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

Introduzione alla Teoria Analitica dei Numeri

Alessandro Zaccagnini

(versione preliminare 12 settembre 2012)

Anno Accademico 2008–2009

Il testo è stato composto per mezzo di un pacchetto di macro creato dall'Autore e basato su LaTeX 2ε, © American Mathematical Society. La figure sono state create con MetaPost. L'ultima versione di questo testo è disponibile all'indirizzo
http://www.math.unipr.it/~zaccagni/psfiles/lezioni/tdn2005.pdf
La data di questa versione è 12 settembre 2012.

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

Prof. Alessandro Zaccagnini
Dipartimento di Matematica
Università degli Studi di Parma
Parco Area delle Scienze, 53/a – Campus Universitario
43100 Parma, ITALIA
Tel. 0521 906902 – Telefax 0521 906950
e-mail: alessandro.zaccagnini@unipr.it
pagina web: http://www.math.unipr.it/~zaccagni/home.html

Indice

Simboli e notazioni

Scriveremo $f := g$ 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.

Quasi sempre p_n indica l'n-esimo numero primo, e $\log_n x$ l'iterata n-esima della funzione logaritmo: $\log_2 x := \log\log x$ e $\log_{n+1} x := \log\log_n x$ per $n \geq 2$.

Scriveremo

$$\sum_{d \mid n} \qquad \sum_{a \bmod q} \qquad \sum_{a \bmod q}^{*}$$

rispettivamente per indicare una somma estesa a tutti i divisori *positivi* d di n (anche quando n è un numero negativo), per indicare una somma su tutte le classi di resto modulo q o su tutte le classi $a \bmod q$ con $(a,q) = 1$ (quando queste somme sono ben definite). Le somme e i prodotti indicati con

$$\sum_{n \leq x} \qquad \text{oppure} \qquad \prod_{n \leq x}$$

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 $[x] := \max\{n \in \mathbb{Z}\colon n \le x\}$ indichiamo la parte intera del numero reale x, e con $\{x\} := x - [x] \in [0,1)$ 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 $\mathrm{e}(x)$ la funzione esponenziale complessa $\mathrm{e}^{2\pi \mathrm{i} x}$ (di solito quando x è un numero reale) e con $\mathrm{e}_q(x)$ la funzione $\mathrm{e}\big(x/q\big)$.

Useremo i simboli di Bachmann–Landau (o, 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 $+\infty$). Se g è non negativa in un intorno di x_0 scriviamo $f(x) = O(g(x))$ 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

$$|f(x)| \le C g(x).$$

Se la costante C non è uniforme, ma dipende dai parametri A, B, $\dots$, scriveremo $f(x) = O_{A,B,\dots}(g(x))$ 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 §2.4, la funzioni Γ e B di Eulero nell'Appendice A.2.

Struttura

Per quanto possibile queste dispense sono autocontenute. Solo qualche risultato
Ɛ 1.2.3 è 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.

Ogni paragrafo contiene un elenco di esercizi e riferimenti bibliografici per approfondimenti. Altri esercizi si possono trovare nei libri di Apostol [5], di Hua [69] e di Landau [85]. Nel paragrafo finale di ogni capitolo presentiamo informalmente e rapidamente alcuni dei piú importanti problemi aperti pertinenti. La scelta naturalmente è arbitraria e discutibile: per una panoramica ben piú vasta, si vedano i libri di Guy [49], di Ribenboim [128] e di Shanks [135].

Un'introduzione molto semplice e discorsiva agli argomenti trattati si trova nel libro di Beiler [8]. La storia della Teoria dei Numeri è trattata in enorme dettaglio nei volumi di Dickson [27], e piú in generale in Ore [113].

Altre letture consigliate sono i libri di Gauss [40], Knopfmacher [77], Landau [83], Narkiewicz [110], Nathanson [111], Prachar [126], Turán [139], Lang [86]. Il libro di Montgomery & Vaughan [105] contiene gli sviluppi della teoria svolta qui ed è un ottimo libro per approfondire seriamente il contenuti di questo corso; inoltre, contiene anche diverse centinaia di esercizi. Si veda anche l'Enciclopedia on-line delle successioni di interi all'indirizzo `http://www.research.att.com/~njas/sequences/`

Ringraziamenti

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

Capitolo 1

Risultati Elementari

In questo Capitolo iniziale parleremo di divisibilità, congruenze e della struttura dei gruppi $\mathbb{Z}_n$ e $\mathbb{Z}_n^*$. Affronteremo anche qualche problema classico o elementare come la determinazione di tutte le terne pitagoriche e dell'insieme degli interi che si possono rappresentare come somma di due o di quattro quadrati di numeri interi. Concluderemo con un importante Teorema di Gauss (la Legge di Reciprocità Quadratica) e con una discussione sulla possibilità di trovare "formule" per ottenere numeri primi.

1.1 L'algoritmo di Euclide

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

𝔈 1-3 **Dim.** È evidente che d divide ogni elemento di $\mathcal{A}$. Sia $\delta = \lambda n + \mu m$ il minimo elemento positivo di $\mathcal{A}$ (che esiste perché almeno uno fra n e m non è 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 Teorema 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* fattorizzazione 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 $n = 1$ allora $k = 0$ e il prodotto è vuoto.

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

Dim. Sia $n \geq 2$ il piú piccolo numero naturale con due fattorizzazioni canoniche diverse

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

con le convenzioni della Definizione 1.1.4. 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 fattorizzazioni canoniche distinte, contro la minimalità di n. □

𝔈 5 **Corollario 1.1.6** *Se $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ con p_i ed α_i come nella Definizione 1.1.4, e $d \mid n$, allora esistono interi β_i con $0 \leq \beta_i \leq \alpha_i$ tali che $d = \prod_{i=1}^{k} p_i^{\beta_i}$.*

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

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

𝔈 6 **Corollario 1.1.8** *Sia p_n l'n-esimo numero primo. Si ha $p_n \leq 2^{2^{n-1}}$.*

Esercizi.

𝔈 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 $0 \leq r < |m|$.

𝔈 2. Dimostrare che se a, $b \in \mathbb{Z}^*$, allora qualunque sia $m \in \mathbb{Z}$, si ha $(a,b) = (a, b - ma)$.

𝔈 3. Determinare tutti gli interi a e b tali che $13a+17b=1$.

𝔈 4. Dimostrare che per $a, b \in \mathbb{N}$ si ha $ab = (a,b)\cdot[a,b]$.

𝔈 5. Dimostrare il Corollario 1.1.6.

𝔈 6. Dimostrare il Corollario 1.1.8, e dedurne che $\limsup_{x\to+\infty} \pi(x)/\log\log x > 0$.

Riferimenti. Hardy & Wright [57], Capitoli 1, 2, 5, 6 e 7, Landau [85], Dirichlet [28].

1.2 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'unico 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. L'insieme quoziente si indica con $\mathbb{Z}_m$. Inoltre, per ogni $c \in \mathbb{Z}$ si ha*

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

l'ultima delle quali segue dal Teorema 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
𝔈 1 *è un campo se e solo se m è primo. $\mathbb{Z}_m^*$ è l'insieme degli elementi invertibili di $\mathbb{Z}_m$.*

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

Teorema 1.2.4 (Teorema Cinese del Resto) *Se $n_1, n_2 \in \mathbb{Z}^*$ ed inoltre $(n_1,n_2) = 1$, il sistema seguente ha un'unica soluzione modulo n_1n_2:*

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

Dim. Sia $\mathcal{A} := \{a_1 + bn_1 \colon b = 0, \dots, n_2-1\}$. È evidente che tutti gli elementi di $\mathcal{A}$ soddisfano la prima congruenza, e vogliamo dimostrare che sono tutti distinti modulo n_2. Supponiamo che $a_1 + b_1n_1 \equiv a_1 + b_2n_1 \mod n_2$ per due valori distinti $b_1, b_2 \in \{0, \dots, n_2-1\}$. Per l'Osservazione 1.2.2 abbiamo $b_1n_1 \equiv b_2n_1 \mod n_2$, 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, 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 Lemma 1.2.3 l'insieme $\mathcal{A} := \{na \mod p : n = 1, \dots, p-1\}$ ha tutti gli elementi distinti e quindi, per il principio dei cassetti, $\mathcal{A} = \{1, \dots, p-1\}$. Dunque, moltiplicando fra loro tutte le congruenze corrispondenti, abbiamo

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

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

𝔈 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 $2^5 \equiv 1 \mod 31$ e quindi $2^{10} \equiv 1 \mod 11 \cdot 31$ per il Teorema Cinese del Resto 1.2.4), 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 $4^{14} = 16^7 \equiv 1^7 \mod 15$. Questa è una situazione generale, come mostra il seguente Teorema.

Teorema 1.2.6 (Cipolla) *Fissato un intero $a \geq 2$, esistono infiniti numeri compositi 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

$$\begin{aligned} m &\stackrel{\text{def}}{=} \frac{a^{2p}-1}{a^2-1} = \frac{a^p-1}{a-1}\,\frac{a^p+1}{a+1} \\ &= \big(a^{p-1}+a^{p-2}+\cdots+a+1\big)\big(a^{p-1}-a^{p-2}+\cdots-a+1\big). \end{aligned} \tag{1.2.1}$$

Per ipotesi a^2-1 è invertibile modulo p, e quindi $m \equiv 1 \mod p$, dato che per definizione $(a^2-1)m = a^{2p}-1 \equiv a^2-1 \mod p$, per il Teorema di Fermat 1.2.5. 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 la condizione $p \nmid a(a^2-1)$ esclude solo un numero finito di numeri primi. □

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* e nel 1992 è
𝔈 4-5 stato dimostrato 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 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 $\not\equiv \pm 1$ 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 $x = 1, \ldots, p-1$ (tutti gli elementi non nulli di $\mathbb{Z}_p$) e quindi si ha la fattorizzazione

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

𝔈 7 Il Teorema di Wilson segue ponendo $x = 0$ in questa identità. □

𝔈 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 le espressioni esplicite $a^{-1} \equiv a^{p-2} \equiv \big((p-2)!/a\big) \mod p$ se $p \nmid a$.*

Osservazione 1.2.9 *Per $p \geq 3$ poniamo*

$$x \stackrel{\text{def}}{=} 1 \cdot 2 \cdots \left(\frac{1}{2}(p-1)\right), \qquad y \stackrel{\text{def}}{=} \left(\frac{1}{2}(p+1)\right) \cdots (p-1),$$

in modo tale che $xy = (p-1)!$. Poiché per ogni fattore n nel prodotto che definisce x c'è il fattore $p - n \equiv -n \mod p$ nel prodotto per y, si ha $x \equiv y(-1)^{(p-1)/2} \mod p$. Moltiplichiamo ambo i membri dell'ultima uguaglianza per x ed usiamo il Teorema di Wilson 1.2.7: si ha 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*

