sull'intervallo di integrazione si ha $\sin(\pi t)\ge 2t$ e dunque

$$\Big|\sum_{n\le x}\chi(n)\Big| \ll q^{1/2}\int_{1/(2q)}^{1/2}\frac{\mathrm{d}t}{t} \ll q^{1/2}\log q,$$

che è la tesi. □

È possibile estendere questa dimostrazione al caso in cui χ non è primitivo: per fare questo, si deve trovare una relazione che lega il valore di $\tau(\chi)$ a quello del carattere che lo induce. Si veda il Capitolo 23 del libro di Davenport [12].

§5.5. Il teorema di Gauss-Jacobi

Torniamo brevemente sul problema di rappresentare $n\in\mathbb{N}$ come somma di due quadrati.

Teorema 5.5.1 (Gauss, Jacobi). *Detto χ è il carattere non principale modulo 4, per $n\ge 1$ si ha $r_2 = 4\chi * N_0$, o, in altre parole,*

$$r_2(n) = 4\sum_{d\mid n}\chi(d).$$

Dim.: La dimostrazione dipende in modo essenziale dal fatto che $\mathbb{Z}[\mathrm{i}]$ è un anello a fattorizzazione unica. Per prima cosa dimostriamo che se $n \in \mathbb{N}$ è dispari allora $r_2(n) = r_2\bigl(2^\alpha n\bigr)$ per ogni $\alpha \in \mathbb{N}$. Infatti, $r_2(m) = r_2(4m)$ qualunque sia $m \in \mathbb{N}$, dato che se $4n = a^2 + b^2$ allora $a \equiv b \equiv 0 \mod 2$. Inoltre, se $n = a^2 + b^2$ è dispari allora $2n = (a+b)^2 + (a-b)^2$ e viceversa, con corrispondenza biunivoca fra le rappresentazioni. Infine, osserviamo che i due membri dell'uguaglianza da dimostrare non cambiano se al posto di n poniamo $2^\alpha n$, dal momento che $\chi(2) = 0$.

Un discorso analogo vale se al posto di n si scrive $q^\alpha n$ per ogni $\alpha \in \mathbb{N}^*$, dove q è un primo $\equiv 3 \mod 4$. In quest'ultimo caso i due membri valgono entrambi 0 se α è dispari, ed $r_2(n)$ se α è pari, per il Lemma 1.4.9, dato che $\chi(q) = -1$.

Quindi è sufficiente dimostrare che l'uguaglianza desiderata vale quando n è prodotto di potenze di primi distinti, tutti $\equiv 1 \mod 4$, $n \stackrel{\text{def}}{=} \prod_{j=1}^k p_j^{\alpha_j}$. Si osservi che in questo caso occorre dimostrare che $r_2(n) = 4d(n)$, poiché $\chi(p_j) = 1$ per ciascuno dei fattori primi di n. Per $j = 1, \dots, k$, per l'Osservazione 1.4.6, esistono a_j, $b_j \in \mathbb{N}^*$ tali che $p_j = a_j^2 + b_j^2$; ricordiamo anche che in $\mathbb{Z}[\mathrm{i}]$ i numeri $a_j \pm \mathrm{i}b_j$ sono tutti primi poiché $N(a_j + \mathrm{i}b_j) = p_j$ è un numero primo in $\mathbb{Z}$. Se $n = A^2 + B^2$ in $\mathbb{Z}[\mathrm{i}]$ vale la fattorizzazione $n = (A + \mathrm{i}B)(A - \mathrm{i}B)$. Quindi, fissato un divisore $d \stackrel{\text{def}}{=} \prod_{j=1}^k p_j^{\beta_j}$ di n, per $r \in \{0,\, 1,\, 2,\, 3\}$ definiamo $A = A(d, r)$ e $B = B(d, r)$ per mezzo delle relazioni

$$A + \mathrm{i}B \stackrel{\text{def}}{=} C(d,r) \stackrel{\text{def}}{=} \mathrm{i}^r \prod_{j=1}^k \{(a_j + \mathrm{i}b_j)^{\beta_j} \cdot (a_j - \mathrm{i}b_j)^{\alpha_j - \beta_j}\}$$

$$A - \mathrm{i}B \stackrel{\text{def}}{=} D(d,r) \stackrel{\text{def}}{=} \mathrm{i}^{-r} \prod_{j=1}^k \{(a_j - \mathrm{i}b_j)^{\beta_j} \cdot (a_j + \mathrm{i}b_j)^{\alpha_j - \beta_j}\}$$

Evidentemente ci sono esattamente 4 scelte per r e $d(n)$ scelte per d: resta quindi da dimostrare che scelte diverse di (r, d) danno origine a valori diversi per A e B. Sfruttando il fatto che $\mathbb{Z}[\mathrm{i}]$ è un anello a fattorizzazione unica e che le unità sono della forma i^t con $t \in \{0,\, 1,\, 2,\, 3\}$, si vede subito che $C(d,r) = \mathrm{i}^t C(d', r')$ implica che $d = d'$ e $t = 0$. Questo conclude la dimostrazione. □

Combinando questo risultato con il Teorema di Gauss 3.2.2, ed utilizzando il metodo dell'iperbole di Dirichlet 3.1.13 con $y = x^{1/2}$ ed il Lemma 5.2.1, si trova

$$\sum_{n \le x} r_2(n) = 4xL(1,\chi) + \mathcal{O}\Bigl(x^{1/2}\Bigr),$$

da cui $L(1,\chi) = \frac{1}{4}\pi$, risultato d'altra parte ovvio poiché

$$L(1,\chi) = \sum_{n \ge 1} \frac{(-1)^n}{2n+1}.$$

Capitolo 6. Metodi di Crivello

§6.1. Il principio di inclusione–esclusione e la formula di Lagrange

Definizione 6.1.1. *Dati $\mathcal{A} \subseteq \mathbb{N}^*$, $\mathcal{B} \subseteq \mathbb{N}$, $x \geq 1$, d ed $M \in \mathbb{N}^*$ poniamo*

$$\mathcal{S}(\mathcal{A}; x; M) \stackrel{\text{def}}{=} \big|\{a \in \mathcal{A} \cap [1, x] \colon (a, M) = 1\}\big| \qquad \mathcal{B}(x) \stackrel{\text{def}}{=} \mathcal{B} \cap [1, x]$$
$$\mathcal{A}_d \stackrel{\text{def}}{=} \{a \in \mathcal{A} \colon d \mid a\} \qquad P(x) \stackrel{\text{def}}{=} \prod_{p \leq x} p = \exp \theta(x).$$

In sostanza, vogliamo contare il numero di elementi di $\mathcal{A}$ che sono primi con M, cioè quanti elementi di $\mathcal{A}$ sopravvivono ad un crivello fatto con i fattori primi di M. Il prossimo Teorema ci permette di trasformare $\mathcal{S}(\mathcal{A}; x; M)$ in una somma su tutti i divisori di M.

Teorema 6.1.2 (Principio di Inclusione–Esclusione). *Dati $\mathcal{A} \subseteq \mathbb{N}^*$, $x \geq 1$ ed $M \in \mathbb{N}^*$ si ha*

$$\mathcal{S}(\mathcal{A}; x; M) = \sum_{d \mid M} \mu(d) \, \big|\mathcal{A}_d(x)\big|.$$

Dim.: Per il Teorema 3.1.9

$$\mathcal{S}(\mathcal{A}; x; M) = \sum_{\substack{a \in \mathcal{A}(x) \\ (a, M) = 1}} 1 = \sum_{a \in \mathcal{A}(x)} \sum_{d \mid (a, M)} \mu(d) = \sum_{d \mid M} \mu(d) \sum_{\substack{a \in \mathcal{A}(x) \\ d \mid a}} 1 = \sum_{d \mid M} \mu(d) \big|\mathcal{A}_d(x)\big|.$$

𝔈 6.1.1 Si osservi che il risultato dipende solo dai fattori primi distinti di M. □

Per esempio, prendendo $\mathcal{A} = \mathbb{N}(M)$ ed $x = M$ si ha

$$\mathcal{S}(\mathcal{A}; M; M) = \varphi(M) = \sum_{d \mid M} \mu(d) \frac{M}{d} = (N_1 * \mu)(M),$$

che è una parte del Teorema 3.2.8. Nel seguito supporremo sempre che $\mu(M) \neq 0$.

Utilizzando le idee di Eratostene, Lagrange scoprí una formula che permette di calcolare
𝔈 6.1.2 $\pi(x)$ iterativamente:

$$\pi(x) - \pi\big(x^{1/2}\big) + 1 = \sum_{d \mid P\left(x^{1/2}\right)} \mu(d) \left[\frac{x}{d}\right]. \tag{6.1.1}$$

La dimostrazione è molto semplice: ci sono esattamente $[x]$ interi $\le x$ (il termine $d=1$). Ogni primo $p \le x^{1/2}$ divide $\left[\frac{x}{p}\right]$ di questi interi; ma ora abbiamo indebitamente sottratto due volte tutti i numeri che sono divisibili per 2 o piú primi distinti, e cosí via. Per esempio

$$\begin{aligned}\sum_{d\mid 210}\mu(d)\left[\frac{100}{d}\right] &= \left[\frac{100}{1}\right] - \left(\left[\frac{100}{2}\right]+\left[\frac{100}{3}\right]+\left[\frac{100}{5}\right]+\left[\frac{100}{7}\right]\right)\\ &\quad + \left(\left[\frac{100}{6}\right]+\left[\frac{100}{10}\right]+\left[\frac{100}{14}\right]+\left[\frac{100}{15}\right]+\left[\frac{100}{21}\right]+\left[\frac{100}{35}\right]\right)\\ &\quad - \left(\left[\frac{100}{30}\right]+\left[\frac{100}{42}\right]+\left[\frac{100}{70}\right]+\left[\frac{100}{105}\right]\right)+\left[\frac{100}{210}\right]\\ &= 100-(50+33+20+14)+(16+10+7+6+4+2)\\ &\quad -(3+2+1+0)+0\\ &= 100-117+45-6=22,\end{aligned} \tag{6.1.2}$$

ed infatti $\pi(100)-\pi(10)+1 = 25-4+1 = 22$. Una dimostrazione altrettanto semplice si può dare utilizzando il Principio di Inclusione–Esclusione con $\mathcal{A}=\mathbb{N}^*$, $M = P\big(x^{1/2}\big)$, poiché la condizione $(M,a)=1$ con $a\in\mathbb{N}(x)$ vuol dire che $a=1$ oppure a è un numero primo $p\in\big(x^{1/2},x\big]$. Il difetto principale della formula di Lagrange è che contiene troppi termini per essere utilizzabile come strumento pratico per il calcolo. Per esempio, consideriamo un parametro reale $z\in\big[2,x^{1/2}\big]$. È evidente che $\{a\in\mathbb{N}(x)\colon \big(a,P(z)\big)=1\}\supseteq\{p\in(z,x]\}$. Applicando la formula di Lagrange otteniamo

$$\begin{aligned}\pi(x)-\pi(z) &\le \mathcal{S}\big(\mathbb{N}^*;x;P(z)\big) = \sum_{d\mid P(z)}\mu(d)\left[\frac{x}{d}\right] = \sum_{d\mid P(z)}\mu(d)\frac{x}{d}+\mathcal{O}\Big(\sum_{\substack{d\mid P(z)\\ d\le x}}1\Big)\\ &= x\prod_{p\le z}\left(1-\frac{1}{p}\right)+\mathcal{O}\Big(2^{\pi(z)}\Big) = e^{-\gamma}\frac{x}{\log z}\big(1+o(1)\big)+\mathcal{O}\Big(2^{2z/\log z}\Big).\end{aligned}$$

per il Teorema di Mertens 4.3.6 ed il Lemma 3.1.5. Se non vogliamo dimostrare banalità tipo $\pi(x)=\mathcal{O}(x)$ (o peggio), siamo costretti a prendere z molto piccolo: in altre parole, non si riesce a scegliere $z=x^{1/2}$ come vorremmo. Prendendo $z=\log x$ si ottiene

$$\pi(x)=\mathcal{O}\left(\frac{x}{\log\log x}\right).$$

In generale, senza adeguate informazioni sul resto non è possibile ottenere informazioni molto precise: questo vale anche per i risultati dei prossimi paragrafi, che sono piú deboli di quelli che si possono dimostrare con i moderni metodi di crivello.

§6.2. Il crivello di Brun

Vogliamo modificare il Teorema 6.1.2 in modo da ottenere una maggiorazione che ci darà, in modo abbastanza semplice, dei risultati non banali. L'idea di base è quella di considerare solo una parte della somma che compare nel Principio di Inclusione–Esclusione, in cui d è ristretto agli interi che non hanno troppi fattori primi. Cominciamo con un semplice Lemma: in tutto il Capitolo è sottinteso che $\binom{n}{r}\stackrel{\text{def}}{=}0$ se $n<0$ oppure $r<0$ oppure $r>n$, osservando che questa convenzione si ha $\binom{n+1}{r}=\binom{n}{r-1}+\binom{n}{r}$ per ogni n, $r\ge 0$.

LEMMA 6.2.1. *Siano n, $m \in \mathbb{N}$. Si ha*

$$\sum_{r=0}^{m} (-1)^r \binom{n+1}{r} = (-1)^m \binom{n}{m}.$$

DIM.: Sostituendo la formula citata sopra nel primo membro si ottiene una somma "telescopica" in cui tutti gli addendi si cancellano, tranne il primo $\binom{n}{-1} = 0$ e l'ultimo $(-1)^m \binom{n}{m}$. Si osservi infine che se $m > n$ il primo membro vale $(1-1)^{n+1} = 0$. □

TEOREMA 6.2.2 (BRUN). *Dati $\mathcal{A} \subseteq \mathbb{N}^*$, $x \geq 1$, $m \in \mathbb{N}^*$ dispari ed $M \in \mathbb{N}^*$ si ha*

$$\sum_{\substack{d \mid M \\ \omega(d) \leq m}} \mu(d) \left|\mathcal{A}_d(x)\right| \leq \mathcal{S}(\mathcal{A}; x; M) \leq \sum_{\substack{d \mid M \\ \omega(d) < m}} \mu(d) \left|\mathcal{A}_d(x)\right|. \tag{6.2.1}$$

DIM.: Consideriamo gli insiemi

$$\mathfrak{A} \stackrel{\text{def}}{=} \{a \in \mathcal{A} \colon a \leq x,\ (a, M) = 1\} \qquad \text{e} \qquad \mathfrak{B} \stackrel{\text{def}}{=} \{a \in \mathcal{A} \colon a \leq x,\ (a, M) > 1\}$$

in modo che $\mathcal{S}(\mathcal{A}; x; M) = |\mathfrak{A}|$ ed osserviamo che gli elementi di $\mathfrak{A}$ sono contati nell'espressione a destra della (6.2.1) esattamente una volta (per $d = 1$). Per gli interi $n \in \mathfrak{B}$ si ha $\delta \stackrel{\text{def}}{=} (n, M) > 1$, ed n è contato in quegli insiemi $\mathcal{A}_d$ per cui $\omega(d) < m$ e $d \mid \delta$. Per il Lemma 6.2.1, il contributo totale di n alla somma di destra nella (6.2.1) è

$$\sum_{\substack{d \mid \delta \\ \omega(d) < m}} \mu(d) = \sum_{r=0}^{m-1} (-1)^r \binom{\omega(\delta)}{r} = (-1)^{m-1} \binom{\omega(d) - 1}{m-1} \geq 0,$$

perché $m - 1$ è pari. L'altra disuguaglianza si dimostra in modo analogo. □

Se $m > \omega(M)$ questa è una dimostrazione alternativa del Principio di Inclusione–Esclusione 6.1.2, poiché allora le due somme nella (6.2.1) sono uguali. Le due somme nella (6.2.1) sono una parte della somma considerata nella 6.1.2: le due disuguaglianze ci danno un altro parametro a disposizione (*viz.* m), e questo ci permetterà di ottenere risultati molto piú precisi di quelli che seguono direttamente dalla 6.1.2. In sostanza, il Teorema 6.2.2 implica che le somme parziali nella 6.1.2, ordinate opportunamente, forniscono alternativamente maggiorazioni e minorazioni di $\mathcal{S}(\mathcal{A}; x; M)$, come per esempio l'ultima somma nella (6.1.2).

È chiaro che il Teorema di Brun 6.2.2 si applica ad insiemi $\mathcal{A}$ qualsiasi: per brevità ci limiteremo a studiare il caso speciale ma estremamente interessante dell'immagine di un polinomio. Consideriamo fissato un polinomio $f \in \mathbb{Z}[x]$ di grado $g \geq 1$ con primo coefficiente $a_g > 0$, mentre l'intero positivo M tale che $\mu(M) \neq 0$ e l'intero positivo dispari m saranno scelti in modo opportuno nelle applicazioni.

LEMMA 6.2.3. *Poniamo $\varrho(d) \stackrel{\text{def}}{=} |\{n \mod d \colon f(n) \equiv 0 \mod d\}|$. La funzione ϱ è moltiplicativa ed inoltre $\varrho(p) \leq \min(p, g)$ per ogni numero primo p.*

𝔈 6.2.1–2

DIM.: La prima parte segue dal Teorema Cinese del Resto 1.2.4; inoltre $\mathbb{Z}_p$ è un campo, e dunque ogni equazione polinomiale ha al piú tante radici quanto il grado. □

Lemma 6.2.4. *Per ogni $x \geq 1$ si ha*

$$|\{n \in \mathbb{N}(x): f(n) \equiv 0 \mod d\}| = \varrho(d)\left(\frac{x}{d} + \mathcal{O}(1)\right).$$

Dim.: Poiché $f(n) \equiv f(m) \mod d$ se $n \equiv m \mod d$, l'equazione $f(n) \equiv 0 \mod d$ ha esattamente $\varrho(d)$ soluzioni in ogni intervallo di d interi consecutivi. Suddividiamo $[1, x]$ in $\left[\frac{x}{d}\right]$ intervalli del tipo $[(k-1)d+1, kd]$, piú un intervallo di lunghezza $\leq d$. In totale $\varrho(d)\left[\frac{x}{d}\right] + \mathcal{O}(\varrho(d)) = \varrho(d)\left(\frac{x}{d} + \mathcal{O}(1)\right)$ soluzioni, come si voleva. □

Lemma 6.2.5. *Sia M un intero positivo tale che $\mu(M) \neq 0$. Allora*

$$\sum_{\substack{d|M \\ \omega(d)<m}} \varrho(d) \leq e\big(g\omega(M)\big)^{m-1}.$$

Dim.: Per il Lemma 6.2.3 si ha $\varrho(d) \leq g^{\omega(d)}$ se $d \mid M$, e quindi

$$\sum_{\substack{d|M \\ \omega(d)<m}} \varrho(d) \leq \sum_{r=0}^{m-1} \sum_{\substack{d|M \\ \omega(d)=r}} g^{\omega(d)} = \sum_{r=0}^{m-1} g^r \binom{\omega(M)}{r} \leq g^{m-1} \sum_{r=0}^{m-1} \frac{\omega(M)^r}{r!} \leq e\big(g\omega(M)\big)^{m-1},$$

poiché $\binom{n}{r} \leq n^r (r!)^{-1}$. □

Lemma 6.2.6. *Sia S_r la funzione simmetrica elementare di ordine r di $\xi_1, \dots, \xi_n \in \mathbb{R}^{0+}$, con $n \geq r$. Si ha*

$$S_r \leq \frac{S_1^r}{r!}.$$

Dim.: Nello sviluppo di S_1^r i termini corrispondenti agli addendi che compaiono in S_r hanno coefficiente $r!$, mentre gli altri addendi danno un contributo non negativo. Piú precisamente, fissato $n \in \mathbb{N}^*$, per ogni "multiindice" $\underline{\alpha} \in \mathbb{N}^n$ con $\underline{\alpha} = (\alpha_1, \dots, \alpha_n)$ poniamo $|\underline{\alpha}| \stackrel{\text{def}}{=} \alpha_1 + \cdots + \alpha_n$ e $\underline{\alpha}! \stackrel{\text{def}}{=} \alpha_1! \cdots \alpha_n!$. Inoltre, per ogni $\underline{x} \in \mathbb{R}^n$ con $\underline{x} = (x_1, \dots, x_n)$ poniamo $\underline{x}^{\underline{\alpha}} \stackrel{\text{def}}{=} x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. Siano

$$\mathfrak{A}_n(r) = \mathfrak{A}(r) \stackrel{\text{def}}{=} \big\{\underline{\alpha} \in \mathbb{N}^n: |\underline{\alpha}| = r\big\} \quad \text{e} \quad \mathfrak{B}_n(r) = \mathfrak{B}(r) \stackrel{\text{def}}{=} \big\{\underline{\beta} \in \mathfrak{A}_n(r): \beta_i \in \{0,1\}\big\}.$$

𝔈 6.2.3 Posto $\underline{\xi} \stackrel{\text{def}}{=} (\xi_1, \dots \xi_n) \in \big(\mathbb{R}^{0+}\big)^n$, si ha quindi

$$S_1^r = \sum_{\underline{\alpha} \in \mathfrak{A}(r)} c(\underline{\alpha})\, \underline{\xi}^{\underline{\alpha}} \qquad \text{dove} \qquad c(\underline{\alpha}) \stackrel{\text{def}}{=} \frac{(\alpha_1 + \cdots + \alpha_n)!}{\alpha_1! \cdots \alpha_n!} = \frac{|\underline{\alpha}|!}{\underline{\alpha}!},$$

mentre, osservando che $c(\underline{\beta}) = r!$ per ogni $\underline{\beta} \in \mathfrak{B}(r)$, si ha

$$S_r = \sum_{\underline{\beta} \in \mathfrak{B}(r)} \underline{\xi}^{\underline{\beta}} \qquad \text{e dunque} \qquad S_1^r \geq \sum_{\underline{\beta} \in \mathfrak{B}(r)} c(\underline{\beta})\, \underline{\xi}^{\underline{\beta}} = r! S_r.$$

In effetti non è necessario conoscere la forma esatta dei coefficienti $c(\underline{\alpha})$, ma solo che sono non negativi e che valgono $r!$ su tutti gli elementi di $\mathfrak{B}(r)$ (dato che per ipotesi $n \geq r$),
𝔈 6.2.4 cosa che si può dimostrare direttamente senza difficoltà. □

LEMMA 6.2.7. *Poniamo* $\Sigma(M) \stackrel{\text{def}}{=} \sum_{p|M} p^{-1}$. *Abbiamo*

$$\sum_{r=m}^{\omega(M)} \sum_{\substack{d|M \\ \omega(d)=r}} \frac{\varrho(d)}{d} \le \sum_{r=m}^{\omega(M)} \left(\frac{eg\Sigma(M)}{r}\right)^r.$$

DIM.: Infatti per il Lemma 6.2.3 si ha

$$\sum_{r=m}^{\omega(M)} \sum_{\substack{d|M \\ \omega(d)=r}} \frac{\varrho(d)}{d} \le \sum_{r=m}^{\omega(M)} g^r \sum_{\substack{d|M \\ \omega(d)=r}} \frac{1}{d}. \tag{6.2.2}$$

La somma interna è precisamente la funzione simmetrica elementare di ordine r sui numeri p^{-1}, dove $p \mid M$. Per il Lemma 6.2.6 il secondo membro della (6.2.2) è

$$\le \sum_{r=m}^{\omega(M)} g^r \frac{S_1^r}{r!} \le \sum_{r=m}^{\omega(M)} \left(\frac{eg\Sigma(M)}{r}\right)^r,$$

poiché $e^r > r^r (r!)^{-1}$ per $r \ge 1$, per lo sviluppo in serie di e^r. □

LEMMA 6.2.8. *Siano* $f \in \mathbb{Z}[x]$ *un polinomio di grado* $g \ge 1$, *con primo coefficiente* $a_g > 0$, m *un intero positivo dispari ed* M *un intero positivo tale che* $\mu(M) \neq 0$. *Sia inoltre* $\mathcal{A} \stackrel{\text{def}}{=} f(\mathbb{N}) \cap \mathbb{N}^*$. *Per* $x \to \infty$ *si ha*

$$\mathcal{S}\big(\mathcal{A}; f(x); M\big) \le x \prod_{p|M} \left(1 - \frac{\varrho(p)}{p}\right) + \mathcal{O}\left(x \sum_{r=m}^{\omega(M)} \left(\frac{eg\Sigma(M)}{r}\right)^r\right) + \mathcal{O}\Big(\big(g\omega(M)\big)^{m-1}\Big).$$

Se m *è pari la disuguaglianza vale con il segno* $\ge$ *al posto di* $\le$.

DIM.: Si osservi che per x sufficientemente grande la condizione $f(n) \le f(x)$ è equivalente ad $n \le x$. Per il Lemma 6.2.4 abbiamo $\big|\mathcal{A}_d \cap [1, f(x)]\big| = \big|\{n \le x \colon f(n) \equiv 0 \mod d\}\big| = \varrho(d) x d^{-1} + \mathcal{O}(\varrho(d))$. Quindi, per il Teorema di Brun 6.2.2 ed il Lemma 3.1.5, si ha

$$\begin{aligned}\mathcal{S}\big(\mathcal{A}; f(x); M\big) &\le x \sum_{\substack{d|M \\ \omega(d)<m}} \frac{\mu(d)\varrho(d)}{d} + \mathcal{O}\Big(\sum_{\substack{d|M \\ \omega(d)<m}} \varrho(d)\Big) \\ &= x \left\{\prod_{p|M} \left(1 - \frac{\varrho(p)}{p}\right) + \mathcal{O}\left(\sum_{r=m}^{\omega(M)} \sum_{\substack{d|M \\ \omega(d)=r}} \frac{\varrho(d)}{d}\right)\right\} + \mathcal{O}\Big(\big(g\omega(M)\big)^{m-1}\Big)\end{aligned}$$

ed il risultato voluto segue dai Lemmi 6.2.7 e 6.2.5. □

Per ottenere un risultato maneggevole (quest'ultimo ha una forma piuttosto complessa) facciamo l'ipotesi che l'insieme $\mathfrak{P}$ di numeri primi con i quali vogliamo fare il crivello abbia una "densità" positiva nell'insieme di tutti i numeri primi.

Teorema 6.2.9. *Siano $f \in \mathbb{Z}[x]$ un polinomio di grado $g \geq 1$, con primo coefficiente $a_g > 0$, $\mathfrak{P}$ un insieme di numeri primi con la proprietà che, per $z \to +\infty$*

$$\sum_{p \in \mathfrak{P}(z)} \frac{1}{p} \sim \kappa \log\log z,$$

dove $\kappa \in \mathbb{R}^+$ è fissato. Allora per $z \stackrel{\text{def}}{=} \exp\bigl(\log x(2(1+\varepsilon)\kappa e g \log\log x)^{-1}\bigr)$ ed $x \to \infty$ si ha

$$\bigl|\{n \leq x : p \mid f(n) \Rightarrow p \notin \mathfrak{P}(z)\}\bigr| \leq x \prod_{p \in \mathfrak{P}(z)} \left(1 - \frac{\varrho(p)}{p}\right) + \mathcal{O}_{g,\kappa}\left(\frac{x}{(\log z)^{2\kappa g}}\right).$$

Dim.: Scegliamo $M = M(z) \stackrel{\text{def}}{=} \prod_{p \in \mathfrak{P}(z)} p$ e quindi si ha $\Sigma(M) \leq (1+\varepsilon)\kappa \log\log z$ e per il Teorema 4.2.2 $\omega(M) \leq (1+\varepsilon) z (\log z)^{-1}$. Inoltre osserviamo che

$$\bigl|\{n \leq x : p \mid f(n) \Rightarrow p \notin \mathfrak{P}(z)\}\bigr| \leq z + \mathcal{S}\bigl(\mathcal{A}; f(x); M(z)\bigr),$$

nella notazione del Lemma 6.2.8. Il primo termine d'errore è

$$\leq x \sum_{r \geq m} \left(\frac{(1+\varepsilon)\kappa e g \log\log z}{m}\right)^r \leq x \sum_{r \geq m} 2^{-r} = 2^{1-m} x,$$

purché $m \geq 2(1+\varepsilon)\kappa e g \log\log z$. Il secondo termine è $\leq \exp\{m(\log g + \log\omega(M))\} \leq \exp\{m \log z\}$. Scegliendo $m = 2[(1+\varepsilon)\kappa e g \log\log z] + 3$ si vede facilmente che $2^m \geq C(g)(\log z)^{2\kappa g}$ per un'opportuna costante positiva $C(g)$ e che $\exp\{m \log z\} \leq x(\log z)^{-2\kappa g}$. Raccogliendo tutte queste stime otteniamo la tesi. □

Corollario 6.2.10. *Sia f come sopra, e $z \stackrel{\text{def}}{=} \exp\bigl(\log x(8 e g \log\log x)^{-1}\bigr)$. Per $x \to \infty$*

$$\bigl|\{n \leq x : p \mid f(n) \Rightarrow p > z\}\bigr| \leq x \prod_{p \leq z} \left(1 - \frac{\varrho(p)}{p}\right) + \mathcal{O}_g\left(\frac{x}{(\log z)^{2g}}\right).$$

Dim.: Basta prendere $\mathfrak{P}$ l'insieme di tutti i numeri primi e $\kappa = 1$ nel Teorema 6.2.9. □

Si osservi che il significativo miglioramento sulle conseguenze dirette del Principio di Inclusione–Esclusione 6.1.2 (si vedano i risultati nel prossimo paragrafo) dipende essenzialmente dal fatto che prendiamo m relativamente piccolo rispetto ad $\omega(M)$.

§6.3. Applicazioni del crivello di Brun

Primi e polinomi. Il Corollario 6.2.10 implica un risultato negativo che esprime in forma quantitativa ciò che abbiamo visto qualitativamente nel Teorema 1.7.1. Si noti che è possibile ottenere informazioni piú esplicite a patto di conoscere il comportamento in media della funzione ϱ. In particolare è nota l'analoga della Seconda Formula di Mertens 4.3.2:

$$\sum_{p \leq x} \frac{\varrho(p) \log p}{p} = \kappa \log x + \mathcal{O}_f(1), \tag{6.3.1}$$

dove κ è il numero di componenti irriducibili di f su $\mathbb{Z}$. Mediante trasformazioni analoghe a quelle già viste, l'enunciato può esser messo nella forma:

$$|\{n \le x : p \mid f(n) \Rightarrow p > z\}| \ll \frac{x}{\log z} \prod_p \left(1 - \frac{\varrho(p)-1}{p-1}\right)\left(1-\frac{1}{p}\right)^{1-\kappa}$$

dove la costante implicita non dipende da f ed il prodotto infinito è convergente. Si noti infine che se f è riducibile su $\mathbb{Z}$ può assumere solo un numero finito di valori primi: se $f = f_1 \cdots f_\kappa$, con $f_j \in \mathbb{Z}[x]$, allora $f(n) = p$ implica che $|f_j(n)| = 1$ per tutti i j, tranne uno.

Maggiorazione di $\pi(x)$. Scegliamo $f(n) = n$, per cui $\varrho(d) = 1$ per ogni $d \in \mathbb{N}^*$ e

$$\pi(x) \le z + \big|\{n \le x : p \mid n \Rightarrow p > z\}\big| \le x \prod_{p \le z}\left(1-\frac{1}{p}\right) + \mathcal{O}\left(\frac{x}{(\log z)^2}\right) \ll \frac{x \log\log x}{\log x}$$

per il Teorema di Mertens 4.3.6. Anche se questo risultato è inferiore a quello ottenuto in modo elementare nel Teorema 4.2.2, è pur sempre nettamente superiore al risultato ottenuto direttamente dal Principio di Inclusione–Esclusione, poiché possiamo prendere z molto grande, quasi quanto una potenza di x ed inoltre prendiamo $m \sim c \log\log z$ invece di $m = \omega(M) \sim z(\log z)^{-1}$. Infine, a differenza di quanto accade nella nostra applicazione della formula di Lagrange, qui non stimiamo i resti con $\mathcal{O}(1)$, ma con $\mathcal{O}\big(\varrho(d)d^{-1}\big)$, che è molto piú piccolo per d grande.

Polinomi di primo grado. Consideriamo il generico polinomio $f \in \mathbb{Z}[x]$ irriducibile di grado 1, cioè $f(x) = qx + a$ con $(a, q) = 1$, e supponiamo che $q \ge 1$ e che $1 \le a \le q$. Si ha

$$\varrho(p) = \begin{cases} 1 & \text{se } p \nmid q, \\ 0 & \text{se } p \mid q. \end{cases}$$

Se x è sufficientemente grande rispetto a q, dal Corollario 6.2.10 ricaviamo

$$|\{n \le x : qn + a \text{ è primo}\}| \le x \prod_{\substack{p \le z \\ p \nmid q}}\left(1-\frac{1}{p}\right) + \mathcal{O}\left(\frac{x}{(\log z)^2}\right) \ll \frac{q}{\varphi(q)}\frac{x\log\log x}{\log x}.$$

Non deve stupire la presenza del fattore q a numeratore, in apparente contrasto con il Teorema dei Numeri Primi nelle Progressioni 5.3.2. Infatti

$$\begin{aligned} |\{n \le x : qn + a \text{ è primo}\}| &= |\{qn + a \le qx + a : qn + a \text{ è primo}\}| \\ &= |\{m \le qx + a : m \equiv a \mod q \text{ ed } m \text{ è primo}\}|. \end{aligned}$$

Polinomi di secondo grado. Possiamo utilizzare i risultati precedenti nel caso di polinomi di secondo grado, poiché siamo in grado di determinare esattamente $\varrho(p)$ per ogni p primo e quindi di dimostrare direttamente che vale la (6.3.1).

Nel caso generale di polinomi di secondo grado $f(n) = an^2 + bn + c$, bisogna distinguere fra i fattori primi del discriminante di f, che è $a(4ac - b^2)$, e tutti gli altri numeri primi. Illustriamo questo caso per mezzo di due esempi. Prendiamo $f(n) = n^2 - 3$. In questo caso il discriminante di f è -12 e quindi per $p \neq 2, 3$ si ha $\varrho(p) = 1 + \big(3 \mid p\big)$. Per la legge di reciprocità quadratica 1.6.4 e per $p > 3$ si ha $\big(3 \mid p\big) = \big(p \mid 3\big)(-1)^{(p-1)/2}$, ed è anche immediato verificare che questo è un carattere di Dirichlet modulo 12, che indichiamo con χ_1 ($\chi_1(1) = \chi_1(11) = 1$, $\chi_1(5) = \chi_1(7) = -1$). Quindi $\varrho(p) = 1 + \chi_1(p)$ (per ogni p) e la (6.3.1) segue in questo caso dai Teoremi 4.3.2 e 5.2.8.