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

Dim. Si dimostra come il Teorema di Fermat 1.2.5, sfruttando il Lemma 1.2.3. □

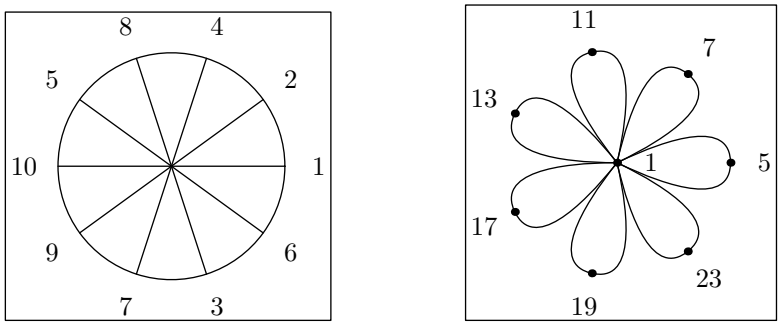


Figura 1.1: Struttura di $\mathbb{Z}_{11}^*$ e di $\mathbb{Z}_{24}^*$. Gli archi connettono le potenze successive dello stesso elemento: nel caso a sinistra le potenze di 2 (che è un generatore di $\mathbb{Z}_{11}^*$), nel caso a destra, poiché ogni elemento di $\mathbb{Z}_{24}^*$ soddisfa $x^2 \equiv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

Lemma 1.2.11 *Per ogni $n \geq 1$ si ha*

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

Dim. Nella seguente uguaglianza gli insiemi a destra sono mutuamente disgiunti: le frazioni a destra si ottengono da quelle a sinistra riducendole ai minimi termini, e raggruppandole per valori comuni dei denominatori delle frazioni ridotte.

$$\left\{ \frac{h}{n} : h \in \{1,\ldots,n\} \right\} = \bigcup_{d|n} \left\{ \frac{a}{d} : a \in \{1,\ldots,d\} \text{ e } (a,d) = 1 \right\}. \tag{1.2.3}$$

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

Definizione 1.2.12 *Diciamo che l'*ordine *di $g \in \mathbb{Z}_n^*$ è r se r è il minimo intero positivo tale che $g^r \equiv 1 \bmod n$. Diciamo che g è una* radice primitiva modulo *n se il suo ordine è $\phi(n)$, cioè se g genera $\mathbb{Z}_n^*$.*

Æ 10

Lemma 1.2.13 *Se r è l'ordine di $a \in \mathbb{Z}_n^*$, allora $a^m \equiv 1 \bmod n$ se e solo se $r \mid m$.*

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

Il vero inverso del Teorema di Fermat 1.2.5 è il seguente risultato di Lucas.

Teorema 1.2.14 (Lucas) *Se $a^d \not\equiv 1 \bmod n$ per ogni $d \mid n-1$ tale che $d < n-1$ ed inoltre $a^{n-1} \equiv 1 \bmod n$, allora n è primo.*

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

Teorema 1.2.15 (Gauss) *Per ogni numero primo p, il gruppo $\mathbb{Z}_p^*$ è ciclico.*

Dim. Sia $h_d(x) := x^d - 1$: 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 $\mathbb{Z}_p$, l'equazione $h_d(x) \equiv 0 \bmod p$ ha esattamente d soluzioni (evidentemente tutte distinte) in $\mathbb{Z}_p$: infatti, poiché $\mathbb{Z}_p$ è un campo, $h_d(x) \equiv 0 \bmod p$ ha al piú d soluzioni, e $h_{p-1}(x)/h_d(x) \equiv 0 \bmod p$ al piú $p-1-d$, ma il loro prodotto h_{p-1} ne ha esattamente $p-1$, e quindi i due
Æ 6 polinomî h_d ed h_{p-1}/h_d devono avere d e $p-1-d$ radici rispettivamente.

Sia $n_p(d)$ il numero delle soluzioni dell'equazione $h_d(x) \equiv 0 \bmod p$ che hanno ordine d. Dimostreremo che $n_p(d) = \phi(d)$ 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 1.2.13 ogni soluzione di $h_d(x) \equiv 0 \bmod p$ ha ordine $\delta \mid d$ e quindi per il Lemma 1.2.11

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

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

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 $g_1 \bmod p$. Inoltre un semplice calcolo mostra che $g_1^{p-1} \not\equiv (g_1 + p)^{p-1} \bmod p^2$ e quindi esiste $g_2 \in \mathbb{Z}_{p^2}^*$ tale che $g_2^{p-1} \not\equiv 1 \bmod p^2$. Sia r l'ordine di $g_2 \bmod p^2$: per il Lemma 1.2.13 si ha $r \mid \phi(p^2) = p(p-1)$ e poiché $g_1 \equiv g_2 \bmod p$ e g_1 ha ordine $p-1 \bmod p$, allora $p-1 \mid r$. Ma $r \neq p-1$ e quindi $r = p(p-1)$, cioè g_2 è una radice primitiva $\bmod p^2$. 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 $\bmod p^\alpha$, poiché, per induzione $g_2^{(p-1)p^{\alpha-2}} \not\equiv 1 \bmod p^\alpha$ e quindi l'ordine di $g_2 \bmod p^\alpha$ è $(p-1)p^{\alpha-1}$. □

Esercizi.

Æ 1. Dimostrare la validità dei cosiddetti "criteri di divisibilità" per 3, 9, 11.

Æ 2. Dimostrare che $5n^3 + 7n^5 \equiv 0 \bmod 12$ per ogni $n \in \mathbb{Z}$.

Æ 3. Si determini il massimo comun divisore degli elementi di $\{n^{13} - n \colon n \in \mathbb{N}\}$.

Equazione	Soluzioni	primitive
$x \equiv 1 \mod 13$	$x = 1$	1
$x^2 \equiv 1 \mod 13$	$x = 1, 12$	12
$x^3 \equiv 1 \mod 13$	$x = 1, 3, 9$	3, 9
$x^4 \equiv 1 \mod 13$	$x = 1, 5, 8, 12$	5, 8
$x^6 \equiv 1 \mod 13$	$x = 1, 3, 4, 9, 10, 12$	4, 10
$x^{12} \equiv 1 \mod 13$	$x = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12$	2, 6, 7, 11

Tabella 1.1: Dimostrazione del Teorema di Gauss per $p = 13$.

Æ 4. Dimostrare che 561, 1105 e 1729 sono numeri di Carmichael.

Æ 5. Dimostrare che se $6n+1$, $12n+1$ e $18n+1$ sono simultaneamente primi, allora il numero $N := (6n+1)(12n+1)(18n+1)$ è di Carmichael.

Æ 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 $\alpha \geq 3$, e determinarle.

Æ 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.

Æ 8. Dimostrare che se $n \geq 6$ non è primo allora $n \mid (n-2)!$.

Æ 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 $P(n) \mod p_j^{\alpha_j}$, $j = 1, \ldots, k$.

Æ 10. Determinare l'ordine $r = r_p$ di 8 modulo i primi $3 \leq p \leq 50$, ricordando che per il Teorema di Fermat 1.2.5 si ha $r \mid p-1$. Usare questo risultato per determinare tutti gli pseudoprimi in base 8 minori di 50.

Æ 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 $f(x) \equiv 0 \mod p$?

Riferimenti. Teorema di Gauss 1.2.15: Hardy & Wright [57], Teorema 110. La struttura dei gruppi $\mathbb{Z}_m^*$ è discussa nei dettagli in Shanks [135] §§23–38: vedi in particolare i diagrammi nel §33. Teorema 1.2.16: Shanks [135] §35. Teorema di Cipolla 1.2.1: Hardy & Wright [57] Teorema 89, ed anche Pomerance [120]. Pseudoprimi: Ribenboim [128] §2.VIII. Numeri di Carmichael: Ribenboim [128] §2.IX ed Alford, Granville & Pomerance [3], dove si dimostra che ne esistono infiniti. Teorema di Lucas 1.2.14 e sue varianti: Crandall & Pomerance [20], Languasco & Zaccagnini [88].

1.3 Terne pitagoriche

Studiamo brevemente un problema classico della Teoria Elementare dei Numeri.

Definizione 1.3.1 *Una terna di interi* $(a,b,c) \in \mathbb{Z}^3$ *tali che* $a^2+b^2=c^2$ *si dice* terna pitagorica. *Questa si dice* 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* $(n,m)=1$, $n \not\equiv m \bmod 2$ *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* $(n,m)=1$, $n \not\equiv m \bmod 2$, *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 $c^2 \equiv 2 \bmod 4$, 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 $\alpha := \frac{1}{2}(c+b)$, $\beta := \frac{1}{2}(c-b)$, osservando che $\alpha, \beta \in \mathbb{Z}$ poiché $b \equiv c \equiv 1 \bmod 2$. Quindi $a_0^2 = \alpha\beta$. Inoltre, se $d := (\alpha,\beta)$, 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 $(n,m)=1$, $n \not\equiv m \bmod 2$ 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 $x := a/c$, $y := b/c$ (dove supponiamo tacitamente che $c \neq 0$, ma è chiaro che se $c = 0$ nella (1.3.1) 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 $\gamma := \{(x,y) \in \mathbb{R}^2 : x^2 + y^2 = 1\}$. 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 1.2). 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 1.2, 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 $t = n/m$ 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 $\big(0, y_0/(x_0+1)\big)$. □

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 polinomî 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

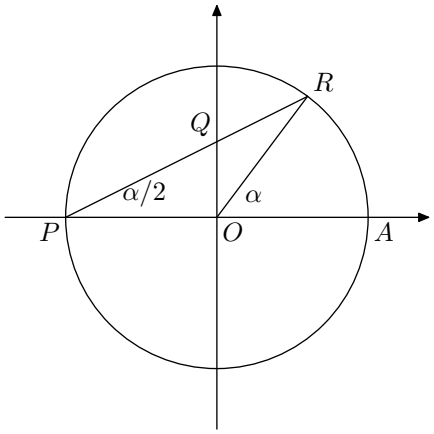


Figura 1.2: Come parametrizzare i punti della circonferenza unitaria.

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.

Riferimenti. La dimostrazione di Diofanto è tratta da Hardy & Wright [57] §13.2. L'altra dimostrazione è ispirata all'Introduzione, pp. 1–21 di Husemöller [70]. Si veda anche Conway & Guy [18] Cap. 6, pp. 147–151.