Consideriamo poi il polinomio (riducibile) $f(n) = n(n + h)$ (dove $h \in \mathbb{N}^*$): se $2 \nmid h$ si vede direttamente che $|\{n \leq x : p \mid n(n+h) \Rightarrow p > 2\}| = \mathcal{O}_h(1)$. Se invece $2 \mid h$ il Corollario 6.2.10 ci dà immediatamente

$$|\{n \leq x : p \mid n(n + h) \Rightarrow p > z\}| \leq x \prod_{p \leq z} \left(1 - \frac{\varrho(p)}{p}\right) + \mathcal{O}\left(\frac{x}{(\log x)^4}\right). \tag{6.3.2}$$

In questo caso il discriminante è $-h^2$ ed abbiamo

$$\varrho(p) = \begin{cases} 2 & \text{se } p \nmid h, \\ 1 & \text{se } p \mid h. \end{cases}$$

Per h pari, $h \neq 0$, poniamo

$$\mathfrak{S}(h) \stackrel{\text{def}}{=} 2C_0 \prod_{\substack{p \mid h \\ p > 2}} \frac{p-1}{p-2} \qquad \text{dove} \qquad C_0 \stackrel{\text{def}}{=} \prod_{p > 2} \left(1 - \frac{1}{(p-1)^2}\right). \tag{6.3.3}$$

Se z è sufficientemente grande, si ha

$$\begin{aligned} \prod_{p \leq z} \left(1 - \frac{\varrho(p)}{p}\right) &= \prod_{p \mid h} \left(1 - \frac{1}{p}\right) \prod_{\substack{p \leq z \\ p \nmid h}} \left(1 - \frac{2}{p}\right) \\ &= \frac{1}{2} \prod_{\substack{p \mid h \\ p > 2}} \left\{ \left(1 - \frac{1}{p}\right) \left(1 - \frac{2}{p}\right)^{-1} \right\} \prod_{3 \leq p \leq z} \left(1 - \frac{2}{p}\right) \\ &= \frac{1}{2} \prod_{\substack{p \mid h \\ p > 2}} \left(\frac{p-1}{p-2}\right) \prod_{3 \leq p \leq z} \frac{p(p-2)}{(p-1)^2} \prod_{3 \leq p \leq z} \left(1 - \frac{1}{p}\right)^2 \\ &= \mathfrak{S}(h)\big(1 + \mathcal{O}\big(z^{-1}\big)\big) \prod_{p \leq z} \left(1 - \frac{1}{p}\right)^2. \end{aligned}$$

In definitiva, prendendo z come nel Corollario 6.2.10, qualunque sia $h \in \mathbb{N}^*$, si ha

$$|\{n \leq x : p \mid n(n + h) \Rightarrow p > z\}| \leq C' \mathfrak{S}(h) \frac{x(\log\log x)^2}{(\log x)^2}, \tag{6.3.4}$$

dove C' è una costante che non dipende da h. Questo risultato dà qualche informazione sul numero dei cosiddetti "primi gemelli" (quelli come 11 e 13, la cui differenza è 2). Posto $\pi_h(x) \stackrel{\text{def}}{=} |\{n \le x : n \text{ ed } n+h \text{ sono primi}\}|$, si ha $\mathfrak{S}(6) = 2\mathfrak{S}(2)$ e $\pi_2(100) = 8$, mentre $\pi_6(100) = 16$. Questo dipende, essenzialmente, dal fatto che se $3 \nmid n$ allora $3 \nmid n+6$, mentre se $3 \nmid n$ non possiamo concludere che $3 \nmid n+2$. Utilizzando la sommazione parziale è facile vedere che la (6.3.4) implica il famoso Teorema di Brun (che in ultima analisi ha introdotto il crivello proprio per questo motivo) per il quale la somma dei reciproci dei
𝔈 6.3.1 primi gemelli converge, a differenza della somma dei reciproci di tutti i numeri primi.

La funzione r_2. Il Teorema 6.2.9 implica una forma debole del Teorema di Landau 3.2.3: piú precisamente, utilizzando il Teorema 6.5.3, non è difficile dimostrare che

$$|\{n \le x : r_2(n) > 0\}| \ll x \left(\frac{\log\log x}{\log x}\right)^{1/2}.$$

Infatti, per il Teorema 1.4.10, se $r_2'(n) > 0$ allora n non ha fattori primi $\equiv 3 \mod 4$ e $4 \nmid n$, e si può utilizzare il Teorema 6.2.9 con $\mathfrak{P} \stackrel{\text{def}}{=} \{2\} \cup \{p : p \equiv 3 \mod 4\}$ poiché la stima richiesta dal Teorema vale con $\kappa = \frac{1}{2}$ per sommazione parziale dal Teorema 5.3.1. Piú avanti otterremo una stima dell'ordine di grandezza corretto.

§6.4. Il crivello "grande"

Vogliamo illustrare brevemente un approccio radicalmente diverso ai crivelli: nell'esempio precedente del crivello combinatorio, si elimina la classe di resto 0 modulo tutti i fattori primi di un certo parametro M. Ora vogliamo eliminare piú classi di resto simultaneamente. Per fare questo, sviluppiamo la teoria dei polinomi trigonometrici.

Definizione 6.4.1. *Dati due interi $M \in \mathbb{Z}$, $N \in \mathbb{N}^*$ chiamiamo* polinomio trigonometrico *di coefficienti $a_{M+1}, \dots, a_{M+N} \in \mathbb{C}$ la funzione*

$$S(x) \stackrel{\text{def}}{=} \sum_{n=M+1}^{M+N} a_n e(nx) = \sum_{n=M+1}^{M+N} a_n e^{2\pi i n x}$$

Definizione 6.4.2. *Dato un numero reale x poniamo*

$$\|x\| \stackrel{\text{def}}{=} \min_{n\in\mathbb{Z}} |x-n| = \min\big\{\{x\}, 1-\{x\}\big\}.$$

Dati R numeri reali $x_1, \dots x_R$, diciamo che essi sono δ-ben spaziati *se*

$$\min_{i\ne j} \|x_i - x_j\| \ge \delta > 0.$$

Teorema 6.4.3. *Se i numeri reali $x_1, \dots x_R$ sono δ-ben spaziati, allora*

$$\sum_{j=1}^{R} |S(x_j)|^2 \le \big(N + 2\delta^{-1}\big) \sum_{n=M+1}^{M+N} |a_n|^2.$$

Per la dimostrazione useremo la seguente generalizzazione della disuguaglianza di Bessel, che si ottiene come caso particolare quando gli $\underline{\xi}_i$ formano un insieme ortonormale.

LEMMA 6.4.4 (SELBERG). *Sia $\mathcal{X}$ uno spazio vettoriale su $\mathbb{C}$ con prodotto scalare $(\cdot,\cdot)$, siano $\underline{\xi}_1, \underline{\xi}_2, \dots, \underline{\xi}_R, \underline{\varphi} \in \mathcal{X} \setminus \{\underline{0}\}$ e sia $\|\underline{\varphi}\|_{\mathcal{X}} \stackrel{\text{def}}{=} (\underline{\varphi},\underline{\varphi})^{1/2}$. Posto*

$$b_j \stackrel{\text{def}}{=} \sum_{k=1}^{R} |(\underline{\xi}_k, \underline{\xi}_j)|, \qquad \text{si ha} \qquad \sum_{j=1}^{R} \frac{|(\underline{\varphi},\underline{\xi}_j)|^2}{b_j} \le \|\underline{\varphi}\|_{\mathcal{X}}^2.$$

DIM.: Qualunque siano i numeri complessi $a_1, \dots, a_R$ si ha

$$\begin{aligned} 0 \le \Big\| \underline{\varphi} - \sum_{j=1}^{R} a_j \underline{\xi}_j \Big\|_{\mathcal{X}}^2 &= \|\underline{\varphi}\|_{\mathcal{X}}^2 - 2\Re\Big\{ \sum_{j=1}^{R} \overline{a}_j (\underline{\varphi}, \underline{\xi}_j) \Big\} + \sum_{i=1}^{R}\sum_{j=1}^{R} a_i \overline{a}_j (\underline{\xi}_i, \underline{\xi}_j) \\ &\le \|\underline{\varphi}\|_{\mathcal{X}}^2 - 2\Re\Big\{ \sum_{j=1}^{R} \overline{a}_j (\underline{\varphi}, \underline{\xi}_j) \Big\} + \frac{1}{2} \sum_{i=1}^{R}\sum_{j=1}^{R} (|a_i|^2 + |a_j|^2) |(\underline{\xi}_i, \underline{\xi}_j)| \\ &= \|\underline{\varphi}\|_{\mathcal{X}}^2 - 2\Re\Big\{ \sum_{j=1}^{R} \overline{a}_j (\underline{\varphi}, \underline{\xi}_j) \Big\} + \sum_{i=1}^{R}\sum_{j=1}^{R} |a_j|^2 |(\underline{\xi}_i, \underline{\xi}_j)|, \end{aligned}$$

dove abbiamo utilizzato la disuguaglianza $|uv| \le \frac{1}{2}\big(|u|^2 + |v|^2\big)$ valida per ogni $u, v \in \mathbb{C}$. La scelta $a_j \stackrel{\text{def}}{=} (\underline{\varphi}, \underline{\xi}_j) b_j^{-1}$ dà il risultato voluto. □

DIM. DEL TEOREMA 6.4.3: Sia $\mathcal{X} \stackrel{\text{def}}{=} \ell^2(\mathbb{Z})$, lo spazio (di Hilbert) delle successioni in $\mathbb{Z}$ di quadrato sommabile, munito del prodotto scalare

$$(\underline{\alpha}, \underline{\beta}) \stackrel{\text{def}}{=} \sum_{n\in\mathbb{Z}} \alpha_n \overline{\beta}_n, \qquad \text{dove} \qquad \alpha \stackrel{\text{def}}{=} (\alpha_n)_{n\in\mathbb{Z}},\ \beta \stackrel{\text{def}}{=} (\beta_n)_{n\in\mathbb{Z}}.$$

Il nostro primo obiettivo è la disuguaglianza

$$\sum_{j=1}^{R} |S(x_j)|^2 \le \big(2N + 1 + 2\delta^{-1}\big) \sum_{n=-N}^{N} |a_n|^2, \qquad \text{dove} \qquad S(x) \stackrel{\text{def}}{=} \sum_{n=-N}^{N} a_n e(nx). \quad (6.4.1)$$

Nel Lemma di Selberg 6.4.4 prendiamo $\underline{\varphi} \stackrel{\text{def}}{=} (\varphi_n)_{n\in\mathbb{Z}}$, $\underline{\xi}_j \stackrel{\text{def}}{=} (\xi(j)_n)_{n\in\mathbb{Z}}$, dove

$$\varphi_n \stackrel{\text{def}}{=} \begin{cases} a_n & \text{se } |n| \le N, \\ 0 & \text{altrimenti;} \end{cases} \qquad \xi(j)_n \stackrel{\text{def}}{=} \begin{cases} e\big(-nx_j\big) & \text{se } |n| \le N, \\ e\big(-nx_j\big) \Big(\frac{N+L-|n|}{L}\Big)^{1/2} & \text{se } N < |n| \le N+L, \\ 0 & \text{altrimenti,} \end{cases}$$

ed L è un intero che sceglieremo piú avanti. Evidentemente

$$\|\underline{\varphi}\|_{\mathcal{X}}^2 = \sum_{n=-N}^{N} |a_n|^2, \qquad (\underline{\varphi}, \underline{\xi}_j) = \sum_{n=-N}^{N} a_n e(nx_j) = S(x_j).$$

Inoltre $(\underline{\xi}_i, \underline{\xi}_i) = 2N + L$, mentre, utilizzando le identità

$$\sum_{n=-N}^{N} e(n\alpha) = \frac{\sin\big((2N+1)\pi\alpha\big)}{\sin(\pi\alpha)}, \qquad \sum_{n=-N}^{N} (N-|n|)e(n\alpha) = \Big|\sum_{n=1}^{N} e(n\alpha)\Big|^2 = \left(\frac{\sin(N\pi\alpha)}{\sin(\pi\alpha)}\right)^2$$

valide per $\alpha \notin \mathbb{Z}$ e che si dimostrano facilmente per induzione, per $i \neq j$ si trova

$$(\underline{\xi}_i, \underline{\xi}_j) = \frac{1}{L} \cdot \frac{\sin^2\big((N+L)\pi(x_i - x_j)\big) - \sin^2\big(N\pi(x_i - x_j)\big)}{\sin^2\big(\pi(x_i - x_j)\big)},$$

e quindi

$$|(\underline{\xi}_i, \underline{\xi}_j)| \leq \frac{1}{L\sin^2\big(\pi(x_i - x_j)\big)}.$$

Inoltre per $|\alpha| \leq \frac{1}{2}$ si ha $|\sin(\pi\alpha)| \geq 2|\alpha|$, e a causa del fatto che gli x_i sono δ-ben spaziati, fissato i ci sono al massimo due indici j per cui $\|x_i - x_j\| \in [k\delta, (k+1)\delta)$. In definitiva

$$\begin{aligned}
\sum_{j=1}^{R} |(\underline{\xi}_i, \underline{\xi}_j)| &\leq 2N + L + \sum_{j\neq i} \frac{1}{L\sin^2\big(\pi(x_i - x_j)\big)} \\
&\leq 2N + L + \sum_{j\neq i} \frac{1}{4L\|x_i - x_j\|^2} \\
&\leq 2N + L + \frac{1}{4L} \sum_{n\geq 1} \frac{1}{(n\delta)^2} |\{j\colon \|x_i - x_j\| \in [n\delta, (n+1)\delta)\}| \\
&\leq 2N + L + \frac{1}{4L\delta^2} \sum_{n\geq 1} \frac{2}{n^2} \\
&\leq 2N + L + \frac{1}{L\delta^2}.
\end{aligned}$$

Scegliendo $L \stackrel{\text{def}}{=} \big[\delta^{-1}\big] + 1$ si ottiene la (6.4.1). Il Teorema segue in generale osservando che il modulo di $S(x)$ non cambia se si moltiplicano tutti gli a_n per la stessa costante di modulo unitario, e questa può essere scelta in modo tale che le "frequenze" n appartengano ad un qualsiasi intervallo dato $[M+1, M+N]$. □

Definizione 6.4.5. *Sia $\mathfrak{P}$ un insieme non vuoto di numeri primi; per ogni $p \in \mathfrak{P}$ sia assegnato un insieme $\Omega_p \subseteq \mathbb{Z}_p$ di cardinalità $\omega(p) \stackrel{\text{def}}{=} |\Omega_p|$. Dato $\mathcal{A} \subseteq \mathbb{N}^*$ poniamo*

$$\mathcal{S}_0(\mathcal{A}; \mathfrak{P}) = \mathcal{S}_0(\mathcal{A}; \mathfrak{P}; \{\Omega_p\}) \stackrel{\text{def}}{=} \{a \in \mathcal{A}\colon a \mod p \notin \Omega_p \, \forall p \in \mathfrak{P}\}.$$
$$\mathcal{S}(\mathcal{A}; \mathfrak{P}) = \mathcal{S}(\mathcal{A}; \mathfrak{P}; \{\Omega_p\}) \stackrel{\text{def}}{=} \big|\mathcal{S}_0(\mathcal{A}; \mathfrak{P}; \{\Omega_p\})\big|.$$

Definizione 6.4.6. *Dato $Q \geq 1$ l'insieme $\mathcal{F} = \mathcal{F}(Q) \stackrel{\text{def}}{=} \big\{\frac{a}{q}\colon q \leq Q,\ 1 \leq a \leq q,\ (a,q) = 1\big\}$ si chiama insieme delle* frazioni di Farey.

Osservazione 6.4.7. *L'insieme $\mathcal{F}(Q)$ è Q^{-2}-ben spaziato; infatti, dati $\frac{a_1}{q_1}$, $\frac{a_2}{q_2} \in \mathcal{F}(Q)$, se essi sono distinti si ha*

$$\left|\frac{a_1}{q_1} - \frac{a_2}{q_2}\right| = \frac{|a_1q_2 - a_2q_1|}{q_1q_2} \geq \frac{1}{q_1q_2} \geq \frac{1}{Q^2}. \tag{6.4.2}$$

Teorema 6.4.8. *Dati M, $N \in \mathbb{N}^*$, un insieme non vuoto di numeri primi $\mathfrak{P}$, siano $\mathcal{A} \stackrel{\text{def}}{=} [M+1, M+N] \cap \mathbb{N}$ e $\mathcal{B} = \mathcal{B}(\mathfrak{P}) \stackrel{\text{def}}{=} \{n \in \mathbb{N}^* : p \mid n \Rightarrow p \in \mathfrak{P}\}$. Si ha la disuguaglianza*

$$\mathcal{S}(\mathcal{A}, \mathfrak{P}) \le \frac{N + 2Q^2}{L} \qquad \textit{dove} \qquad L \stackrel{\text{def}}{=} \sum_{q \in \mathcal{B} \cap [1,Q]} \mu^2(q) \prod_{p \mid q} \frac{\omega(p)}{p - \omega(p)}.$$

Dim.: Si osservi che questo risultato *non dipende* dalle particolari classi di resto negli insiemi Ω_p, ma solo dalla loro cardinalità $\omega(p)$. Inoltre, ponendo $\Omega(p) \stackrel{\text{def}}{=} \emptyset$ per $p \notin \mathfrak{P}$, si può sempre supporre che $\mathfrak{P}$ sia l'insieme di tutti i numeri primi. Poniamo

$$S(x) \stackrel{\text{def}}{=} \sum_{n=M+1}^{M+N} a_n e(nx), \qquad J(q) \stackrel{\text{def}}{=} \prod_{p \mid q} \frac{\omega(p)}{p - \omega(p)}.$$

Si osservi che J è moltiplicativa. Poniamo $a_n \stackrel{\text{def}}{=} 0$ se $n \notin \mathcal{S}_0(\mathcal{A}, \mathfrak{P})$: per il Teorema 6.4.3 e per la (6.4.2) è sufficiente dimostrare la disuguaglianza

$$\Big| \sum_{n=M+1}^{M+N} a_n \Big|^2 \mu^2(q) J(q) = |S(0)|^2 \mu^2(q) J(q) \le \sum_{a \bmod q}^{*} \Big| S\Big(\frac{a}{q}\Big) \Big|^2, \tag{6.4.3}$$

dove $\sum^*$ indica che la somma è fatta solo sugli elementi di $\mathbb{Z}_q^*$. Infatti la disuguaglianza cercata segue prendendo $a_n \stackrel{\text{def}}{=} 1$ per $n \in \mathcal{S}_0(\mathcal{A}, \mathfrak{P})$, e poi sommando su q. Evidentemente è sufficiente dimostrare la (6.4.3) quando $\mu(q) \neq 0$. Supponiamo che sia vera per ogni scelta dei coefficienti complessi a_n (ferma restando la condizione $a_n = 0$ per $n \notin \mathcal{S}_0(\mathcal{A}, \mathfrak{P})$). Sostituendo a_n con $a_n e(n\beta)$ si ottiene la disuguaglianza

$$|S(\beta)|^2 J(q) \le \sum_{a \bmod q}^{*} \Big| S\Big(\frac{a}{q} + \beta\Big) \Big|^2. \tag{6.4.4}$$

Supponiamo dunque di aver dimostrato la (6.4.3) per $q = q_1$ e per $q = q_2$ con $(q_1, q_2) = 1$. Per il Teorema Cinese del Resto 1.2.4 e per la (6.4.4) si ha

$$\begin{aligned} \sum_{a \bmod q_1 q_2}^{*} \Big| S\Big(\frac{a}{q_1 q_2}\Big) \Big|^2 &= \sum_{a_1 \bmod q_1}^{*} \sum_{a_2 \bmod q_2}^{*} \Big| S\Big(\frac{a_1}{q_1} + \frac{a_2}{q_2}\Big) \Big|^2 \\ &\ge J(q_2) \sum_{a_1 \bmod q_1}^{*} \Big| S\Big(\frac{a_1}{q_1}\Big) \Big|^2 \ge J(q_1) J(q_2) |S(0)|^2, \end{aligned}$$

cioè la (6.4.3) è vera per $q = q_1 q_2$. Dunque è sufficiente dimostrare che vale quando $q = p$, un numero primo. Poniamo

$$S(p, a) \stackrel{\text{def}}{=} \sum_{\substack{n=M+1 \\ n \equiv a \bmod p}}^{M+N} a_n,$$

osservando che, per costruzione, $S(p,a)=0$ se $a\in\Omega_p$. Si ha quindi

$$\sum_{a=1}^{p-1}\Big|S\Big(\frac{a}{p}\Big)\Big|^2=\sum_{a=1}^{p-1}\Big|\sum_{n=M+1}^{M+N}a_n e\big(\tfrac{a}{p}n\big)\Big|^2=\sum_{a=1}^{p-1}\sum_{n,m=M+1}^{M+N}a_n\overline{a}_m e\big(\tfrac{a}{p}(n-m)\big)$$
$$=\sum_{n,m=M+1}^{M+N}a_n\overline{a}_m\sum_{a=1}^{p-1}e\big(\tfrac{a}{p}(n-m)\big)=p\sum_{a=1}^{p}|S(p,a)|^2-|S(0)|^2. \tag{6.4.5}$$

D'altra parte, per la disuguaglianza di Cauchy, poiché $S(p,a)=0$ se $a\in\Omega_p$,

$$|S(0)|^2=\Big|\sum_{a=1}^{p}S(p,a)\Big|^2\le\big(p-\omega(p)\big)\sum_{a=1}^{p}|S(p,a)|^2,$$

e si ottiene quanto voluto dividendo per $\big(p-\omega(p)\big)$ e sostituendo nella (6.4.5). □

§6.5. Applicazioni del crivello grande

La prima applicazione di questi risultati è un'importantissima disuguaglianza, la seconda è una maggiorazione del giusto ordine di grandezza della quantità a primo membro nel
𝔈 6.5.1–2 Teorema di Landau 3.2.3 e la terza una maggiorazione per il numero dei primi gemelli.

Lemma 6.5.1. *Se $k\in\mathbb{N}^*$ e $Q\ge 1$ allora*

$$\frac{k}{\varphi(k)}\sum_{\substack{q\le Q\\(q,k)=1}}\frac{\mu^2(q)}{\varphi(q)}>\log Q.$$

Dim.: È sufficiente dimostrare che

$$\frac{k}{\varphi(k)}\sum_{\substack{q\le Q\\(q,k)=1}}\frac{\mu^2(q)}{\varphi(q)}\ge\sum_{n\le Q}\frac{1}{n}>\int_1^Q\frac{\mathrm{d}t}{t}=\log Q.$$

Per il Teorema 3.2.8 si ha

$$\frac{k}{\varphi(k)}\sum_{\substack{q\le Q\\(q,k)=1}}\frac{\mu^2(q)}{\varphi(q)}=\sum_{\substack{q\le Q\\(q,k)=1}}\frac{\mu^2(q)}{q}\prod_{p\mid q}\Big(1+\frac{1}{p}+\frac{1}{p^2}+\dots\Big)\prod_{p\mid k}\Big(1+\frac{1}{p}+\frac{1}{p^2}+\dots\Big).$$

Dato $n\in\mathbb{N}^*$ indicheremo con $\ker(n)$ il piú grande $q\mid n$ con $\mu(q)\neq 0$; in altre parole, $\ker(n)$ è il prodotto di tutti i fattori primi *distinti* di n. Sviluppando i prodotti (con il Teorema 3.3.1) si vede che quest'ultima quantità è

$$\sum_{\substack{q\le Q\\(q,k)=1}}\frac{\mu^2(q)}{q}\sum_{\substack{m\ge 1\\p\mid m\Rightarrow p\mid qk}}\frac{1}{m}\ge\sum_{n\le Q}\frac{1}{n},$$

poiché è possibile scrivere ogni $n\le Q$ nella forma $n=n_1n_2$, con $(n_1,n_2)=(n_1,k)=1$, e quindi n compare nella prima somma qui sopra quando $q=\ker(n_1)\le Q$ ed $m=nq^{-1}$. □

Teorema 6.5.2 (Brun-Titchmarsh). *Per ogni $q \in \mathbb{N}^*$, $a \in \mathbb{Z}$ con $(a,q)=1$, $M>1$, $N>3q$ si ha*

$$\pi(M+N;q,a)-\pi(M;q,a)=\sum_{\substack{p\in(M,M+N]\\ p\equiv a \mod q}} 1 \le \frac{2N}{\varphi(q)\log(N/q)}\left(1+\mathcal{O}\left(\frac{\log\log(N/q)}{\log(N/q)}\right)\right),$$

dove la costante in $\mathcal{O}(\cdot)$ è assoluta.

Dim.: Possiamo evidentemente supporre che $1 \le a \le q$. Prendiamo

$$\mathcal{A} \stackrel{\text{def}}{=} \left[\frac{M+1-a}{q}, \frac{M+N-a}{q}\right] \cap \mathbb{N}, \qquad \text{da cui} \qquad |\mathcal{A}| \le \frac{N}{q}+1$$
$$\mathfrak{P} \stackrel{\text{def}}{=} \{p \le Q : p \nmid q\}, \qquad \Omega_p \stackrel{\text{def}}{=} \{-aq^{-1} \mod p\} \qquad \text{per } p \in \mathfrak{P}.$$

Dunque $\mathcal{B} \supseteq \{n \le Q : (n,q)=1\}$ e $\omega(p)=1$ per ogni $p \in \mathfrak{P}$. Se $r \equiv a \mod q$ è un numero primo $>Q$ allora $p \nmid r$ per ogni primo $p \in \mathfrak{P}$; in altre parole $n \stackrel{\text{def}}{=} \frac{1}{q}(r-a) \notin \Omega_p$ per ogni primo $p \in \mathfrak{P}$ e quindi $n \in \mathcal{S}_0(\mathcal{A},\mathfrak{P})$, da cui

$$\pi(M+N;q,a)-\pi(M;q,a) \le \mathcal{S}(\mathcal{A},\mathfrak{P})+Q. \tag{6.5.1}$$

Dal Teorema 6.4.8 deduciamo

$$\mathcal{S}(\mathcal{A},\mathfrak{P}) \le \frac{N/q+1+2Q^2}{L} \quad \text{dove} \quad L \stackrel{\text{def}}{=} \sum_{n\in\mathcal{B}\cap[1,Q]} \mu^2(n)\prod_{p\mid n}\frac{1}{p-1} = \sum_{\substack{n\le Q\\(n,q)=1}}\frac{\mu^2(n)}{\varphi(n)}.$$

Per il Lemma 6.5.1 si ha $\dfrac{q}{\varphi(q)}L > \log Q$ e la (6.5.1) dà

$$\pi(M+N;q,a)-\pi(M;q,a) \le \frac{N+q+2qQ^2}{\varphi(q)\log Q}+Q,$$

ed il risultato cercato segue prendendo $Q \stackrel{\text{def}}{=} (N/q)^{1/2}\big(\log(N/q)\big)^{-1}$. □

Teorema 6.5.3. *Poniamo $\mathfrak{P}(x;q,a) \stackrel{\text{def}}{=} \{p \le x : p \equiv a \mod q\}$. Per ogni a, $q \in \mathbb{N}^*$ con $(a,q)=1$ esiste una costante $C=C(q,a)>0$ tale che per $x \to \infty$ si ha*

$$\prod_{p\in\mathfrak{P}(x;q,a)}\left(1-\frac{1}{p}\right) = \frac{C(q,a)}{(\log x)^{1/\varphi(q)}}\left(1+\mathcal{O}_{q,a}\left(\frac{1}{\log x}\right)\right).$$

Dim.: Procediamo come nella dimostrazione del Teorema di Mertens 4.3.6, omettendo qualche dettaglio: per sommazione parziale dal Teorema 5.3.1 otteniamo

$$\sum_{\substack{p\le x\\ p\equiv a \mod q}}\frac{1}{p} = \frac{1}{\varphi(q)}\log\log x + C_1(q,a) + \mathcal{O}\big((\log x)^{-1}\big).$$

Inoltre

$$\sum_{\substack{p\le x\\ p\equiv a \mod q}}\log\left(1-\frac{1}{p}\right) = -\sum_{\substack{p\le x\\ p\equiv a \mod q}}\frac{1}{p} + \sum_{p\equiv a \mod q}\left(\log\left(1-\frac{1}{p}\right)+\frac{1}{p}\right)+\mathcal{O}\left(\frac{1}{x}\right).$$

Il risultato desiderato segue ora passando all'esponenziale. □

TEOREMA 6.5.4. *Si ha*

$$|\{n \le N : r_2(n) > 0\}| \ll \frac{N}{(\log N)^{1/2}}.$$

DIM.: Poniamo $r_2'(n) \stackrel{\text{def}}{=} |\{(a,b) \in \mathbb{Z}^2 : a^2 + b^2 = n \text{ e } (a,b) = 1\}|$, e cioè $r_2'(n)$ è il numero delle rappresentazioni primitive di n come somma di due quadrati. Per il Teorema 1.4.10, $r_2'(n) > 0$ se e solo se n non ha fattori primi $\equiv 3 \mod 4$ e $4 \nmid n$. Utilizziamo il Teorema 6.4.8 con $\mathcal{A} \stackrel{\text{def}}{=} [1, N] \cap \mathbb{N}$, $\mathfrak{P} \stackrel{\text{def}}{=} \{2\} \cup \mathfrak{P}(Q; 4, 3)$, ed $\Omega_p \stackrel{\text{def}}{=} \{0\}$ per ogni $p \in \mathfrak{P}$. Si ha quindi

$$|\{n \le N : (n,2) = 1,\, r_2'(n) > 0\}| \le \frac{N + 2Q^2}{L} \qquad \text{dove} \qquad L \stackrel{\text{def}}{=} \sum_{q \in \mathcal{B}(\mathfrak{P}) \cap [1,Q]} \frac{\mu^2(q)}{\varphi(q)}.$$

Se poniamo $k = k(Q) \stackrel{\text{def}}{=} \prod p$, dove il prodotto è esteso all'insieme $\mathfrak{P}(Q; 4, 1)$, la condizione $q \in \mathcal{B}(\mathfrak{P}) \cap [1, Q]$ è equivalente a $(q, k) = 1$, $q \le Q$. Dal Lemma 6.5.1 otteniamo

$$L = \sum_{\substack{q \le Q \\ (q,k)=1}} \frac{\mu^2(q)}{\varphi(q)} > \frac{\varphi(k)}{k} \log Q = \log Q \prod_{\substack{p \le Q \\ p \equiv 1 \mod 4}} \left(1 - \frac{1}{p}\right).$$

Per il Lemma 6.5.3 si ha $L \ge \big(C(4,1) + o(1)\big)\big(\log Q\big)^{1/2}$ e la scelta $Q \stackrel{\text{def}}{=} N^{1/2}$ ci dà quindi

$$|\{n \le N : (n,2) = 1,\, r_2'(n) > 0\}| \ll \frac{N}{(\log N)^{1/2}}. \tag{6.5.2}$$

Infine osserviamo che

$$\big|\{n \le N : r_2(n) > 0\}\big| \le 2 \sum_{m \le N^{1/2}} \big|\big\{n \le Nm^{-2} : (n,2) = 1,\, r_2'(n) > 0\big\}\big|.$$

Se $m \in \big(N^{1/3}, N^{1/2}\big]$ maggioriamo il corrispondente addendo a secondo membro in modo banale, e per gli altri usiamo la (6.5.2). In definitiva

$$\big|\{n \le N : r_2(n) > 0\}\big| \ll \sum_{m \le N^{1/3}} \frac{N}{m^2\big(\log\big(Nm^{-2}\big)\big)^{1/2}} + \sum_{N^{1/3} < m \le N^{1/2}} \frac{N}{m^2}.$$

In ciascun addendo della prima somma si ha $\log\big(Nm^{-2}\big) \ge \log N^{1/3} = \frac{1}{3}\log N$, e la seconda somma è banalmente $\mathcal{O}\big(N \cdot N^{-1/3}\big) = \mathcal{O}\big(N^{2/3}\big)$. La tesi segue immediatamente. □

LEMMA 6.5.5. *Dato $h \in \mathbb{N}^*$, per $Q \to \infty$ si ha*

$$D_h(Q) \stackrel{\text{def}}{=} \sum_{\substack{q \le Q \\ (q,h)=1}} d(q) = \left\{\frac{\varphi(h)}{h}\right\}^2 Q \left(\log Q + 2\gamma - 1 + 2\sum_{p \mid h} \frac{\log p}{p-1}\right) + \mathcal{O}\Big(Q^{1/2} d(h)\Big).$$

Dim.: Per il Teorema 3.2.5 possiamo ovviamente supporre che $h > 1$ e che $\mu(h) \neq 0$ (cioè che $h = \ker(h)$). Poniamo $\mathcal{B} = \mathcal{B}(h) \stackrel{\text{def}}{=} \{n \in \mathbb{N}^* : \ker(n) \mid h\}$, e definiamo la funzione aritmetica d_h come segue: $d_h(n) = d(n)$ se $n \in \mathcal{B}$, e 0 altrimenti. Poiché ogni $q \geq 1$ può essere scritto in modo unico come rq', con $r \in \mathcal{B}$, $(h, q') = 1$, si ha evidentemente

$$D(Q) \stackrel{\text{def}}{=} D_1(Q) = \sum_{r \in \mathcal{B}} d(r) D_h\left(\frac{Q}{r}\right) = \sum_{r \geq 1} d_h(r) D_h\left(\frac{Q}{r}\right),$$

e quindi per la seconda formula di inversione di Möbius 3.1.12 ed il Teorema 3.2.5 si ha

$$D_h(Q) = \sum_{r \geq 1} d_h^{-1}(r) D\left(\frac{Q}{r}\right) = \sum_{r \in \mathcal{B}} \mu * \mu(r) \left\{ \frac{Q}{r} \log \frac{Q}{r} + c\frac{Q}{r} + \mathcal{O}\Big(Q^{1/2} r^{-1/2}\Big) \right\},$$

dove abbiamo scritto per brevità $c \stackrel{\text{def}}{=} 2\gamma - 1$; inoltre $d^{-1} = (N_0 * N_0)^{-1} = \mu * \mu$. Poiché $\mu * \mu\big(p^\alpha\big) = 0$ per ogni p, se $\alpha \geq 3$, gli unici addendi non nulli nelle somme che seguono sono quelli per cui $r \mid h^2$. Dunque per il Teorema 3.1.5 abbiamo

$$\sum_{r \in \mathcal{B}} \mu * \mu(r) \frac{1}{r} = \prod_{p \mid h} \left\{ 1 + \mu * \mu(p) \frac{1}{p} + \mu * \mu\big(p^2\big) \frac{1}{p^2} \right\} = \left\{ \frac{\varphi(h)}{h} \right\}^2.$$

Inoltre si dimostra facilmente per induzione sul numero di fattori primi di h che

$$\sum_{r \mid h^2} \mu * \mu(r) \frac{\log r}{r} = -2 \left\{ \frac{\varphi(h)}{h} \right\}^2 \sum_{p \mid h} \frac{\log p}{p-1}.$$

Infine, sempre per il Teorema 3.1.5

$$\sum_{r \mid h^2} \big|\mu * \mu(r)\big| r^{-1/2} = \prod_{p \mid h} \left(1 + \frac{1}{p^{1/2}}\right)^2 \leq 8d(h),$$

che conclude la dimostrazione. □

Teorema 6.5.6. *Sia $h \in \mathbb{N}^*$ un numero pari. Per $x \to \infty$ si ha*

$$\big|\{p \leq x : p + h \text{ è primo}\}\big| \ll_h \frac{x}{(\log x)^2}.$$

Dim.: Prendiamo $\mathcal{A} \stackrel{\text{def}}{=} [1, x] \cap \mathbb{N}$, e per $p \leq Q$ poniamo $\Omega_p \stackrel{\text{def}}{=} \{0, -h \mod p\}$. Evidentemente $\omega(p) = 2$ se $p \nmid h$, $\omega(p) = 1$ se $p \mid h$. Quindi abbiamo

$$\begin{aligned} L &\stackrel{\text{def}}{=} \sum_{q \leq Q} \mu(q)^2 \prod_{p \mid q} \frac{\omega(p)}{p - \omega(p)} = \sum_{q \leq Q} \mu(q)^2 \prod_{p \mid q} \left\{ \frac{\omega(p)}{p} + \frac{\omega(p)^2}{p^2} + \cdots \right\} \\ &= \sum_{\substack{q \geq 1 \\ \ker(q) \leq Q}} \frac{1}{q} \prod_{p^\alpha \| q} \omega(p)^\alpha \geq \sum_{\substack{q \leq Q \\ (q,h)=1}} \frac{2^{\Omega(q)}}{q} \geq \sum_{\substack{q \leq Q \\ (q,h)=1}} \frac{d(q)}{q}, \end{aligned}$$

dove $\Omega(q)$ è il numero totale dei fattori primi di q, poiché $d\big(p^\alpha\big) = \alpha + 1 \leq 2^\alpha$ e $2^\Omega \in \mathfrak{M}^*$.