1.4 Somme di due 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 $n = 0, \ldots, N$, ed ordiniamoli in ordine crescente $0 = \xi_0 < \xi_1 < \cdots < \xi_N < 1$. La notazione *non* implica che $\xi_n = \{n\xi\}$: questo è falso in generale. Osserviamo che questi numeri sono tutti distinti poiché $\xi \notin \mathbb{Q}$. La distanza media fra gli ξ_j è $(N+1)^{-1}$, e quindi esiste un indice $n \in \{1, \ldots, N\}$ tale che $\xi_n - \xi_{n-1} < (N+1)^{-1}$, oppure $1 - \xi_N < (N+1)^{-1}$. Nel primo caso, poniamo $\xi_{n-1} = \{a\xi\}$ e $\xi_n = \{b\xi\}$: quindi

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

Abbiamo dunque le equazioni

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

Il risultato cercato segue ponendo $m := [b\xi] - [a\xi]$ e $q := b - a$.

Nel secondo caso, se $\xi_N = \{b\xi\}$, dove ovviamente $b \neq 0$, è sufficiente prendere $q = b$ ed $m = [b\xi] + 1$ per ottenere la tesi. □

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

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

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 $n \geq 2$. Sia $N := \left[\sqrt{n}\right] \leq \sqrt{n} < n$. Poiché $(n,a) = 1$, per il Lemma precedente esistono m, $q \in \mathbb{N}$ con $q \leq N$ ed $(m,q) = 1$, tali che

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

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 $1 \leq q \leq N$ e $|aq - mn| < \sqrt{n}$. Quindi $1 \leq (aq - mn)^2 + q^2 < n + N^2 < 2n$. 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 $1 = q^2(a^2+1)/n + (nm^2 - 2amq)$ e quindi

$$1 = q\left(q\frac{a^2+1}{n} - 2am \right) + nm^2.$$

Dal Teorema 1.1.1 segue immediatamente che $(q,n) = 1$. □

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 $p \equiv 1 \bmod 4$, allora esistono m, $x \in \mathbb{N}$ tali che $0 < m < p$ e $x^2+1 = mp$.*

Dim. L'equazione $x^2 \equiv -1 \bmod p$ 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 $x \equiv g^{(p-1)/4} \bmod p$, dove g è un generatore di $\mathbb{Z}_p^*$, e piú precisamente, per l'Osservazione 1.2.9, possiamo prendere $x \equiv \left(\frac{1}{2}(p-1)\right)! \bmod p$. Poiché i quadrati degli interi $1, 2, \ldots, \frac{1}{2}(p-1)$ 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 Lemma 1.4.12 ed il Lemma 1.4.5, se p è un numero primo con $p \equiv 1 \bmod 4$ 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_0, $y_0 \in \mathbb{N}$ tali che $0 < m < p$ e $x_0^2+y_0^2+1 = mp$.*

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

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

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_0 ed y_0 tali che $x_0^2 \equiv -1-y_0^2 \bmod p$. Per le scelte fatte sopra si ha $x_0^2+y_0^2+1 < p^2$, e la tesi segue anche in questo caso. □

Quindi per il Lemma 1.4.5, se $p \equiv 1 \bmod 4$ 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 **Lemma 1.4.9** *Se esiste $p \mid n$ con $p \equiv -1 \bmod 4$, allora n non ha rappresentazioni primitive.*

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

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

Quindi $p \mid a$ da cui segue $p \mid b$. In altre parole, se $n = a^2 + b^2$ ed esiste $p \equiv -1 \bmod 4$ tale che $p \mid n$, esistono anche $\alpha, \beta \in \mathbb{Z}$ 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 $p \equiv 3 \bmod 4$. Inoltre esiste una rappresentazione primitiva di n se e solo se $n \equiv 1,\ 2 \bmod 4$ e tutti i fattori primi dispari di n sono $\equiv 1 \bmod 4$.*

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 $p \equiv 1 \bmod 4$, e dimostrare che se $p \equiv 3 \bmod 4$ e $p \mid a^2 + b^2$ allora esiste un numero pari $\alpha \geq 2$ 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. □

Il Lemma di Thue dà una dimostrazione alternativa dell'Osservazione di Fermat 1.4.6.

Lemma 1.4.11 (Thue) *Dato un numero primo p sia $k = \lfloor p^{1/2} \rfloor$. Se $a \in \mathbb{Z}$ non è divisibile per p, allora esistono $x,\ y \in \{1, \ldots, k\}$ tali che $ax \equiv \pm y \bmod p$.*

Dim. Si consideri l'insieme dei numeri $ax - y \bmod p$, dove $x,\ y \in \{0, \ldots, k\}$. Il numero totale di scelte possibili è $(k+1)^2 > p$, e dunque esistono $(x_1, y_1) \neq (x_2, y_2)$ tali che $ax_1 - y_1 \equiv ax_2 - y_2 \bmod p$, cioè $(x_1 - x_2)a \equiv y_1 - y_2 \bmod p$. Se $y_1 = y_2$ allora $x_1 = x_2$, dato che $p \nmid a$; analogamente, se $x_1 = x_2$ allora dovremmo avere $y_1 = y_2$, che di nuovo è impossibile. La tesi segue prendendo $x = |x_1 - x_2|$ ed $y = \pm(y_1 - y_2)$. □

Lemma 1.4.12 *Se l'equazione $a^2 + 1 \equiv 0 \bmod p$ è risolubile, allora il numero primo p può essere rappresentato come somma di due quadrati.*

Dim. Sia a una soluzione dell'equazione nell'enunciato, e siano x, y due interi per i quali è soddisfatto il Lemma di Thue 1.4.11. Dunque $y^2 \equiv a^2x^2 \equiv -x^2 \bmod p$, cioè $x^2 + y^2 \equiv 0 \bmod p$. Per costruzione $0 < x^2 + y^2 < 2p$ e quindi $x^2 + y^2 = p$. □

Esercizi.

Æ 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 $x^2 \equiv -1 \bmod p$, allora l'ordine di $\mathbb{Z}_p^*$ è divisibile per 4.

Riferimenti. Dimostrazione alternativa del Lemma 1.4.1: Hardy & Wright [57] Teorema 36 ed anche i §§20.2-20.4. La dimostrazione del Lemma di Thue 1.4.11 è quella in [113]. Il Teorema contenuto nell'Osservazione 1.4.6 è di Fermat: vedi Edwards [32] §2.4 e §2.6; Weil [145] 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 Conway & Guy [18] Cap. 8. Zagier [151] dà una dimostrazione molto breve, ma non particolarmente illuminante. Wagon [143] dà una dimostrazione costruttiva basata sull'algoritmo di Euclide. Si veda anche Friedlander & Iwaniec [38].

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 $m_0 := \min\{m \in \mathbb{N}^* : mp = x^2+y^2+z^2+t^2$ 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 $x \equiv y \bmod 2$ e $z \equiv t \bmod 2$, 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 $\alpha \equiv \beta \equiv \gamma \equiv \delta \equiv 0 \bmod m_0$. Infatti, sempre dalla (1.5.1), abbiamo $\alpha = xx_2+yy_2+zz_2+tt_2 \equiv x_2^2+y_2^2+z_2^2+t_2^2 \equiv 0 \bmod m_0$, 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. □

Riferimenti. Teorema di Lagrange 1.5.1: Hardy & Wright [57], Teorema 369.

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*

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

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

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.*

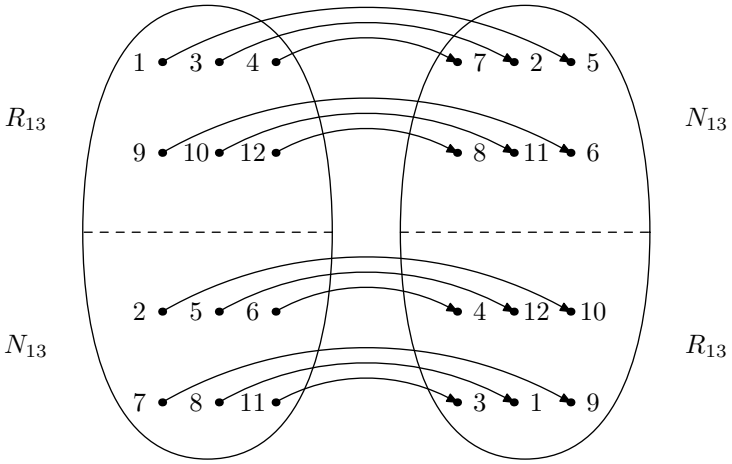


Figura 1.3: Dimostrazione dell'ultima parte del Lemma 1.6.3 per $p = 13$ ed $a = 5$.

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 $\left(a \mid p\right) = \left(b \mid p\right) = 1$ è ovvio che l'equazione $x^2 \equiv ab \bmod p$ abbia soluzione. Se invece, per esempio, $\left(a \mid p\right) = 1$ e $\left(b \mid p\right) = -1$, sia y una soluzione di $y^2 \equiv a \bmod p$. L'equazione $x^2 \equiv ab \bmod p$ diventa $\left(xy^{-1}\right)^2 \equiv b \bmod p$, che quindi non ha soluzione. Resta il caso $\left(a \mid p\right) = \left(b \mid p\right) = -1$. Per quanto appena visto, posto $f\colon \mathbb{Z}_p^* \to \mathbb{Z}_p^*$, $f(x) = ax \bmod p$ si ha $f(R_p) = N_p$ dove $R_p := \{x \in \mathbb{Z}_p^*\colon \left(x \mid p\right) = 1\}$, $N_p := \{x \in \mathbb{Z}_p^*\colon \left(x \mid p\right) = -1\}$, e, per il Lemma 1.2.3, $f(N_p) = R_p$. 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 $x, y \in \mathbb{F}_{q^d}$, dove q è un numero primo e $d \geq 1$, allora
$$(x+y)^q \equiv x^q + y^q \mod q$$
poiché i coefficienti binomiali $\binom{q}{n}$ con $1 \leq n \leq q-1$ sono divisibili per q. Ɛ 1

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
$$\sum_{h \bmod q} f(hm) = \sum_{r \bmod q} f(r),$$
perché per il Lemma 1.2.3 l'applicazione $h \mapsto hm \bmod q$ è una biiezione.

4. Se $nm \equiv 1 \bmod q$ allora $\left(n \mid q\right) = \left(m \mid q\right)$. Infatti, per il Lemma 1.6.3, $\left(nm \mid q\right) = \left(n \mid q\right)\left(m \mid q\right)$, e $\left(nm \mid q\right) = \left(1 \mid q\right) = 1$ per periodicità.