Per sommazione parziale dal Lemma 6.5.5 si ha infine $L \geq \frac{1}{2}\left\{\frac{\varphi(h)}{h}\right\}^2 (\log Q)^2 + \mathcal{O}_h(\log Q)$, ed il Teorema segue prendendo $Q \stackrel{\text{def}}{=} x^{1/2}$. □

Con tecniche piú raffinate (quelle accennate nel Capitolo 7) è possibile dare una stima che fornisce la "giusta" dipendenza da h come nella (6.3.4).

Capitolo 7. Introduzione alla Teoria Analitica dei Numeri

La Teoria Analitica dei Numeri nasce con la dimostrazione di Eulero del fatto che esistono infiniti numeri primi. Qui daremo solo qualche breve cenno ai risultati principali, senza alcuna pretesa di completezza. Assumeremo qualche conoscenza della teoria delle funzioni olomorfe: si veda anche l'Appendice §A2. Da qui in poi $s \stackrel{\text{def}}{=} \sigma + \mathrm{i}t$ è una variabile complessa con parte reale $\sigma = \Re(s)$ e parte immaginaria $t = \Im(s)$.

§7.1. La funzione zeta di Riemann

Teorema 7.1.1 (Eulero-Riemann). *La serie ed il prodotto*

$$\sum_{n\geq 1} \frac{1}{n^s} \qquad \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}$$

convergono totalmente e quindi uniformemente in tutti i compatti contenuti nel semipiano $\{s \in \mathbb{C} \colon \Re(s) > 1\}$ *e rappresentano la stessa funzione olomorfa, detta funzione* ζ *di Riemann. La funzione* ζ *ha un prolungamento meromorfo a* $\sigma > 0$*, e nel punto* $s = 1$ *ha un polo semplice con residuo* 1*.*

Dim.: La convergenza totale della somma e del prodotto è una conseguenza immediata delle disuguaglianze

$$\left|\sum_{n\geq 1} \frac{1}{n^s}\right| \leq \sum_{n\geq 1} \left|\frac{1}{n^s}\right| = \sum_{n\geq 1} \frac{1}{n^\sigma} = \zeta(\sigma).$$

La rappresentazione come prodotto di Eulero segue immediatamente dal Teorema 3.3.1, poiché $N_{-s} \in \mathfrak{M}^*$. Preso poi un numero reale $x > 1$, per la formula di sommazione parziale, nel semipiano $\{s \in \mathbb{C} \colon \Re(s) > 1\}$ si ha

$$\sum_{n\leq x} \frac{1}{n^s} = \frac{[x]}{x^s} + s\int_1^x \frac{[t]}{t^{s+1}}\mathrm{d}t = \frac{[x]}{x^s} + \frac{s}{s-1}\left(1 - x^{1-s}\right) - s\int_1^x \frac{\{t\}}{t^{s+1}}\mathrm{d}t.$$

Dunque,

$$\zeta(s) = \lim_{x\to+\infty} \sum_{n\leq x} \frac{1}{n^s} = \frac{s}{s-1} - s\int_1^{+\infty} \frac{\{t\}}{t^{s+1}}\mathrm{d}t. \tag{7.1.1}$$

Quest'ultima formula fornisce il prolungamento analitico di ζ al semipiano $\sigma > 0$, privato del punto $s = 1$, in quanto l'integrale è totalmente convergente in ogni compatto contenuto in $\sigma > 0$, ed è anche chiaro che in ζ ha un polo semplice con residuo 1 in $s = 1$. □

Inoltre, ricordando la definizione della costante di Eulero, si verifica immediatamente che

$$\lim_{s\to 1}\left(\zeta(s)-\frac{1}{s-1}\right)=1-\int_1^\infty \frac{\{t\}}{t^2}\mathrm{d}t=\gamma.$$

TEOREMA 7.1.2. *In $\sigma>1$ vale la rappresentazione*

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

dove μ è la funzione di Möbius e sia la serie che il prodotto sono uniformemente convergenti in ogni compatto contenuto nel semipiano $\sigma>1$.

DIM.: La convergenza uniforme di serie e prodotto nel semipiano $\sigma>1$ si dimostrano esattamente come sopra, dato che $|\mu(n)|\leq 1$ per ogni $n\in\mathbb{N}^*$. Inoltre è chiaro dal Teorema 7.1.1 che il prodotto vale $1/\zeta(s)$. □

COROLLARIO 7.1.3. *$\zeta(s)\neq 0$ nel semipiano $\sigma=\Re(s)>1$.*

DIM.: La convergenza assoluta della serie $g(s)\stackrel{\text{def}}{=}\sum_n \mu(n)n^{-s}$ ed il Prodotto di Eulero implicano che $g(s)\zeta(s)=1$ per ogni s con $\Re(s)>1$, da cui evidentemente $\zeta(s)\neq 0$ (in altre parole, un eventuale zero di ζ in $\sigma>1$ comporterebbe un polo di $1/\zeta$). Ci si può anche basare sulla seconda dimostrazione del Teorema 3.3.1. Si ha $f(n)=n^{-s}$ e quindi la (3.3.1) e la (3.3.2) implicano

$$\left|\zeta(s)\prod_{p\leq x}\left(1-\frac{1}{p^s}\right)-1\right|\leq\sum_{n>x}\frac{1}{n^\sigma}\leq\int_{x-1}^{+\infty}\frac{\mathrm{d}t}{t^\sigma}=\frac{1}{\sigma-1}(x-1)^{1-\sigma}<1$$

se, e. g., $x=1+\big(2/(\sigma-1)\big)^{1/(\sigma-1)}$, e questo dà una contraddizione se $\zeta(s)=0$. □

TEOREMA 7.1.4 (RIEMANN). *La funzione ξ definita da*

$$\xi(s)\stackrel{\text{def}}{=}\frac{1}{2}s(s-1)\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s),$$

è olomorfa su $\mathbb{C}$, non ha zeri per $\sigma>1$ né per $\sigma<0$, e soddisfa l'equazione funzionale

$$\xi(s)=\xi(1-s). \tag{7.1.2}$$

La (7.1.2) fornisce dunque il prolungamento analitico di ζ a $\mathbb{C}\setminus\{1\}$.

DIM.: Diamo una dimostrazione senza troppi dettagli: per $\sigma>0$ ed $n\in\mathbb{N}^*$

$$\Gamma(s)=\int_0^{+\infty}t^{s-1}e^{-t}\,\mathrm{d}t=n^s\int_0^{+\infty}x^{s-1}e^{-nx}\,\mathrm{d}x$$

e quindi per $\sigma>1$ si ha

$$\zeta(s)\Gamma(s)=\sum_{n\geq 1}\Gamma(s)n^{-s}=\int_0^{+\infty}\frac{x^{s-1}}{e^x-1}\mathrm{d}x. \tag{7.1.3}$$

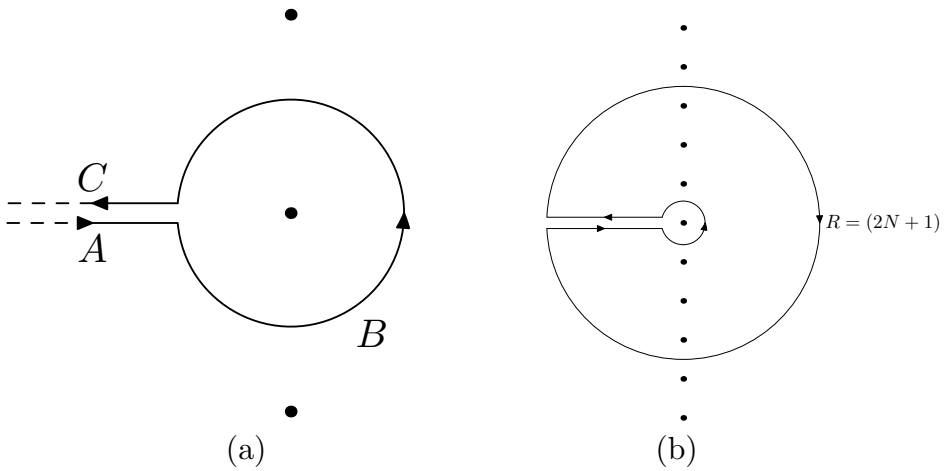


Figura 7.1. *I cammini di integrazione nel Teorema* 7.1.4.

Consideriamo l'integrale

$$I(s) \stackrel{\text{def}}{=} \frac{1}{2\pi\mathrm{i}} \int_\gamma \frac{z^{s-1}}{e^{-z}-1}\mathrm{d}z \tag{7.1.4}$$

dove γ è il cammino nella Figura 7.1 (a), nella quale è sottinteso che le semirette indicate con A e C giacciono entrambe sull'asse reale, e che il raggio della circonferenza è $\varrho < 2\pi$. Inoltre definiamo $z^s \stackrel{\text{def}}{=} \exp\bigl(s \log z\bigr)$ dove $|\arg(z)| \leq \pi$. Si può far vedere che la (7.1.4) definisce una funzione analitica di s il cui valore è indipendente da ϱ, e che per $\varrho \to 0+$ l'integrale sulla circonferenza tende a 0; combinando i due integrali sulle semirette A e C mediante i cambiamenti di variabile $z \stackrel{\text{def}}{=} re^{-\pi\mathrm{i}}$, $z \stackrel{\text{def}}{=} re^{\pi\mathrm{i}}$ rispettivamente, si trova

$$\pi I(s) = \sin(\pi s)\Gamma(s)\zeta(s) \qquad \text{da cui} \qquad \zeta(s) = \Gamma(1-s)I(s). \tag{7.1.5}$$

Questa formula fornisce il prolungamento analitico di ζ a $\mathbb{C}$, privato dei punti in cui $\Gamma(1-s)$ ha dei poli, e cioè $\mathbb{N}^*$, e possiamo dunque usarla per $\sigma < 0$. Consideriamo la funzione

$$I_N(s) \stackrel{\text{def}}{=} \frac{1}{2\pi\mathrm{i}} \int_{C(N)} \frac{z^{s-1}}{e^{-z}-1}\mathrm{d}z$$

dove $C(N)$ è il cammino nella Figura 7.1 (b), con convenzioni simili a quelle sopra, e la circonferenza esterna ha raggio $R = (2N+1)\pi$, $N \in \mathbb{N}$. Si può dimostrare che per $N \to \infty$ l'integrale sulla circonferenza esterna tende a 0; per il teorema di Cauchy abbiamo dunque

$$\begin{aligned} I_N(s) &= \sum_{n=1}^{N} \bigl((2\pi\mathrm{i}n)^{s-1} + (-2\pi\mathrm{i}n)^{s-1}\bigr) \\ &= \sum_{n=1}^{N} (2n\pi)^{s-1} 2\cos\bigl(\tfrac{1}{2}\pi(s-1)\bigr) = 2(2\pi)^{s-1}\sin\bigl(\tfrac{1}{2}\pi s\bigr)\sum_{n=1}^{N} n^{s-1} \\ &\to 2(2\pi)^{s-1}\sin\bigl(\tfrac{1}{2}\pi s\bigr)\zeta(1-s) \qquad \text{per } N \to +\infty. \end{aligned} \tag{7.1.6}$$

Ma per $N \to \infty$ si ha anche $I_N(s) \to I(s)$ e confrontando le due espressioni (7.1.5) e (7.1.6) si ottiene l'equazione funzionale nella forma asimmetrica

$$\zeta(s) = \frac{(2\pi)^s \sin\bigl(\frac{1}{2}\pi s\bigr)}{\sin(\pi s)\Gamma(s)}\zeta(1-s) = \frac{(2\pi)^s}{2\cos\bigl(\frac{1}{2}\pi s\bigr)\Gamma(s)}\zeta(1-s).$$

Per ottenere la forma dell'enunciato si usano le proprietà della funzione Γ. □

Corollario 7.1.5. *La funzione ζ è olomorfa su $\mathbb{C}\setminus\{1\}$, non ha zeri in $\sigma \geq 1$ e per $\sigma \leq 0$ si annulla solo nei punti $s = -2n$, $n \in \mathbb{N}^*$. Nella striscia $0 < \sigma < 1$ ha gli stessi zeri di ξ, detti zeri non banali. Inoltre, dalle (7.1.3) e (7.1.5) si ricava la rappresentazione $\zeta(2n) = 2^{2n-1}B_n\pi^{2n}(2n)!^{-1}$ per $n \in \mathbb{N}^*$, dove i B_n sono i numeri di Bernoulli definiti*
𝔈 7.1.1 *nell'Appendice A4. Dunque $\zeta(2n)\pi^{-2n} \in \mathbb{Q}$.*

Teorema 7.1.6 (Prodotto infinito). *ξ ha un'infinità di zeri $\varrho \stackrel{\text{def}}{=} \beta + \mathrm{i}\gamma$ nella striscia $0 < \sigma < 1$, disposti simmetricamente rispetto all'asse reale ed alla retta $\sigma = \frac{1}{2}$. Inoltre, esistono costanti A, $B \in \mathbb{R}$ tali che*

$$\xi(s) = e^{A+Bs}\prod_{\varrho}\left(1-\frac{s}{\varrho}\right)e^{s/\varrho} \stackrel{\text{def}}{=} e^{A+Bs}\lim_{T\to+\infty}\prod_{|\varrho|<T}\left(1-\frac{s}{\varrho}\right)e^{s/\varrho},$$

dove il prodotto converge per tutti gli $s \in \mathbb{C}$, e ϱ indica il generico zero non banale di ζ.

Dim.: L'esistenza della fattorizzazione data nell'enunciato (detta prodotto di Weierstrass sugli zeri) dipende dalla teoria generale delle funzioni intere di ordine finito, della quale ricordiamo brevemente qualche rudimento. Si definisce *ordine* della funzione intera f l'estremo inferiore dei numeri reali positivi μ tali che

$$f(z) = \mathcal{O}_\mu\bigl(\exp\bigl(|z|^\mu\bigr)\bigr). \tag{7.1.7}$$

C'è una relazione molto stretta fra l'ordine di una funzione intera ed il numero di zeri che questa può avere all'interno del cerchio con centro nell'origine e raggio $R > 0$. Infatti si ha

Lemma 7.1.7 (Formula di Jensen). *Sia f una funzione olomorfa in $\{|z| \leq R\}$, priva di zeri su $\{|z| = R\}$ e tale che $f(0) \neq 0$. Siano $\varrho_1 \leq \varrho_2 \leq \cdots \leq \varrho_n$ i moduli degli zeri di f in questo cerchio, ripetuti secondo la molteplicità. Si ha dunque*

$$\frac{1}{2\pi}\int_0^{2\pi}\log\left|\frac{f(Re^{\mathrm{i}\theta})}{f(0)}\right|\mathrm{d}\theta = \log\frac{R^n}{\varrho_1\cdots\varrho_n} = \int_0^R\frac{n(t)}{t}\mathrm{d}t. \tag{7.1.8}$$

Non è difficile dare una dimostrazione di questo Lemma osservando che se vale separatamente per f e per g, è immediato che valga per $f\cdot g$. Dunque è sufficiente dimostrare che vale per funzioni del tipo $f(z) = z - z_k$, e per le funzioni che non hanno zeri in $\{|z| \leq R\}$. La prima parte è semplice, mentre la seconda è una conseguenza immediata della formula di Cauchy, poiché, se f è olomorfa e non nulla in $\{|z| \leq R\}$, allora anche $\log f$ è olomorfa nello stesso insieme. In questo caso, tutti i membri della (7.1.8) valgono 0. L'uguaglianza a destra si dimostra per sommazione parziale (A.1.1) con $a_n \stackrel{\text{def}}{=} 1$ e $\varphi(t) \stackrel{\text{def}}{=} \log(R/t)$.

Sia ora $n(R)$ il numero di zeri che la funzione intera f ha all'interno del cerchio $\{|z| = R\}$, ed α l'ordine di f. Per R grande, il primo membro della Formula di Jensen (7.1.8) è $\mathcal{O}_\varepsilon(R^{\alpha+\varepsilon})$. Dato che $n(R)$ è monotona crescente, si ha

$$n(R) = n(R)\int_R^{eR} \frac{1}{t}\mathrm{d}t \le \int_R^{eR} \frac{n(t)}{t}\mathrm{d}t = \mathcal{O}_\varepsilon\big(R^{\alpha+\varepsilon}\big),$$

e, in definitiva, che $n(R) = \mathcal{O}_\varepsilon(R^{\alpha+\varepsilon})$. Da questo si deduce immediatamente che

$$\sum_\varrho |\varrho|^{-\alpha-\varepsilon} \tag{7.1.9}$$

converge, dove ϱ indica il generico zero della funzione f, supponendo che $f(0) \neq 0$. Infatti, sempre per la formula di sommazione parziale, si ha

$$\sum_{|\varrho_n|\le R} \frac{1}{\varrho_n^{\alpha+\varepsilon}} = \frac{n(R)}{R^{\alpha+\varepsilon}} + (\alpha+\varepsilon)\int_0^R \frac{n(t)}{t^{\alpha+\varepsilon+1}}\,\mathrm{d}t.$$

Ma $n(t) = \mathcal{O}_\varepsilon\big(t^{\alpha+\varepsilon/2}\big)$, e quindi quest'ultimo integrale è convergente.

L'equazione funzionale soddisfatta dalla funzione ξ implica che l'ordine di ξ è 1: infatti, a causa della presenza della funzione Γ, per la formula di Stirling (A.2.2) si ha $\log\xi(s) \sim Cs\log s$ quando $s \to +\infty$ lungo l'asse reale. Inoltre, per la (7.1.1), la funzione ζ è limitata da $C|s|$ nel semipiano $\sigma \ge \frac{1}{2}$ privato di un intorno del punto $s = 1$, e per la formula di Stirling la funzione Γ è "grande" solo in prossimità dell'asse reale.

Questo significa che la (7.1.7) non vale con $\mu = 1$, e si può dimostrare che questo fatto implica l'esistenza di infiniti zeri di ξ: infatti si dimostra che la serie (7.1.9) diverge per $\varepsilon = 0$, e questo può accadere solo se ξ (e dunque ζ) ha infiniti zeri. L'equazione funzionale ed il Lemma 7.2.1 implicano che questi zeri sono nella striscia $0 \le \sigma \le 1$. È possibile dimostrare che $A = -\log 2$, $B = \frac{1}{2}\log(4\pi) - 1 - \frac{1}{2}\gamma$, e che l'ordinata dello zero con $\gamma > 0$ piú piccolo è ≈ 14.13. □

Osservazione 7.1.8. *In un certo senso questo risultato "corrisponde" alla fattorizzazione che vale per i polinomi: se $f(z) = a_n z^n + \cdots + a_0$ è un polinomio di grado $n > 0$ con $a_0 \neq 0$, e con radici $\lambda_1, \ldots, \lambda_n$ (ripetute secondo la molteplicità) si ha $f(z) = a_0\big(1-\frac{z}{\lambda_1}\big)\cdots\big(1-\frac{z}{\lambda_n}\big)$. Nel caso della funzione ξ, il fattore $e^{s/\varrho}$ permette la convergenza del prodotto infinito.*

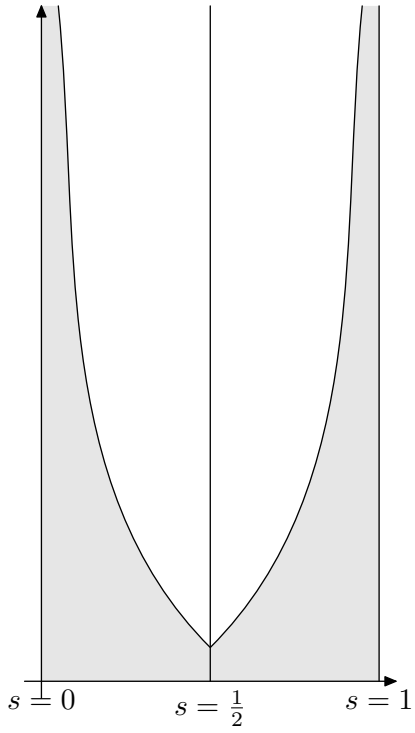
§7.2. Proprietà della funzione zeta: distribuzione degli zeri

Teorema 7.2.1. *Esiste una costante $c \in \mathbb{R}^+$ tale che per ogni zero non banale di zeta $\varrho = \beta + \mathrm{i}\gamma$ si ha*

$$\beta < 1 - \frac{c}{\log|\gamma|}.$$

Dim.: Partiamo da un'osservazione di Mertens:

$$2(1+\cos\theta)^2 = 3 + 4\cos\theta + \cos 2\theta \ge 0$$



La parte della regione libera da zeri nel semipiano $t = \Im(s) \geq 0$. Per $t \to +\infty$ l'ampiezza della regione all'altezza t è $\gg (\log t)^{-1}$.

Figura 7.2. *La regione libera da zeri.*

per ogni $\theta \in \mathbb{R}$. Inoltre, nella regione $\sigma > 1$ si ha

$$\Re \log \zeta(\sigma + \mathrm{i}t) = \sum_p \sum_{m \geq 1} \frac{\cos\bigl(t \log p^m\bigr)}{m p^{m\sigma}}.$$

Usiamo quest'ultima formula con $s = \sigma$, $s = \sigma + \mathrm{i}t$ ed $s = \sigma + 2\mathrm{i}t$, ottenendo

$$3 \log \zeta(\sigma) + 4\Re \log \zeta(\sigma + \mathrm{i}t) + \Re \log \zeta(\sigma + 2\mathrm{i}t) \geq 0,$$

da cui, passando all'esponenziale,

$$\zeta^3(\sigma) \bigl| \zeta^4(\sigma + \mathrm{i}t) \zeta(\sigma + 2\mathrm{i}t) \bigr| \geq 1. \tag{7.2.1}$$

Poiché per $\sigma \to 1+$ si ha che $\zeta(\sigma) \sim (\sigma - 1)^{-1}$ e che $\zeta(\sigma + 2\mathrm{i}t)$ resta limitata, se $1 + \mathrm{i}t$ fosse uno zero di ζ il primo membro della (7.2.1) sarebbe infinitesimo, una contraddizione. Questo ragionamento può essere esteso per dare il risultato dell'enunciato. □

Teorema 7.2.2 (Riemann-von Mangoldt). *Per $T \to +\infty$ si ha*

$$N(T) \stackrel{\text{def}}{=} \bigl| \{ \varrho = \beta + \mathrm{i}\gamma \colon \zeta(\varrho) = 0,\ \beta \in [0,1],\ \gamma \in [0,T] \} \bigr| = \frac{T}{2\pi} \log \frac{T}{2\pi} - \frac{T}{2\pi} + \mathcal{O}(\log T).$$

Dim.: Supponiamo che $T > 0$ non coincida con l'ordinata di uno zero della funzione ξ: per il principio dell'argomento si ha

$$N(T) = \frac{1}{2\pi} \Delta_{R(T)} \arg \xi(s)$$

dove $R(T)$ è il rettangolo con vertici in $s_1 = 2$, $s_2 = 2 + \mathrm{i}T$, $s_3 = -1 + \mathrm{i}T$, $s_4 = -1$. Dato che ξ è reale e non nulla sul segmento $[-1, 2]$ non c'è variazione dell'argomento. Inoltre, per l'equazione funzionale 7.1.4, la variazione sulla parte del rettangolo con $\sigma \leq \frac{1}{2}$ è esattamente uguale a quella sul resto, e quindi

$$N(T) = \frac{1}{\pi}\Delta_{L(T)} \arg \xi(s)$$

dove $L(T)$ è la spezzata costituita dai due segmenti di estremi s_1 ed s_2, s_2 ed $s_5 = \frac{1}{2} + \mathrm{i}T$. Per la formula di Stirling generalizzata (A.2.2) per la funzione Γ di Eulero abbiamo

$$\begin{aligned}
\Delta_{L(T)} \arg(s-1) &= \frac{1}{2}\pi + \mathcal{O}\big(T^{-1}\big), \\
\Delta_{L(T)} \arg \pi^{-s/2} &= -\frac{1}{2}T \log \pi, \\
\Delta_{L(T)} \arg \Gamma\left(\frac{1}{2}s + 1\right) &= \frac{1}{2}T \log \frac{1}{2}T - \frac{1}{2}T + \frac{3}{8}\pi + \mathcal{O}\big(T^{-1}\big).
\end{aligned}$$

Per ottenere la tesi resta da dimostrare che $\Delta_{L(T)} \arg \zeta(s) = \mathcal{O}(\log T)$, che omettiamo. □

§7.3. La formula esplicita

Lemma 7.3.1 (Formula di Perron). *Per $x > 0$ e $c > 1$ si ha*

$$\frac{1}{2\pi\mathrm{i}} \int_{(c)} x^s \frac{\mathrm{d}s}{s} = \begin{cases} 0 & \text{se } x \in (0,1), \\ \frac{1}{2} & \text{se } x = 1, \\ 1 & \text{se } x > 1. \end{cases}$$

Dim.: È un'applicazione immediata del Teorema dei residui. □

Teorema 7.3.2 (Riemann–von Mangoldt). *Per $x > 1$ vale la* formula esplicita*:*

$$\psi_0(x) = x - \sum_{\varrho} \frac{x^\varrho}{\varrho} - \frac{\zeta'(0)}{\zeta(0)} - \frac{1}{2}\log\big(1 - x^{-2}\big),$$

dove la somma deve essere intesa in senso simmetrico (i termini provenienti da ϱ e da $\overline{\varrho}$ devono essere presi insieme), e $\psi_0(x)$ è la media dei valori di ψ a destra ed a sinistra di x,

$$\psi_0(x) \stackrel{\text{def}}{=} \lim_{\varepsilon \to 0+} \frac{\psi(x+\varepsilon) + \psi(x-\varepsilon)}{2}.$$

Dim.: È un'applicazione (non banale) della Formula di Perron: infatti per $c > 1$ si ha

$$\psi_0(x) = \frac{1}{2\pi\mathrm{i}} \int_{(c)} -\frac{\zeta'}{\zeta}(s) \frac{x^s}{s} \mathrm{d}s. \tag{7.3.1}$$

Il risultato si ottiene modificando in modo opportuno il cammino di integrazione. □

Utilizzando una forma troncata della Formula di Perron, possiamo ottenere la seguente forma approssimata della formula esplicita, piú utile nelle applicazioni:

Teorema 7.3.3. *Per $x > 1$ e $T \in [1, x]$ si ha*

$$\psi(x) = x - \sum_{|\gamma| \leq T} \frac{x^\varrho}{\varrho} + \mathcal{O}\Big(\frac{x}{T}\big(\log xT\big)^2\Big).$$

§7.4. Dimostrazione del teorema dei numeri primi

Riassumiamo brevemente la strategia seguita per dimostrare il Teorema dei Numeri Primi
ℭ 7.4.2–3 nella forma 4.1.3: utilizzando l'equazione funzionale e le proprietà della funzione Γ di Eulero si ottiene una rappresentazione di $-\zeta'/\zeta$ che dà la formula esplicita 7.3.3 nella forma approssimata, per mezzo della Formula di Perron. Poi, utilizziamo la regione libera da zeri del Teorema 7.2.1 per stimare il contributo degli zeri non banali alla formula esplicita, e quindi per ottenere il resto dato dal Teorema 4.1.3.

Dalla formula esplicita del Teorema 7.3.3 ricaviamo

$$\psi(x)-x \ll \Big\{\max_{0<\gamma\le T} x^{\beta}\Big\} \sum_{0<\gamma\le T} \frac{1}{\gamma} + \frac{x}{T}\big(\log xT\big)^2,$$

dove abbiamo scritto implicitamente $\varrho=\beta+\mathrm{i}\gamma$ per il generico zero non banale di zeta. Si ricordi che gli zeri sono disposti simmetricamente rispetto all'asse reale. Il massimo può essere stimato usando la regione libera da zeri fornita dal Teorema 7.2.1, mentre per la somma utilizziamo la stima per il numero degli zeri della funzione zeta con parte immaginaria $|\gamma|\le T$ data dalla 7.2.2, con la sommazione parziale. In definitiva, possiamo scrivere

$$\psi(x)-x \ll x(\log T)^2 \exp\left\{-c\frac{\log x}{\log T}\right\} + \frac{x}{T}\big(\log xT\big)^2, \tag{7.4.1}$$

nella quale scegliamo T come funzione di x in modo tale che $(\log T)^2=\log x$. Sostituendo e semplificando si trova infine $\psi(x)-x\ll x\exp\{-c'(\log x)^{1/2}\}$.

Per ottenere il risultato che riguarda $\pi(x)$, conviene ricordare che $\theta(x)=\psi(x)+\mathcal{O}\big(x^{1/2}\big)$. Per sommazione parziale ed integrazione per parti, si ottiene

$$\pi(x)=\mathrm{li}(x)+\mathcal{O}\Big(x\exp\{-c''(\log x)^{1/2}\}\Big),$$

che è molto piú forte del risultato ottenuto nel Capitolo 4.

§7.5. La congettura di Riemann

Teorema 7.5.1. *Sia* $\Theta \stackrel{\mathrm{def}}{=} \sup\{\beta\colon \varrho=\beta+\mathrm{i}\gamma \text{ è uno zero di } \zeta\}$. *La congettura di Riemann* 4.1.4 *è equivalente a* $\Theta=\frac12$.

Dim.: Posto $R(x)\stackrel{\mathrm{def}}{=}\psi(x)-x$, con la formula di sommazione parziale si trova la rappresentazione

$$-\frac{\zeta'}{\zeta}(s)=s\int_1^\infty \frac{\psi(x)}{x^{s+1}}\mathrm{d}s=\frac{s}{s-1}+s\int_1^\infty\frac{R(x)}{x^{s+1}}\mathrm{d}s, \tag{7.5.1}$$

inizialmente in $\sigma>1$. Ma se $R(x)\ll x^{1/2}(\log x)^2$, l'ultimo integrale è uniformemente convergente in $\sigma\ge\frac12+\delta$ per ogni $\delta>0$, e quindi il secondo membro definisce una funzione analitica in $\sigma>\frac12$ privato del punto $s=1$. Per prolungamento analitico, l'unica singolarità della funzione a primo membro in $\sigma>\frac12$ può essere in $s=1$. In altre parole, ζ non si annulla in questo semipiano. L'altra implicazione si dimostra utilizzando la formula esplicita, come nel paragrafo precedente, scegliendo $T=x^{1/2}$. □

Si osservi che le due formule (7.3.1) e (7.5.1) rappresentano una coppia trasformata–antitrasformata di Mellin (che formalmente sono trasformazioni dello stesso tipo di quella di Fourier, e il cui esempio piú noto è la coppia e^{-x}, $\Gamma(s)$). È possibile scrivere una coppia di formule analoga che coinvolge indirettamente $\pi(x)$:

$$\log\zeta(s) = s\int_1^\infty \frac{\Pi(t)}{t^{s+1}}\mathrm{d}t \qquad\qquad \Pi_0(x) = \frac{1}{2\pi\mathrm{i}}\int_{(c)} \log\zeta(s)\frac{x^s}{s}\mathrm{d}s$$

dove

$$\Pi(x) \stackrel{\text{def}}{=} \pi(x) + \pi\big(x^{1/2}\big) + \pi\big(x^{1/3}\big) + \cdots$$

e Π_0 è la regolarizzata di Π definita come ψ_0 a partire da ψ (cfr l'enunciato del Teorema 7.3.2). Inoltre si ha

$$\log\zeta(s) = s\int_1^\infty \frac{\pi(t)}{t\big(t^s-1\big)}\mathrm{d}t,$$

ma è piú difficile trovare l'inversa di questa. Il motivo analitico per cui la funzione ψ è piú "naturale" deriva dal fatto che la funzione $-\zeta'/\zeta$ ha singolarità di tipo polare agli zeri ed al polo di ζ e non presenta difficoltà di prolungamento analitico, mentre la funzione $\log\zeta$ ha evidenti problemi di prolungamento negli stessi punti.

§7.6. Considerazioni finali

Ancora sul teorema di Dirichlet. Vogliamo motivare brevemente la dimostrazione del Teorema di Dirichlet data nel Capitolo 5. La dimostrazione di Eulero del fatto che esistono infiniti numeri primi può essere messa in questa forma: per $\sigma > 1$ si ha

$$\begin{aligned}\log\zeta(s) &= -\sum_p \log\left(1-\frac{1}{p^s}\right) = \sum_{m\ge1}\sum_p \frac{1}{mp^{ms}}\\ &= \sum_p \frac{1}{p^s} + \sum_{m\ge2}\sum_p \frac{1}{mp^{ms}} = f(s) + \mathcal{O}(1),\end{aligned}$$

diciamo. Ma se $s \to 1^+$ rimanendo reale, $\log\zeta(s) \to +\infty$, mentre $f(s)$ tenderebbe ad un limite finito se esistessero un numero finito di numeri primi. In modo analogo,

$$\log L(s,\chi) = f(s,\chi) + \mathcal{O}_q(1), \qquad \text{dove} \qquad f(s,\chi) \stackrel{\text{def}}{=} \sum_p \frac{\chi(p)}{p^s}.$$

Inoltre $L(s,\chi_0) = \zeta(s)\prod_{p|q}(1-p^{-s})$ e quindi $f(s,\chi_0) = f(s) + \mathcal{O}_q(1)$. Per ortogonalità

$$\sum_{p\equiv a \bmod q} \frac{1}{p^s} = \frac{1}{\varphi(q)}\sum_{\chi \bmod q} \overline{\chi}(a)\log L(s,\chi) + \mathcal{O}_q(1). \tag{7.6.1}$$

Quindi, se si riesce a dimostrare che $L(1,\chi) \neq 0$ per $\chi \neq \chi_0$, si ha che $\log L(s,\chi)$ è una funzione limitata in un intorno di $s = 1$, ed il Teorema di Dirichlet segue dalla (7.6.1).

Distribuzione degli zeri e termine d'errore. Si può dimostrare che il Teorema dei Numeri Primi nella forma che abbiamo dimostrato nel Capitolo 4 (cioè la relazione $\pi(x) \sim x(\log x)^{-1}$) è equivalente all'affermazione $\zeta(1+\mathrm{i}t) \neq 0$ per ogni $t > 0$. In altre parole, non è necessario conoscere la distribuzione degli zeri della funzione ζ, né altre informazioni relative alla regione $\sigma < 1$. Questo fatto segue dalla teoria di Wiener. Bombieri ha studiato la relazione fra una forma generalizzata delle formule di Selberg (4.4.2) ed il termine d'errore nel Teorema dei Numeri Primi che si può ottenere elementarmente. Pintz ha dimostrato che c'è una relazione quantitativa molto precisa fra regioni libere da zeri per la funzione zeta e termine d'errore nel Teorema dei Numeri Primi. Poniamo

$$M(x) \stackrel{\text{def}}{=} \max\{|\pi(t) - \mathrm{li}(t)| : t \in [2, x]\}.$$

In effetti, si ha che

$$\log \frac{x}{M(x)} \sim \min_{\varrho=\beta+\mathrm{i}\gamma} \{(1-\beta)\log x + \log|\gamma|\},$$

quando $x \to +\infty$. Per esempio, se $\pi(x) = \mathrm{li}(x) + \mathcal{O}\big(x\exp(-(\log x)^b)\big)$ per qualche $b \in (0,1)$, allora il risultato di Pintz implica che qualunque sia $x \geq 2$ e qualunque sia lo zero non banale $\varrho = \beta + \mathrm{i}\gamma$ di ζ, si ha

$$(1-\beta)\log x + \log|\gamma| \geq (1+o(1))(\log x)^b$$

da cui segue (essenzialmente)

$$1 - \beta \geq (\log x)^{b-1} - \frac{\log|\gamma|}{\log x}.$$

Si cerca il massimo assoluto della funzione a secondo membro (ricordando che $b < 1$), e si trova che questa ha un massimo per $\log x_0 = \big((\log|\gamma|)/(1-b)\big)^{1/b}$ da cui segue che la funzione ζ non ha zeri nella regione

$$\sigma > 1 - \frac{c(b)}{(\log|t|)^{(1-b)/b}}.$$

L'implicazione inversa (da una regione libera da zeri della forma $\sigma > 1 - c(\log t)^{-\theta}$ alla stima $\mathcal{O}\big(x\exp\big(-c'(\log x)^{1/(\theta+1)}\big)\big)$ per il termine d'errore) si può dimostrare scegliendo $(\log T)^{\theta+1} = \log x$ nella (7.4.1).