5. Per il Lemma 1.6.2 (nella notazione del Lemma 1.6.3) si ha
$$\sum_{m \bmod q} \left(\frac{m}{q}\right) = |R| - |N| = 0.$$

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

7. Se $q \nmid n$ allora $\left(n \mid q\right) \equiv n^{(q-1)/2} \bmod q$ per il Teorema di Fermat 1.2.5. Ɛ 2

Consideriamo ora la somma di Gauss $\tau = \tau(q)$ definita da
$$\tau \stackrel{\text{def}}{=} \sum_{m \bmod q} \left(\frac{m}{q}\right) \mathrm{e}_q(m).$$

Per le osservazioni fatte sopra si ha
$$\left(\frac{n}{q}\right)^2 \tau^2 = \left(\frac{n^{-1}}{q}\right)^2 \tau^2 = \sum\sum_{m_1, m_2 \bmod q} \left(\frac{n^{-1}m_1}{q}\right)\left(\frac{n^{-1}m_2}{q}\right) \mathrm{e}_q(m_1+m_2)$$
$$= \sum\sum_{h_1, h_2 \bmod q} \left(\frac{h_1}{q}\right)\left(\frac{h_2}{q}\right) \mathrm{e}_q\big(n(h_1+h_2)\big).$$

Ora sommiamo questa relazione su tutti i valori di $n \in \mathbb{Z}_q^*$:
$$\tau^2 \sum_{n=1}^{q-1} \left(\frac{n}{q}\right)^2 = \sum\sum_{h_1, h_2 \bmod q} \left(\frac{h_1}{q}\right)\left(\frac{h_2}{q}\right) \sum_{n=1}^{q-1} \mathrm{e}_q\big(n(h_1+h_2)\big)$$
$$= \sum\sum_{h_1, h_2 \bmod q} \left(\frac{h_1}{q}\right)\left(\frac{h_2}{q}\right) \begin{cases} -1 & \text{se } h_1+h_2 \not\equiv 0 \bmod q, \\ q-1 & \text{se } h_1+h_2 \equiv 0 \bmod q. \end{cases}$$

Il primo membro vale $(q-1)\tau^2$ perché tutti gli addendi sono uguali. Quindi

$$\begin{aligned}(q-1)\tau^2 &= q\sum_{h \bmod q}\left(\frac{-h^2}{q}\right) - \sum_{h_1,h_2 \bmod q}\left(\frac{h_1h_2}{q}\right)\\ &= q\sum_{h=1}^{q-1}\left(\frac{-1}{q}\right) - \left(\sum_{h \bmod q}\left(\frac{h}{q}\right)\right)^2\\ &= q(q-1)\left(\frac{-1}{q}\right).\end{aligned}$$

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

$$\begin{aligned}\tau^p &= \sum_{m \bmod q}\left(\frac{m}{q}\right)^p \mathrm{e}_q(pm) = \sum_{h \bmod q}\left(\frac{hp^{-1}}{q}\right)\mathrm{e}_q(h)\\ &= \left(\frac{p}{q}\right)\sum_{h \bmod q}\left(\frac{h}{q}\right)\mathrm{e}_q(h) = \left(\frac{p}{q}\right)\tau.\end{aligned}$$

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 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 $x^2 \equiv a \bmod p$ è risolubile.*

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

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

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

Esercizi.

Æ 1. Dimostrare che se p è primo allora $p \mid \binom{p}{r}$ per $r = 1, \dots, p-1$.

Æ 2. Dimostrare che $\left(n \mid p\right) \equiv n^{(p-1)/2} \bmod p$ usando il Teorema di Fermat 1.2.5.

Æ 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 $p \equiv 1 \bmod 8$, $K = \mathbb{F}_{p^2}$ 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 $\alpha := u + u^{-1}$ 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 $\alpha^p = -\alpha$.

Æ 4. Sia $f(x) = x^2 + 3x - 1$. Dire per quali primi p l'equazione $f(x) \equiv 0 \bmod p$ ha soluzione e determinarle esplicitamente, se possibile, per $p \leq 10$.

Æ 5. Risolvere se possibile l'equazione $5x^4 \equiv 1 \bmod p$ per ciascun $p \leq 11$.

Æ 6. Esprimere il numero delle soluzioni della congruenza $f(x) \equiv 0 \bmod p$ 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 $p \mid 2a$.

Riferimenti. Estensioni del simbolo di Legendre: per i simboli di Jacobi e di Kronecker si veda Landau [85] Parte I, Cap. 6, pag. 65 e 70 rispettivamente. Reciprocità quadratica 1.6.4: per altre tre dimostrazioni vedi [57] Teorema 98, Apostol [5] Teorema 9.8 oppure Frame [36].

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, queste formule non sono utilizzabili nella pratica, perché ri-
Æ 1.2.8 chiedono 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 $(p-2)! \equiv 1 \bmod p$. Quindi, per $x \geq 3$,

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

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

$$p_n = 1 + \sum_{d=1}^{2^{2^n}} f\big(n, \pi(d)\big), \tag{1.7.1}$$

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

𝔈 1

Non è difficile dimostrare che nessun polinomio in una variabile non costante può assumere solo valori primi, ma esistono polinomî in piú variabili che hanno questa proprietà: si veda Ribenboim [128], §3.III. Vedremo nel Capitolo 5 che i polinomî assumono valori composti per "quasi tutti" i valori dell'argomento: in particolare il Corollario 5.2.10. In compenso, l'insieme dei fattori primi dei valori non nulli di un polinomio non può essere troppo piccolo: è il Teorema di Schur [133], del quale diamo la dimostrazione originale che è basata su proprietà algebriche dei polinomî ed una dimostrazione basata sul conteggio.

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 $p := f(0)$. Si ha ovviamente $f(np) \equiv f(0) \equiv 0 \bmod p$ per ogni $n \in \mathbb{Z}$. Dunque $p \mid f(np)$ per ogni $n \in \mathbb{Z}$ e quindi $f(np) = \pm p$ poiché deve essere un numero primo, ma questo è assurdo se f non è costante, perché l'equazione $|f(m)| = p$ ha al massimo $2\deg(f)$ soluzioni. □

Ricordiamo un esempio di Eulero: il polinomio $f(n) = n^2 - n + 41$ è primo per $n = 0, 1, \ldots, 40$, ma evidentemente non è primo per $n = 41$.

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

Dim. Sia $f(x) = a_r x^r + \cdots + a_0$ con $a_r \neq 0$. Possiamo supporre $a_0 \neq 0$, altrimenti $\mathfrak{P}_f$ è l'insieme di tutti i numeri primi. Per assurdo, sia $\mathfrak{P}_f = \{p_1, \ldots, p_k\}$, e sia $c \in \mathbb{Z}$ tale che $|f(ca_0 p_1 \cdots p_k)| > |a_0|$. Ma $(1/a_0) f(ca_0 p_1 \cdots p_k) \equiv 1 \bmod p_1 \cdots p_k$, e quindi esiste un primo $p \notin \mathfrak{P}_f$ tale che $p \mid (1/a_0) f(ca_0 p_1 \cdots p_k)$. □

𝔈 2

Dimostrazione alternativa. Per assurdo, sia $\mathfrak{P}_f = \{p_1, \ldots, p_k\}$. Se $f(x) = a_r x^r + \cdots + a_0$ con $r \ge 1$ ed $a_r \neq 0$, poniamo $U(x) := \{m \le x\colon m \in f(\mathbb{N})\}$; si ha $|U(x)| \sim \big(x/|a_r|\big)^{1/r}$ per $x \to +\infty$. Consideriamo il semigruppo moltiplicativo generato dall'insieme di numeri primi $\mathfrak{P}_f$, e cioè l'insieme

$$\mathcal{S}(\mathfrak{P}_f) \stackrel{\text{def}}{=} \{n \in \mathbb{N}^*\colon\ p \mid n \Longrightarrow p \in \mathfrak{P}_f\}. \tag{1.7.2}$$

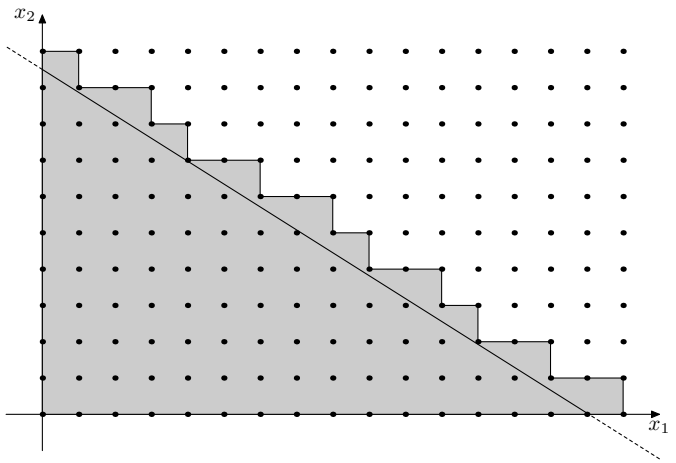


Figura 1.4: La dimostrazione del Teorema di Schur 1.7.2 nel caso in cui $k = 2$ e $\mathfrak{P}_f = \{2, 3\}$. L'area in grigio è uguale a $|V(x)|$.

Poniamo $V(x) := [1,x] \cap \mathcal{S}(\mathfrak{P}_f)$: si ha $m \in V(x)$ se e solo se esistono α_1, ..., $\alpha_k \in \mathbb{N}$ tali che $m = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ e quindi $\log m = \alpha_1 \log p_1 + \cdots + \alpha_k \log p_k \le \log x$. In altre parole

$$|V(x)| \sim \int \cdots \int_T \mathrm{d}x_1 \cdots \mathrm{d}x_k$$

dove

$$T \stackrel{\text{def}}{=} \{(x_1, \ldots, x_k) \in \mathbb{R}^k \colon x_i \ge 0, x_1 \log p_1 + \cdots + x_k \log p_k \le \log x\},$$

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 $U(x) \subseteq V(x)$. □

La Figura 1.4 illustra il caso $k = 2$, $\mathfrak{P}_f = \{2, 3\}$ della dimostrazione. La cardinalità di $V(x)$ è uguale al numero di punti a coordinate intere nel triangolo delimitato dagli assi cartesiani e dalla retta di equazione $x_1 \log 2 + x_2 \log 3 = \log x$. Assegniamo ad ogni punto $(a_1, a_2) \in \mathbb{N}^2$ che soddisfa questa diseguaglianza il quadrato di vertici opposti (a_1, a_2), $(a_1 + 1, a_2 + 1)$. Il numero di questi punti è uguale all'area indicata in grigio, cioè all'area del triangolo con un errore dell'ordine del perimetro del triangolo stesso, e quindi l'area vale $(\log x)^2/(2 \log 2 \log 3) + O(\log x)$. Si veda il Capitolo 5 di Hardy [53] per una discussione della stima di $V(x)$ con un termine d'errore estremamente accurato.

Evidentemente non è necessario conoscere $|V(x)|$ con precisione: è sufficiente osservare che da $\log m = \alpha_1 \log p_1 + \cdots + \alpha_k \log p_k \le \log x$ segue che $0 \le \alpha_i \le \left[(\log x)/\log p_i\right]$ e quindi $|V(x)| \le \prod_i \left(2 + (\log x)/\log p_i\right) = O_{p_1,\ldots,p_k}\left((\log x)^k\right)$. In altre parole, si può dire che il semigruppo moltiplicativo $\mathcal{S}$ generato dall'insieme di numeri primi $\mathfrak{P}_f$ definito nella (1.7.2) è poco denso e non riesce a coprire tutti i valori assunti da un polinomio.