Un calcolo molto semplice mostra che se $\pi(x) = \mathrm{li}(x) + \mathcal{O}\big(x^{\Theta}\big)$, si ha $(1-\beta)\log x + \log|\gamma| \geq (1+o(1))(1-\Theta)\log x$ da cui segue $\log|\gamma| \geq (1+o(1))(\beta-\Theta)\log x$. Se esistesse uno zero $\varrho_0 = \beta_0 + \mathrm{i}\gamma_0$ di ζ con $\beta_0 > \Theta$, si potrebbe prendere x abbastanza grande da rendere falsa quest'ultima relazione. Quindi, come abbiamo visto anche sopra, si ha necessariamente $\beta_0 \leq \Theta$.

Concludiamo il Capitolo con una scherzosa (ma istruttiva) canzone sulla funzione zeta.

The Zeta Function Song (Sung to the tune of "Sweet Betsy from Pike")

Where are the zeros of zeta of s?
G. F. B. Riemann has made a good guess,
They're all on the critical line, said he,
And their density's[1] one over $2\pi \log t$.

This statement of Riemann's has been like a trigger,
And many good men, with vim and with vigor,
Have attempted to find, with mathematical rigor,
What happens to zeta as mod t gets bigger.

The names of Landau and Bohr and Cramer,
And Hardy and Littlewood and Titchmarsh are there,
In spite of their efforts and skill and finesse,
In locating the zeros no one's had success.

In 1914 G. H. Hardy did find,
An infinite number that lay on the line[2],
His theorem, however, won't rule out the case,
That there might be a zero at some other place.

Let P be the function π minus li,
The order of P is not known for x high,
If square root of x times $\log x$ we could show,
Then Riemann's conjecture would surely be so[3].

Related to this is another enigma,
Concerning the Lindelöf function $\mu(\sigma)$
Which measures the growth in the critical strip[4],
And on the number of zeros it gives us a grip.

But nobody knows how this function behaves,
Convexity tells us it can have no waves,
Lindelöf said that the shape of its graph,
Is constant when sigma is more than one half.

Oh, where are the zeros of zeta of s?
We must know exactly, we cannot just guess,
In order to strengthen the prime number theorem,
The path of integration must not get too near'em[5].

Tom Apostol, Number Theory Conference, Caltech, June 1955

What Tom Apostol Didn't Know

Andre Weil has bettered old Riemann's fine guess,
By using a fancier zeta of s,
He proves that the zeros are where they should be[6],
Provided the characteristic is p.

There's a good moral to draw from this long tale of woe
That every young genius among you should know:
If you tackle a problem and seem to get stuck,
Just take it mod p and you'll have better luck.

Anonymous (Saunders Mac Lane?), Cambridge University, 1973

What fraction of zeros on the line will be found
When mod t is kept below some given bound?
Does the fraction, whatever, stay bounded below
As the bound on mod t is permitted to grow?

The efforts of Selberg did finally banish
All fears that the fraction might possibly vanish[7].
It stays bounded below, which is just as it should,
But the bound he determined was not very good.

Norm Levinson managed to show, better yet,
At two-to-one odds it would be a good bet,
If over a zero you happen to trip
It would lie on the line and not just in the strip[8].

Levinson tried in a classical way,
Weil brought modular means into play,
Atiyah then left and Paul Cohen quit,
So now there's no proof at all that will fit.

But now we must study this matter anew,
Serre points out manifold things it makes true,
A medal[9] might be the reward in this quest,
For Riemann's conjecture is surely the best.

Saunders Mac Lane

Note.

(1) Vedi il Teorema di Riemann–von Mangoldt 7.2.2.
(2) Sia $N_0(T) \stackrel{\text{def}}{=} \left|\{\varrho = \frac{1}{2} + \mathrm{i}\gamma \colon \zeta(\varrho) = 0,\ \gamma \in [0,T]\}\right|$ il numero degli zeri di zeta sulla retta critica $\sigma = \frac{1}{2}$. Hardy ha dimostrato che per $T \to +\infty$ si ha $N_0(T) > AT$ per qualche $A > 0$.
(3) Si veda il Teorema 7.5.1.
(4) Per $\sigma \in \mathbb{R}$ si ponga $\mu(\sigma) = \inf\{\alpha \in \mathbb{R} \colon |\zeta(\sigma + \mathrm{i}t)| \ll |t|^\alpha \text{ per } |t| \to +\infty\}$. La teoria generale delle serie di Dirichlet implica che μ è convessa, e la (7.1.1) implica che $\mu(\sigma) = 0$ per $\sigma > 1$. La Congettura di Riemann implica che $\mu(\sigma) = 0$ per $\sigma \geq \frac{1}{2}$.
(5) Questo è necessario nella dimostrazione del Teorema 7.3.3.
(6) André Weil ha dimostrato l'analoga della Congettura di Riemann per certe curve.
(7) Selberg ha dimostrato che $N_0(T) > AN(T)$ per $T \to \infty$ per qualche $A > 0$.
(8) Levinson ha dimostrato che la costante A qui sopra vale almeno $\frac{1}{3}$.
(9) Chi dimostrerà la Congettura di Riemann riceverà certamente la Medaglia Fields.

Capitolo 8. Il problema di Goldbach

In questo Capitolo cercheremo di spiegare perché la congettura di Goldbach è difficile, tanto da non essere stata ancora dimostrata. Si tengano presenti le Congetture espresse dalle (9.1.2) e (9.1.3), nonché le argomentazioni che conducono alla (6.3.4) ed al Teorema 6.5.6.

§8.1. Problemi additivi: il metodo del cerchio

Nel corso degli ultimi secoli si sono presentati all'attenzione dei matematici molti problemi di natura additiva, come per esempio il problema di Waring ed il problema di Goldbach. Posto in generale, il tipico problema additivo può essere visto cosí: sono dati s sottoinsiemi di $\mathbb{N}$, $\mathcal{A}_1, \dots, \mathcal{A}_s$, non necessariamente distinti, dove $s \in \mathbb{N}$ è almeno 2. Il problema consiste nel determinare il numero di soluzioni dell'equazione

$$n = a_1 + a_2 + \cdots + a_s \tag{8.1.1}$$

dove $n \in \mathbb{N}$ è dato, e $a_j \in \mathcal{A}_j$ per $j = 1, \dots, s$, o per lo meno, dimostrare che per n sufficientemente grande questa equazione ha almeno una soluzione. Nel problema di Waring si prendono tutti gli insiemi $\mathcal{A}_j$ uguali alle k-esime potenze e si cerca di determinare il minimo s per cui l'equazione (8.1.1) ha soluzione per ogni $n \in \mathbb{N}$, oppure il minimo s per cui l'equazione (8.1.1) ha soluzione per ogni $n \in \mathbb{N}$ sufficientemente grande. Nel Teorema di Lagrange 1.5.1 abbiamo visto che ogni intero $n \in \mathbb{N}$ si rappresenta come somma di al piú 4 quadrati. Nel problema binario di Goldbach si prendono $\mathcal{A}_1 = \mathcal{A}_2 = \mathfrak{P}$, l'insieme di tutti i primi. Si osservi che in questo ed in casi analoghi ci sono motivi aritmetici che impongono delle restrizioni agli n per cui ci si chiede se la (8.1.1) abbia una soluzione.

Il metodo per affrontare i problemi additivi che vedremo ha la sua origine in un articolo del 1918 di Hardy & Ramanujan sulle partizioni, ma dato il numero di problemi affrontati e risolti in questo modo da Hardy & Littlewood negli anni '20 ormai ha preso il loro nome o quello di "metodo del cerchio." Descriveremo le idee di Hardy, Littlewood & Ramanujan, con una certa dose di dettagli. Per semplicità, inizieremo dal caso in cui $s = 2$ ed $\mathcal{A}_1 = \mathcal{A}_2 = \mathcal{A}$. Si parte ponendo

$$f(z) = f_{\mathcal{A}}(z) \stackrel{\text{def}}{=} \sum_{n=0}^{\infty} a(n) z^n, \qquad \text{dove} \qquad a(n) = \begin{cases} 1 & \text{se } n \in \mathcal{A}, \\ 0 & \text{altrimenti.} \end{cases}$$

Se $\mathcal{A}$ è infinito (in caso contrario il problema non ha interesse) allora f è una serie di potenze con raggio di convergenza uguale ad 1. Ci interessa il numero delle "rappresentazioni" di n nella forma $a_1 + a_2$ con $a_j \in \mathcal{A}$, $j = 1, 2$. Poniamo quindi

$$r_2(n) \stackrel{\text{def}}{=} \big|\{(a_1, a_2) \in \mathcal{A} \times \mathcal{A} : n = a_1 + a_2\}\big|,$$

Per le note proprietà delle serie di potenze (prodotto di Cauchy), per $|z|<1$ si ha

$$f^2(z)=\sum_{n=0}^{\infty}c(n)z^n \qquad \text{dove} \qquad c(n)=\sum_{\substack{0\le h,k\le n\\ h+k=n}}\sum a(h)a(k)$$

ed $a(h)a(k)\neq 0$ se e solo se h, $k\in\mathcal{A}$; dunque $c(n)=r_2(n)$. Allo stesso modo si dimostra che $f^s(z)=\sum_{n=0}^{\infty}r_s(n)z^n$ dove $r_s(n)\stackrel{\text{def}}{=}\bigl|\{(a_1,\dots,a_s)\in\mathcal{A}^s\colon n=a_1+\cdots+a_s\}\bigr|$. Per il teorema di Cauchy, per $\varrho<1$ si ha quindi

$$r_2(n)=\frac{1}{2\pi\mathrm{i}}\int_{\gamma(\varrho)}\frac{f^2(z)}{z^{n+1}}\,\mathrm{d}z, \tag{8.1.2}$$

dove $\gamma(\varrho)$ è la circonferenza di centro l'origine e raggio ϱ. Per certi insiemi $\mathcal{A}$ è possibile determinare uno sviluppo asintotico per f in un intorno delle singolarità presenti sulla circonferenza $\gamma(1)$ e quindi si può stimare l'integrale nella (8.1.2) prendendo ϱ una funzione di n che ha limite 1.

Possiamo usare questo metodo per "risolvere" un problema piuttosto semplice: dato $k\in\mathbb{N}^*$, determinare in quanti modi è possibile scrivere $n\in\mathbb{N}$ come somma di esattamente k numeri naturali. In altre parole, vogliamo determinare $r_k(n)\stackrel{\text{def}}{=}\bigl|\{(a_1,\dots,a_k)\in\mathbb{N}^k\colon n=a_1+\cdots+a_k\}\bigr|$. Naturalmente è possibile dimostrare direttamente che $r_k(n)=\binom{n+k-1}{k-1}$. Evidentemente si ha $f(z)=\sum_{n=0}^{\infty}z^n=(1-z)^{-1}$. Quindi, per $\varrho<1$,

$$r_k(n)=\frac{1}{2\pi\mathrm{i}}\int_{\gamma(\varrho)}\frac{\mathrm{d}z}{(1-z)^k z^{n+1}}. \tag{8.1.3}$$

Si osservi che la funzione integranda ha una sola singolarità sulla circonferenza $\gamma(1)$, e di un tipo piuttosto semplice. In questo caso particolare è possibile calcolare esattamente il valore dell'integrale a destra nella (8.1.3): infatti, poiché $\varrho<1$, vale lo sviluppo

$$\frac{1}{(1-z)^k}=1+\binom{-k}{1}(-z)+\binom{-k}{2}(-z)^2+\cdots=\sum_{m=0}^{\infty}\binom{-k}{m}(-z)^m.$$

La serie a destra converge totalmente in tutti i compatti contenuti in $\{z\in\mathbb{C}\colon|z|<1\}$ e dunque possiamo sostituire nella (8.1.3) e scambiare l'integrale con la serie:

$$\begin{aligned} r_k(n)&=\frac{1}{2\pi\mathrm{i}}\sum_{m=0}^{\infty}\binom{-k}{m}(-1)^m\int_{\gamma(\varrho)}z^{m-n-1}\,\mathrm{d}z\\ &=\frac{1}{2\pi\mathrm{i}}\sum_{m=0}^{\infty}(-1)^m\binom{-k}{m}\begin{cases}2\pi\mathrm{i} & \text{se } m=n,\\ 0 & \text{altrimenti,}\end{cases}=(-1)^n\binom{-k}{n}, \end{aligned}$$

e non è difficile vedere che $(-1)^n\binom{-k}{n}=\binom{n+k-1}{k-1}$. Si osservi infine che la funzione integranda è relativamente piccola su tutta la circonferenza $\gamma(\varrho)$ a parte un piccolo arco vicino al punto $z=\varrho$, il quale dà il contributo principale all'integrale nella (8.1.3).

In generale non è possibile valutare direttamente ed esattamente l'integrale, ed inoltre la funzione integranda avrà piú singolarità sulla circonferenza $\gamma(1)$. Per esempio, per determinare in quanti modi è possibile scrivere $n \in \mathbb{N}$ come somma di esattamente k interi dispari, dobbiamo prendere la funzione $g(z) = \sum_{m=0}^{\infty} z^{2m+1} = \dfrac{z}{1-z^2}$, che ha singolarità in $z = \pm 1$. In questi casi si dovrà cercare uno sviluppo asintotico per la funzione integranda valido in prossimità di ciascuna singolarità.

Questo procedimento è stato utilizzato da Hardy & Littlewood negli anni '20 per dimostrare molti risultati relativi al problema di Waring e per portare il primo vero attacco al problema di Goldbach. Negli anni '30 Vinogradov introdusse alcune semplificazioni che rendono la sua versione del metodo del cerchio piú facile da esporre. L'idea di base di Hardy & Littlewood è quella di avere una funzione fissata, $f(z)^k$ nell'esempio precedente, e prendere ϱ come funzione di n che ha limite 1; inoltre si devono cercare opportuni sviluppi asintotici nei pressi delle singolarità che la funzione integranda presenta sulla circonferenza $\gamma(1)$. Vinogradov osserva che alla quantità $r_2(n)$ contribuiscono solo gli interi $m \leq n$: dunque si può introdurre la funzione

$$f_N(z) \stackrel{\text{def}}{=} \sum_{m=0}^{N} z^m = \frac{1-z^{N+1}}{1-z} \tag{8.1.4}$$

(l'ultima uguaglianza è valida per $z \neq 1$). Per $n \leq N$, il Teorema di Cauchy dà

$$r_k(n) = \frac{1}{2\pi \mathrm{i}} \int_{\gamma(1)} \frac{f_N^k(z)}{z^{n+1}}\, \mathrm{d}z. \tag{8.1.5}$$

In questo caso non ci sono singolarità della funzione integranda (si ricordi che f_N è una somma *finita*, e quindi non ci sono problemi di convergenza): per questo motivo possiamo fissare una volta per tutte la circonferenza su cui si integra. Poniamo $e(x) \stackrel{\text{def}}{=} e^{2\pi \mathrm{i} x}$ e facciamo il cambiamento di variabile $z = e(\alpha)$ nella (8.1.5):

$$r_k(n) = \int_0^1 f_N^k\big(e(\alpha)\big)\, e(-n\alpha)\, \mathrm{d}\alpha. \tag{8.1.6}$$

Questa è anche la formula che dà l'n-esimo coefficiente di Fourier della funzione $f_N^k\big(e(\alpha)\big)$, per l'ortogonalità della funzione esponenziale complessa. Per futura comodità poniamo $T_N(\alpha) = T(\alpha) \stackrel{\text{def}}{=} f_N\big(e(\alpha)\big)$; per la (8.1.4) si ha quindi

$$T(\alpha) \stackrel{\text{def}}{=} \sum_{m=0}^{N} e(m\alpha) = \begin{cases} \dfrac{1-e\big((N+1)\alpha\big)}{1-e(\alpha)} = e\big(\tfrac{1}{2}N\alpha\big)\dfrac{\sin(\pi(N+1)\alpha)}{\sin(\pi\alpha)} & \text{se } \alpha \notin \mathbb{Z}; \\ N+1 & \text{se } \alpha \in \mathbb{Z}. \end{cases} \tag{8.1.7}$$

Si veda la Figura 8.2 per il grafico di $|T_{20}(\alpha)|$. La proprietà che ci serve per concludere la nostra analisi "elementare" riguarda la rapidità con cui la funzione T decade quando α si allontana dai valori interi: dalla (8.1.7) si ricava facilmente che

$$|T_N(\alpha)| \leq \min\left(N+1, \frac{1}{|\sin(\pi\alpha)|}\right) \leq \min\big(N+1, \|\alpha\|^{-1}\big) \tag{8.1.8}$$

poiché T è periodica di periodo 1 ed inoltre $\alpha \le \sin(\pi\alpha)$ per $\alpha \in \bigl(0, \frac12\bigr]$. Questa disuguaglianza mostra che se $\delta = \delta(N)$ non è troppo piccolo, l'intervallo $[\delta, 1-\delta]$ non dà un contributo apprezzabile all'integrale nella (8.1.6): infatti, se $\delta \ge \frac{1}{N}$ e $k \ge 2$ abbiamo

$$\left| \int_\delta^{1-\delta} T_N^k(\alpha) e(-n\alpha)\,\mathrm{d}\alpha \right| \le \int_\delta^{1-\delta} |T_N^k(\alpha)|\,\mathrm{d}\alpha \le \int_\delta^{1-\delta} \frac{\mathrm{d}\alpha}{\|\alpha\|^k} \le \frac{2}{k-1}\delta^{1-k} \tag{8.1.9}$$

e questo è $o\bigl(N^{k-1}\bigr)$ non appena $\delta^{-1} = o(N)$. In altre parole, è sufficiente che δ sia appena piú grande di N^{-1} affinché il contributo dell'intervallo $[\delta, 1-\delta]$ all'integrale nella (8.1.6) sia piú piccolo del termine principale che, ricordiamo, è dell'ordine di $N^{k-1}(k-1)!^{-1}$. In altre parole ancora, il termine principale è concentrato attorno ad $\alpha = 0$. Può essere interessante notare che, almeno nel caso $k = 2$, è possibile spingere la nostra analisi ancora piú avanti: prendendo $n = N$ e $\delta^{-1} = o(N)$, per le (8.1.6) ed (8.1.9) si ha

$$r_2(N) = \int_0^1 \left(\frac{\sin\bigl(\pi(N+1)\alpha\bigr)}{\sin(\pi\alpha)} \right)^2 \mathrm{d}\alpha = 2\int_0^\delta \left(\frac{\sin\bigl(\pi(N+1)\alpha\bigr)}{\sin(\pi\alpha)} \right)^2 \mathrm{d}\alpha + o(N), \tag{8.1.10}$$

perché la funzione integranda è periodica di periodo 1 (se ne veda la definizione). Suddividiamo l'intervallo $[0,\delta]$ negli intervalli $\mathcal{I}_h \stackrel{\text{def}}{=} [\delta_h, \delta_{h+1}]$, per $h = 0, \dots$, dove abbiamo posto $\delta_h \stackrel{\text{def}}{=} \frac{h}{N+1}$. Stimando l'integrale su $\mathcal{I}_h$ con l'area del triangolo inscritto nel grafico si trova che quest'ultimo vale approssimativamente $4N^2(\pi h)^{-2}$ quando h è dispari. Facendo la somma su tutti i valori ammissibili di h si trova, coerentemente con quanto già sappiamo, che l'integrale a destra nella (8.1.10) vale $N + o(N)$.

§8.2. Il problema di Goldbach

Dopo questa lunga introduzione volta alla spiegazione del meccanismo del metodo del cerchio in un caso (relativamente) semplice, siamo pronti ad affrontare il ben piú complicato problema di Goldbach. Da qui in poi, le variabili p, p_1, p_2, $\dots$, indicano sempre numeri primi. Ci interessa il numero di rappresentazioni di n come somma di due primi

$$r_2(n) \stackrel{\text{def}}{=} \bigl|\{(p_1,p_2) \in \mathfrak{P}\times\mathfrak{P} : n = p_1 + p_2\}\bigr|,$$

dove p_1 e p_2 non sono necessariamente distinti, ma consideriamo distinte le rappresentazioni p_1+p_2 e p_2+p_1 se $p_1 \ne p_2$. Per il momento non facciamo l'ipotesi che n sia pari. Prendiamo un intero grande N e poniamo

$$V(\alpha) = V_N(\alpha) \stackrel{\text{def}}{=} \sum_{p\le N} e(p\alpha).$$

Per l'ortogonalità della funzione esponenziale complessa, per $n \le N$ si ha

$$\int_0^1 V(\alpha)^2 e(-n\alpha)\,\mathrm{d}\alpha = \sum_{p_1\le N}\sum_{p_2\le N} \int_0^1 e\bigl((p_1+p_2-n)\alpha\bigr)\,\mathrm{d}\alpha = r_2(n). \tag{8.2.1}$$

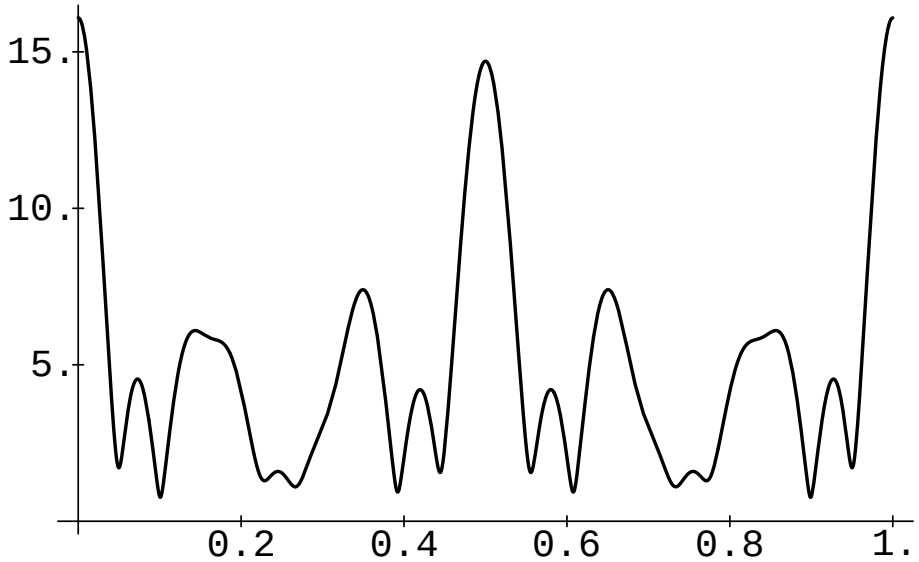


Figura 8.1. *Il grafico della funzione $|S_{20}(\alpha)|$ nel quale si notano molto bene i picchi in prossimità dei valori razionali di $\alpha = 0$, $\frac{1}{2}$, $\frac{1}{3}$, $\frac{2}{3}$, $\frac{1}{6}$, $\frac{5}{6}$, mentre in $\alpha = \frac{1}{4}$, $\frac{3}{4}$ non c'è picco poiché $\mu(4) = 0$.*

Di nuovo, questa è la formula che dà l'n-esimo coefficiente di Fourier della funzione $V(\alpha)^2$ (cfr la (8.1.6)), e permette di trasformare il problema di Goldbach in un problema che può essere affrontato con le tecniche dell'analisi reale e complessa.

Suddividiamo l'intervallo unitario $[0, 1]$ (o il cerchio unitario che si ottiene mediante l'applicazione $x \mapsto e^{2\pi i x}$) in sotto-intervalli centrati approssimativamente sui numeri razionali con denominatore $q \leq Q$, dove $Q = Q(N)$ è un parametro: questa si chiama dissezione di Farey di ordine Q (vedi la Definizione 6.4.6). Gli intervalli corrispondenti ai numeri razionali con denominatore $q \leq P$ (dove $P = P(N)$ è un altro parametro, che di solito viene scelto in modo tale che PQ sia dell'ordine di N) si chiamano *archi principali* e gli altri *archi secondari* (ma in italiano non è infrequente la dizione impropria di archi maggiori e minori). Hardy & Littlewood [A1-2] osservarono che la funzione V_N ha uno sviluppo asintotico su ciascuno degli archi principali, che corrisponde ad un picco della funzione vicino ai punti razionali con denominatore "piccolo" (vedi Figura 8.1). Sfruttando il contributo di questi picchi, e trascurando i termini d'errore, Hardy & Littlewood ritrovarono le formule asintotiche espresse nelle Congetture (9.1.2) e (9.1.3).

Per motivi tecnici che saranno piú chiari in seguito, invece di studiare la funzione $r_2(n)$ consideriamo piuttosto la versione "pesata"

$$R_2(n) \stackrel{\text{def}}{=} \sum_{p_1+p_2=n} \log p_1 \log p_2.$$

In altre parole, invece di contare ogni rappresentazione di n come $p_1 + p_2$ con peso 1, la facciamo pesare $\log p_1 \log p_2$. Naturalmente $r_2(n)$ è positiva se e solo se $R_2(n)$ lo è, e quindi se l'obiettivo è semplicemente quello di dimostrare la congettura di Goldbach nella sua forma originaria, possiamo tranquillamente formularla mediante $R_2(n)$. Con notazione

ormai tradizionale scriviamo

$$S(\alpha) = S_N(\alpha) \stackrel{\text{def}}{=} \sum_{p\le N} \log p\, e(p\alpha) \qquad \text{e} \qquad \theta(N;q,a) \stackrel{\text{def}}{=} \sum_{\substack{p\le N\\ p\equiv a \mod q}} \log p.$$

Per il Teorema dei Numeri Primi nelle progressioni aritmetiche 5.3.2 si ha

$$\theta(N;q,a) = \frac{N}{\varphi(q)} + E_1(N;q,a) \quad \text{dove} \quad E_1(N;q,a) = \mathcal{O}_A\Big(N\exp\{-C(A)\sqrt{\log N}\}\Big),$$

uniformemente per $q \le (\log N)^A$, dove $A>0$ è una costante arbitraria ma fissata e $C(A)$ è una costante positiva che dipende solo da A, purché $(a,q)=1$. In analogia con la (8.2.1), per $n \le N$ si ha

$$R_2(n) = \int_0^1 S(\alpha)^2 e(-n\alpha)\,\mathrm{d}\alpha. \tag{8.2.2}$$

Calcoliamo S su un razionale $\frac{a}{q}$, quando $1\le a\le q$ ed $(a,q)=1$:

$$\begin{aligned} S\left(\frac{a}{q}\right) &= \sum_{h=1}^{q} \sum_{\substack{p\le N\\ p\equiv h \mod q}} \log p\, e\big(p\tfrac{a}{q}\big) = \sum_{h=1}^{q} e\big(h\tfrac{a}{q}\big) \sum_{\substack{p\le N\\ p\equiv h \mod q}} \log p \\ &= \sum_{h=1}^{q} e\big(h\tfrac{a}{q}\big)\theta(N;q,h) = \sum_{h=1}^{q}{}^{*} e\big(h\tfrac{a}{q}\big)\theta(N;q,h) + \mathcal{O}(\log q \log N), \end{aligned} \tag{8.2.3}$$

dove * significa che alla somma abbiamo aggiunto la condizione supplementare $(h,q)=1$. Per il Teorema 3.2.11 e per la (8.2.3) abbiamo dunque

$$\begin{aligned} S\left(\frac{a}{q}\right) &= \frac{N}{\varphi(q)} \sum_{h=1}^{q}{}^{*} e\big(h\tfrac{a}{q}\big) + \sum_{h=1}^{q}{}^{*} e\big(h\tfrac{a}{q}\big) E_1(N;q,h) + \mathcal{O}(\log q\log N) \\ &= \frac{\mu(q)}{\varphi(q)} N + \sum_{h=1}^{q}{}^{*} e\big(h\tfrac{a}{q}\big) E_1(N;q,h) + \mathcal{O}(\log q\log N), \end{aligned} \tag{8.2.4}$$

dove μ è la funzione di Möbius. È questo il senso preciso in cui si deve intendere l'affermazione precedente che $|S(\alpha)|$ è grande quando α è un numero razionale: si noti che la grandezza di $\big|S\big(\frac{a}{q}\big)\big|$ decresce essenzialmente come q^{-1}. Poiché S è una funzione continua, ci si aspetta che $|S|$ sia grande in un intorno di $\frac{a}{q}$, e si sfrutta questo fatto per trovare una formula approssimata per $R_2(n)$. Per cominciare, estendiamo l'influenza del picco vicino ad $\frac{a}{q}$ per quanto ci è possibile: lo strumento piú semplice da usare a questo proposito è la formula di sommazione parziale A.1.1. È essenziale sottolineare il fatto che il numero e la larghezza degli archi principali dipendono in modo cruciale dalla possibilità di ottenere una buona stima per il termine d'errore che compare nel passaggio da $S\big(\frac{a}{q}\big)$ ad $S(\alpha)$, dove α appartiene all'arco che contiene $\frac{a}{q}$.

LEMMA 8.2.1. *Scelta arbitrariamente la costante $A > 0$, esiste una costante positiva $C = C(A)$ tale che per $1 \le a \le q \le P \stackrel{\text{def}}{=} (\log N)^A$, $(a,q) = 1$ e per $|\eta| \le PN^{-1}$ si ha*

$$S\left(\frac{a}{q} + \eta\right) = \frac{\mu(q)}{\varphi(q)} T(\eta) + E_2(N; q, a, \eta) \tag{8.2.5}$$

dove

$$E_2(N; q, a, \eta) = \mathcal{O}_A\Big(N \exp\{-C(A)\sqrt{\log N}\}\Big).$$

DIM.: Questo è il Lemma 3.1 di Vaughan [49]. Gli ingredienti fondamentali sono il Teorema dei Numeri Primi nelle progressioni aritmetiche 5.3.2, la formula di sommazione parziale, la (8.2.4) ed il Teorema 3.2.11. □

La dimostrazione di questo Lemma mostra piuttosto chiaramente che non possiamo prendere gli archi principali troppo numerosi o troppo ampi oppure q troppo grande se vogliamo ancora avere un termine d'errore sufficientemente piccolo. Indichiamo dunque con $\mathfrak{M}(q,a) \stackrel{\text{def}}{=} \left[\frac{a}{q} - \frac{P}{N}, \frac{a}{q} + \frac{P}{N}\right]$ l'arco principale relativo al numero razionale $\frac{a}{q}$, e scriviamo

$$\mathfrak{M} \stackrel{\text{def}}{=} \bigcup_{q \le P} \bigcup_{a=1}^{q}{}^{*} \mathfrak{M}(q,a) \qquad \text{e} \qquad \mathfrak{m} \stackrel{\text{def}}{=} [\xi(1,1), 1 + \xi(1,1)] \setminus \mathfrak{M},$$

dove di nuovo * indica che abbiamo aggiunto la condizione supplementare $(a,q) = 1$. $\mathfrak{M}$ è dunque l'insieme degli archi principali, ed il suo complementare $\mathfrak{m}$ è l'insieme degli archi secondari. Abbiamo traslato l'intervallo di integrazione da $[0,1]$ a $\big[\xi(1,1), 1 + \xi(1,1)\big]$ per evitare di avere due "semi-archi" in 0 ed in 1, ma questo è legittimo perché tutte le funzioni di cui ci stiamo occupando hanno periodo 1. Per $n \le N$ dalla (8.2.2) abbiamo

$$\begin{aligned} R_2(n) &= \int_0^1 S(\alpha)^2 e(-n\alpha)\,\mathrm{d}\alpha = \left(\int_{\mathfrak{M}} + \int_{\mathfrak{m}}\right) S(\alpha)^2 e(-n\alpha)\,\mathrm{d}\alpha \\ &= \sum_{q \le P} \sum_{a=1}^{q}{}^{*} \int_{-\xi(q,a)}^{\xi'(q,a)} S\left(\frac{a}{q} + \eta\right)^2 e\left(-n\big(\tfrac{a}{q} + \eta\big)\right) \mathrm{d}\eta + \int_{\mathfrak{m}} S(\alpha)^2 e(-n\alpha)\,\mathrm{d}\alpha \\ &= R_{\mathfrak{M}}(n) + R_{\mathfrak{m}}(n), \end{aligned}$$

diciamo. D'ora in avanti scriveremo $\approx$ per indicare un'uguaglianza asintotica attesa (ma non ancora dimostrata). Se per il momento trascuriamo il contributo degli archi secondari $R_{\mathfrak{m}}(n)$ e tutti i termini d'errore trovati fin qui, per la (8.2.5) abbiamo

$$\begin{aligned} R_{\mathfrak{M}}(n) &\approx \sum_{q \le P} \sum_{a=1}^{q}{}^{*} \int_{-\xi(q,a)}^{\xi'(q,a)} \frac{\mu(q)^2}{\varphi(q)^2} T(\eta)^2 e\big(-n\big(\tfrac{a}{q} + \eta\big)\big)\,\mathrm{d}\eta \\ &= \sum_{q \le P} \frac{\mu(q)^2}{\varphi(q)^2} \sum_{a=1}^{q}{}^{*} e\big(-n\tfrac{a}{q}\big) \int_{-\xi(q,a)}^{\xi'(q,a)} T(\eta)^2 e(-n\eta)\,\mathrm{d}\eta. \end{aligned} \tag{8.2.6}$$

Se estendiamo l'integrale a tutto l'intervallo $[0,1]$ troviamo

$$\int_0^1 T(\eta)^2 e(-n\eta)\,\mathrm{d}\eta = \sum_{\substack{m_1+m_2=n\\ m_1\geq 0,\, m_2\geq 0}} 1 = n+1 \sim n. \tag{8.2.7}$$

Dunque, si può pensare che $R_2(n)$ sia ben approssimato da

$$R_{\mathfrak{M}}(n) \approx n \sum_{q\leq P} \frac{\mu(q)^2}{\varphi(q)^2} \sideset{}{^*}\sum_{a=1}^{q} e\big(-n\tfrac{a}{q}\big) = n \sum_{q\leq P} \frac{\mu(q)^2}{\varphi(q)^2} c_q(n). \tag{8.2.8}$$

Per il Teorema 3.2.11 la (8.2.8) diventa

$$R_{\mathfrak{M}}(n) \approx n \sum_{q\leq P} \frac{\mu(q)^2}{\varphi(q)^2} \mu\left(\frac{q}{(q,n)}\right) \frac{\varphi(q)}{\varphi\left(\frac{q}{(q,n)}\right)} = n \sum_{q\leq P} \frac{\mu(q)^2}{\varphi(q)} \frac{\mu\left(\frac{q}{(q,n)}\right)}{\varphi\left(\frac{q}{(q,n)}\right)}.$$

Ora estendiamo la somma a tutti gli interi $q \geq 1$ (commettendo un errore stimabile in modo preciso): osserviamo che l'addendo della somma è una funzione moltiplicativa di q e quindi per il Lemma 3.1.5 abbiamo

$$R_{\mathfrak{M}}(n) \approx n \sum_{q\leq P} \frac{\mu(q)^2}{\varphi(q)} \frac{\mu\left(\frac{q}{(q,n)}\right)}{\varphi\left(\frac{q}{(q,n)}\right)} \approx n \sum_{q\geq 1} \frac{\mu(q)^2}{\varphi(q)} \frac{\mu\left(\frac{q}{(q,n)}\right)}{\varphi\left(\frac{q}{(q,n)}\right)} = n \prod_p \big(1+f_n(p)\big) \tag{8.2.9}$$

dove il prodotto è esteso a tutti i numeri primi ed

$$f_n(p) \stackrel{\text{def}}{=} \frac{\mu(p)^2}{\varphi(p)} \frac{\mu\left(\frac{p}{(p,n)}\right)}{\varphi\left(\frac{p}{(p,n)}\right)} = \begin{cases} \dfrac{1}{p-1} & \text{se } p \mid n, \\ -\dfrac{1}{(p-1)^2} & \text{se } p \nmid n. \end{cases}$$

Se n è dispari il fattore $1+f_n(2)$ vale 0, e quindi la (8.2.9) predice che non ci dobbiamo aspettare rappresentazioni di n come somma di due numeri primi. In effetti, se n è dispari allora $R_2(n)=0$ se $n-2$ non è primo, ed $R_2(n) = 2\log(n-2)$ se $n-2$ è primo: il risultato della formula (8.2.9) deve essere inteso nel senso che $R_2(n) = o(n)$. Viceversa, se n è pari possiamo trasformare la (8.2.9) con qualche calcolo:

$$\begin{aligned} R_2(n) &\approx n \prod_{p\mid n} \left(1+\frac{1}{p-1}\right) \prod_{p\nmid n} \left(1-\frac{1}{(p-1)^2}\right) \\ &= 2n \prod_{\substack{p\mid n\\ p>2}} \left(\frac{p}{p-1}\cdot\frac{(p-1)^2}{p(p-2)}\right) \prod_{p>2} \left(1-\frac{1}{(p-1)^2}\right) = 2C_0 n \prod_{\substack{p\mid n\\ p>2}} \frac{p-1}{p-2} = n\mathfrak{S}(n), \end{aligned}$$

dove $2C_0$ è la costante dei primi gemelli e $\mathfrak{S}(n)$ è la cosiddetta "serie singolare" definita nella (6.3.3). Questa è dunque la formula asintotica per $R_2(n)$ data dall'euristica basata sul Teorema dei Numeri Primi nelle progressioni aritmetiche. È piú grande di un fattore $(\log n)^2$ della formula per $r_2(n)$ che si otterrebbe con il procedimento usato nel Teorema 6.5.6 (cfr la (9.1.3)) a causa dei "pesi" $\log p_1 \log p_2$ che abbiamo dato alle rappresentazioni. Nel prossimo paragrafo indicheremo brevemente quali dei punti lasciati in sospeso qui sopra rappresentano davvero un problema.