Esempio 1.7.3 *Sia $f(x) = qx + a$ con a, $q \in \mathbb{Z}$, e $q \neq 0$. Se $(a,q) = 1$ allora il Lemma 1.2.3 implica che $\mathfrak{P}_f = \{p\colon p \nmid q\}$. Se $(a,q) > 1$, allora $\mathfrak{P}_f = \{p\colon p \nmid q\} \cup \{p\colon p \mid (a,q)\}$.*

Esempio 1.7.4 *Se $f(x) = x^2 + 1$, allora l'Osservazione 1.2.9 implica che $\mathfrak{P}_f = \{2\} \cup \{p\colon p \equiv 1 \bmod 4\}$. Piú in generale, se $f(x) = ax^2 + bx + c$ con $a \neq 0$, sia $\Delta = b^2 - 4ac$ il discriminante di f: se $\Delta \neq 0$, per il Lemma 1.2.3 e la Definizione 1.6.1 in questo caso $\mathfrak{P}_f = A \cup \{p\colon \left(\Delta \mid p\right) = 1\}$, dove A è un sottoinsieme dell'insieme dei divisori primi di $2a\Delta$. Infatti, se $p \nmid 2a$ l'equazione $f(x) \equiv 0 \bmod p$ è equivalente a $4a^2x^2 + 4abx + b^2 \equiv \Delta \bmod p$, cioè $(2ax+b)^2 \equiv \Delta \bmod p$ e questa è risolubile se e solo se $\left(\Delta \mid p\right) = 1$. Inoltre $2 \in \mathfrak{P}_f$ se e solo se $c(a+b+c) \equiv 0 \bmod 2$. Infine, se $p \mid a\Delta$ oppure se $\Delta = 0$ ricadiamo nel caso descritto nell'Esempio 1.7.3.*

Teorema 1.7.5 *Esistono infiniti numeri primi in ciascuna delle progressioni aritmetiche $4n+1$ e $4n-1$.*

Dim. Supponiamo che esistano solo un numero finito di primi $p_i \equiv 1 \bmod 4$. Poniamo $N := (2p_1 \cdots p_k)^2 + 1$. 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 $q \equiv 1 \bmod 4$, ma $q \nmid N$. Se esistessero solo un numero finito di numeri primi $p_i \equiv -1 \bmod 4$, posto $N := 4p_1 \cdots p_k - 1$, si avrebbe $N \equiv -1 \bmod 4$, ed evidentemente non è possibile che tutti i fattori primi di N siano congrui a $1 \bmod 4$. □

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 4 otterremo un risultato molto piú preciso.

Nel XVII secolo, Fermat e Mersenne proposero "formule" che danno primi: purtroppo le loro congetture si sono rivelate sbagliate.

Teorema 1.7.6 *Se il numero $2^m + 1$ è primo, allora $m = 2^n$ per qualche intero n.*

Definizione 1.7.7 *Per $n \in \mathbb{N}$ si chiama n-esimo* numero di Fermat *il numero $F_n := 2^{2^n} + 1$. Per $n \in \mathbb{N}^*$ si chiama n-esimo* numero di Mersenne *il numero $M_n := 2^n - 1$.*

Teorema 1.7.8 *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
𝔈 4-9 per $n = 0, \ldots, 4$, e falso per $n = 5, \ldots, 32$. Esistono criteri di primalità *ad hoc* per i numeri di Fermat che hanno permesso di dimostrare che i numeri F_n con

$n = 5, \ldots, 32$ sono composti, nella maggior parte dei casi senza poterne esibire esplicitamente un fattore primo.

Mersenne dette una lista di numeri primi p per i quali M_p è primo, ma questa lista contiene varî errori ed omissioni. Anche nel caso dei numeri di Mersenne esistono criteri di primalità speciali.

Esercizi.

𝔈 1. Si verifichi la (1.7.1) quando $n = 4$ scrivendo esplicitamente tutti gli addendi della somma.

𝔈 2. Facendo riferimento all'enunciato del Teorema di Schur 1.7.2, si dimostri che se $a_0 = 0$ allora $\mathfrak{P}_f$ è l'insieme di tutti i numeri primi.

𝔈 3. Procedendo come nel Teorema 1.7.5, dimostrare che esistono infiniti primi $p \equiv 1 \bmod 6$ ed infiniti primi $p \equiv 5 \bmod 6$. Perché la stessa dimostrazione non funziona se consideriamo le progressioni modulo 8?

𝔈 4. 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.

𝔈 5. Dimostrare che se $p = F_n$ è primo, h genera $\mathbb{Z}_p^*$ se e solo se $\left(h \mid p\right) = -1$.

𝔈 6. * Dimostrare che se $p \mid F_n$ ed $n \geq 2$ allora $p \equiv 1 \bmod 2^{n+2}$. 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 $\left(2 \mid p\right) \equiv 2^{(p-1)/2} \bmod p$. Dedurne che $r \mid \frac{1}{2}(p-1)$ e quindi la tesi.

𝔈 7. 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 F_5.

𝔈 8. Dimostrare i Teoremi 1.7.6 e 1.7.8.

𝔈 9. Dimostrare che se p e q sono numeri primi e $p \mid M_q$, allora $p \equiv 1 \bmod 2q$.

Riferimenti. Formule per i primi: Hardy & Wright [57] §2.7, Teorema 419 e App. 1 e 2; Dudley [30], Vanden Eynden [140]; Languasco & Zaccagnini [89]. Ulteriori riferimenti si possono trovare nella recensione dell'articolo di Golomb [44] a cura di Gandhi [39]. Il problema è discusso in dettaglio nel Capitolo 3 del libro di Ribenboim [128]. Una semplice dimostrazione del Teorema di Schur 1.7.2 con varie estensioni si può trovare in Morton [106]. Numeri di Fermat e di Mersenne: [57] §2.5. Lo stato attuale dei numeri di Fermat con gli eventuali fattori primi noti è consultabile in `www.prothsearch.net/fermat.html`. Per i numeri di Mersenne si veda `www.mersenne.org`.

1.8 Problemi aperti

Detto $C(x)$ il numero dei numeri di Carmichael $\leq x$, Alford, Granville & Pomerance [3] hanno dimostrato che si ha $C(x) > x^{2/7}$ per x sufficientemente grande. Questo risultato è stato migliorato nel 2005 da Harman [58], che ha dimostrato la disuguaglianza $C(x) > x^{33/100}$ per x sufficientemente grande. Pomerance, Selfridge & Wagstaff [125] hanno dimostrato che

$$C(x) \leq x \exp\Big(-(1-\varepsilon)\frac{\log x \log_3 x}{\log_2 x}\Big)$$

per $x > x_0(\varepsilon)$. Si congettura che quest'ultima relazione debba valere con $\sim$ al posto di $\leq$ ed $o(1)$ al posto di ε. Si può dimostrare che tutti i numeri di Carmichael sono dispari, senza fattori primi ripetuti, ed hanno almeno tre fattori primi distinti. Non è noto se per ogni $k \geq 3$ esistano infiniti numeri di Carmichael con esattamente k 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 [60] 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 dimo-
Ɛ 1.7.7 strato che $641 \mid F_5$. Oggi è noto che F_n non è primo per $n = 5, \ldots, 32$. 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 1.2.14 o sue varianti (vedi Lehmer [91]). Per una discussione di metodi di fattorizzazione, criteri di primalità, questioni computazionali varie ed applicazioni alla crittografia rimandiamo agli articoli di Adleman, Pomerance & Rumely [1], Dixon [29], Pomerance [121], [122], [123], [124] e alle monografie di Cohen [16], Crandall & Pomerance [20], Knuth [78], Koblitz [79], Languasco & Zaccagnini [88], Riesel [130].

Capitolo 2

Funzioni Aritmetiche

In questo Capitolo studieremo varî aspetti legati alle funzioni aritmetiche: queste non sono altro che funzioni definite su $\mathbb{N}^*$ a valori in $\mathbb{C}$, e quindi potremmo chiamarle successioni, se adottassimo il punto di vista dell'analisi matematica. Ma il nostro interesse è rivolto principalmente agli aspetti *aritmetici* (si veda la Definizione 2.1.3) piuttosto che alle proprietà quali esistenza del limite, sommabilità, ..., che sono quelle che si studiano quando si considerano le successioni.

Nel primo paragrafo vedremo una trattazione *algebrica* delle funzioni aritmetiche e definiremo un particolare modo di combinare due funzioni aritmetiche, il prodotto di Dirichlet della Definizione 2.1.2, che trae la sua origine da questioni legate alle serie di Dirichlet (vedi §2.4) ed alle funzioni generatrici.

Poi rivolgeremo la nostra attenzione ad un insieme concreto di funzioni aritmetiche, e di queste studieremo il comportamento asintotico (quando questo è possibile) ed il comportamento *medio*. Infatti, vedremo che per molte funzioni interessanti il comportamento *puntuale* è estremamente irregolare (si veda a titolo di esempio il Teorema 2.2.4), nel senso che il valore massimo ed il valore minimo di alcune funzioni hanno ordine di grandezza molto diverso. Piú precisamente, data una funzione aritmetica reale f si cercano due funzioni *elementari* f_1 ed f_2 tali che $f_1(n) \leq f(n) \leq f_2(n)$ per ogni $n \geq 1$, in modo da determinare l'intervallo di oscillazione dei valori assunti da f. Per molte funzioni aritmetiche interessanti, queste due funzioni associate f_1 ed f_2 hanno ordini di grandezza radicalmente diversi. Ma se definiamo media della funzione aritmetica f la quantità

$$F(x) = \frac{1}{x} \sum_{n \leq x} f(n),$$

questa si comporta in modo molto regolare per la maggior parte delle funzioni aritmetiche interessanti. Nei casi che studieremo, in effetti, saremo in grado di stimare F trovando un *termine principale* ed un *termine d'errore* di ordine di grandezza (quando $x \to +\infty$) piú piccolo.

2.1 Definizioni e prime proprietà

Definizione 2.1.1 (Funzioni aritmetiche) *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 seguenti funzioni aritmetiche elementari:*

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

sono rispettivamente la potenza di esponente β *e la funzione di Eulero.*

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

sono la somma delle potenze dei divisori di n ed il numero dei suoi divisori.

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

sono il numero di fattori primi distinti e totali di n.

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

sono la funzione logaritmo e il numero di rappresentazioni di n come somma di k quadrati.

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

sono la funzione identità e la funzione di von Mangoldt.

Può sembrare strano, a prima vista, l'aver assegnato nomi a funzioni standard quali la potenza e il logaritmo, ma già dalle prossime definizioni dovrebbe risultare chiaro il motivo formale per cui questa scelta risulta convieniente.

𝔈 1 **Definizione 2.1.2** *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 2.1.3 (Funzioni moltiplicative) *Una funzione aritmetica* f *si dice* moltiplicativa *se* $f(1) = 1$ *e per ogni* n, $m \in \mathbb{N}^*$ *con* $(n,m) = 1$ *si ha* $f(nm) = f(n)f(m)$. *Se questo vale per ogni* n, $m \in \mathbb{N}^*$, f *si dice* completamente moltiplicativa. *Indicheremo con* $\mathfrak{M}$ *ed* $\mathfrak{M}^*$ *rispettivamente l'insieme delle funzioni moltiplicative e quello delle funzioni completamente moltiplicative.*

Per esempio, ϕ, d, $\sigma_\beta \in \mathfrak{M}$, mentre 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
Ɛ 2 moltiplicative (ma, ovviamente, $e^\omega \in \mathfrak{M}$, mentre $e^L = N_1$, $e^\Omega \in \mathfrak{M}^*$). Potrebbe sembrare piú naturale dire che f è moltiplicativa se non è identicamente nulla ed $f(nm) = f(n)f(m)$ quando $(n,m) = 1$, ma si verifica facilmente che questa definizione è equivalente a quella data sopra, considerando $n_0 \in \mathbb{N}$ tale che $f(n_0) \neq 0$ ed osservando che $f(n_0 \cdot 1) = f(n_0)f(1)$, e quindi $f(1) = 1$.

Teorema 2.1.4 *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

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

□

Osserviamo però che se f, $g \in \mathfrak{M}^*$, non è detto che $f * g \in \mathfrak{M}^*$, come mostra
Ɛ 3 l'esempio $d = N_0 * N_0$. In altre parole, $\mathfrak{M}^*$ non è un sottogruppo di $\mathfrak{M}$.

Lemma 2.1.5 *Sia $f \in \mathfrak{M}$. Valgono le seguenti relazioni:*

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

Dim. La prima segue immediatamente dalla definizione di moltiplicatività; nella seconda entrambi i membri sono uguali ad $(f * N_0)(n)$, per il Teorema 2.1.4. □

In altre parole, una funzione di $\mathfrak{M}$ è completamente determinata dai suoi valori sulle potenze dei primi, ed, in modo analogo, una funzione di $\mathfrak{M}^*$ è determinata dai suoi valori sui primi, dato che in questo caso $f\left(p^\alpha\right) = f(p)^\alpha$.

Teorema 2.1.6 *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

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

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

$$\begin{aligned}\big((f*g)*h\big)(n)&=\sum_{d_1d_2=n}(f*g)(d_1)h(d_2)=\sum_{d_1d_2=n}\sum_{\delta_1\delta_2=d_1}f(\delta_1)g(\delta_2)h(d_2)\\&=\sum_{\delta_1\delta_2\delta_3=n}f(\delta_1)g(\delta_2)h(\delta_3)=\big(f*(g*h)\big)(n).\end{aligned}$$

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

$$\sum_{d|n}f\left(\frac{n}{d}\right)f^{-1}(d)=0\quad\Rightarrow\quad f(1)f^{-1}(n)=-\sum_{d|n,\,d<n}f\left(\frac{n}{d}\right)f^{-1}(d),\qquad(2.1.1)$$

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 (2.1.1), procedendo come nella dimostrazione del Teorema 2.1.4, si ha

$$\begin{aligned}f^{-1}(nm)&=-\sum_{\substack{d|nm\\ d<nm}}f\left(\frac{nm}{d}\right)f^{-1}(d)\\&=-\sum_{\substack{d_1|n,\ d_2|m\\ d_1d_2<nm}}\sum f\left(\frac{n}{d_1}\right)f\left(\frac{m}{d_2}\right)f^{-1}(d_1)f^{-1}(d_2)\\&=-\sum_{d_1|n}f\left(\frac{n}{d_1}\right)f^{-1}(d_1)\sum_{d_2|m}f\left(\frac{m}{d_2}\right)f^{-1}(d_2)+f^{-1}(n)f^{-1}(m)\\&=-I(n)I(m)+f^{-1}(n)f^{-1}(m)=f^{-1}(n)f^{-1}(m),\end{aligned}$$

poiché almeno uno fra n ed m è >1 e quindi $I(n)I(m)=0$. □

Corollario 2.1.7 *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 2.1.8 *Sia $n \in \mathbb{N}^*$ con la fattorizzazione canonica della Definizione 1.1.4. Si dice* funzione μ di Möbius *la funzione aritmetica $\mu \in \mathfrak{M}$ definita da*

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

𝔈 4 **Teorema 2.1.9** *Si ha $N_0*\mu = I$, cioè $\mu = N_0^{-1}$.*

Dim. Per il Lemma 2.1.5 è sufficiente dimostrare che l'uguaglianza desiderata vale quando n è potenza di un numero primo: se $\alpha \geq 1$

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

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

Corollario 2.1.10 *Se $f \in \mathfrak{M}^*$, allora $f^{-1} = \mu f$, cioè $f^{-1}(n) = \mu(n)f(n)$.*

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

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

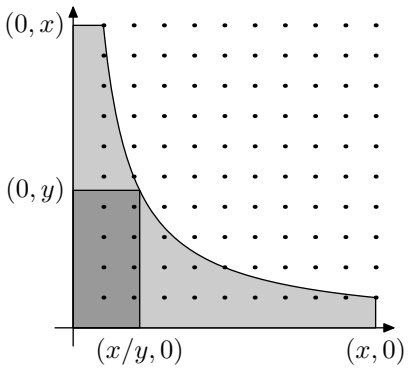
poiché $f(p)f(p)^{\alpha-1} = f(p)^\alpha$. □

Corollario 2.1.11 (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. Se $f = g*\mu$, moltiplichiamo ambo i membri per N_0, ottenendo $f*N_0 = (g*\mu)*N_0 = g*(\mu*N_0) = g*I = g$, e viceversa. □

Teorema 2.1.12 (Seconda formula di inversione di Möbius) *Se $h \in \mathfrak{M}$, allora*

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



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 nella (2.1.2) 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 2.1: Dimostrazione del Teorema 2.1.13.

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

Teorema 2.1.13 (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

$$\sum_{n\le x} f*g(n) = \sum_{n\le y} F\left(\frac{x}{n}\right) g(n) + \sum_{n\le x/y} f(n)G\left(\frac{x}{n}\right) - F\left(\frac{x}{y}\right) G(y). \tag{2.1.2}$$

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. Si veda la Figura 2.1. In effetti

$$\sum_{1\le n\le x} f*g(n) = \sum_{1\le n\le x} \sum_{hk=n} f(h)g(k)$$
$$= \sum_{1\le k\le y} g(k) \sum_{1\le h\le x/k} f(h) + \sum_{y<k\le x} \sum_{1\le h\le x/k} f(h)g(k)$$

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

□

Esercizi.

𝔈 1. Dimostrare che nell'anello delle funzioni aritmetiche, la moltiplicazione puntuale per L è una derivazione, cioè che per ogni $f, g\colon \mathbb{N}^* \to \mathbb{C}$ e per ogni $c \in \mathbb{C}$ si ha $L(cf) = cLf$, $L(f+g) = Lf + Lg$ e $L(f*g) = (Lf)*g + f*(Lg)$.

𝔈 2. Dimostrare che posto $f(n) := \left[\sqrt{n}\right] - \left[\sqrt{n-1}\right]$, si ha $f \in \mathfrak{M} \setminus \mathfrak{M}^*$.

𝔈 3. Dimostrare che $N_k \in \mathfrak{M}^*$ per ogni $k \in \mathbb{C}$, ma che $N_0 * N_0 = d \notin \mathfrak{M}^*$.

𝔈 4. Dare una dimostrazione alternativa del Teorema 2.1.9 osservando che se $n > 1$ ha la fattorizzazione canonica 1.1.4, allora gli unici termini diversi da zero nella somma $(N_0 * \mu)(n) = \sum_{d|n} \mu(d)$ sono quelli per cui d divide $p_1 \cdots p_k$.

𝔈 5. * Utilizzando la Seconda Formula di Möbius 2.1.12 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.

Riferimenti. Varî Teoremi e dimostrazioni sono adattati da Apostol [5] Cap. 2. Si veda anche Apostol [4] per la caratterizzazione delle funzioni completamente moltiplicative.

2.2 Alcune funzioni aritmetiche importanti

Teorema 2.2.1 *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 $r_2(1) = 4$, $(1 = 0^2 + (\pm 1)^2 = (\pm 1)^2 + 0^2)$, ma osserviamo che $\frac{1}{4} r_2$, invece, è moltiplicativa: cfr Teorema 4.6.1. La seconda affermazione segue dal fatto che $r_2(4n+3) = 0$ per ogni $n \in \mathbb{N}$, poiché $x^2 \in \{0, 1\} \bmod 4$, e dunque $x^2 + y^2 \in \{0, 1, 2\} \bmod 4$.

Dimostreremo la terza provando che se $p \equiv 1 \bmod 4$, allora $r_2\big(p^\alpha\big) \geq 4\alpha + 4$. Questo è certamente vero per $\alpha = 0$, dato che $1 = 0^2 + (\pm 1)^2 = (\pm 1)^2 + 0^2$. Ricordiamo inoltre che, per l'Osservazione di Fermat 1.4.6, 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. □

Æ 1-2

Teorema 2.2.2 (Gauss) *Per $x \to +\infty$ si ha*

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

Dim. A ciascuna coppia di interi (a,b) associamo in modo univoco il quadrato $Q(a,b)$ di vertici $\big(a - \frac{1}{2}, b - \frac{1}{2}\big)$, $\big(a + \frac{1}{2}, b - \frac{1}{2}\big)$, $\big(a + \frac{1}{2}, b + \frac{1}{2}\big)$, $\big(a - \frac{1}{2}, b + \frac{1}{2}\big)$. 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 $\rho_1 = \sqrt{x} - \sqrt{2}$ ed $\rho_2 = \sqrt{x} + \sqrt{2}$, rispettivamente. È chiaro che $C_1 \subseteq U(x) \subseteq C_2$, e quindi $\pi\rho_1^2 \leq \iint_{U(x)} \mathrm{d}u\, \mathrm{d}v \leq \pi\rho_2^2$. Ma $\pi\rho^2 = \pi x + O\big(x^{1/2}\big)$ sia per $\rho = \rho_1$ che per $\rho = \rho_2$, ed il risultato voluto segue. □

Æ 3

Una dimostrazione simile è illustrata nella Figura 2.2: la circonferenza continua ha raggio $x^{1/2}$, quelle tratteggiate hanno raggio $x^{1/2} \pm 2^{1/2}$. L'area in grigio è