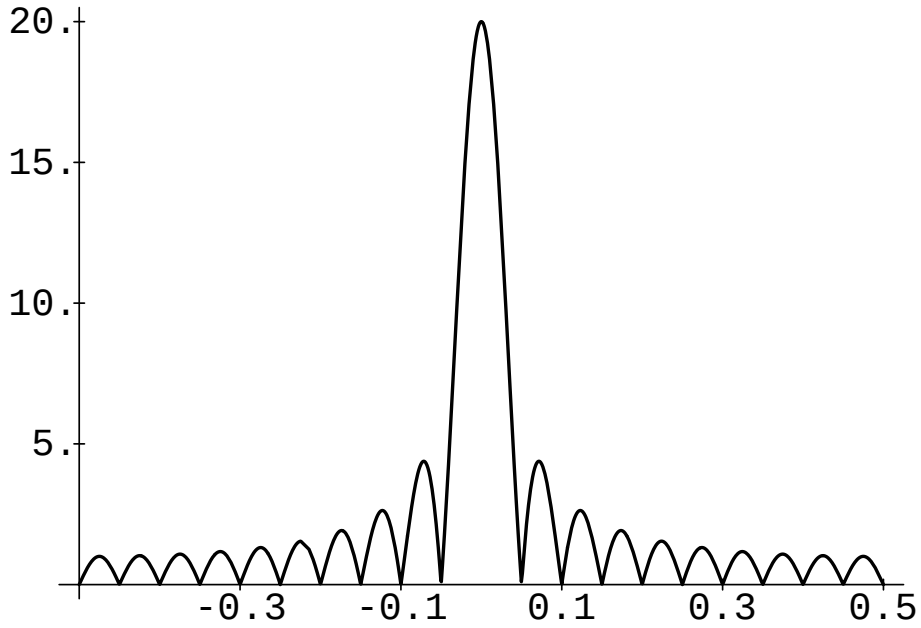


Figura 8.2. *Il grafico della funzione $|T_{20}(\alpha)|$ nel quale si nota molto bene che questa funzione ha un grosso picco in prossimità dei valori interi di α, ed è altrimenti molto piccola.*

§8.3. Dove sono le difficoltà?

Per brevità parleremo soltanto delle due piú importanti questioni che rimangono da risolvere. Infatti, l'approssimazione che facciamo nel passare dalla (8.2.6) alla (8.2.7) può essere giustificata ricordando che per la (8.1.8) si ha $|T(\alpha)| \le \min\bigl(N+1, \|\alpha\|^{-1}\bigr)$: la Figura 8.2 mostra che $T(\alpha)$ decade molto rapidamente allontanandosi dai valori interi di α. L'errore commesso nella (8.2.9) può essere messo in una forma quantitativa sfruttando il fatto che la serie è assolutamente convergente e che la funzione f_n è moltiplicativa. Rivolgiamo dunque la nostra attenzione all'approssimazione di $\theta(N;q,a)$ ed al contributo degli archi secondari.

L'approssimazione di θ. L'approssimazione di θ fornita dal Teorema dei Numeri Primi nelle progressioni aritmetiche 5.3.2 è piuttosto debole per due motivi: come abbiamo già osservato, questa è valida in un intervallo di valori di q ristretto e siamo quindi costretti a prendere il parametro P (che serve per distinguere gli archi principali da quelli secondari) piuttosto piccolo come funzione di N.

In secondo luogo la maggiorazione oggi nota per l'errore è troppo grande: si congettura che questo errore sia in realtà molto piú piccolo. È noto che la differenza $\theta(N;q,a) - \frac{N}{\varphi(q)}$ dipende essenzialmente da una somma i cui addendi sono del tipo $\frac{N^\varrho}{\varphi(q)\varrho}$, dove ϱ indica il generico zero complesso di opportune funzioni L di Dirichlet. Nel caso piú semplice, quando $q = a = 1$, la formula esplicita 7.3.3 implica che per $T \le N$

$$\theta(N) = N - \sum_{\substack{\varrho\in\mathbb{C} \text{ t. c. } \zeta(\varrho)=0 \\ \varrho=\beta+\mathrm{i}\gamma \\ |\gamma|\le T}} \frac{N^\varrho}{\varrho} + \mathcal{O}\left(\frac{N}{T}(\log N)^2 + \sqrt{N}\log N\right) \tag{8.3.1}$$

dove $\varrho = \beta + \mathrm{i}\gamma$ è il generico zero della funzione zeta di Riemann con $\beta \in (0,1)$. Questa formula mostra che al posto della funzione $T(\eta)$ definita dalla (8.1.7), conviene prendere come approssimazione di $S\big(\frac{a}{q}+\eta\big)$ la funzione

$$K(\eta) \stackrel{\text{def}}{=} \sum_{n\le N} \Big(1 - \sum_{|\gamma|\le T} n^{\varrho-1}\Big) e(n\eta)$$

dove il coefficiente di $e(n\eta)$ è la derivata rispetto ad N dei primi due termini nella (8.3.1), calcolata in n (poiché se f è regolare $\sum f(n) \sim \int f(t)\,\mathrm{d}t$). L'approssimazione di S cosí ottenuta è valida solo vicino a 0, ma introducendo le funzioni L di Dirichlet si possono trovare approssimazioni simili, valide su ciascun arco principale.

È anche noto che il caso ottimale per la distribuzione dei numeri primi è quello in cui *tutte* le parti reali β di tutti gli zeri $\varrho = \beta + \mathrm{i}\gamma$ della funzione ζ con $\gamma \neq 0$ sono uguali ad $\frac12$ (Congettura di Riemann 4.1.4): se cosí è, allora si ha la buona approssimazione $\theta(N) = N + \mathcal{O}\big(N^{1/2}(\log N)^2\big)$ che è equivalente alla 4.1.4. Analogamente, se si riuscisse a dimostrare che *tutti* gli zeri di tutte le funzioni L di Dirichlet hanno parte reale uguale ad $\frac12$ (Congettura di Riemann Generalizzata), per $q \le x$ si avrebbe anche la stima

$$\theta(N;q,a) = \frac{N}{\varphi(q)} + \mathcal{O}\Big(N^{1/2}(\log N)^2\Big). \tag{8.3.2}$$

Si osservi che le stime 4.1.4 e (8.3.2) sono ottimali, e cioè l'esponente di N nel termine d'errore non può essere ulteriormente abbassato. Questo significa che non si riuscirebbe a dimostrare la congettura di Goldbach neppure se si dimostrasse la (8.3.2). La situazione nel caso generale $q > 1$ è piú complicata di quella nel caso $q = 1$: infatti non è ancora possibile escludere che qualcuna delle funzioni L di Dirichlet abbia uno zero reale $\beta \in (0,1)$, con β molto prossimo ad 1, e questo è essenzialmente il motivo per cui siamo costretti ad imporre una severa limitazione per q come detto a proposito del Teorema 5.3.2. Il contributo di questo eventuale zero sarebbe $\pm\frac{N^\beta}{\varphi(q)\beta}$, e cioè molto prossimo al "termine principale" $\frac{N}{\varphi(q)}$, cosí da vanificare la possibilità di avere un errore sufficientemente piccolo nella formula asintotica per $\theta(N;q,a)$ per questo particolare valore di q, e di conseguenza per $R_2(n)$.

Il contributo degli archi secondari. Il problema principale presentato dagli archi secondari è costituito dal fatto che non si riesce a dare una buona stima individuale del loro contributo: in altre parole, è relativamente semplice dimostrare che in media su tutti gli interi $n \in [1,N]$ gli archi secondari non danno un grande contributo ad $R_2(n)$, ma non è possibile trovare una maggiorazione altrettanto buona per ogni singolo valore di n. Per la formula che dà il coefficiente di Fourier n-esimo, la disuguaglianza di Bessel ed il Teorema dei Numeri Primi 4.1.3 si ha

$$\begin{aligned}\sum_{n\le N}\Big|\int_{\mathfrak{m}} S(\alpha)^2 e(-n\alpha)\,\mathrm{d}\alpha\Big|^2 &\le \int_{\mathfrak{m}} |S(\alpha)|^4\,\mathrm{d}\alpha \le \sup_{\alpha\in\mathfrak{m}}|S(\alpha)|^2 \int_0^1 |S(\alpha)|^2\,\mathrm{d}\alpha \\ &= \mathcal{O}\bigg(N\log N \sup_{\alpha\in\mathfrak{m}}|S(\alpha)|^2\bigg).\end{aligned}$$

Dalla (8.2.4) possiamo aspettarci (e questo può essere dimostrato rigorosamente in una forma piú debole) che l'estremo superiore qui sopra valga essenzialmente N^2P^{-2} dato che se $\alpha \in \mathfrak{m}$ allora è "vicino" ad un razionale con denominatore $> P$.

LEMMA 8.3.1. *Per $1 \le a \le q \le N$, $(a,q) = 1$ ed $|\eta| \le q^{-2}$ si ha*

$$S\left(\frac{a}{q} + \eta\right) \ll (\log N)^4 \big(Nq^{-1/2} + N^{4/5} + N^{1/2}q^{1/2}\big).$$

Per mezzo di questo Lemma, in effetti si riesce a dimostrare che

$$\sum_{n\le N} |R_{\mathfrak{m}}(n)|^2 = \sum_{n\le N} \Big| \int_{\mathfrak{m}} S(\alpha)^2 e(-n\alpha)\,\mathrm{d}\alpha \Big|^2 = \mathcal{O}\big(N^3(\log N)^9 P^{-1}\big) \tag{8.3.3}$$

e questo dice che, per la "maggioranza" degli interi $n \in [1,N]$ si ha $|R_{\mathfrak{m}}(n)| = \mathcal{O}\big(NP^{-1/3}\big)$, che ha ordine di grandezza minore del contributo degli archi principali dato dalla (8.2.9).

§8.4. Risultati "per quasi tutti" gli interi pari

In questo paragrafo indichiamo brevemente come sia possibile dimostrare che gli interi pari n per cui $R_2(n) = 0$ sono piuttosto rari: piú precisamente, posto $\mathcal{E}(N) \stackrel{\text{def}}{=} \big\{n \le N : n \text{ è pari e } R_2(2n) = 0\big\}$, dimostreremo che dato $B > 0$ si ha $|\mathcal{E}(N)| = \mathcal{O}_B\big(N(\log N)^{-B}\big)$. Questa è una conseguenza immediata del

TEOREMA 8.4.1. *Dato $B > 0$ si ha*

$$\sum_{n\le N} \big|R_2(n) - n\mathfrak{S}(n)\big|^2 \ll_B N^3\big(\log N\big)^{-B}.$$

SCHEMA DELLA DIMOSTRAZIONE: Non è troppo difficile dimostrare che per $n \le N$ si ha

$$R_{\mathfrak{M}}(n) = n\mathfrak{S}(n,P) + \mathcal{O}_A\big(n(\log n)P^{-1}\big) \tag{8.4.1}$$

usando il Lemma 8.2.1 e le (8.1.8), (8.2.6)–(8.2.7), dove

$$\mathfrak{S}(n,P) \stackrel{\text{def}}{=} \sum_{q\le P} \frac{\mu(q)^2}{\varphi(q)^2} c_q(n). \tag{8.4.2}$$

Per il Teorema 3.3.1, sfruttando anche il Teorema 3.2.11 ed alcune stime elementari che riguardano la funzione φ di Eulero, si trova che

$$\sum_{n\le N} \big|\mathfrak{S}(n,P) - \mathfrak{S}(n)\big|^2 \ll N(\log N)^2 P^{-1}. \tag{8.4.3}$$

Ricordiamo la disuguaglianza elementare $|a+b+c|^2 \le 3\big(|a|^2 + |b|^2 + |c|^2\big)$. Abbiamo

$$\begin{aligned}
\sum_{n\le N} \big|R_2(n) - n\mathfrak{S}(n)\big|^2 &\ll \sum_{n\le N} \big|R_{\mathfrak{M}}(n) - n\mathfrak{S}(n,P)\big|^2 + \sum_{n\le N} \big|n\mathfrak{S}(n,P) - n\mathfrak{S}(n)\big|^2 \\
&\qquad + \sum_{n\le N} \big|R_{\mathfrak{m}}(n)\big|^2 \\
&\ll N^3(\log N)^{2-2A} + N^3(\log N)^{2-A} + N^3(\log N)^{9-A} \\
&\ll N^3(\log N)^{9-A}
\end{aligned}$$

per le (8.3.3), (8.4.1)–(8.4.3). Scegliendo ora $A \ge B+9$ si ottiene il Teorema 8.4.1. □

Infine, sia $\mathcal{E}'(N) \stackrel{\text{def}}{=} \{n \in [\frac12 N, N] : n \text{ è pari e } R_2(2n) = 0\} = \mathcal{E}(N) \cap [\frac12 N, N]$. Dato che per la (6.3.3) $\mathfrak{S}(n) \ge 2C_0$ quando n è pari, si ha

$$\sum_{n\le N} \bigl|R_2(n) - n\mathfrak{S}(n)\bigr|^2 \ge \sum_{\substack{n\le N,\, 2|n\\ R_2(n)=0}} |2C_0 n|^2 \ge \sum_{\substack{N/2\le n\le N,\, 2|n\\ R_2(n)=0}} |2C_0 n|^2 \ge \frac{C_0^2}{2}\bigl|\mathcal{E}'(N)\bigr| N^2,$$

e quindi $|\mathcal{E}'(N)| = \mathcal{O}_B\bigl(N(\log N)^{-B}\bigr)$ per ogni $B > 0$. Il risultato relativo ad $\mathcal{E}(N)$ segue decomponendo l'intervallo $[1, N]$ in $\mathcal{O}(\log N)$ intervalli del tipo $[\frac12 M, M]$.

§8.5. Varianti: il teorema dei tre primi ed i primi gemelli

Il metodo di Hardy & Littlewood è estremamente flessibile e si può applicare ad una grande quantità di problemi diversi. Per esempio, con notazione analoga a quella di sopra abbiamo

$$R_3(n) \stackrel{\text{def}}{=} \sum_{p_1+p_2+p_3=n} \log p_1 \log p_2 \log p_3 = \int_0^1 S(\alpha)^3 e(-n\alpha)\,\mathrm{d}\alpha$$

se $n \le N$. Un'argomentazione simile a quella qui sopra mostra che $R_3(n)$ può essere bene approssimata dal solo contributo degli archi principali e questo dà la relazione

$$R_3(n) = \frac12 n^2 \mathfrak{S}_3(n) + \mathcal{O}_A\bigl(n^2(\log n)^{-A}\bigr), \tag{8.5.1}$$

qualunque sia la costante positiva A. Qui abbiamo

$$\mathfrak{S}_3(n) \stackrel{\text{def}}{=} \prod_{p\nmid n}\left(1 + \frac{1}{(p-1)^3}\right)\cdot \prod_{p|n}\left(1 - \frac{1}{(p-1)^2}\right).$$

Il fatto di avere 3 addendi invece di 2 fa mutare completamente la natura del problema: ci limitiamo ad osservare che in questo caso è piuttosto semplice trovare una buona maggiorazione individuale (cioè per ogni n) per il contributo degli archi secondari. Infatti, dal Lemma 8.3.1, per $n \le N$ e $q > P$ si ha

$$\Bigl|\int_{\mathfrak{m}} S(\alpha)^3 e(-n\alpha)\,\mathrm{d}\alpha\Bigr| \le \sup_{\alpha\in\mathfrak{m}} |S(\alpha)| \int_0^1 |S(\alpha)|^2\,\mathrm{d}\alpha = \mathcal{O}\Bigl(n^2(\log n)^4 P^{-1/2}\Bigr). \tag{8.5.2}$$

Deshouillers, Effinger, te Riele & Zinoviev hanno dimostrato che se è vera la Congettura di Riemann Generalizzata allora *tutti* gli interi dispari $n \ge 7$ si possono scrivere come somma di tre numeri primi. Una semplice osservazione mostra anche come il problema dei primi gemelli sia naturalmente legato al problema di Goldbach:

$$\theta_N(n) \stackrel{\text{def}}{=} \sum_{\substack{p_2\le N\\ p_2-p_1=n}} \log p_1 \log p_2 = \int_0^1 |S(\alpha)|^2 e(-n\alpha)\,\mathrm{d}\alpha,$$

come si vede con un breve calcolo. Questo mostra che i due problemi sono strettamente legati e della stessa difficoltà.

Capitolo 9. Problemi Aperti

In questo Capitolo finale vogliamo presentare informalmente e rapidamente alcuni dei piú importanti problemi aperti, suddivisi per capitolo. La scelta naturalmente è arbitraria e discutibile: per una panoramica ben piú vasta, si vedano i libri di Guy [18], di Ribenboim [42] e di Shanks [45]. In questo Capitolo p_n indica l'n-esimo numero primo, e $\log_k x$ l'iterata k-esima della funzione logaritmo: $\log_2 x \stackrel{\text{def}}{=} \log\log x$ e $\log_{n+1} x \stackrel{\text{def}}{=} \log\log_n x$.

Capitolo 1. Detto $C(x)$ il numero dei numeri di Carmichael $\le x$, Alford, Granville & Pomerance hanno dimostrato che si ha $C(x) > x^{2/7}$ per x sufficientemente grande, e Pomerance, Selfridge & Wagstaff che $C(x) \le x\exp\{-(1-\varepsilon)\log x \log_3 x(\log_2 x)^{-1}\}$ per $x > x_0(\varepsilon)$. Si congettura che quest'ultima relazione debba valere con $\sim$ al posto di $\le$. Non è noto se per ogni $k \ge 3$ esistano infiniti numeri di Carmichael n tali che $\omega(n) = k$, ma abbiamo dimostrato nel Capitolo 2 che tutti i numeri di Carmichael sono dispari, liberi da quadrati ed hanno almeno tre fattori primi.

Artin ha congetturato che se $n \in \mathbb{Z}$ è $\neq -1$ e non è un quadrato perfetto, allora n genera $\mathbb{Z}_p^*$ per infiniti numeri primi p. Heath-Brown ha dimostrato che le eccezioni a questa congettura, se esistono, sono molto rare.

Fermat ha congetturato che F_n sia primo per ogni $n \in \mathbb{N}$, ma Eulero ha dimostrato che
𝔈 1.7.5 $641 \mid F_5$. Oggi è noto che F_n non è primo per $n = 5, \dots, 20$. Mersenne ha congetturato che M_p sia primo per infiniti valori di p: oggi se ne conoscono solo una trentina. A questo proposito è bene osservare che esistono metodi di fattorizzazione estremamente efficienti per numeri interi n per i quali sia disponibile una fattorizzazione completa di $n+1$ o di $n-1$, ed i numeri di Mersenne e di Fermat, rispettivamente, appartengono a questi insiemi. Questi metodi si basano sul Teorema di Lucas 2.3.1 o sue varianti.

Capitolo 3. Posto

$$E_1(x) \stackrel{\text{def}}{=} D(x) - x\log x - (2\gamma - 1)x,$$
$$E_2(x) \stackrel{\text{def}}{=} R_2(x) - \pi x,$$

nei Teoremi 3.2.2 e 3.2.4 abbiamo visto che $E_i(x) = \mathcal{O}\big(x^{1/2}\big)$ per $i = 1, 2$. Questi risultati sono stati migliorati ed ora è noto che $E_1(x) = \mathcal{O}\big(x^{139/429+\varepsilon}\big)$ e che $E_2(x) = \mathcal{O}\big(x^{35/108}\big)$. Hardy ha dimostrato che $E_1(x) = \Omega_\pm\left(x^{1/4}\right)$ e lo stesso vale per $E_2(x)$. Per i risultati piú forti (che sono complicati da enunciare) si rimanda ai libri di Ivić [27] e Titchmarsh [47].

Per $s,\ k \in \mathbb{N}^*$ si definisca $r_{s,k}(n) \stackrel{\text{def}}{=} |\{(x_1, \dots, x_s) \in \mathbb{N}^s : x_1^k + \cdots + x_s^k = n\}|$. Waring nelle *Meditationes Algebraicæ* del 1770 si chiese se dato $k \ge 2$ esiste $s = s(k)$ tale che $r_{s,k}(n) > 0$ per ogni $n \in \mathbb{N}$. Il minimo s possibile si indica tradizionalmente con $g(k)$.

Hilbert ha dimostrato che $g(k) < \infty$ per ogni $k \geq 2$, ed oggi si conosce il valore esatto di $g(k)$ per ogni $k \geq 2$, e $g(k) \leq 2^k + \big[\big(\frac{3}{2}\big)^k\big] + \big[\big(\frac{4}{3}\big)^k\big] - 2$. Il punto è che il valore di $g(k)$ è enormemente gonfiato dagli interi relativamente piccoli che richiedono un s piuttosto grande. Si definisca quindi $G(k)$ come il minimo intero s tale che esiste $C_0 = C_0(k)$ tale che $r_{s,k}(n) > 0$ per ogni $n \geq C_0$. In altre parole, $r_{G(k),k}(n) > 0$ per ogni n sufficientemente grande, mentre $r_{G(k)-1,k}(n) = 0$ ha infinite soluzioni. Il valore di G è noto solo per $k = 2$ e per $k = 4$ ($G(2) = 4$ e $G(4) = 16$) e Wooley ha recentemente dimostrato che $G(k) \leq k\big(\log k + \log\log k + \mathcal{O}(1)\big)$ per $k \to \infty$. È relativamente facile dimostrare che $G(k) \geq k + 1$.

Capitolo 4. La domanda piú importante naturalmente riguarda il vero ordine di grandezza di $\pi(x) - \mathrm{li}(x)$. Littlewood ha dimostrato che $\pi(x) - \mathrm{li}(x) = \Omega\big(x^{1/2}\log_3 x(\log x)^{-1}\big)$, e si congettura che debba essere $\pi(x) = \mathrm{li}(x) + \mathcal{O}\big(x^{1/2}\log x\big)$. Quest'ultima affermazione è nota come Congettura di Riemann, ed è equivalente a $\psi(x) = x + \mathcal{O}\big(x^{1/2}(\log x)^2\big)$.

Il Teorema dei Numeri Primi 4.1.3 suggerisce che

$$\pi(x) - \pi(x-y) \sim \int_{x-y}^{x} \frac{\mathrm{d}t}{\log t}, \tag{9.1.1}$$

almeno quando y non è troppo piccolo rispetto ad x. Heath-Brown ha dimostrato che questo è vero uniformemente per $x^{7/12-\varepsilon(x)} \leq y \leq x$, dove $\varepsilon(x)$ è una qualsiasi funzione positiva ed infinitesima. È altresí noto che questa relazione cessa di valere se $y \leq (\log x)^A$, per ogni $A > 0$ fissato, ed anche per funzioni di x che crescono piú rapidamente: il miglior risultato noto (Hildebrand & Maier), è un po' complicato da enunciare. In ogni caso per $x > 0$ ed $y > 1$ vale la maggiorazione universale (Montgomery & Vaughan)

$$\pi(x+y) - \pi(x) \leq \frac{2y}{\log y}.$$

Si confronti con la versione della disuguaglianza di Brun–Titchmarsh nel Teorema 6.5.2.

In vista del Teorema dei Numeri Primi si deve necessariamente avere

$$\limsup_{n\to\infty}(p_{n+1} - p_n) = \infty.$$

In un certo senso, il valor medio di $p_{n+1} - p_n$ è $\log p_n$. Cramér ha congetturato che

$$\limsup_{n\to\infty} \frac{p_{n+1} - p_n}{(\log p_n)^2} = 1,$$

ma al momento attuale il miglior risultato è quello di Maier & Pomerance:

$$\limsup_{n\to\infty} \frac{p_{n+1} - p_n}{\log p_n} \frac{(\log_3 p_n)^2}{\log_2 p_n \log_4 p_n} \geq ce^{\gamma},$$

dove $c = 1.31256\ldots$. Inoltre Baker, Harman & Pintz hanno recentemente dimostrato che

$$p_{n+1} - p_n = \mathcal{O}\big(p_n^{0.525}\big).$$

Nell'altra direzione ci si chiede se esistano infiniti "primi gemelli" (cfr Capitolo 6), ma non è noto neppure se valga la relazione

$$\liminf_{n\to\infty} \frac{p_{n+1} - p_n}{\log p_n} = 0.$$

Maier ha dimostrato che questo liminf è $\leq 0.248\ldots$

Capitolo 5. Le domande piú interessanti sono le analoghe di quelle esposte sopra a proposito dei numeri primi. Per esempio, si congettura che per q fissato ed $(a,q)=1$ si abbia

$$\psi(x;q,a) \stackrel{\text{def}}{=} \sum_{\substack{n\le x\\ n\equiv a \mod q}} \Lambda(n) = \frac{x}{\varphi(q)} + \mathcal{O}\Big(x^{1/2}\log^2 x\Big),$$

(Congettura di Riemann Generalizzata). Inoltre, ci si chiede quale sia la vera uniformità che si può avere nel Teorema dei Numeri Primi nelle Progressioni 5.3.2. La situazione è complicata dal fatto che non si è riusciti ancora ad escludere la possibilità che una funzione L associata ad un carattere reale abbia uno zero reale sul segmento $[0,1]$.

Linnik ha dimostrato che, detto $P(q,a)$ il piú piccolo numero primo $\equiv a \mod q$, esiste una costante assoluta $L \ge 1$ tale che $P(q,a) \ll q^L$ per ogni $(a,q)=1$. Heath-Brown e Pomerance hanno dimostrato rispettivamente che $L \le 5.5$ e che

$$\limsup_{q\to\infty}\Big(\max_{(a,q)=1} P(q,a)\Big)\Big(q\log q\log_2 q\frac{\log_4 q}{(\log_3 q)^2}\Big)^{-1} > 0$$

e se vale la Congettura Generalizzata di Riemann allora

$$\max_{(a,q)=1} P(q,a) = \mathcal{O}_\varepsilon\big(q^{2+\varepsilon}\big).$$

Capitolo 6. Il Teorema di Dirichlet implica che tutti i polinomi del tipo $f(n)=qn+a$ con $(q,a)=1$ assumono valori primi per infiniti valori della variabile n. In altre parole, tutti i polinomi di primo grado irriducibili su $\mathbb{Q}$ assumono infiniti valori primi, e questo può essere anche espresso in forma quantitativa (cfr il Teorema dei Numeri Primi nelle Progressioni 5.3.2). Ci si chiede dunque se sia vero che tutti i polinomi $f\in\mathbb{Z}[x]$ irriducibili su $\mathbb{Q}$ che non siano costanti debbano assumere valori primi per infiniti $n\in\mathbb{N}$, purché $\varrho(p)<p$ per ogni primo p. Per esempio, ci si chiede se il polinomio $f(n)=n^2+1$ assuma infinite volte valori primi, o, in altre parole, se esistono infiniti numeri primi della forma n^2+1. La forma ottimale del Teorema 6.2.10 asserisce che

$$|\{n\le x\colon \big(f(n),P(z)\big)=1\}| = x\prod_{p\le z}\left(1-\frac{\varrho(p)}{p}\right)\times$$
$$\times\left(1+\mathcal{O}\big(\exp\big\{-u\big(\log u-\log_2 3u-\log\deg(f)-2\big)\big\}\big)+\mathcal{O}_{\deg(f)}\Big(\exp\{-(\log x)^{1/2}\}\Big)\right)$$

purché $\varrho(p)<p$ per ogni primo p (questo significa che f non ha divisori primi fissi; si noti che per il Lemma 6.2.3 $\varrho(p)\le\deg(f)$ e quindi questa è una condizione che può essere verificata in un numero finito di passi) ed $u\stackrel{\text{def}}{=}\log x(\log z)^{-1}\ge 1$. Recentemente Friedlander & Iwaniec hanno dimostrato che a^2+b^4 assume valore primo il numero "atteso" di volte.

È noto che

$$\pi_h(x)\stackrel{\text{def}}{=}|\{n\le x\colon n \text{ ed } n+h \text{ sono primi}\}| \le 4\mathfrak{S}(h)\frac{x}{(\log x)^2}\big(1+o(1)\big)$$

uniformemente in $h \in \mathbb{N}^*$. Questo segue da una generalizzazione del risultato citato sopra. Hardy & Littlewood hanno congetturato che

$$\pi_h(x) \sim \mathfrak{S}(h)\frac{x}{(\log x)^2}. \tag{9.1.2}$$

Non sono però noti valori di $h \in \mathbb{N}^*$ per cui si abbia $\pi_h(x) \to \infty$ quando $x \to \infty$.

In una lettera ad Eulero del 1742, Christian Goldbach ha congetturato che per ogni intero pari $n \geq 6$ dovessero esistere due numeri primi dispari p_1 e p_2 tali che $n = p_1 + p_2$. Detto $r(n)$ il numero delle soluzioni (contando $p_1 + p_2$ e $p_2 + p_1$ come soluzioni distinte se $p_1 \neq p_2$), Hardy & Littlewood hanno congetturato che

$$r(n) \sim \mathfrak{S}(n)\frac{n}{(\log n)^2}. \tag{9.1.3}$$

Vinogradov ha dimostrato nel 1937 che per n dispari sufficientemente grande l'equazione $n = p_1 + p_2 + p_3$ ha soluzione. Ramaré ha recentemente dimostrato che l'equazione $n = p_1 + p_2 + \cdots + p_r$ ha soluzione per ogni $n > 1$ con $r \leq 7$. Montgomery & Vaughan hanno dimostrato che esiste $\delta > 0$ tale che

$$|\{n \leq x : n \text{ è pari ed } r(n) = 0\}| \ll x^{1-\delta}.$$

Capitolo 7. Congettura di Riemann a parte, un miglioramento della regione libera da zeri porterebbe immediatamente ad un corrispondente miglioramento delle stime per $\pi(x) - \mathrm{li}(x)$. Al momento attuale non è noto se, con la notazione del Capitolo 7, si abbia $\Theta < 1$. Questo risultato sarebbe probabilmente il piú importante degli ultimi 130 anni.

Una congettura piú debole di quella di Riemann, ma che avrebbe importanti conseguenze per le applicazioni, è l'Ipotesi di Densità: posto

$$N(\sigma, T) \stackrel{\text{def}}{=} \big|\{\varrho = \beta + \mathrm{i}\gamma : \zeta(\varrho) = 0,\, \beta \geq \sigma,\, |\gamma| \leq T\}\big|,$$

si congettura che $N(\sigma, T) \ll T^{2(1-\sigma)+\varepsilon}$ uniformemente per $\frac{1}{2} \leq \sigma \leq 1$. J. Bourgain ha recentemente dimostrato che la stima di densità vale in $\frac{25}{32} \leq \sigma \leq 1$, ed è noto che stime piú forti sono valide vicino a $\sigma = 1$. Se fosse vera questa congettura, si avrebbe che (9.1.1) vale uniformemente per $x^{\frac{1}{2}+\varepsilon} \leq y \leq x$. Al momento attuale il risultato migliore vede $\frac{12}{5}$ al posto di 2 nell'esponente.