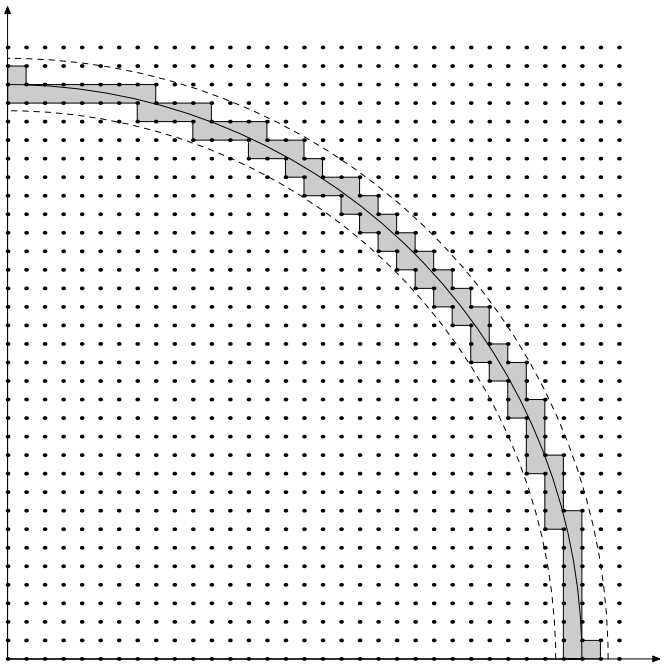


Figura 2.2: Dimostrazione del Teorema di Gauss 2.2.2.

uguale al numero delle coppie (n,m) per cui $n^2+m^2 \le x$, ma $(n+1)^2+(m+1)^2 > x$, e quindi il quadrato di vertici opposti (n,m) ed $(n+1,m+1)$ è solo parzialmente contenuto nel cerchio di raggio $x^{1/2}$. Quest'area vale $O\big(x^{1/2}\big)$.

Teorema 2.2.3 (Landau) *Per $x \to +\infty$ si ha*

$$R_2'(x) \stackrel{\text{def}}{=} |\{n \le x\colon\ r_2(n) \ge 1\}| \sim \frac{x}{(K\log x)^{1/2}}$$

dove

$$K \stackrel{\text{def}}{=} 2 \prod_{p \equiv 3 \bmod 4} \left(1 - \frac{1}{p^2}\right).$$

𝔈 4 Si vedano anche il Teorema 4.6.1 e il Capitolo 5. Il Teorema di Gauss 2.2.1 dice che $r_2(n)$ in media vale π, ma il Teorema di Landau 2.2.3 afferma che $r_2(n)$ vale 0 per "quasi tutti" gli interi n.

A questo punto è opportuno leggere le Appendici A.1 e A.4.

Teorema 2.2.4 *La funzione $d \in \mathfrak{M}$, e $d\big(p^\alpha\big) = \alpha+1$. 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 $k-1 \leq \Delta < k$, e $\delta := k - \Delta > 0$. Siano p_i l'i-esimo numero primo ed $n := p_1 \cdots p_k$. Per quanto già dimostrato, $d\big(n^m\big) = (m+1)^k > m^k$, e quindi

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

𝔈 6 dove $c(k) > 0$ è una costante che dipende solo da k. Dunque

$$d\big(n^m\big) > c(k) \big(\log(n^m)\big)^{\Delta+\delta}$$

da cui $d\big(n^m\big)\big(\log(n^m)\big)^{-\Delta} > c(k)\big(\log(n^m)\big)^{\delta} \to +\infty$ quando $m \to +\infty$. □

Teorema 2.2.5 (Dirichlet) *Sia γ la costante di Eulero definita dalla (A.4.1). Per $x \to +\infty$ si ha*

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

𝔈 8 **Dim.** Segue dal Teorema 2.1.13 con $y = x^{1/2}$ e dal Teorema A.4.1 per $k = -1$. □

Dirichlet introdusse il Metodo dell'Iperbole 2.1.13 per migliorare il termine di errore che proviene da una stima ingenua della funzione D: infatti si potrebbe procedere cosí

$$\begin{aligned} D(x) &= \sum_{n \leq x} d(n) = \sum_{n \leq x} \sum_{d \mid n} 1 = \sum_{d \leq x} \sum_{\substack{n \leq x \\ d \mid n}} 1 \\ &= \sum_{d \leq x} \left[\frac{x}{d} \right] = \sum_{d \leq x} \left(\frac{x}{d} + O(1) \right) = x \log x + O(x). \end{aligned}$$

Sostanzialmente questo è il caso $y = x$ della (2.1.2). Il vantaggio del Teorema 2.1.13 risiede nel fatto che possiamo scegliere $y = x^{1/2}$ e quindi avere una somma "corta" e di conseguenza un termine d'errore molto piú piccolo.

Teorema 2.2.6 *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 9 ed il risultato segue dal Lemma 2.1.5. □

Osservazione 2.2.7 (Eulero) *Se esistessero un numero finito di primi $p_1, \ldots, p_r$, posto $M := p_1 \cdots p_r$, si avrebbe $\phi(M) = 1$, dato che ogni intero > 1 dovrebbe essere divisibile per un fattore di M, ma per $M \geq 3$ si ha $\phi(M) \geq 2$, poiché $(1, M) = (M-1, M) = 1$.*

Teorema 2.2.8 *La funzione $\phi \in \mathfrak{M}$, e $\phi(p^\alpha) = p^\alpha - p^{\alpha-1}$. Inoltre $\phi = N_1 * \mu$,*

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

Dim. Per dimostrare che $\phi \in \mathfrak{M}$ 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 $f(a,b) := am + bn \bmod nm$. È chiaro che f è iniettiva: se $am + bn \equiv \alpha m + \beta n \bmod nm$ allora $bn \equiv \beta n \bmod m$ e quindi $b \equiv \beta \bmod m$, ed allo stesso modo $a \equiv \alpha \bmod n$. Per dimostrare che f è suriettiva, ricordiamo che per il Teorema 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 $\phi(p^\alpha)$ contiamo quanti interi dell'intervallo $[1, p^\alpha]$ 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 $\phi = N_1 * \mu$ osserviamo che N_1, $\mu \in \mathfrak{M}$, e quindi dobbiamo verificare quest'uguaglianza quando $n = p^\alpha$. In questo caso abbiamo

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

dato che tutti gli eventuali altri addendi sono nulli. Osserviamo che abbiamo già dimostrato la relazione equivalente $N_1 = \phi * N_0$ nel Lemma 1.2.11. L'affermazione sul massimo limite segue dal fatto che $\phi(p) = p - 1$ per ogni primo p, e che $\phi(n) \leq n$ per ogni intero $n \in \mathbb{N}^*$. L'ultima affermazione è una riscrittura delle
𝔈 10-12 proprietà appena dimostrate. □

Lemma 2.2.9 *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 2.1.11. Inoltre, se n ha la fattorizzazione canonica 1.1.4, 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 2.2.10 *Si ha $\mu \cdot L = -\mu * \Lambda$ o, equivalentemente,*

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

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

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

□

Teorema 2.2.11 (Ramanujan) *La funzione di Ramanujan $c_q(n)$ definita nella (2.2.1) qui sotto è una funzione moltiplicativa di q e si ha*

$$c_q(n) \stackrel{\text{def}}{=} \sum_{h=1}^{q}{}^{*} \mathrm{e}\Big(\frac{hn}{q}\Big) = \mu\Big(\frac{q}{(q,n)}\Big) \frac{\phi(q)}{\phi(q/(q,n))}. \tag{2.2.1}$$

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

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

cioè $c_q \in \mathfrak{M}$. Per la (1.2.3) si ha

$$f_n(q) \stackrel{\text{def}}{=} \sum_{h=1}^{q} \mathrm{e}\Big(\frac{hn}{q}\Big) = \sum_{d|q} \sum_{a=1}^{d}{}^{*} \mathrm{e}\Big(\frac{an}{d}\Big) = \sum_{d|q} c_d(n). \tag{2.2.2}$$

Inoltre $f_n(q) = 0$ se $q \nmid n$ ed $f_n(q) = q$ se $q \mid n$. Per la prima formula di Möbius 2.1.11

$$c_q(n) = \sum_{d|q} \mu\Big(\frac{q}{d}\Big) \sum_{a=1}^{d} \mathrm{e}\Big(\frac{an}{d}\Big) = \sum_{d|q, d|n} \mu\Big(\frac{q}{d}\Big) d.$$

$$
\begin{array}{rr}
d=1 & 0\,.\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\,1\ldots \\
d=2 & -0\,.\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\,0\,1\ldots \\
d=3 & -0\,.\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\,0\,0\,1\ldots \\
d=5 & -0\,.\,0\,0\,0\,0\,1\,0\,0\,0\,0\,1\,0\,0\,0\,0\,1\,0\,0\,0\,0\,1\,0\,0\,0\,0\,1\,0\,0\,0\,0\,1\ldots \\
d=6 & 0\,.\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,1\ldots \\
d=10 & 0\,.\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\ldots \\
d=15 & 0\,.\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\ldots \\
d=30 & -0\,.\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,0\,1\ldots \\
\hline
S_3 = & 0\,.\,1\,0\,0\,0\,0\,0\,1\,0\,0\,0\,1\,0\,1\,0\,0\,0\,1\,0\,1\,0\,0\,0\,1\,0\,0\,0\,0\,0\,1\,0\ldots
\end{array}
$$

Figura 2.3: La formula di Gandhi 2.2.12 "corrisponde" a fare un crivello con i fattori primi di P_n, scrivendo in binario le quantità $\mu(d)/(2^d-1)$ e sommando in colonna, bit per bit. Si veda il Principio di Inclusione–Esclusione 5.1.2.

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

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

e questo si vede facilmente distinguendo varî 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 $\phi\big(p^\alpha\big)$. □

Si noti che nel caso $(n,q)=1$ il Teorema 2.2.11 si riduce a $c_q(n)=\mu(q)$, che quindi è indipendente da n. Quest'ultima affermazione si può giustificare facilmente se osserviamo che in questo caso (come abbiamo già fatto nella dimostrazione del Teorema 1.6.4) l'applicazione $h\mapsto hn^{-1}$ è ben definita modulo q e lascia invariata la somma che definisce $c_q(n)$. Sfruttando poi il fatto che $c_q\in\mathfrak{M}$,
𝔈 14 è sufficiente determinare $c_{p^\alpha}(1)$, che lasciamo come esercizio.