Appendici

§A1. Formule di sommazione

Teorema A.1.1 (Formula di sommazione parziale di Abel). *Sia $(\lambda_n)_{n\in\mathbb{N}}$ una successione strettamente crescente di numeri reali e positivi tali che $\lim_{n\to\infty}\lambda_n = +\infty$, e sia $(a_n)_{n\in\mathbb{N}}$ una successione di numeri complessi. Inoltre, sia $\varphi\colon \mathbb{R}^{0+}\to\mathbb{C}$ una funzione qualsiasi. Posto*

$$A(x) \stackrel{\text{def}}{=} \sum_{\lambda_n\le x} a_n,$$

si ha

$$\sum_{1\le n\le N} a_n\varphi\big(\lambda_n\big) = A\big(\lambda_N\big)\varphi\big(\lambda_N\big) - \sum_{n=1}^{N-1} A\big(\lambda_n\big)\Big(\varphi\big(\lambda_{n+1}\big) - \varphi\big(\lambda_n\big)\Big).$$

Se $\varphi\in\mathcal{C}^1\big(\mathbb{R}^+\big)$ ed $x\ge\lambda_1$ allora

$$\sum_{\lambda_n\le x} a_n\varphi\big(\lambda_n\big) = A(x)\varphi(x) - \int_{\lambda_1}^{x} A(t)\varphi'(t)\,\mathrm{d}t.$$

Dim.: Poniamo $A\big(\lambda_0\big)\stackrel{\text{def}}{=}0$ per comodità. Si ha

$$\begin{aligned}\sum_{n=1}^{N} a_n\varphi\big(\lambda_n\big) &= \sum_{n=1}^{N}\big[A\big(\lambda_n\big) - A\big(\lambda_{n-1}\big)\big]\varphi\big(\lambda_n\big)\\ &= A\big(\lambda_N\big)\varphi\big(\lambda_N\big) - \sum_{n=1}^{N-1} A\big(\lambda_n\big)\Big(\varphi\big(\lambda_{n+1}\big) - \varphi\big(\lambda_n\big)\Big).\end{aligned} \tag{A.1.1}$$

Dato $x>0$, sia N il piú grande intero tale che $\lambda_N\le x$. Se φ ha derivata continua, possiamo scrivere la somma a destra nella (A.1.1) come

$$\sum_{n=1}^{N-1} A\big(\lambda_n\big)\int_{\lambda_n}^{\lambda_{n+1}}\varphi'(t)\,\mathrm{d}t = \sum_{n=1}^{N-1}\int_{\lambda_n}^{\lambda_{n+1}} A(t)\varphi'(t)\,\mathrm{d}t = \int_{\lambda_1}^{\lambda_N} A(t)\varphi'(t)\,\mathrm{d}t,$$

poiché A è costante in ciascun intervallo $(\lambda_n,\lambda_{n+1})$ ed in $[\lambda_N, x)$, mentre il primo termine è

$$A\big(\lambda_N\big)\varphi\big(\lambda_N\big) = A(x)\varphi(x) - \int_{\lambda_N}^{x} A(t)\varphi'(t)\,\mathrm{d}t,$$

il che conclude la dimostrazione. □

Teorema A.1.2 (Formula di Sommazione di Euler-McLaurin). *Sia $f\colon (x,y]\to\mathbb{C}$ una qualunque funzione derivabile. Si ha*

$$\sum_{x<n\le y} f(n) = \int_x^y f(t)\,\mathrm{d}t + \int_x^y \{t\}f'(t)\,\mathrm{d}t - \{y\}f(y) + \{x\}f(x).$$

Dim.: Si può facilmente dare una dimostrazione che sfrutta la precedente Formula di
Ɛ A.1.1 Sommazione Parziale A.1.1. Qui diamo una dimostrazione alternativa: se $t\notin\mathbb{Z}$ si ha

$$\frac{\mathrm{d}}{\mathrm{d}t}\big(\{t\}f(t)\big) = \{t\}f'(t) + f(t). \tag{A.1.2}$$

Dunque

$$\int_{n-1}^{n} \big(\{t\}f'(t)+f(t)\big)\,\mathrm{d}t = \lim_{\varepsilon\to 0+}\int_{n-1+\varepsilon}^{n-\varepsilon} \big(\{t\}f'(t)+f(t)\big)\,\mathrm{d}t = f(n),$$

e si può usare di nuovo la (A.1.2) anche negli intervalli $\big[x,[x]+1\big]$, $\big[[y],y\big]$. □

Lemma A.1.3. *Sia $f\colon\mathbb{R}^+\to\mathbb{R}^+$ una funzione debolmente decrescente e infinitesima. Esiste una costante reale E tale che per $x\to\infty$ si ha*

$$\sum_{n\le x} f(n) = \int_1^x f(t)\,\mathrm{d}t + E + \mathcal{O}(f(x)).$$

Dim.: Poniamo $E_n \stackrel{\text{def}}{=} f(n) - \int_n^{n+1} f(t)\,\mathrm{d}t$. Poiché f è decrescente si ha che $0\le E_n\le f(n)-f(n+1)$. Per induzione si verifica immediatamente che

$$0\le \sum_{h\le n\le k} E_n \le f(h) - f(k+1). \tag{A.1.3}$$

Dunque, posto $E\stackrel{\text{def}}{=}\sum_{n\ge 1}E_n$, questa serie è convergente ed inoltre $E\le f(1)$. Quindi

$$\begin{aligned}\sum_{n\le x} f(n) - \int_1^x f(t)\,\mathrm{d}t &= \sum_{n\le x}\left(f(n) - \int_n^{n+1} f(t)\,\mathrm{d}t\right) + \int_x^{[x]+1} f(t)\,\mathrm{d}t\\ &= \sum_{n\le x} E_n + \mathcal{O}(f(x)) = E + \mathcal{O}\Big(\sum_{n\ge[x]+1} E_n\Big) + \mathcal{O}(f(x)),\end{aligned}$$

e la tesi segue dalla (A.1.3) con $h=[x]+1$. □

Questo Lemma può essere un utile sostituto della formula di sommazione parziale quando questa non è applicabile perché f non è derivabile, oppure può essere piú semplice da usare: per esempio una conseguenza immediata è

$$\sum_{2\le n\le N}\frac{1}{\log n} = \mathrm{li}(N) + C + \mathcal{O}\big((\log N)^{-1}\big),$$

per un'opportuna costante positiva C. Tenendo presente il Teorema dei Numeri Primi 4.1.3, questa relazione viene talvolta espressa dicendo che la "probabilità" che un intero $n\ge 3$ sia primo è $(\log n)^{-1}$. Bisogna però avere una grande cautela nell'introdurre nozioni probabilistiche in Teoria dei Numeri.

§A2. Le funzioni Gamma e Beta

Definizione A.2.1: Funzione Gamma di Eulero. *Per $z = x+\mathrm{i}y \in \mathbb{C}$ con $x = \Re(z) > 0$ definiamo*

$$\Gamma(z) \stackrel{\text{def}}{=} \int_0^{+\infty} t^{z-1} e^{-t}\, \mathrm{d}t.$$

L'integrale è totalmente convergente in ogni compatto contenuto nel semipiano $\Re(z) > 0$.

Ricordiamo senza dimostrazione le principali proprietà della funzione Gamma di Eulero: Γ soddisfa l'equazione funzionale $\Gamma(z+1) = z\Gamma(z)$ ed inoltre $\Gamma(1) = 1$, $\Gamma\left(\frac{1}{2}\right) = \pi^{1/2}$, e quindi $\Gamma(n+1) = n!$ per $n \in \mathbb{N}$. Inoltre Γ ha un prolungamento analitico a $\mathbb{C}$ privato di $\mathbb{Z} \setminus \left(\mathbb{N}^*\right)$, e in questo insieme vale la Formula di Weierstrass

$$\frac{1}{z\Gamma(z)} = e^{\gamma z} \prod_{n \geq 1} \left(1 + \frac{z}{n}\right) e^{-z/n}, \tag{A.2.1}$$

dove γ è la costante di Eulero definita dalla (A.4.1). Si osservi infine che vale la Formula di Stirling Generalizzata (cfr Appendice A3): per ogni $\delta > 0$ fissato si ha

$$\log \Gamma(z) = \left(z - \frac{1}{2}\right) \log z - z + \frac{1}{2} \log(2\pi) + \mathcal{O}_\delta\left(|z|^{-1}\right), \tag{A.2.2}$$

quando $|z| \to \infty$ nell'angolo $|\arg(z)| \leq \pi - \delta$. Questa formula è un ingrediente essenziale della dimostrazione del Teorema 7.2.2.

Definizione A.2.2: Funzione Beta. *Per $\Re(z)$, $\Re(w) > 0$ definiamo*

$$\mathrm{B}(z,w) \stackrel{\text{def}}{=} \int_0^1 t^{z-1}(1-t)^{w-1}\, \mathrm{d}t = \frac{\Gamma(z)\Gamma(w)}{\Gamma(z+w)}.$$

Mediante un semplice cambiamento di variabili si ottiene

$$\mathrm{B}(x,y) = 2\int_0^{\pi/2} (\cos u)^{2x-1} (\sin u)^{2y-1}\, \mathrm{d}u. \tag{A.2.3}$$

§A3. Formula di Stirling

Teorema A.3.1 (Formula di Wallis per π). *Si ha*

$$\lim_{N\to+\infty} \left\{ \frac{2}{1} \cdot \frac{2}{3} \cdot \frac{4}{3} \cdot \frac{4}{5} \cdots \frac{2N}{2N-1} \cdot \frac{2N}{2N+1} \right\} = \lim_{N\to+\infty} \prod_{m=1}^{N} \frac{4m^2}{4m^2-1} = \frac{\pi}{2}.$$

Dim.: Per $m \in \mathbb{N}$ definiamo $0!! \stackrel{\text{def}}{=} (-1)!! \stackrel{\text{def}}{=} 1$ e $(m+2)!! \stackrel{\text{def}}{=} m!!(m+2)$, osservando che $(2m)!! = 2^m(m!)$ e che $(2m-1)!! \cdot (2m)!! = (2m)!$. Consideriamo la successione $(I_m)_{m\in\mathbb{N}}$ definita da

$$I_m \stackrel{\text{def}}{=} \int_0^{\pi} (\sin x)^m\, \mathrm{d}x.$$

Si verifica immediatamente che I_m è una successione positiva e decrescente, che $I_0 = \pi$ e che $I_1 = 2$, ed integrando due volte per parti si ottiene la formula ricorrente

$$I_{m+2} = \frac{m+1}{m+2} I_m. \tag{A.3.1}$$

Da questa, osservando che $I_{m+2} \le I_{m+1} \le I_m$ ricaviamo

$$\lim_{m\to\infty} \frac{I_m}{I_{m+1}} = 1. \tag{A.3.2}$$

Usando la formula ricorrente (A.3.1), si ottiene per induzione

$$\frac{I_{2m}}{I_{2m+1}} = \frac{\pi}{2}(2m+1)\cdot \frac{(2m-1)!!^2}{\big(2m\big)!!^2} = \frac{\pi}{2}\frac{(2m)!^2(2m+1)}{2^{4m}\big(m!^4\big)} = \binom{2m}{m}^2 \frac{(2m+1)\pi}{2^{4m+1}}, \tag{A.3.3}$$

che insieme alla (A.3.2) implica la tesi ed anche la relazione asintotica $\binom{2m}{m} \sim \frac{2^{2m}}{\sqrt{\pi m}}$. □

𝔈 A.3.1 Teorema A.3.2 (Formula di Stirling). *Per $N \to \infty$ ed $N \in \mathbb{N}$ si ha*

$$\log N! = N\log N - N + \frac{1}{2}\log\big(2\pi N\big) + \mathcal{O}\big(N^{-1}\big).$$

Dim.: Per la formula di sommazione parziale, se $N \in \mathbb{N}$ si ha

$$\log N! = \sum_{n=1}^{N} \log n = N\log N - \int_1^N [t]\frac{\mathrm{d}t}{t} = N\log N - (N-1) + \int_1^N \frac{\{t\}\,\mathrm{d}t}{t}. \tag{A.3.4}$$

Posto $g(t) \stackrel{\text{def}}{=} \frac{1}{2}\big(t - \{t\} + \{t\}^2\big)$, si verifica immediatamente che g è continua, derivabile per $t \notin \mathbb{Z}$ e che $g'(t) = \{t\}$. Quindi, integrando per parti,

$$\int_1^N \frac{\{t\}\,\mathrm{d}t}{t} = \left[\frac{g(t)}{t}\right]_1^N + \int_1^N \frac{g(t)\,\mathrm{d}t}{t^2} = \frac{1}{2}\log N + \frac{1}{2}\int_1^N \frac{\{t\}^2 - \{t\}}{t^2}\,\mathrm{d}t.$$

L'ultimo integrale esteso a tutto l'intervallo $[1, +\infty)$ è chiaramente convergente, e si ha

$$\int_1^N \frac{\{t\}^2 - \{t\}}{t^2}\,\mathrm{d}t = \int_1^\infty \frac{\{t\}^2 - \{t\}}{t^2}\,\mathrm{d}t + \mathcal{O}\big(N^{-1}\big).$$

Sostituendo in (A.3.4) otteniamo immediatamente, per qualche $C \in \mathbb{R}$,

$$\log N! = N\log N - N + \frac{1}{2}\log N + C + \mathcal{O}\big(N^{-1}\big). \tag{A.3.5}$$

Per dimostrare che $C = \frac{1}{2}\log(2\pi)$ è sufficiente combinare le (A.3.2), (A.3.3) e (A.3.5). □

Si osservi che per la (A.2.3) $I_m = \mathrm{B}\big(\frac{1}{2}, \frac{1}{2}(m+1)\big)$ e quindi non è sorprendente che I_m sia legata alla funzione $m!$. Inoltre, integrando per parti ed utilizzando opportuni sviluppi in serie di Fourier, è possibile dare uno sviluppo asintotico per la funzione $\log N! - \big(N\log N - N + \frac{1}{2}\log(2\pi N)\big)$. In particolare si può dimostrare che

$$\log N! = N\log N - N + \frac{1}{2}\log(2\pi N) + \frac{1}{12N} + \mathcal{O}\big(N^{-2}\big),$$

cioè che

$$N! = \sqrt{2\pi N}\left(\frac{N}{e}\right)^N \left(1 + \frac{1}{12N} + \mathcal{O}\big(N^{-2}\big)\right).$$

§A4. Lemmi

𝔈 A.4.1 Teorema A.4.1. *Per ogni $k \in \mathbb{R}$ fissato si ha, quando $x \to \infty$ ed $x \in \mathbb{N}$,*

$$\sum_{n\le x} n^k = \begin{cases} \frac{1}{k+1}x^{k+1} + \frac{1}{2}x^k + \mathcal{O}_k\big(x^{k-1}\big) & \text{se } k > 0, \\ x & \text{se } k = 0, \\ \frac{1}{k+1}x^{k+1} + c_k + \mathcal{O}_k\big(x^k\big) & \text{se } k \in (-1,0), \\ \log x + c_{-1} + \mathcal{O}\big(x^{-1}\big) & \text{se } k = -1, \\ \zeta(-k) + \mathcal{O}_k\big(x^{k+1}\big) & \text{se } k < -1, \end{cases}$$

dove ζ è la funzione zeta di Riemann e c_k indica un'opportuna costante che dipende solo da k. In particolare c_{-1} si indica di solito con γ, vale approssimativamente $0.577215\ldots$ e si chiama costante di Eulero–Mascheroni.

Dim.: Usando la formula di sommazione parziale troviamo per $k > -1$

$$\begin{aligned} \sum_{n=1}^{x} n^k &= x^{k+1} - k\int_1^x [t]t^{k-1}\,\mathrm{d}t = \frac{x^{k+1}+k}{k+1} + k\int_1^x \{t\}t^{k-1}\,\mathrm{d}t \\ &= \frac{x^{k+1}+k}{k+1} + \frac{k}{2}\int_1^x t^{k-1}\,\mathrm{d}t + k\int_1^x \left(\{t\} - \frac{1}{2}\right)t^{k-1}\,\mathrm{d}t \\ &= \frac{x^{k+1}+k}{k+1} + \frac{x^k-1}{2} + k\big[g(t)t^{k-1}\big]_1^x - k(k-1)\int_1^x g(t)t^{k-2}\,\mathrm{d}t \end{aligned}$$

dove $g(t) \stackrel{\text{def}}{=} \frac{1}{2}\big(\{t\}^2 - \{t\}\big)$ è una primitiva di $\{t\} - \frac{1}{2}$. Se $k \ge 0$ il risultato segue immediatamente, poiché g è una funzione limitata. Per $k \in (-1,0)$ l'ultimo integrale può essere esteso ad $[1,+\infty)$ e vale $c'_k + \mathcal{O}\big(x^{k-1}\big)$.

Per la penultima relazione la formula di sommazione parziale dà immediatamente

$$\begin{aligned} \sum_{n\le x}\frac{1}{n} &= 1 + \int_1^x \frac{[t]}{t^2}\,\mathrm{d}t = 1 + \log x - \int_1^x \frac{\{t\}}{t^2}\,\mathrm{d}t \\ &= \log x + 1 - \int_1^\infty \frac{\{t\}}{t^2}\,\mathrm{d}t + \mathcal{O}\left(\int_x^\infty \frac{\mathrm{d}t}{t^2}\right), \end{aligned}$$

e dunque il risultato segue, con

$$c_{-1} = \gamma \stackrel{\text{def}}{=} 1 - \int_1^\infty \frac{\{t\}}{t^2}\,\mathrm{d}t. \tag{A.4.1}$$

Per l'ultima relazione basta osservare che per $k < -1$

$$\sum_{n\le x} n^k = \sum_{n\ge 1} n^k + \mathcal{O}\left(\int_x^{+\infty} t^k\,\mathrm{d}t\right) = \zeta(-k) + \mathcal{O}_k\big(x^{k+1}\big).$$

Si noti che nel caso $k = -1$ il termine d'errore ottenuto è particolarmente soddisfacente in quanto "ottimale": dato che l'ultimo addendo nella somma è $[x]^{-1} \sim x^{-1}$, l'errore *non può* essere $o\big(x^{-1}\big)$. □

Definizione A.4.2: Numeri di Bernoulli. *I numeri di Bernoulli B_n sono i coefficienti dello sviluppo*

$$\frac{z}{e^z-1} = 1 - \frac{1}{2}z + \frac{B_1}{2!}z^2 - \frac{B_2}{4!}z^4 + \frac{B_3}{6!}z^6 + \cdots$$

valido per $|z| < 2\pi$. In particolare, $B_1 = \frac{1}{6}$, $B_2 = \frac{1}{30}$, $B_3 = \frac{1}{42}$.

Teorema A.4.3. *Posto $\beta_0 \stackrel{\text{def}}{=} 1$, $\beta_1 \stackrel{\text{def}}{=} -\frac{1}{2}$, $\beta_{2k} \stackrel{\text{def}}{=} (-1)^{k-1}B_k$, $\beta_{2k+1} \stackrel{\text{def}}{=} 0$ per $k \in \mathbb{N}^*$, dove i B_k sono i numeri di Bernoulli, si ha*

$$\sum_{m=1}^{n-1} m^k = \sum_{r=0}^{k} \frac{1}{k+1-r}\binom{k}{r} n^{k+1-r}\beta_r.$$

Dim.: La dimostrazione si ottiene confrontando i coefficienti di x^{k+1} nelle espressioni

$$k!x\big(1 + e^x + \cdots + e^{(n-1)x}\big) = k!\left(\beta_0 + \frac{\beta_1}{1!}x + \frac{\beta_2}{2!}x^2 + \cdots\right)\left(nx + \frac{n^2x^2}{2!} + \cdots\right),$$

che sono uguali entrambe a $k!x\big(e^{nx}-1\big)\big(e^x-1\big)^{-1}$. □

Lemma A.4.4. *Per ogni $k \in \mathbb{R}^{0+}$ si ha*

$$\sum_{d\le x}\Big(\log\frac{x}{d}\Big)^k \le x\Gamma(k+1).$$

Dim.: Per $d \in \mathbb{N}^*$ si ha

$$\Big(\log\frac{x}{d}\Big)^k \le \int_{d-1}^{d}\Big(\log\frac{x}{t}\Big)^k\,\mathrm{d}t,$$

mentre se $d = 1$ l'integrale è improprio nell'estremo sinistro, ma convergente. Dunque

$$\sum_{d=1}^{[x]}\Big(\log\frac{x}{d}\Big)^k \le \int_0^x\Big(\log\frac{x}{t}\Big)^k\,\mathrm{d}t = x\int_0^\infty u^k e^{-u}\,\mathrm{d}u = x\Gamma(k+1),$$

mediante il cambiamento di variabile $t = xe^{-u}$. □

Per $k = 1$ questa relazione implica la formula di Stirling nella forma piú debole $\log N! = N\log N + \mathcal{O}(N)$, che è comunque sufficiente per ottenere i risultati del Capitolo 4.

Lemma A.4.5. *Sia $f\colon\mathbb{R}\to\mathbb{R}$ una funzione convessa. Per ogni $\delta > 0$ si ha*

$$f(x) \le \frac{1}{\delta}\int_{x-\frac{1}{2}\delta}^{x+\frac{1}{2}\delta} f(t)\,\mathrm{d}t.$$

Dim.: Per ogni $\alpha \in \big[-\frac{1}{2}\delta, \frac{1}{2}\delta\big]$ si ha

$$f(x) = f\left(\frac{1}{2}(x-\alpha) + \frac{1}{2}(x+\alpha)\right) \le \frac{1}{2}\big(f(x-\alpha) + f(x+\alpha)\big).$$

La tesi si ottiene integrando questa disuguaglianza su tutto l'intervallo $\big[-\frac{1}{2}\delta, \frac{1}{2}\delta\big]$. □

Bibliografia

§B1. Riferimenti Bibliografici

- [1] T. M. Apostol, "Introduction to Analytic Number Theory," Springer, 1975.
- [2] A. H. Beiler, "Recreations in the Theory of Numbers," Dover, New York, 1964.
- [3] E. Bombieri, "Le Grand Crible dans la Théorie Analytique des Nombres," Astérisque n. 18, Societé Mathématique de France, Parigi, 1974.
- [4] E. Bombieri & C. Viola, "Lezioni di Teoria dei Numeri," (dispense), Pisa.
- [5] Z. I. Borevich & I. R. Shafarevich, "Number Theory," Academic Press, New York, 1966.
- [6] J. W. S. Cassels, "An Introduction to the Geometry of Numbers," Springer, 1959.
- [7] K. Chandrasekharan, "Introduction to Analytic Number Theory," Springer, 1968.
- [8] K. Chandrasekharan, "Arithmetical Functions," Springer, 1970.
- [9] H. Cohen, "A Course in Computational Algebraic Number Theory," GTM 138, 3ª ed., Springer, 1996.
- [10] J. H. Conway & R. K. Guy, "The Book of Numbers," Springer, 1997. Trad. it. Hoepli, Milano, 1999.
- [11] R. Crandall & C. Pomerance, "Prime numbers. A computational perspective," Springer, 2001.
- [12] H. Davenport, "Multiplicative Number Theory," GTM 74, 3ª ed., Springer, 2000.
- [13] L. E. Dickson, "History of the Theory of Numbers," Carnegie, 1919–1923.
- [14] P. G. L. Dirichlet, "Lectures on Number Theory," (with supplements by R. Dedekind), Amer. Math. Soc., Providence, RI, 1999.
- [15] H. M. Edwards, "Fermat's Last Theorem," Springer, 1977.
- [16] K. F. Gauss, "Disquisitiones Arithmeticae," Lipsia, 1801.
- [17] G. Greaves, "Sieves in Number Theory," Springer, 2001.
- [18] R. K. Guy, "Unsolved Problems in Number Theory," 2ª ed., Springer, 1994.
- [19] H. Halberstam & H.-E. Richert, "Sieve Methods," Academic Press, Londra, 1974.
- [20] H. Halberstam & K. F. Roth, "Sequences," Oxford U. P., 1966.
- [21] G. H. Hardy, "Ramanujan, Twelve lectures on subjects suggested by his life and works," 3ª ed., Chelsea, New York, 1999.
- [22] G. H. Hardy & E. M. Wright, "An Introduction to the Theory of Numbers," 5ª ed., Oxford Science Publications, 1979.
- [23] Hua L.-K., "Introduction to Number Theory," Springer, 1982.
- [24] D. Husemöller, "Elliptic curves," GTM 111, Springer, New York, 1987.
- [25] M. Huxley, "The Distribution of Prime Numbers," Clarendon Press, Oxford, 1972.
- [26] A. E. Ingham, "The Distribution of Prime Numbers," Cambridge U. P., rist. 1990.

- [27] A. Ivić, "The Theory of the Riemann Zeta–Function," J. Wiley, New York, 1985.
- [28] J. Knopfmacher, "Abstract Analytic Number Theory," Dover, New York, 1989.

[29] D. E. Knuth, "The Art of Computer Programming. Vol. 2. Seminumerical Algorithms," 2ª ed., Addison Wesley, Reading (Mass.), 1981.

[30] N. Koblitz, "A Course in Number Theory and Cryptography," GTM 114, 2ª ed., Springer, 1994.

[31] E. Landau, "Elementary Number Theory," Chelsea, New York, 1960.

[32] E. Landau, "Handbuch der Lehre von der Verteilung der Primzahlen," Teubner, Lipsia, 1909.

[33] E. Landau, "Vorlesungen über Zahlentheorie," Hirzel, Lipsia, 1927.

[34] D. A. Marcus, "Number Fields," Springer, 1977.

[35] A. Menezes, P. van Oorschot & S. Vanstone, "Handbook of Applied Cryptography," CRC Press, 1996. `http://www.cacr.math.uwaterloo.ca/hac`

- [36] H. L. Montgomery, "Topics in Analytic Number Theory," LNM 227, Springer, 1971.
- [37] H. L. Montgomery, "Ten Lectures on the Interface Between Analytic Number Theory and Harmonic Analysis," CBMS n. 84, Amer. Math. Soc., Providence, RI, 1994.

[38] W. Narkiewicz, "The Development of Prime Number Theory," Springer, 2000.

[39] M. B. Nathanson, "Additive Number Theory: the Classical Bases," GTM 164, Springer, 1996.

- [40] O. Ore, "Number Theory and its History," Dover, New York, 1976.

[41] K. Prachar, "Primzahlverteilung," Springer, 1957.

- [42] P. Ribenboim, "The New Book of Prime Numbers Records," Springer, 1996.

[43] H. Riesel, "Prime numbers and computer methods for factorization," 2ª ed., Birkhäuser, Boston, 1994.

[44] J.-P. Serre, "A Course in Arithmetic," Springer, 1973.

[45] D. Shanks, "Solved and Unsolved Problems in Number Theory," 4ª ed., Chelsea, 1993.

[46] G. Tenenbaum & M. Mendès France, "The Prime Numbers and their Distribution," A. M. S., 2000.

- [47] E. C. Titchmarsh, "The Theory of the Riemann Zeta–Function," 2ª ed., Oxford U. P., 1986.

[48] P. Turán, "On a New Method of Analysis and its Applications," J. Wiley, 1984.

- [49] R. C. Vaughan, "The Hardy–Littlewood Method," 2ª ed., Cambridge U. P., 1997.
- [50] A. Weil, "Teoria dei Numeri," Einaudi, Torino, 1993.

Altri Testi di Riferimento

[51] L. V. Ahlfors, "Complex Analysis," 3ª ed., Mc Graw-Hill, 1979.

[52] L. Childs, "A Concrete Introduction to Higher Algebra," Springer, 1979.

[53] G. H. Hardy, "Divergent Series," 2ª ed., Chelsea, New York, 1991.

[54] W. Rudin, "Functional Analysis," Mc Graw-Hill, 1973, rist. TMH, New Delhi, 1985.

[55] E. C. Titchmarsh, "The Theory of Functions," 2ª ed., Oxford U. P., rist. 1988.

[56] E. T. Whittaker & G. N. Watson, "Modern Analysis," 4ª ed., Cambridge U. P., 1927.

[57] N. Wiener, "The Fourier Integral and Certain of its Applications," Cambridge U. P., 1933, rist. Dover, New York, 1958.

Articoli

[A1] L. M. Adleman, C. Pomerance, R. S. Rumely, *On distinguishing prime numbers from composite numbers*, Ann. Math. **117** (1983), 173–206.

[A1] M. Agrawal, N. Kayal & N. Saxena, *PRIMES is in P*, To appear (2002). `http://www.cse.ac.iitk.ac.in/primality.pdf`

[A1] W. R. Alford, A. Granville & C. Pomerance, *There are infinitely many Carmichael numbers*, Ann. Math. **140** (1994), 703–722.

[A1] T. M. Apostol, *Some properties of completely multiplicative arithmetical functions*, AMM **78** (1971), 266–271.

[A1] R. C. Baker, G. Harman & J. Pintz, *The difference between consecutive primes, II*, Proc. London Math. Soc. (3) **83** (2001), 532–562.

[A1] P. T. Bateman & H. G. Diamond, *A hundred years of prime numbers*, AMM **103** (1996), 729–741.

[A1] E. Bombieri, *Sulle formule di A. Selberg generalizzate per classi di funzioni aritmetiche e le applicazioni al problema del resto nel "Primzahlsatz"*, Riv. Mat. Univ. Parma (2) **3** (1962), 393–440.

[A2] ———, *Problems of the Millennium: the Riemann Hypothesis*. `http://www.claymath.org/prize_problems/index.html`

[A1] J. Bourgain, *On large values estimates for Dirichlet polynomials and the density hypothesis for the Riemann zeta function*, Int. Math. Res. Not. **2000, No. 3** (2000), 133–146.

[A1] H. Cramér, *On the order of magnitude of the difference between consecutive prime numbers*, Acta Arith. **2** (1937), 23–46.

[A1] H. Daboussi, *Sur le Théorème des Nombres Premiers*, C. R. Acad. Sc. Paris Série I **298** (1984), 161–164.

[A1] M. Deléglise & J. Rivat, *Computing $\pi(x)$: The Meissel, Lehmer, Lagarias, Miller, Odlyzko Method*, Math. Comp. **65** (1996), 235–245.

[A2] ———, *Computing $\psi(x)$*, Math. Comp. **67** (1998), 1691–1696.

[A1] J.-M. Deshouillers, G. Effinger, H. te Riele & D. Zinoviev, *A complete Vinogradov 3-primes theorem under the Riemann Hypothesis*, Electr. Res. Announcements Amer. Math. Soc. **3** (1997), 99–104.

• [A1] H. G. Diamond, *Elementary Methods in the Study of the Distribution of Prime Numbers*, Bull. Amer. Math. Soc. **3** (1982), 553–589.

• [A1] J. D. Dixon, *Factorization and primality tests*, AMM **91** (1984), 333–352.

[A1] U. Dudley, *History of a formula for primes*, AMM **76** (1969), 23–28.

• [A1] W. J. Ellison, *Waring's problem*, AMM **78** (1971), 10–36.

[A1] J. Elstrodt, *A quick proof of the prime number theorem for arithmetic progressions*, in "Charlemagne and his heritage. 1200 years of civilization and science in Europe," vol. 2 (Aachen 1995), Brepols, Turnhout, 1998, pp. 521–530.

[A1] J. S. Frame, *A short proof of quadratic reciprocity*, AMM **85** (1978), 818–819.

[A1] J. Friedlander, A. Granville, A. Hildebrand & H. Maier, *Oscillation theorems for primes in arithmetic progressions and for sifting functions*, J. Amer. Math. Soc. **4** (1991), 25–86.

[A1] J. Friedlander & H. Iwaniec, *The polynomial $X^2 + Y^4$ captures its primes*, Ann. Math. **148** (1998), 945–1040.

[A1] J. M. Gandhi, *Review n. 7003*, Math. Rev. **50** (1975), p. 963.

[A1] S. Gerig, *A Simple Proof of the Prime Number Theorem*, J. Number Theory **8** (1976), 131–136.

[A1] L. J. Goldstein, *A History of the Prime Number Theorem*, AMM **80** (1973), 599–615.

[A1] S. W. Golomb, *A direct interpretation of Gandhi's formula*, AMM **81** (1974), 752–754.

[A1] A. Granville, *On Elementary Proofs of the Prime Number Theorem for Arithmetic Progressions, Without Characters*, in "E. Bombieri (ed.) *et al.*, Proceedings of the Amalfi Conference on Analytic Number Theory, held at Maiori, Amalfi, Italy, from 25 to 29 September, 1989," Università di Salerno, 1992, pp. 157–194.

[A2] ———, *Unexpected irregularities in the distribution of prime numbers*, in "Proceedings of the International Congress of Mathematicians, Zürich, Switzerland, 1994," Birkhäuser, 1995, pp. 388–399.

[A3] ———, *Harald Cramér and the distribution of prime numbers*, Scand. Actuarial J. **1** (1995), 12–28.

[A1] G. H. Hardy & J. E. Littlewood, *Some problems in "Partitio Numerorum"; III. On the expression of a number as a sum of primes*, Acta Math. **44** (1923), 1–70.

[A2] ———, *Some problems of "Partitio Numerorum"; V. A further contribution to the study of Goldbach's problem*, Proc. London Math. Soc. (2) **22** (1923), 46–56.

[A1] G. H. Hardy & S. Ramanujan, *Asymptotic formulae in combinatory analysis*, Proc. London Math. Soc. (2) **17** (1918), 75–115. = S. Ramanujan, "Collected papers," edited by G. H. Hardy, P. V. Seshu Aiyar & B. M. Wilson, 3ª ed., AMS–Chelsea, 1999; n. 36, 276–309.

[A1] D. R. Heath-Brown, *Artin's conjecture for primitive roots*, Quart. J. Math. Oxford (2) **37** (1986), 27–38.

[A2] ———, *The number of primes in a short interval*, J. reine angew. Math. **389** (1988), 22–63.

[A3] ———, *Zero-free regions for Dirichlet L-functions and the least prime in an arithmetic progression*, Proc. London Math. Soc. (3) **64** (1992), 265-338.

[A4] ———, *Primes represented by $x^2 + y^3$*, Acta Math. **186** (2001), 1–84.

[A1] A. Hildebrand, *The Prime Number Theorem via the Large Sieve*, Mathematika **33** (1986), 23–30.

[A2] ———, *On the constant in the Pólya–Vinogradov inequality*, Canad. Bull. Math. **31** (1988), 347–352.

[A3] ———, *Large values of character sums*, J. Number Theory **29** (1988), 271–296.

[A1] A. Hildebrand & H. Maier, *Irregularities in the distribution of primes in short intervals*, J. reine angew. Math. **397** (1989), 162–193.

• [A1] A. Hildebrand & G. Tenenbaum, *Integers without large prime factors*, J. Théorie des Nombres Bordeaux **5** (1993), 411–484.

[A1] A. E. Ingham, *Review*, Math. Rev. **10** (1949), 595–596.

[A1] R. D. James, *On the sieve method of Viggo Brun*, Bull. Amer. Math. Soc. **49** (1943), 422–432.

[A2] ———, *Recent progress in the Goldbach problem*, Bull. Amer. Math. Soc. **55** (1949), 246–260.

[A1] E. Landau, *Über die Enteilung der positiven ganzen Zahlen in vier Klassen nach der Mindeszahl der zu ihrer additiven Zusammensetzung erforderlichen Quadrate*, Arch. Math. Phys. (3) **13** (1908), 305–312.

[A1] A. Languasco, *Some results on Goldbach's problem*, Rend. Sem. Mat. Univ. Pol. Torino **53 (4)** (1995), 325–337.

[A1] D. H. Lehmer, *On the converse of Fermat's Theorem*, AMM **43** (1936), 347–350.

[A2] D. H. Lehmer, *On the exact number of primes less than a given limit*, Illinois J. Math. **3** (1959), 381–388.

[A1] N. Levinson, *A Motivated Account of an Elementary Proof of the Prime Number Theorem*, AMM **76** (1969), 225–245.

[A1] L. S. Levy, *Summation of the series $1^n + 2^n + \cdots + x^n$ using elementary calculus*, AMM **77** (1970), 840–847; *Corrigendum*, *ibidem* **78** (1971), p. 987.

[A1] J. E. Littlewood, *Sur la distribution des nombres premiers*, C. R. Acad. Sc. Paris **158** (1914), 1869–1872.

[A1] H. Maier, *Primes in short intervals*, Michigan Math. J. **32** (1985), 221–225.

[A1] H. Maier & C. Pomerance, *Unusually large gaps between consecutive primes*, Trans. Amer. Math. Soc. **322** (1990), 201–237.

[A1] G. Marsaglia & J. C. W. Marsaglia, *A new derivation of Stirling's approximation to n!*, AMM **97** (1990), 826–829.

• [A1] H. Montgomery, *The analytic principle of the large sieve*, Bull. Amer. Math. Soc. **84** (1978), 547–567.

[A1] H. L. Montgomery & R. C. Vaughan, *The large sieve*, Mathematika **20** (1973), 119–134.

[A2] ———, *The exceptional set in Goldbach's problem*, Acta Arith. **27** (1975), 353–370.

[A1] P. Morton, *Musings on the prime divisors of arithmetic sequences*, AMM **97** (1990), 323–328.

[A1] T. Nagel, *Généralisation d'un théorème de Tchebycheff*, J. Math. Pures Appl. (8) **4** (1921), 343–356.

[A1] M. Nair, *On Chebyshev-type inequalities for primes*, AMM **89** (1982), 126–129.

[A2] ———, *A new method in elementary prime number theory*, J. London Math. Soc. (2) **25** (1982), 385–391.

[A1] D. J. Newman, *Simple analytic proof of the prime number theorem*, AMM **87** (1980), 693–696.

[A1] J. Pintz, *On Legendre's prime number formula*, AMM **87** (1980), 733–735.
[A2] _____, *On the remainder term of the prime number formula and the zeros of the Riemann zeta-function*, in "Number Theory, Noordwijkerhout," LNM 1068, Springer, 1984, pp. 186–197.
[A1] E. A. Poe, *The Gold Bug*, in "The complete tales and poems of Edgar Allan Poe," Random House, 1975. Trad. it. *Lo scarabeo d'oro*, in "Racconti," L'Unità–Einaudi.
[A1] G. Pólya, *Heuristic reasoning in the theory of numbers*, AMM **66** (1959), 375–384.
[A1] C. Pomerance, *A note on the least prime in an arithmetic progression*, J. Number Theory **12** (1980), 218–223.
[A2] _____, *Recent developments in primality testing*, Math. Intellig. **3** (1981), 97–105.
[A3] _____, *Alla ricerca dei numeri primi*, Le Scienze **174** (febb. 1983), 86–94.
[A4] _____, *The quadratic sieve factoring algorithm*, in "Advances in Cryptology, Proceedings of EUROCRYPT 84," LNCS 209, Springer, 1985, pp. 169–182.
[A5] _____, *Factoring*, in "Cryptology and computational number theory," Lect. Notes AMS Short Course, Boulder, CO (USA), 1989. Proc. Symp. Appl. Math., 1990, pp. 27–47.
[A6] _____, *A tale of two sieves*, Notices Amer. Math. Soc. **43** (1996), 1473–1485.
[A7] _____, *Smooth numbers and the quadratic sieve*, in "Algorithmic Number Theory: Lattices, Number Fields, Curves and Cryptography, Ed. by J. P. Buhler and P. Stevenhagen," Proceedings of an MSRI workshop, 2002. `http://cm.bell-labs.com/cm/ms/who/carlp/pub.html`
[A7] _____, *Primality testing: variations on a theme of Lucas*, in "Algorithmic Number Theory: Lattices, Number Fields, Curves and Cryptography, Ed. by J. P. Buhler and P. Stevenhagen," Proceedings of an MSRI workshop, 2002. `http://cm.bell-labs.com/cm/ms/who/carlp/pub.html`
[A8] _____, *Elementary thoughts on discrete logarithms*, in "Algorithmic Number Theory: Lattices, Number Fields, Curves and Cryptography, Ed. by J. P. Buhler and P. Stevenhagen," Proceedings of an MSRI workshop, 2002. `http://cm.bell-labs.com/cm/ms/who/carlp/pub.html`
[A1] C. Pomerance, J. L. Selfridge & S. S. Wagstaff, *The pseudoprimes to* $25 \cdot 10^9$, Math. Comp. **35** (1980), 1003–1026.
[A1] O. Ramaré, *On Šnirel'man's Constant*, Ann. Scuola Norm. Sup. IV **22** (1995), 645–706.
[A1] J. B. Rosser & L. Schoenfeld, *Approximate formulae for some functions of prime numbers*, Illinois J. Math. **6** (1962), 64–94.
[A1] C. Vanden Eynden, *A proof of Gandhi's formula for the n-th prime*, AMM **79** (1982), p. 625.
[A1] S. Wagon, *Editor's corner: the euclidean algorithm strikes again*, AMM **97** (1990), 125–129.
[A1] T. D. Wooley, *Large improvements in Waring's problem*, Ann. Math. **135** (1992), 131–164.
[A1] A. Zaccagnini, *Additive problems with prime numbers*, Rend. Sem. Mat. Univ. Pol. Torino **53 (4)** (1995), 471–486.
[A2] _____, *Variazioni Goldbach: problemi con numeri primi*, L'Educazione Matematica, Anno XXI, Serie VI **2** (2000), 47–57. `http://www.math.unipr.it/~zaccagni/psfiles/Goldbach_I.ps`
[A3] _____, *Alcune proprietà dei numeri primi e loro applicazioni alla crittografia.* `http://www.math.unipr.it/~zaccagni/psfiles/Crittografia.ps`
[A1] D. Zagier, *A one-sentence proof that every prime* $p \equiv 1 \mod 4$ *is a sum of two squares*, AMM **97** (1990), p. 144.

Per brevità abbiamo indicato l'American Mathematical Monthly con la sigla AMM. Libri ed articoli contrassegnati da • contengono ulteriori riferimenti bibliografici. Si veda anche l'Enciclopedia on-line delle successioni di interi all'indirizzo
`http://www.research.att.com/~njas/sequences/`

§B2. Fonti e Letture Ulteriori

Capitolo 1.

§1.1 Si vedano i Capitoli 1, 2, 5, 6 e 7 di [22] ed il libro [31]. Risultati elementari: vedi [14].
§1.2 Teorema 1.2.15: [22] Teorema 110. La struttura dei gruppi $(\mathbb{Z}/m\mathbb{Z})^*$ è discussa nei dettagli in [45] §§23–38: vedi in particolare i diagrammi nel §33. Teorema 1.2.16: [45] §35. Teorema di Cipolla 1.2.6:

[22] Teorema 89, ed anche Pomerance [A2]. Pseudoprimi: [42] §2.VIII. Numeri di Carmichael: [42] §2.IX ed Alford, Granville & Pomerance [A1], dove si dimostra che ne esistono infiniti.

§1.3 La dimostrazione di Diofanto si trova in [22] §13.2. L'altra dimostrazione è ispirata all'Introduzione, pp. 1–21 di [24]. Ulteriori informazioni si trovano in [10] Cap. 6, pp. 147–151.

§1.4 Dimostrazione alternativa del Lemma 1.4.1: [22] Teorema 36 ed anche i §§20.2-20.4. Il Teorema contenuto nell'Osservazione 1.4.6 è di Fermat: [15] §2.4 e §2.6; Weil [50] ricostruisce una plausibile dimostrazione che Fermat potrebbe aver scoperto nel Cap. 2, §§VII–IX e riassume i contributi di Eulero nel Cap. 3, §IX. Una dimostrazione elementare si trova in [10] Cap. 8. Zagier [A1] dà una dimostrazione molto breve, ma non particolarmente illuminante. Wagon [A1] dà una dimostrazione costruttiva basata sull'algoritmo di Euclide. Si veda anche Friedlander & Iwaniec [A1]. Per la dimostrazione dell'implicazione inversa nel Teorema 1.4.11 si veda l'Appendice al Cap. IV del libro di Serre [44] o il Cap. IV, parte III del libro di Landau [31].

§1.5 Teorema di Lagrange 1.5.1: [22] Teorema 369.

§1.6 Estensioni del simbolo di Legendre: per i simboli di Jacobi e di Kronecker si veda [31] Parte I, Cap. 6, pag. 65 e 70 rispettivamente. Reciprocità quadratica 1.6.4: per altre tre dimostrazioni vedi [22] Teorema 98, [1] Teorema 9.8 oppure Frame [A1].

§1.7 Formule per i primi: [22] §2.7, Teorema 419 e App. 1 e 2. Numeri di Fermat e di Mersenne: [22] §2.5. Altre formule per i numeri primi si trovano anche in Dudley [A1] ed in Vanden Eynden [A1]. Ulteriori riferimenti si possono trovare nella recensione di quest'ultimo articolo a cura di Gandhi [A1]. Una semplice dimostrazione del Teorema di Schur 1.7.2 con varie estensioni si può trovare in Morton [A1].

Capitolo 2.

§2.1 Si veda [52] §§3.A-B, [45] §1.2 pp. 4–8 e [22] §10.6 per la relazione con il calcolo della frazione continua per il numero razionale n/m.

§2.3 Teorema 2.3.1: [22] Teorema 90. Dixon [A1], Lehmer [A1], [42] §§2.II.C, 2.II.F, 2.III, [9] Cap. 9.

§2.4 Si vedano Dixon [A1], Pomerance [A2–5], [13] pp. 92–95, [9] Capp. 8 e 10.

§2.5 Si vedano [16] §§73–74 e [42] §2.II.A.

§2.8 Si vedano [30] §4.2, [42] §2.XII.B, ed i primi 3 Capitoli di [35].

Capitolo 3.

§3.1 Vari Teoremi e dimostrazioni sono adattati da [1] Cap. 2. Si veda anche Apostol [A1] per la caratterizzazione delle funzioni completamente moltiplicative.

§3.2 Funzione r_2: Teoremi 336 e 337 di [22]. Teorema di Gauss 3.2.2: [22] Teorema 339. Teorema di Landau 3.2.3: l'articolo originale è Landau [A1]. Si vedano anche [21] §§4.4–4.7 per una breve descrizione della dimostrazione, oppure [33] §§176–183 per i dettagli. Altri problemi di natura simile ai Teoremi 3.2.2 e 3.2.3 si possono trovare in [21] Cap. 5, ed in [22] §§18.2-18.7. Per l'Osservazione di Eulero si veda [45] §27, pag. 70. Il Lemma 3.2.11 è il Teorema 272 di [22].

§3.3 Prodotto di Eulero 3.3.1: [1] Teorema 11.6 oppure [26] §1.6. Definizione e proprietà dei prodotti infiniti: [55] §1.4–1.44; per il prodotto di serie assolutamente convergenti, *ibidem*, §§1.6–1.65.

§3.4 Si veda il Cap. 17 di [22], in particolare i paragrafi 6–7.

Capitolo 4.

§4.1 Teorema di Eulero 4.1.5: [26] §1.2. Storia del Teorema dei Numeri Primi 4.1.3: Goldstein [A1] dà anche una breve descrizione della dimostrazione analitica. Si vedano anche Bateman & Diamond [A1], Granville [A2–3]. Congettura di Legendre: Pintz [A1]. Per l'andamento numerico delle funzioni π, θ e ψ e la bontà delle varie approssimazioni: Rosser & Schoenfeld [A1] e Deléglise & Rivat [A1–2].

§4.2 La minorazione nel Lemma di Chebyshev 4.2.2 è tratta da Nair [A1-2]. Per ulteriori considerazioni al riguardo, si veda [37] Cap. 10. La maggiorazione nello stesso Lemma è quella del Teorema 415 di [22]. Si veda anche [26] §§1.4–1.5.

§4.3 Formule di Mertens 4.3.1-4.3.4: [22] Teoremi 424, 425, (22.6.1) e Teorema 427, oppure [26] §1.9. Teorema di Chebyshev 4.3.5: vedi [26] §1.8 per una dimostrazione alternativa. Teorema 4.3.6: si veda [22] Teorema 429, [26] §1.9.

§4.4 La dimostrazione delle Formule di Selberg 4.4.2 per mezzo del Lemma di Iseki–Tatuzawa 4.4.1, è adattata da [8] Cap. 1.

§4.5 Dimostrazione elementare del Teorema dei Numeri Primi 4.1.3: [22], Cap. 22. Altre dimostrazioni elementari: Diamond [A1], Levinson [A1], Daboussi [A1] (questa è basata su un'idea totalmente diversa) e Bombieri [A1] (questa dà anche stime per il termine d'errore).

§4.6 La dimostrazione del Teorema 4.6.1 è adattata da [22] Teorema 328. Per i Teoremi 4.6.2 e 4.6.3 si veda il §22.10 ed il Teorema 430 di [22]. Per la funzione $\Psi(x, y)$ si vedano Hildebrand & Tenenbaum [A1] e Tenenbaum & Mendès France [46].

§4.7 Diamond [A1] elenca le "equivalenze" elementari delle relazioni fra le funzioni di Chebyshev.

Capitolo 5.

§5.1 Si vedano anche [12] Capp. 1, 4–6, ed [1] Cap. 6.

§5.2 I Lemmi 5.2.6–5.2.9 sono i Lemmi 1–4 nel Capitolo 9.8 di [23].

§5.3 Teorema di Dirichlet 5.3.1: [23] Teorema 8.2 oppure [1] Cap. 7. Dimostrazione del Teorema dei Numeri Primi nelle Progressioni 5.3.2: [12] Capp. 8–22. Dimostrazione elementare del Teorema dei Numeri Primi nelle Progressioni Aritmetiche 5.3.2: per le relazioni fra la formula di Selberg generalizzata e la distribuzione dei numeri primi nelle progressioni, si veda Granville [A1].

§5.4 Disuguaglianza di Pólya–Vinogradov 5.4.3: [12] Cap. 23, oppure [1] Teorema 8.21. Per il valore della costante e per altri problemi legati si vedano Hildebrand [A2–3].

§5.5 La dimostrazione del Teorema di Gauss-Jacobi 5.5.1 è adattata da [22] Teorema 278.

Capitolo 6.

§6.1 Principio di Inclusione–Esclusione 6.1.2: si veda anche [22] Teorema 260. Formula di Lagrange 6.1.1: [19] §1.5 e relative note, o Lehmer [A2].

§6.2 Questo paragrafo è ispirato a [31] Parte II, Cap. II. Per la moltiplicatività di ϱ, [22] Teorema 122. Altri tipi di crivello sono descritti in [19], [20] §§4.1–9, James [A1–2].

§6.3 Il Teorema 2.6 in [19], citato anche nel Capitolo 9, dà risultati uniformi e del corretto ordine di grandezza. Per la (6.3.1) in generale si veda Nagel [A1]. Il prodotto infinito converge per il Teorema degli Ideali Primi. Per la definizione generale di discriminante di un polinomio, [52] Parte III, Cap. 15. Per la possibilità di esprimere il simbolo di Legendre tramite opportuni caratteri, [12] Cap. 5.

§6.4 Questo paragrafo è un adattamento del §3 di [3]. Si vedano anche il §27 di [12], i Capp. 2–5 di [36], il §4.10 di [20], i Capp. 7, 8, 18, 19 di [25] e Montgomery [A1].

§6.5 La dimostrazione del Teorema di Brun-Titchmarsh 6.5.2 è adattata dal §3 di [3].

Capitolo 7.

§7.1 Per la teoria delle funzioni olomorfe si vedano [51], [55] oppure [56]. Prolungamento analitico ed equazione funzionale: [12] Cap. 8, [26] §3.2 o [47] Cap. 2, dove ne sono riportate ben sette dimostrazioni, oppure [55] §§4.43–4.45. L'equazione funzionale è stata scoperta da Eulero: si vedano i §§2.2-2.3 di [53]. Prodotto infinito: [26] §3.8.

§7.2 Teorema 7.2.1: [12] Cap. 13, [26] §3.9 o [47] §6.19. Teorema 7.2.2: [12] Cap. 15, [26] §4.2.

§7.3 Formula di Perron 7.3.1: [12] Cap. 17, [26] §4.5 o [47] Lemma 3.12. Formula esplicita 7.3.3: [12] Cap. 17 o [26] §4.6.

§7.4 Dimostrazione del Teorema dei Numeri Primi: [12], Cap. 18. Per un'accurata descrizione delle relazioni fra la dimostrazione elementare e quella analitica, si veda la recensione di Ingham [A1] degli articoli originali di Selberg e di Erdős. Si vedano anche i Capp. 1–4 di [21] per una descrizione dei risultati di questo Capitolo nel loro contesto e senza troppi dettagli. Una dimostrazione non elementare basata sul crivello è data da Hildebrand [A1]. Un'altra dimostrazione analitica si trova in Wiener [57] §17, o in Rudin [54] §§9.8–9.12. Gerig [A1] ha dato una breve dimostrazione non elementare, nella quale si usano solo dell'analisi armonica e le proprietà della serie di Dirichlet per zeta in $\sigma > 1$. Una semplice dimostrazione analitica si trova in Newman [A1]. Per la dimostrazione corrispondente del Teorema 5.3.2, si veda Elstrodt [A1]. Si veda anche [26] Cap. 2.

§7.5 Congettura di Riemann 4.1.4 e sue conseguenze: [12] Cap. 18, [26] §§4.8–4.9 oppure [47] Cap. 14. Per una vasta panoramica su analoghe congetture in situazioni diverse si veda Bombieri [A2].

§7.6 [12] Capp. 1 e 4.

Capitolo 8.

§8.1 Il riferimento classico per il metodo del cerchio è la monografia [49]: in particolare, per quanto riguarda questo paragrafo si veda il Cap. 1. Si vedano anche [21] Cap. 8 (in particolare i §§8.1–8.7) e James [A2] §5. La genesi dell'idea di studiare il comportamento della funzione generatrice in prossimità di diverse singolarità è esposta molto chiaramente in Hardy & Ramanujan [A1] (in particolare i §§1.2–1.5) ed in [21] Cap. 8 (in particolare i §§8.6–8.7). Per il problema di Waring si vedano [22] Capp. 20–21 per un'introduzione, e [49] per uno studio piú approfondito). Per la relazione fra serie di Laurent e serie di Fourier vedi [55] §13.12.

§8.2 Nel §3.2 di [49] si dimostra che, posto $\mathcal{E}(N) \stackrel{\text{def}}{=} \{2n \le N : r_2(2n) = 0\}$, per ogni $A > 0$ si ha $|\mathcal{E}(N)| = \mathcal{O}_A\left(N(\log N)^{-A}\right)$. Un'applicazione del metodo del cerchio a diversi problemi legati alla congettura di Goldbach si può trovare in Languasco [A1], mentre in Zaccagnini [A1] si può trovare anche una breve introduzione al metodo del cerchio simile alla presente. Un'altra argomentazione euristica per il numero dei primi gemelli si trova in [22] §22.20. Le congetture di cui si parla in questo Capitolo ed in Zaccagnini [A2] sono inquadrate nel contesto generale della congettura di Schinzel & Sierpiński nell'introduzione di [19]; si vedano le Note relative per la versione quantitativa di Bateman & Horn (vedi anche Zaccagnini [A2], formule (6), (8) e (10) e la "Coda" per il caso delle "costellazioni" di primi). Una maggiorazione per $r_2(n)$ del giusto ordine di grandezza è contenuta nel Teorema 3.11 di [19]. Per altre strategie per la dimostrazione della congettura di Goldbach si veda [42] §4.VI, e per ulteriori riferimenti [18] §C.1.

§8.3 La (8.3.2) è in [12] Cap. 20. Il Lemma 8.3.1 è il Teorema 3.1 di Vaughan [49]. Per la (8.3.3) vedi [12] Cap. 25. Chen ha dimostrato che ogni numero pari sufficientemente grande può essere scritto come somma di un primo e di un intero che ha al massimo 2 fattori primi ([19] Cap. 10). Una dimostrazione relativamente semplice di questo fatto (ma con 4 al posto di 2) si trova nel §9 di [3].

§8.5 Per la (8.5.2) vedi [12] Cap. 26. Problema ternario di Goldbach: [12] Cap. 26, [49] §3.1. La relazione (8.5.1) è giustificata euristicamente in Zaccagnini [A2], dove però la formula (8) deve essere moltiplicata per $(\log n)^3$, sempre a causa della presenza dei pesi nella somma che definisce $R_3(n)$. Vedi anche Deshouillers, Effinger, te Riele & Zinoviev [A1].

Capitolo 9.

§9.1 Capitolo 1: Alford, Granville & Pomerance, [A1]. Pomerance, Selfridge & Wagstaff, [A1]. Heath-Brown [A1]. Capitolo 3: [47] Cap. 13 e relative note, oppure [27] §13.2, 13.8 e Note. Problema di Waring: [49], Ellison [A1], Wooley [A1]. Capitolo 4: Littlewood [A1], Heath-Brown [A2], Hildebrand & Maier [A1], Friedlander, Granville, Hildebrand & Maier [A1], Montgomery & Vaughan [A1], Cramér [A1], Maier & Pomerance [A1], Baker & Harman [A1], Maier [A1]. Capitolo 5: [12] Capp. 9–22. Heath-Brown [A3], Pomerance [A1]. Capitolo 6: [19] Teorema 2.6. Per $\pi_h(x)$ si veda l'argomentazione euristica nel §22.20 di [22], e la maggiorazione del Teorema 3.11 di [19]. Altre argomentazioni euristiche diverse si trovano in Pólya [A1] ed in Hardy & Littlewood [A1]. Problema di Goldbach: Hardy & Littlewood [A1]. Un'argomentazione euristica elementare (non troppo dettagliata) si trova in Zaccagnini [A2]. Per il Teorema di Vinogradov: [12] Cap. 26, oppure [49] Cap. 3. Ramaré [A1], Montgomery & Vaughan [A2]. Capitolo 7: [12] Capp. 7–18, oppure [27] Capp. 11–12.

Appendici.

§A.1 Formula di Sommazione Parziale A.1.1: si veda la dimostrazione del Teorema 4.2 di [1]. Formula di Euler-McLaurin A.1.2: [1], Teorema 3.1; sue generalizzazioni in [53] Cap. 13. Lemma A.1.3: [7], Teorema 7, Cap. VI.

§A.2 Funzioni Gamma e Beta: [55] §§1.86–1.87, [12] §10. Formula di Stirling in generale: [55] §4.42.

§A.3 Formula di Stirling A.3.2: per una dimostrazione simile, ma con una conclusione leggermente piú debole, si veda [1] Teorema 3.15, oppure [55] §1.87. Una dimostrazione della Formula di Stirling completamente diversa si trova in Marsaglia & Marsaglia [A1].

§A.4 Teoremi A.4.1 e A.4.4: [1] Teorema 3.2, e [22] Teoremi 422 (per il caso $k = -1$) e 423. Per il caso di $k \in \mathbb{N}$ si veda anche Levy [A1]. Numeri di Bernoulli: [22] §7.9 o [1] §12.12.

Caratteri di Dirichlet

Per $q = 2$ c'è solo il carattere principale χ_0, mentre per $q = 3$, oltre al carattere principale $\chi_0 \mod 3$, c'è anche un altro carattere $\chi_1 \mod 3$, detto carattere quadratico, poiché $\chi_1^2 = \chi_0$. Le tabelle seguenti danno i caratteri per $q = 3$, $q = 5$ e $q = 8$. Ricordiamo che i gruppi $\mathbb{Z}_q^*$ per $q = 3$, $q = 4$ e $q = 6$ sono isomorfi a $\mathbb{Z}_2$, e quindi hanno gruppi dei caratteri isomorfi, mentre $\mathbb{Z}_5^* \simeq \mathbb{Z}_{10}^* \simeq \mathbb{Z}_4$ e $\mathbb{Z}_8^* \simeq \mathbb{Z}_{12}^* \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$.

Nelle tabelle che seguono daremo soltanto i valori dei caratteri sugli elementi di $\mathbb{Z}_n^*$; pertanto i caratteri devono essere pensati come estesi a $\mathbb{Z}$ per periodicità, ponendoli uguali a zero sulle classi di resto non indicate.

	χ_0	χ_1
1	1	1
2	1	-1

	χ_0	χ_1	χ_2	χ_3
1	1	1	1	1
2	1	i	-1	$-$ i
3	1	$-$ i	-1	i
4	1	-1	1	-1

	χ_0	χ_1	χ_2	χ_3
1	1	1	1	1
3	1	-1	-1	1
5	1	-1	1	-1
7	1	1	-1	-1

Ricordiamo che $\mathbb{Z}_7^*$ è generato da 3. Dunque i caratteri modulo 7 (e, a meno di isomorfismi, modulo 9, 14 e 18) sono i seguenti, dove ω è una radice sesta primitiva dell'unità, e soddisfa $\omega^2 - \omega + 1 = 0$.

	χ_0	χ_1	χ_2	χ_3	χ_4	χ_5
1	1	1	1	1	1	1
2	1	ω^2	$-\omega$	1	ω^2	$-\omega$
3	1	ω	ω^2	-1	$-\omega$	$-\omega^2$
4	1	$-\omega$	ω^2	1	$-\omega$	ω^2
5	1	$-\omega^2$	$-\omega$	-1	ω^2	ω
6	1	-1	1	-1	1	-1

La prossima tabella riporta i caratteri modulo 15 (ed anche, a meno di isomorfismi, modulo 16 e 20). Conviene ricordare che $\mathbb{Z}_{15}^* \simeq \mathbb{Z}_2 \times \mathbb{Z}_4$.

	χ_0	χ_1	χ_2	χ_3	χ_4	χ_5	χ_6	χ_7
1	1	1	1	1	1	1	1	1
2	1	i	-1	$-\mathrm{i}$	1	i	-1	$-\mathrm{i}$
4	1	-1	1	-1	1	-1	1	-1
7	1	$-\mathrm{i}$	-1	i	-1	i	1	$-\mathrm{i}$
8	1	$-\mathrm{i}$	-1	i	1	$-\mathrm{i}$	-1	i
11	1	-1	1	-1	-1	1	-1	1
13	1	i	-1	$-\mathrm{i}$	-1	$-\mathrm{i}$	1	i
14	1	1	1	1	-1	-1	-1	-1

Infine ecco i caratteri modulo 24. Ricordiamo che $\mathbb{Z}_{24}^* \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, dato che ogni elemento soddisfa $x^2 = 1$.

	χ_0	χ_1	χ_2	χ_3	χ_4	χ_5	χ_6	χ_7
1	1	1	1	1	1	1	1	1
5	1	-1	1	1	-1	-1	1	-1
7	1	1	-1	1	-1	1	-1	-1
11	1	-1	-1	1	1	-1	-1	1
13	1	1	1	-1	1	-1	-1	-1
17	1	-1	1	-1	-1	1	-1	1
19	1	1	-1	-1	-1	-1	1	1
23	1	-1	-1	-1	1	1	1	-1

In generale, se $p \neq 2$ ed x è un generatore di $\mathbb{Z}_p^*$, fissato $k \in \{0, \dots, p-2\}$, si ha un carattere χ_k ponendo $\chi_k\big(x^r\big) \stackrel{\text{def}}{=} e^{2\pi \mathrm{i} r k/(p-1)}$, dove evidentemente χ_0 è il carattere principale. Si osservi inoltre che i caratteri χ_1, χ_2 e χ_3 nella prima, seconda e quarta tabella rispettivamente, sono precisamente $\big(\cdot \mid p\big)$ per $p = 3$, 5 e 7. In generale, per ogni primo p, il simbolo di Legendre è un carattere.

Distribuzione dei Numeri Primi

Qui metteremo a confronto il numero esatto dei numeri primi $\le N$ con le formule approssimate proposte da Legendre, Gauss e Riemann. Ricordiamo che Legendre propose l'approssimazione $N/\log N$, Gauss $\mathrm{li}(N)$, mentre Riemann dette l'approssimazione piú complicata

$$R(N) \stackrel{\text{def}}{=} \sum_{n\ge 1} \frac{\mu(n)}{n}\,\mathrm{li}\big(N^{1/n}\big), \qquad \text{dove} \qquad \mathrm{li}(x) \stackrel{\text{def}}{=} \int_0^x \frac{\mathrm{d}t}{\log t}.$$

N	$\pi(N)$	$\Delta_L(N)$	$\Delta_G(N)$	$\Delta_R(N)$
10	4	0	2	
10^2	25	−3	5	1
10^3	168	−23	10	0
10^4	1229	−143	17	−2
10^5	9592	−906	38	−5
10^6	78498	−6116	130	29
10^7	664579	−44158	339	88
10^8	5761455	−332774	754	97
10^9	50847534	−2592592	1701	−79
10^{10}	455052511	−20758029	3104	−1828
10^{11}	4118054813	−169923159	11588	−2318
10^{12}	37607912018	−1416705183	38263	−1476
10^{13}	346065536839	−11992858452	108971	−5773
10^{14}	3204941750802	−102838308636	314890	−19200
10^{15}	29844570422669	−891604962452	1052619	73218
10^{16}	279238341033925	−7804289844393	3214632	327052
10^{17}	2623557157654233	−68883734693928	7956589	−598255
10^{18}	24739954287740860	−612483070893536	21949555	−3501366

Tavola A.1. *Le funzioni Δ_L, Δ_G e Δ_R sono definite rispettivamente da $\Delta_L(N) \stackrel{\text{def}}{=} N/\log N - \pi(N)$, $\Delta_G(N) \stackrel{\text{def}}{=} \mathrm{li}(N) - \pi(N)$ e $\Delta_R(N) \stackrel{\text{def}}{=} R(N) - \pi(N)$. I valori sono approssimati all'intero piú vicino. Questi dati sono tratti dalla Tavola 5.2 di Conway & Guy* [10]*, e dalle Tavole 26 e 27 di Ribenboim* [42].

N	$\psi(N)$	$\psi(N)-N$
10^6	999586.60	-413.40
10^7	9998539.40	-1460.60
10^8	99998242.80	-1757.20
10^9	1000001595.99	1595.99
10^{10}	10000042119.83	42119.83
10^{11}	100000058456.43	58456.43
10^{12}	1000000040136.77	40136.77
10^{13}	10000000171997.12	171997.12
10^{14}	100000000618647.55	618647.55
10^{15}	999999997476930.51	-2523069.49

Tavola A.2. *Questi dati sono tratti da Deléglise & Rivat* [A1–2].

Si calcola $\pi(x)$ in modo efficiente per mezzo di una variante della formula di Lagrange 6.1.1. Indichiamo con p_1, p_2, ... , i numeri primi in ordine crescente. Fissati a e $k \in \mathbb{N}$ poniamo

$$\varphi(x;a) \stackrel{\text{def}}{=} \bigl|\{n \le x : p \mid n \Rightarrow p > p_a\}\bigr|$$
$$P_k(x;a) \stackrel{\text{def}}{=} \bigl|\{n \le x : \Omega(n) = k \text{ e } p \mid n \Rightarrow p > p_a\}\bigr|$$

Per convenzione poniamo $P_0(x;a) \stackrel{\text{def}}{=} 1$. Raggruppando gli interi con $\Omega(n) = k$ si ha

$$\varphi(x;a) = \sum_{k=0}^{\infty} P_k(x;a),$$

dove la somma in effetti è finita poiché $P_k(x;a) = 0$ se $k \ge k_0$, dove $k_0 = k_0(a)$ è tale che $p_a^{k_0} > x$. I calcoli in Deléglise & Rivat sono fatti scegliendo $y \in \bigl[x^{1/3}, x^{1/2}\bigr]$, $a \stackrel{\text{def}}{=} \pi(y)$, da cui si ottiene $P_1(x;a) = \pi(x) - a$, $P_k(x;a) = 0$ per $k \ge 3$ e quindi

$$\pi(x) = \varphi(x;a) + a - 1 - P_2(x;a).$$

Il calcolo di φ e di P_2 è relativamente meno oneroso del Crivello di Eratostene o della formula di Lagrange. Il calcolo nel caso di ψ si basa su identità che hanno la loro origine nella teoria delle serie di Dirichlet, e non è il caso di includerle qui.

Si consultino anche le Tavole II e III di Rosser & Schoenfeld, che contengono valori numerici approssimati (con 10 cifre decimali) delle funzioni $\psi(x)$, $\sum_{p\le x} p^{-1}$, $\sum_{p\le x} (\log p)p^{-1}$ e $\prod_{p\le x} p(p-1)^{-1}$, per x fra 500 e 16000, e di $\psi(x) - \theta(x)$ per $x \le 50000$, con 15 cifre decimali.

Esercizi

Suggeriamo qualche esercizio, approssimativamente nell'ordine in cui gli argomenti sono trattati nel testo. Quelli piú difficili sono indicati da •.

§1.1 **1.1.1** Dimostrare che, fissato un intero $m \in \mathbb{Z}^*$, per ogni intero a esistono unici $q \in \mathbb{Z}$ ed $r \in \mathbb{N}$ tali che $a = mq + r$, e $0 \le r < |m|$.

1.1.2 Dimostrare che se a, $b \in \mathbb{Z}^*$, allora qualunque sia $m \in \mathbb{Z}$, $(a, b) = (b - ma, a)$.

1.1.3 Determinare tutti gli interi a e b tali che $13a + 17b = 1$.

1.1.4 Per a, $b \in \mathbb{N}$ si ha $ab = (a, b) \cdot [a, b]$.

1.1.5 Dimostrare il Corollario 1.1.8, e dedurne che $\limsup_{x\to\infty} \dfrac{\pi(x)}{\log\log x} > 0$.

§1.2 **1.2.1** Dimostrare la validità dei cosiddetti "criteri di divisibilità" per 3, 9, 11.

1.2.2 Dimostrare che $5n^3 + 7n^5 \equiv 0 \mod 12$ per ogni $n \in \mathbb{Z}$.

1.2.3 Determinare il massimo comun divisore D degli elementi di $\{n^{13} - n : n \in \mathbb{N}\}$.

1.2.4 Dimostrare che 561, 1105 e 1729 sono numeri di Carmichael.

1.2.5 Dimostrare che se $6n + 1$, $12n + 1$ e $18n + 1$ sono simultaneamente primi, allora il numero $N \stackrel{\text{def}}{=} (6n + 1)(12n + 1)(18n + 1)$ è di Carmichael.

1.2.6 Dimostrare che se p è un numero primo allora in $\mathbb{Z}_p$ l'equazione $x^2 \equiv 1 \mod p$ ha 2 soluzioni. Piú in generale, se $f \in \mathbb{Z}[x]$ ha grado ≥ 1, allora l'equazione $f(x) \equiv 0 \mod p$ ha al piú $\min\big(\deg(f), p\big)$ soluzioni. Verificare che in $\mathbb{Z}_{2^\alpha}$ l'equazione $x^2 \equiv 1 \mod 2^\alpha$ ha 4 soluzioni se $\alpha \ge 3$, e determinarle.

1.2.7 Dato il numero primo p dimostrare che $\mathbb{Z}_p$ non è un campo algebricamente chiuso utilizzando il polinomio $f(x) = x^p - x + 1$. Piú in generale, dimostrare che nessun campo finito è algebricamente chiuso, sfruttando la dimostrazione del Teorema di Wilson 1.2.7.

1.2.8 Dimostrare che se $n \ge 6$ non è primo allora $n \mid (n - 2)!$.

1.2.9 Teorema di Wilson generalizzato: determinare il valore di

$$P(n) \stackrel{\text{def}}{=} \prod_{m\in\mathbb{Z}_n^*} m \mod n.$$

Suggerimento: si consideri $P(n)^2$, e se $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ con $p_1 < p_2 < \cdots$ si calcoli $P(n)$ mod $p_j^{\alpha_j}$, $j = 1, \ldots, k$.

1.2.10 Determinare l'ordine $r = r_p$ di 8 modulo i primi $3 \le p \le 50$, ricordando che per il Teorema di Fermat 1.2.5 $r \mid p - 1$. Usare questo risultato per determinare tutti gli pseudoprimi in base 8 minori di 50.

1.2.11 Dimostrare che il polinomio $f(x) = x^4 + 1$ è riducibile su $\mathbb{Z}_p$ per ogni numero primo p, ma non su $\mathbb{Z}$. Scrivere esplicitamente la fattorizzazione completa di f quando $p = 3$, $p = 5$ e $p = 17$. Quante sono le soluzioni di $f(x) \equiv 0 \mod p$?

§1.4 **1.4.1** Dare una dimostrazione alternativa del Lemma 1.4.9 usando il fatto che per il Teorema 1.2.15, se esiste x tale che $x^2 \equiv -1 \mod p$, allora l'ordine di $\mathbb{Z}_p^*$ è divisibile per 4.

§1.6 **1.6.1** Dimostrare che se p è primo allora $p \mid \binom{p}{r}$ per $r = 1, \dots, p-1$.

1.6.2 Usare il Teorema di Fermat 1.2.5 per dimostrare che $\left(n \mid p\right) \equiv n^{(p-1)/2} \mod p$.

• **1.6.3** Dimostrare che $\left(2 \mid p\right) = (-1)^{(p^2-1)/8}$ (cfr Teorema 1.6.4). Suggerimento: sia K il campo di spezzamento di $x^8 - 1$ su $\mathbb{F}_p$ (cioè $K = \mathbb{F}_p$ se $p \equiv 1 \mod 8$, $K = \mathbb{F}_{p^2}$ altrimenti), ed u una radice ottava primitiva di 1. Si scriva $p = 8k + r$ con $k \in \mathbb{N}$ ed $r \in \mathbb{Z}$ tale che $|r| < 4$, e si osservi che detto $\alpha \stackrel{\text{def}}{=} u + u^{-1}$ si ha $\alpha^2 = 2$. Si concluda utilizzando l'osservazione 6 nella dimostrazione del Teorema 1.6.4, dato che se $|r| = 1$ allora $\alpha^p = \alpha$, mentre se $|r| = 3$ allora $\alpha^p = -\alpha$.

1.6.4 Sia $f(x) = x^2 + 3x - 1$. Dire per quali primi p l'equazione $f(x) \equiv 0 \mod p$ ha soluzione e determinarle esplicitamente, se possibile, per $p \leq 10$.

1.6.5 Risolvere se possibile l'equazione $5x^4 \equiv 1 \mod p$ per ciascun $p \leq 11$.

1.6.6 Esprimere il numero delle soluzioni della congruenza $f(x) \equiv 0 \mod p$ per mezzo del simbolo di Legendre, dove p è un numero primo ed $f(x) = ax^2 + bx + c$, a, b, $c \in \mathbb{Z}$, con $a \neq 0$. Attenzione al caso $p \mid 2a$.

§1.7 **1.7.1** Procedendo come nel Teorema 1.7.3, dimostrare che esistono infiniti primi $p \equiv 1 \mod 6$ ed infiniti primi $p \equiv 5 \mod 6$. Perché la stessa dimostrazione non funziona se consideriamo le progressioni modulo 8?

1.7.2 Dimostrare che $F_{n+1} = (F_n - 1)^2 + 1 = 2 + \prod_{i=0}^{n} F_i$. Dedurre che se $n \neq m$ allora $(F_n, F_m) = 1$ e quindi che esistono infiniti numeri primi.

1.7.3 Dimostrare che se $p = F_n$ è primo, allora h genera $\mathbb{Z}_p^*$ se e solo se $\left(h \mid p\right) = -1$.

• **1.7.4** Dimostrare che se $p \mid F_n$ allora $p \equiv 1 \mod 2^{n+2}$. Suggerimento: sia r l'ordine di 2 in $\mathbb{Z}_p^*$. Dimostrare che $r = 2^{n+1}$, osservare che $\left(2 \mid p\right) = 1$ e che per il Teorema 1.6.4 si ha $\left(2 \mid p\right) \equiv 2^{(p-1)/2} \mod p$. Dedurne che $r \mid \frac{1}{2}(p-1)$ e quindi la tesi.

1.7.5 Dimostrare che $641 \mid F_5$. Suggerimento: $641 = 2^4 + 5^4 = 5 \cdot 2^7 + 1$, e quindi $641 \mid 2^{32} + 2^{28} \cdot 5^4$ e $641 \mid 2^{28} \cdot 5^4 - 1$, ed anche la loro differenza.

1.7.6 Dimostrare i Teoremi 1.7.4 e 1.7.6.

1.7.7 Dimostrare che se $p \mid M_q$, dove p e q sono numeri primi, allora $p \equiv 1 \mod 2q$.

§2.1 **2.1.1** Sia f_n la successione definita per ricorrenza da $f_0 = a$, $f_1 = b$, ed $f_{n+2} = \alpha f_{n+1} + \beta f_n$. Dimostrare che è possibile trovare costanti γ e δ tali che $f_n = \gamma\lambda_1^n + \delta\lambda_2^n$ dove i λ sono le soluzioni distinte dell'equazione caratteristica $\lambda^2 = \alpha\lambda + \beta$, oppure $f_n = \gamma\lambda^n + n\delta\lambda^n$ se le radici sono coincidenti. In particolare determinare λ_1, λ_2, γ e δ se $a = 0$, $b = 1$, $\alpha = \beta = 1$ (numeri di Fibonacci).

2.1.2 Dimostrare che $(f_n, f_{n+1}) = 1$ dove gli f_n sono i numeri di Fibonacci definiti nell'esercizio precedente. Dimostrare che il calcolo di (f_n, f_{n+1}) richiede $n - 2$ passi dell'algoritmo

di Euclide. Dimostrare che se $1 \le a < b$ sono interi per cui il calcolo di (a, b) richiede $n-2$ passi nell'algoritmo di Euclide, allora $f_n \le a$. Se ne deduca che se $2 \le a < b$ l'algoritmo di Euclide richiede al piú $c \log a$ passi, dove $c \approx 1.6$. Dimostrare inoltre che i numeri di Fibonacci hanno le seguenti proprietà:

$$f_{n+2} = f_{k+1} f_{n+2-k} + f_k f_{n+1-k} \qquad \text{per ogni } k \in \mathbb{N} \text{ con } k \le n+1$$
$$f_{n+1}^2 = f_n f_{n+2} + (-1)^n.$$

§2.4 **2.4.1** Come scomporre "a mano" il numero di Jevons $N = 8\,616\,460\,799$. Si calcoli $N \bmod m$ per $m = 5$, 8, 9, 11, e si determinino le classi di resto modulo m in cui può giacere un'eventuale soluzione intera x dell'eqazione $x^2 - y^2 = N$. Da questi calcoli segue che $x \equiv 0 \mod 12$. Utilizzando il fatto che x soddisfa anche congruenze mod 5 e 11, si cerchino possibili soluzioni fra gli x interi $\ge \lceil \sqrt{N} \rceil = 92825$.

§2.8 **2.8.1** Decifrare il messaggio qui sotto sapendo che è stato cifrato con la tecnica e con l'alfabeto descritti nella didascalia della Tavola 2.4, e che la chiave pubblica utilizzata è $(n, e) = (2109137, 10001)$. Il messaggio da decifrare è 744567, 1726777, 1556755, 957672, 689457, 858349, 866725.

§3.1 **3.1.1** Dimostrare che nell'anello delle funzioni aritmetiche, la moltiplicazione puntuale per L è una derivazione, cioè che per ogni f, $g : \mathbb{N}^* \to \mathbb{C}$ e per ogni $c \in \mathbb{C}$ si ha $L(cf) = cLf$, $L(f+g) = Lf + Lg$ e $L(f * g) = (Lf) * g + f * (Lg)$.

3.1.2 Dimostrare che posto $f(n) \stackrel{\text{def}}{=} \lfloor \sqrt{n} \rfloor - \lfloor \sqrt{n-1} \rfloor$, $f \in \mathfrak{M} \setminus \mathfrak{M}^*$.

3.1.3 Dimostrare che $N_k \in \mathfrak{M}^*$ per ogni $k \in \mathbb{C}$, ma che $N_0 * N_0 = d \notin \mathfrak{M}^*$.

3.1.4 Dare una dimostrazione alternativa del Teorema 3.1.9 osservando che se $n > 1$ ha la forma canonica $\prod_{i=1}^{k} p_i^{\alpha_i}$, allora gli unici termini diversi da zero nella somma $(N_0 * \mu)(n) = \sum_{d|n} \mu(d)$ sono quelli per cui d divide $p_1 \cdots p_k$.

• **3.1.5** Utilizzando la Formula (3.1.12) dimostrare che per ogni $x \ge 1$ si ha

$$\sum_{d \le x} \mu(d) \left[\frac{x}{d} \right] = 1.$$

Se ne deduca che $\sum_{n \le x} \mu(n) n^{-1}$ è limitata.

§3.2 **3.2.1** Dimostrare che se $n = x_1^2 + x_2^2 = y_1^2 + y_2^2$ con $0 < x_1 < y_1 < y_2 < x_2$, allora è possibile determinare due fattori non banali di n.

3.2.2 Utilizzando il Teorema 3.2.1 con $p = 5$ ed $n = 5^\alpha$, si dimostri che

$$\limsup_{n \to \infty} \frac{r_2(n)}{\log n} \ge \frac{4}{\log 5}.$$

3.2.3 Procedendo come nella dimostrazione del Teorema di Gauss 3.2.2, si dimostri che

$$R_k(x) \stackrel{\text{def}}{=} \sum_{n \le x} r_k(n) = V_k x^{k/2} + \mathcal{O}_k\Big(x^{(k-1)/2}\Big),$$

dove V_k indica il volume della sfera unitaria di $\mathbb{R}^k$.

3.2.4 Si sfrutti il Teorema di Landau 3.2.3 per dimostrare che

$$\max_{n\le x} r_2(n) \ge \pi\sqrt{K\log x}\big(1+o(1)\big),$$

dove K è la costante nel Teorema. Suggerimento: $\sum_{n\le x} r_2(n) \le (\max_{n\le x} r_2(n))\cdot R_2'(x)$.

3.2.5 Dato $n\in\mathbb{N}^*$ determinare $\big|\{(x,y)\in\mathbb{N}^2 : n = x^2-y^2\}\big|$.

3.2.6 Dimostrare che $d(n)$ è dispari se e solo se $n=m^2$.

3.2.7 Per $k\in\mathbb{N}^*$ si ponga $d_k \stackrel{\text{def}}{=} N_0 * \cdots * N_0$, dove ci sono k fattori (e quindi $d_2 = d$). Dimostrare che $d_k\in\mathfrak{M}$ e che $d_k\big(p^\alpha\big) = \binom{\alpha+k-1}{k-1}$.

3.2.8 Dimostrare che esistono a, b, $c\in\mathbb{R}$ tali che $\sum_{n\le x} d_3(n) = x(a\log^2 x + b\log x + c) + \mathcal{O}\big(x^{2/3}\log x\big)$. Suggerimento: usare la formula di Euler-McLaurin A.1.2.

- **3.2.9** (Euclide–Eulero) Il numero $n\in\mathbb{N}$ si dice perfetto se $\sigma(n) = 2n$, cioè se n è uguale alla somma dei suoi divisori proprî. Dimostrare che n è un numero perfetto pari se e solo se esiste un numero primo p tale che $M_p = 2^p-1$ è primo ed inoltre $n = 2^{p-1}\big(2^p-1\big)$. Non è noto se esistano numeri perfetti dispari.

3.2.10 Determinare tutti gli $n\in\mathbb{N}^*$ per cui $\varphi(n)\not\equiv 0 \mod 4$ e quelli per cui $\varphi(n)\mid n$.

3.2.11 Dimostrare che $\varphi(n)\ne 14$ per ogni $n\in\mathbb{N}^*$.

3.2.12 Dimostrare che se $\mu(n)\ne 0$ e si conosce $\varphi(n)n^{-1}$, è possibile determinare n.

§3.4 **3.4.1** Dimostrare che $\sum_{n\ge1} a_n n^{-s}$ converge in qualche insieme se e solo se esiste $c\in\mathbb{R}$ tale che $a_n = \mathcal{O}(n^c)$, e quindi la serie converge assolutamente per $\sigma > c+1$.

§4.1 **4.1.1** Dimostrare che $\psi(x) = \log\big[1,\,2,\,\dots,\,[x]\big]$.

4.1.2 Dimostrare che se p è primo e $p^\alpha \parallel n!$, allora

$$\alpha = \sum_{r\ge1}\left[\frac{n}{p^r}\right] \le \frac{n}{p-1}.$$

4.1.3 Con quante cifre 0 termina la rappresentazione decimale di 1000!?

4.1.4 Senza usare il Teorema dei Numeri Primi 4.1.3 dimostrare che dato $n\in\mathbb{N}$ è possibile trovare n interi consecutivi non primi.

§4.2 **4.2.1** Dimostrare per induzione la formula (4.2.2).

4.2.2 Dimostrare che $\psi(x)\ge \frac12 x\log 5 + \mathcal{O}(1)$ usando il polinomio $f(x) = x^4(1-2x)^2(1-x)^4$ nella dimostrazione del Teorema 4.2.2.

- **4.2.3** (Postulato di Bertrand) Dimostrare che $\pi(2x)-\pi(x) > 0$ per ogni $x\ge 2$.

§4.3 **4.3.1** Dimostrare il Corollario 4.3.5 usando la terza formula di Mertens (4.3.3).

§4.5 **4.5.1** Utilizzando il Teorema dei Numeri Primi 4.1.3, dimostrare che

$$\lambda \stackrel{\text{def}}{=} \liminf_{n\to+\infty} \frac{p_{n+1}-p_n}{\log p_n} \le 1, \qquad \Lambda \stackrel{\text{def}}{=} \limsup_{n\to+\infty} \frac{p_{n+1}-p_n}{\log p_n} \ge 1.$$

4.5.2 Dimostrare che per ogni $c > 1$ fissato si ha $\pi(cx) - \pi(x) \sim \frac{(c-1)x}{\log x}$.

4.5.3 Dimostrare per induzione la formula (4.5.7).

§4.6 **4.6.1** Dimostrare che

$$\sum_{d\geq y} \frac{\mu(d)}{d^2} = \mathcal{O}\big(y^{-1}\big) \quad \text{e che} \qquad \sum_{d\geq 1} \frac{\mu(d)}{d^2} = \frac{1}{\zeta(2)} = \left(\sum_{d\geq 1} \frac{1}{d^2}\right)^{-1}.$$

§4.7 **4.7.1** Dimostrare le formule (4.7.1).

§5.1 **5.1.1** Dato $q \in \mathbb{N}^*$, si chiami A la matrice quadrata di ordine $\varphi(q)$ dei caratteri modulo q. In altre parole, se $1 = a_1 < a_2 < \cdots < a_{\varphi(q)} = q-1$ sono gli interi fra 1 e q primi con q, e $\chi_0, \ldots, \chi_{\varphi(q)-1}$ sono i $\varphi(q)$ caratteri modulo q, allora $A_{i,j} = \chi_{j-1}\big(a_i\big)$. Determinare $|\det(A)|$. Suggerimento: sia $B = \overline{A}$. Allora $|\det(A)|^2 = \det(A)\det(B) = \det(AB)$ ed $AB = \varphi(q) I_{\varphi(q)}$, dove I_k è la matrice identica k per k.

- **5.1.2** Dimostrare che se $X\colon \mathbb{N}^* \to \mathbb{C}$, $X \in \mathfrak{M}^*$ è periodica con periodo $q \geq 1$ e tale che $X(n) = 0$ se $(n, q) > 1$, allora X è uno dei caratteri modulo q. Suggerimento: dato χ carattere modulo q, si consideri $\sum_{a \mod q} X(a)\overline{\chi}(a)$.

§5.4 **5.4.1** Dimostrare che se χ è un carattere modulo q ed n è un intero tale che $\chi(n) = 0$ allora $\sum_{h \mod q} \chi(h) e_q(nh) = 0$.

§6.1 **6.1.1** Dimostrare il Principio di Inclusione-Esclusione 6.1.2 utilizzando la formula

$$\left|\bigcap_{i\in I} B_i\right| = \sum_{\substack{J\subseteq I \\ J\neq\emptyset}} (-1)^{1+|J|} \left|\bigcup_{j\in J} B_j\right|$$

valida qualunque sia l'insieme finito I e qualunque siano gli insiemi finiti B_i, $i \in I$. Suggerimento: Porre $I \stackrel{\text{def}}{=} \{p\colon p \mid M\}$, $B_d \stackrel{\text{def}}{=} \mathbb{N} \cap [1, x] \setminus \mathcal{A}_d$ ed utilizzare il Teorema 3.1.9.

6.1.2 Utilizzando alcuni degli esercizi precedenti, dimostrare la Formula di Lagrange (6.1.1) osservando che

$$\pi(x) = \pi\big(x^{1/2}\big) + \sum_{x^{1/2}<p\leq x} 1 = \pi\big(x^{1/2}\big) + \sum_{x^{1/2}<p\leq x} \sum_{d\leq x/p} \mu(d) \left[\frac{x}{pd}\right].$$

§6.2 **6.2.1** Dimostrare che la funzione ϱ definita nel Lemma 6.2.3 è moltiplicativa.

6.2.2 Dato $f \in \mathbb{Z}[x]$ poniamo $\varphi_f(n) \stackrel{\text{def}}{=} |\{m \in \mathbb{N} \cap [1, n]\colon \big(n, f(m)\big) = 1\}|$. Dimostrare che $\varphi_f \in \mathfrak{M}$ e che se $\varrho_f(p) \stackrel{\text{def}}{=} |\{n \mod p\colon f(n) \equiv 0 \mod p\}|$, allora

$$\varphi_f(n) = n \prod_{p\mid n} \left(1 - \frac{\varrho_f(p)}{p}\right).$$

6.2.3 Dimostrare che se $n_i \geq 0$ per $i = 1, \dots, k$, allora $N \stackrel{\text{def}}{=} \frac{(n_1+\cdots+n_k)!}{n_1!\, n_2! \cdots n_k!}$ è un intero.

6.2.4 Dimostrare che se f è sviluppabile in serie di Taylor in un intorno del punto $\underline{x} = (x_1, \dots, x_n) \in \mathbb{R}^n$, allora nella notazione del Lemma 6.2.6 si ha

$$f\big(\underline{x} + \underline{\xi}\big) = \sum_{r \geq 0} \frac{1}{r!} \sum_{\underline{\alpha} \in \mathfrak{A}(r)} c(\underline{\alpha}) \frac{\partial^{|\underline{\alpha}|} f}{\partial x_1^{\alpha_1} \cdots \partial x_n^{\alpha_n}} (\underline{x})\, \underline{\xi}^{\underline{\alpha}}.$$

§6.3 **6.3.1** (Brun) Dimostrare che $\sum p^{-1}$, dove la somma è estesa a tutti i numeri primi p tali che $p + h$ è primo ed $h \in \mathbb{N}^*$ è fissato, è convergente.

§6.5 **6.5.1** Posto $\Omega_2 \stackrel{\text{def}}{=} \emptyset$, $\Omega_p \stackrel{\text{def}}{=} \{n \mod p \colon \big(n \mid p\big) = -1\}$ per $p > 2$, dimostrare che $|\{n \leq x \colon n = m^2\}| = \mathcal{O}\big(x^{1/2}\big)$ per mezzo del Teorema 6.4.8.

• **6.5.2** Fissato $h \in \mathbb{N}^*$ e posto $\Omega_p \stackrel{\text{def}}{=} \{0\}$ se $p \mid h$, $\Omega_p \stackrel{\text{def}}{=} \emptyset$ altrimenti, dimostrare che $|\{n \leq x \colon (n, h) = 1\}| \leq \frac{\varphi(h)}{h} x + 2h\varphi(h)$. Se $\mu(h) \neq 0$, posto invece $\Omega_p \stackrel{\text{def}}{=} \mathbb{Z}_p \setminus \{0\}$ se $p \mid h$, $\Omega_p \stackrel{\text{def}}{=} \emptyset$ altrimenti, dimostrare che $|\{n \leq x \colon h \mid n\}| \leq \frac{1}{h} x + 2h$.

§7.1 **7.1.1** Dimostrare che per ogni $n \in \mathbb{N}^*$ si ha $\zeta(2n)\pi^{-2n} \in \mathbb{Q}^+$. In particolare, $\zeta(2) = \frac{\pi^2}{6}$, $\zeta(4) = \frac{\pi^4}{90}$ e $\zeta(6) = \frac{\pi^6}{945}$. Suggerimento: sviluppare in serie di Fourier sull'intervallo $[-\pi, \pi]$ la funzione $f(x) = x^n$, e poi usare l'identità di Parseval, procedendo per induzione.

7.1.2 Dimostrare che $\sum_{n \leq x} \log^2 n = x(\log^2 x - 2 \log x + 2) + \mathcal{O}\big((\log x)^2\big)$. Suggerimento: usare la formula di Euler-McLaurin A.1.2.

• **7.1.3** (Ingham) Dimostrare che per $\sigma > 1$ vale l'identità

$$\left(\frac{\zeta'}{\zeta}\right)' + \left(\frac{\zeta'}{\zeta}\right)^2 = \frac{\zeta''}{\zeta}.$$

Riconoscere che la somma dei coefficienti a_n con $n \leq x$ delle due serie di Dirichlet è il primo membro di una delle formule di Selberg 4.4.2. Usando anche alcuni degli esercizi precedenti, dimostrare che esistono costanti a, b, $c \in \mathbb{R}$ tali che per $\sigma > 1$ $\zeta''(s) = a\zeta(s)^3 + b\zeta(s)^2 + c\zeta(s) + \sum_{n \geq 1} a_n n^{-s}$ dove $\sum_{n \leq x} a_n = \mathcal{O}(x^\alpha)$ per qualche $\alpha < 1$. Utilizzare tutti questi risultati per dimostrare le formule di Selberg. In un certo senso, si può dire che la dimostrazione elementare data nel Capitolo 4 "corrisponde" a dimostrare queste relazioni senza usare l'analisi complessa.

§A1 **A1.1** Dimostrare la formula di sommazione di Euler-McLaurin A.1.2 per mezzo della Formula di Sommazione Parziale A.1.1. Suggerimento: sfruttare il fatto che $\sum_{x < n \leq t} 1 = [t] - [x] = t - x - \{t\} + \{x\}$, e poi integrare per parti la funzione $tf'(t)$.

§A3 **A3.1** Ridimostrare la formula di Stirling A.3.2 mediante la formula di Euler-McLaurin A.1.2.

§A4 **A4.1** Ridimostrare il Teorema A.4.1 per mezzo della formula di Euler-McLaurin A.1.2.

Altri esercizi si possono trovare nei libri di Apostol [1], di Hua [23] e di Landau [31].

Funzioni Aritmetiche Elementari

Queste Tavole contengono i valori delle funzioni aritmetiche elementari per $1 \leq n \leq 120$.

n	φ	d	μ	ω	Ω	Λ
1	1	1	1	0	0	0
2	1	2	−1	1	1	$\log 2$
3	2	2	−1	1	1	$\log 3$
4	2	3	0	1	2	$\log 2$
5	4	2	−1	1	1	$\log 5$
6	2	4	1	2	2	0
7	6	2	−1	1	1	$\log 7$
8	4	4	0	1	3	$\log 2$
9	6	3	0	1	2	$\log 3$
10	4	4	1	2	2	0
11	10	2	−1	1	1	$\log 11$
12	4	6	0	2	3	0
13	12	2	−1	1	1	$\log 13$
14	6	4	1	2	2	0
15	8	4	1	2	2	0
16	8	5	0	1	4	$\log 2$
17	16	2	−1	1	1	$\log 17$
18	6	6	0	2	3	0
19	18	2	−1	1	1	$\log 19$
20	8	6	0	2	3	0
21	12	4	1	2	2	0
22	10	4	1	2	2	0
23	22	2	−1	1	1	$\log 23$
24	8	8	0	2	4	0
25	20	3	0	1	2	$\log 5$
26	12	4	1	2	2	0
27	18	4	0	1	3	$\log 3$
28	12	6	0	2	3	0
29	28	2	−1	1	1	$\log 29$
30	8	8	−1	3	3	0

n	φ	d	μ	ω	Ω	Λ
31	30	2	−1	1	1	$\log 31$
32	16	6	0	1	5	$\log 2$
33	20	4	1	2	2	0
34	16	4	1	2	2	0
35	24	4	1	2	2	0
36	12	9	0	2	4	0
37	36	2	−1	1	1	$\log 37$
38	18	4	1	2	2	0
39	24	4	1	2	2	0
40	16	8	0	2	4	0
41	40	2	−1	1	1	$\log 41$
42	12	8	−1	3	3	0
43	42	2	−1	1	1	$\log 43$
44	20	6	0	2	3	0
45	24	6	0	2	3	0
46	22	4	1	2	2	0
47	46	2	−1	1	1	$\log 47$
48	16	10	0	2	5	0
49	42	3	0	1	2	$\log 7$
50	20	6	0	2	3	0
51	32	4	1	2	2	0
52	24	6	0	2	3	0
53	52	2	−1	1	1	$\log 53$
54	18	8	0	2	4	0
55	40	4	1	2	2	0
56	24	8	0	2	4	0
57	36	4	1	2	2	0
58	28	4	1	2	2	0
59	58	2	−1	1	1	$\log 59$
60	16	12	0	3	4	0

n	φ	d	μ	ω	Ω	Λ
61	60	2	-1	1	1	$\log 61$
62	30	4	1	2	2	0
63	36	6	0	2	3	0
64	32	7	0	1	6	$\log 2$
65	48	4	1	2	2	0
66	20	8	-1	3	3	0
67	66	2	-1	1	1	$\log 67$
68	32	6	0	2	3	0
69	44	4	1	2	2	0
70	24	8	-1	3	3	0
71	70	2	-1	1	1	$\log 71$
72	24	12	0	2	5	0
73	72	2	-1	1	1	$\log 73$
74	36	4	1	2	2	0
75	40	6	0	2	3	0
76	36	6	0	2	3	0
77	60	4	1	2	2	0
78	24	8	-1	3	3	0
79	78	2	-1	1	1	$\log 79$
80	32	10	0	2	5	0
81	54	5	0	1	4	$\log 3$
82	40	4	1	2	2	0
83	82	2	-1	1	1	$\log 83$
84	24	12	0	3	4	0
85	64	4	1	2	2	0
86	42	4	1	2	2	0
87	56	4	1	2	2	0
88	40	8	0	2	4	0
89	88	2	-1	1	1	$\log 89$
90	24	12	0	3	4	0

n	φ	d	μ	ω	Ω	Λ
91	72	4	1	2	2	0
92	44	6	0	2	3	0
93	60	4	1	2	2	0
94	46	4	1	2	2	0
95	72	4	1	2	2	0
96	32	12	0	2	6	0
97	96	2	-1	1	1	$\log 97$
98	42	6	0	2	3	0
99	60	6	0	2	3	0
100	40	9	0	2	4	0
101	100	2	-1	1	1	$\log 101$
102	32	8	-1	3	3	0
103	102	2	-1	1	1	$\log 103$
104	48	8	0	2	4	0
105	48	8	-1	3	3	0
106	52	4	1	2	2	0
107	106	2	-1	1	1	$\log 107$
108	36	12	0	2	5	0
109	108	2	-1	1	1	$\log 109$
110	40	8	-1	3	3	0
111	72	4	1	2	2	0
112	48	10	0	2	5	0
113	112	2	-1	1	1	$\log 113$
114	36	8	-1	3	3	0
115	88	4	1	2	2	0
116	56	6	0	2	3	0
117	72	6	0	2	3	0
118	58	4	1	2	2	0
119	96	4	1	2	2	0
120	32	16	0	3	5	0

Generatori e Ordini modulo p

p, n	2	3	4	5	6	7	8	9	10	11	12	13
2		$1^\star$		$1^\star$		$1^\star$		$1^\star$		$1^\star$		$1^\star$
3	$2^\star$		1	$2^\star$		1	$2^\star$		1	$2^\star$		1
5	$4^\star$	$4^\star$	2		1	$4^\star$	$4^\star$	2		1	$4^\star$	$4^\star$
7	3	$6^\star$	3	$6^\star$	2		1	3	$6^\star$	3	$6^\star$	2
11	$10^\star$	5	5	5	$10^\star$	$10^\star$	$10^\star$	5	2		1	$10^\star$
13	$12^\star$	3	6	4	$12^\star$	$12^\star$	4	3	6	$12^\star$	2	
17	8	$16^\star$	4	$16^\star$	$16^\star$	$16^\star$	8	8	$16^\star$	$16^\star$	$16^\star$	4
19	$18^\star$	$18^\star$	9	9	9	3	6	9	$18^\star$	3	6	$18^\star$
23	11	11	11	$22^\star$	11	$22^\star$	11	11	$22^\star$	$22^\star$	11	11
29	$28^\star$	$28^\star$	14	14	14	7	$28^\star$	14	$28^\star$	$28^\star$	4	14
31	5	$30^\star$	5	3	6	15	5	15	15	$30^\star$	$30^\star$	$30^\star$
37	$36^\star$	18	18	$36^\star$	4	9	12	9	3	6	9	$36^\star$
41	20	8	10	20	$40^\star$	$40^\star$	20	4	5	$40^\star$	$40^\star$	$40^\star$
43	14	$42^\star$	7	$42^\star$	3	6	14	21	21	7	$42^\star$	21
47	23	23	23	$46^\star$	23	23	23	23	$46^\star$	$46^\star$	23	$46^\star$
53	$52^\star$	$52^\star$	26	$52^\star$	26	26	$52^\star$	26	13	26	$52^\star$	13
59	$58^\star$	29	29	29	$58^\star$	29	$58^\star$	29	$58^\star$	$58^\star$	29	$58^\star$
61	$60^\star$	10	30	30	$60^\star$	$60^\star$	20	5	$60^\star$	4	15	3
67	$66^\star$	22	33	22	33	$66^\star$	22	11	33	$66^\star$	$66^\star$	$66^\star$
71	35	35	35	5	35	$70^\star$	35	35	35	$70^\star$	35	$70^\star$

Gli ordini degli interi $n = 2, \ldots, 13$ modulo i primi $p = 2, \ldots, 31$. Le colonne corrispondenti ai generatori sono indicate da un $\star$.

$341 = 11 \cdot 31$	$2^{10} \equiv 1\ (341)$	$10 \mid 340$	$561 = 3 \cdot 11 \cdot 17$	$5^{80} \equiv 1\ (561)$	$80 \mid 560$
$561 = 3 \cdot 11 \cdot 17$	$2^{40} \equiv 1\ (561)$	$40 \mid 560$	$35 = 5 \cdot 7$	$6^2 \equiv 1\ (35)$	$2 \mid 34$
$645 = 3 \cdot 5 \cdot 43$	$2^{28} \equiv 1\ (645)$	$28 \mid 644$	$217 = 7 \cdot 31$	$6^6 \equiv 1\ (217)$	$6 \mid 216$
$91 = 7 \cdot 13$	$3^6 \equiv 1\ (91)$	$6 \mid 90$	$25 = 5^2$	$7^4 \equiv 1\ (25)$	$4 \mid 24$
$703 = 19 \cdot 37$	$3^{18} \equiv 1\ (703)$	$18 \mid 702$	$561 = 3 \cdot 11 \cdot 17$	$7^{80} \equiv 1\ (561)$	$80 \mid 560$
$15 = 3 \cdot 5$	$4^2 \equiv 1\ (15)$	$2 \mid 14$	$9 = 3^2$	$8^2 \equiv 1\ (9)$	$2 \mid 8$
$85 = 5 \cdot 17$	$4^8 \equiv 1\ (85)$	$8 \mid 84$	$21 = 3 \cdot 7$	$8^2 \equiv 1\ (21)$	$2 \mid 20$
$561 = 3 \cdot 11 \cdot 17$	$4^{20} \equiv 1\ (561)$	$20 \mid 560$	$45 = 3^2 \cdot 5$	$8^4 \equiv 1\ (45)$	$4 \mid 44$
$217 = 7 \cdot 31$	$5^6 \equiv 1\ (217)$	$6 \mid 216$	$65 = 5 \cdot 13$	$8^4 \equiv 1\ (65)$	$4 \mid 64$

Alcuni pseudoprimi nelle basi 2, ... , 8. La prima colonna contiene la fattorizzazione dello pseudoprimo, la seconda la congruenza soddisfatta con il minimo esponente possibile. Per motivi di spazio la congruenza $\alpha \equiv \beta \mod n$ è stata scritta nella forma alternativa $\alpha \equiv \beta(n)$.

Osserviamo che questa tabella può essere costruita abbastanza rapidamente a partire da quella alla pagina precedente. Per esempio, vogliamo determinare gli pseudoprimi in base $a > 1$ della forma $n = pq$ ($p < q$ primi). Siano rispettivamente r_p ed r_q gli ordini di a mod p e mod q, ricavati dalla tabella alla pagina precedente. Ma

$$a^{n-1} \equiv 1 \mod n \quad \Longleftrightarrow \quad \begin{cases} a^{pq-1} \equiv 1 \mod p \\ a^{pq-1} \equiv 1 \mod q \end{cases} \quad \Longleftrightarrow \quad \begin{cases} r_p \mid pq-1 \\ r_q \mid pq-1. \end{cases}$$

Dato che $pq - 1 = q(p-1) + q - 1 = p(q-1) + p - 1$ e che $r_p \mid p-1$, $r_q \mid q-1$, queste ultime relazioni equivalgono a

$$\begin{cases} p \equiv 1 \mod r_q, \\ q \equiv 1 \mod r_p. \end{cases}$$

Indice

Capitolo 0. Simboli e Notazioni 1

Capitolo 1. Risultati Elementari 3
1.1. L'algoritmo di Euclide 3
1.2. Congruenze: i teoremi di Fermat, Eulero, Wilson e Gauss 4
1.3. Terne pitagoriche 7
1.4. Somme di due e tre quadrati 9
1.5. Il teorema dei quattro quadrati 12
1.6. La legge di reciprocità quadratica 13
1.7. Formule per i numeri primi 15

Capitolo 2. Algoritmi Fondamentali e Crittografia 17
2.1. L'algoritmo di Euclide 17
2.2. Il crivello di Eratostene 18
2.3. Criteri di primalità 18
2.4. Algoritmi di fattorizzazione 19
2.5. Radici primitive 23
2.6. Logaritmo discreto 23
2.7. Numeri pseudocasuali 24
2.8. Applicazioni alla crittografia 25
2.9. Calcolo di prodotti e potenze modulo N 27

Capitolo 3. Funzioni Aritmetiche 29
3.1. Definizioni e prime proprietà 29
3.2. Le funzioni r_2, d, σ_k, φ, Λ e c_q 33
3.3. Il prodotto di Eulero 36
3.4. Serie di Dirichlet formali 38

Capitolo 4. Distribuzione dei Numeri Primi 39
4.1. Risultati elementari 39
4.2. I teoremi di Chebyshev 40
4.3. Le formule di Mertens 42
4.4. Le formule di Selberg 43
4.5. Dimostrazione del teorema dei numeri primi 46
4.6. Altri risultati su alcune funzioni aritmetiche 51
4.7. Considerazioni finali 56

Capitolo 5. Primi nelle Progressioni Aritmetiche 57
5.1. Caratteri di un gruppo abeliano 57
5.2. Caratteri e funzioni L di Dirichlet 59
5.3. Il teorema di Dirichlet 63
5.4. La disuguaglianza di Pólya–Vinogradov 63
5.5. Il teorema di Gauss-Jacobi 65

Capitolo 6. Metodi di Crivello 67
6.1. Il principio di inclusione–esclusione e la formula di Lagrange 67
6.2. Il crivello di Brun 68
6.3. Applicazioni del crivello di Brun 72
6.4. Il crivello "grande" 75
6.5. Applicazioni del crivello grande 79

Capitolo 7. Introduzione alla Teoria Analitica dei Numeri 83
7.1. La funzione zeta di Riemann 83
7.2. Proprietà della funzione zeta: distribuzione degli zeri 87
7.3. La formula esplicita 89
7.4. Dimostrazione del teorema dei numeri primi 90
7.5. La congettura di Riemann 90
7.6. Considerazioni finali 91

Capitolo 8. Il problema di Goldbach 95
8.1. Problemi additivi: il metodo del cerchio 95
8.2. Il problema di Goldbach 98
8.3. Dove sono le difficoltà? 103
8.4. Risultati "per quasi tutti" gli interi pari 105
8.5. Varianti: il teorema dei tre primi ed i primi gemelli 106

Capitolo 9. Problemi Aperti 107

Appendici 111
A1. Formule di sommazione 111
A2. Le funzioni Gamma e Beta 113
A3. Formula di Stirling 113
A4. Lemmi 115

Bibliografia 117
B1. Riferimenti Bibliografici 117
B2. Fonti e Letture Ulteriori 121

Caratteri di Dirichlet 125

Distribuzione dei Numeri Primi 127

Esercizi 129

Funzioni Aritmetiche Elementari 135

Generatori e Ordini modulo p 137

Indice 139