Torniamo di nuovo alla questione delle "formule" per i numeri primi discussa nel §1.7, dimostrando una relazione che permette, in linea di principio, di calcolare iterativamente tutti i numeri primi. In pratica, naturalmente, questo procedimento risulta piú oneroso del Crivello di Eratostene discusso nel §5.1: infatti, la somma S_n definita sotto contiene 2^n addendi, che è necessario calcolare con una precisione di almeno $n\log n$ cifre binarie. Per questo motivo, la sua complessità computazionale la rende inutilizzabile.

Teorema 2.2.12 (Formula di Gandhi) *Sia p_n l'n-esimo numero primo. Poniamo $P_n:=p_1\cdot p_2\cdots p_n$. Allora per $n\geq 0$ si ha*

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

Dim. Per $n=0$ si ha $P_0=1$ e quindi la formula dà $p_1=2$. Per $n\geq 1$ si ha

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

dove I è la funzione 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 $n\geq 1$

$$\frac{1}{2}+\frac{1}{2^{p_{n+1}}} < S_n < \frac{1}{2}+\frac{1}{2^{p_{n+1}}}\left(1+\frac{1}{2}+\frac{1}{2^2}+\frac{1}{2^3}+\cdots\right) = \frac{1}{2}+\frac{2}{2^{p_{n+1}}}.$$

Da questo segue che

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

che implica la tesi. La Figura 2.3 illustra il caso $n=3$ della dimostrazione. □

Esercizi.

𝔈 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.

𝔈 2. Utilizzando il Teorema 2.2.1 con $p=5$ ed $n=5^\alpha$, si dimostri che

$$\limsup_{n\to+\infty} \frac{r_2(n)}{\log n} \geq \frac{4}{\log 5}.$$

𝔈 3. Procedendo come nella dimostrazione del Teorema di Gauss 2.2.2, si dimostri che

$$R_k(x) \stackrel{\text{def}}{=} \sum_{n\leq x} r_k(n) = V_k x^{k/2} + O_k\left(x^{(k-1)/2}\right),$$

dove V_k indica il volume della sfera unitaria di $\mathbb{R}^k$.

𝔈 4. Si sfrutti il Teorema di Landau 2.2.3 per dimostrare che

$$\max_{n\leq x} r_2(n) \geq \pi\sqrt{K\log x}\big(1+o(1)\big),$$

dove K è la costante nel Teorema. Suggerimento:

$$\sum_{n\leq x} r_2(n) \leq \left(\max_{n\leq x} r_2(n)\right)\cdot R_2'(x).$$

Ɛ 5. Dato $n \in \mathbb{N}^*$ determinare $\big|\{(x,y) \in \mathbb{N}^2 : n = x^2 - y^2\}\big|$.

Ɛ 6. Dimostrare che $d(n)$ è dispari se e solo se $n = m^2$.

Ɛ 7. Per $k \in \mathbb{N}^*$ si ponga $d_k := N_0 * \cdots * N_0$, dove ci sono k fattori (e quindi $d_2 = d$). Dimostrare che $d_k \in \mathfrak{M}$ e che $d_k(p^\alpha) = \binom{\alpha+k-1}{k-1}$.

Ɛ 8. Usare la formula di Euler-McLaurin A.1.2 per dimostrare che esistono a, b, $c \in \mathbb{R}$ tali che $\sum_{n\le x} d_3(n) = x(a\log^2 x + b\log x + c) + O\big(x^{2/3}\log x\big)$.

Ɛ 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 $n = 2^{p-1}M_p$. Non si sa se esistono numeri perfetti dispari.

Ɛ 10. Determinare tutti gli $n \in \mathbb{N}^*$ per cui $\phi(n) \not\equiv 0 \bmod 4$ e quelli per cui $\phi(n) \mid n$.

Ɛ 11. Dimostrare che $\phi(n) \neq 14$ per ogni $n \in \mathbb{N}^*$.

Ɛ 12. Sapendo che $\mu(n) \neq 0$ e conoscendo $\phi(n)n^{-1}$, determinare n.

Ɛ 13. Dimostrare che $d(n) = \Omega_+((\log n)^\Delta)$ (Teorema 2.2.4) dando una minorazione per $d(n!)$: fissato m tale che $\pi(m) > \Delta$, per n grande si ha $d(n!) \ge (n/p_1)\cdots(n/p_m) = c(m)n^{\pi(m)}$ poiché l'esponente di p_i nella fattorizzazione canonica di $n!$ vale almeno $\lfloor n/p_i \rfloor \ge n/p_i - 1$. Inoltre $\log(n!) \sim n\log n$ per la formula di Stirling A.3.2.

Ɛ 14. Determinare $c_{p^\alpha}(1)$ sfruttando l'identità (2.2.2).

Riferimenti. Funzione r_2: Teoremi 336 e 337 di Hardy & Wright [57]. Teorema di Gauss 2.2.2: Hardy & Wright [57] Teorema 339. Teorema di Landau 2.2.3: l'articolo originale è Landau [82]. Si vedano anche Hardy [53] §§4.4–4.7 per una breve descrizione della dimostrazione, oppure Landau [84] §§176–183 per i dettagli. Altri problemi di natura simile ai Teoremi 2.2.2 e 2.2.3 si possono trovare in [53] Cap. 5, ed in Hardy & Wright [57] §§18.2-18.7. Per l'Osservazione di Eulero 2.2.7 si veda Shanks [135] §27, pag. 70. Il Lemma 2.2.11 è il Teorema 272 di Hardy & Wright [57]. Per la formula di Gandhi 2.2.12 si veda Gandhi [39], Golomb [44], Vanden Eynden [140].

2.3 Il prodotto di Eulero

Ricordiamo che, per definizione, il prodotto infinito

$$\prod_{n\ge 1}(1+a_n) \stackrel{\text{def}}{=} \lim_{N\to\infty}\prod_{n\le N}(1+a_n)$$

è convergente se il limite in questione esiste ed è un numero complesso diverso da 0, con la condizione supplementare che $a_n \neq -1$ per ogni $n \geq 1$. Per i prodotti *finiti* non c'è una convenzione analoga. Per questo motivo dobbiamo dare una versione del prossimo enunciato in un modo apparentemente un po' bizzarro.

Teorema 2.3.1 (Prodotto di Eulero) *Sia $f \in \mathfrak{M}$ una funzione aritmetica moltiplicativa tale che $\sum_{n\geq 1} |f(n)|$ sia convergente. Per ogni numero primo p poniamo*

$$F(p) \stackrel{\text{def}}{=} f(p) + f\big(p^2\big) + f\big(p^3\big) + \cdots = \sum_{\nu \geq 1} f\big(p^\nu\big).$$

Se $F(p) \neq -1$ per ogni numero primo p, allora vale l'identità

$$\sum_{n\geq 1} f(n) = \prod_{p} \big(1 + F(p)\big), \tag{2.3.1}$$

dove il prodotto è esteso a tutti i numeri primi ed è assolutamente convergente. Se esiste un numero primo p_0 tale che $F(p_0) = -1$ allora la somma a sinistra nella (2.3.1) vale 0. Infine, se $f \in \mathfrak{M}^*$ allora $F(p) \neq -1$ per ogni numero primo p e

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

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

$$S \stackrel{\text{def}}{=} \sum_{n\geq 1} f(n) \qquad \text{e} \qquad P(x) \stackrel{\text{def}}{=} \prod_{p\leq x} \big(1 + F(p)\big). \tag{2.3.2}$$

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

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

Osserviamo che se $n \notin \mathcal{A}(x)$ allora $n > x$. Dunque

$$\Big|S - P(x)\Big| \leq \sum_{n\notin\mathcal{A}(x)} \big|f(n)\big| \leq \sum_{n>x} \big|f(n)\big| \to 0$$

quando $x \to +\infty$. La prima parte della tesi segue sia nel caso in cui $F(p) \neq -1$ per ogni p primo sia se, viceversa, esiste un numero primo p_0 per cui $F(p_0) = -1$, perché allora $P(x) = 0$ per $x \geq p_0$. Nel solo primo caso, il prodotto converge assolutamente poiché

$$\Big|\sum_{p} F(p)\Big| \leq \sum_{p} \sum_{n\geq 1} \big|f\big(p^n\big)\big| \leq \sum_{n\geq 1} |f(n)|.$$

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 dalla formula per la somma di una progressione geometrica.

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: sfruttando la moltiplicatività otteniamo

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

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

$$\begin{aligned}\sum_{n\geq 1} f(n) &= \Big(1+F(2)\Big) \sum_{\nu\geq 0} \sum_{\substack{n\geq 1 \\ 2\nmid n,\, 3^\nu \| n}} f(n) \\ &= \Big(1+F(2)\Big)\Big(1+F(3)\Big) \sum_{\substack{m\geq 1 \\ (2\cdot 3, m)=1}} f(m).\end{aligned}$$

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

$$\sum_{n\geq 1} f(n) = \Big(\prod_{j=1}^{k} \big(1+F(p_j)\big)\Big) \sum_{\substack{m\geq 1 \\ p\mid m \Rightarrow p > p_k}} f(m). \tag{2.3.3}$$

Notiamo che nel caso in cui esiste un numero primo p_0 tale che $F(p_0) = -1$ la tesi segue immediatamente. In caso contrario, si ha evidentemente

$$\Big| \sum_{\substack{m\geq 1 \\ p\mid m \Rightarrow p > p_k}} f(m) - 1 \Big| \leq \sum_{n > p_k} |f(n)| \tag{2.3.4}$$

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

$$\lim_{k\to+\infty} \sum_{\substack{m\geq 1 \\ p\mid m \Rightarrow p > p_k}} f(m) = 1. \tag{2.3.5}$$

In generale, la (2.3.3) e la (2.3.5) 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 $P(x)$ è definito nella (2.3.2). □

Esercizi.

𝔈 1. Si dimostri che l'ipotesi di convergenza assoluta nell'enunciato del Teorema 2.3.1 è necessaria, prendendo $f(n) = \mu(n)$.

Riferimenti. Prodotto di Eulero 2.3.1: Apostol [5], Teorema 11.6 oppure Ingham [73], §1.6. Definizione e proprietà dei prodotti infiniti: Titchmarsh [138], §1.4–1.44; per il prodotto di serie assolutamente convergenti, *ibidem*, §§1.6–1.65.

2.4 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 6 che le serie di Dirichlet sono molto piú utili nello studio dei numeri primi se introdotte nel loro appropriato contesto analitico.

Definizione 2.4.1 *Data una qualsiasi successione* $(a_n)_{n\in\mathbb{N}^*}$ *a valori in* $\mathbb{C}$*, definiamo la* serie di Dirichlet formale *associata mediante*

$$f(s) \stackrel{\text{def}}{=} \sum_{n\geq 1} \frac{a_n}{n^s}. \tag{2.4.1}$$

La funzione f nella (2.4.1) si dice *funzione generatrice* della successione a_n. È chiaro che è possibile studiare la successione a_n, o meglio, la funzione aritmetica a_n, e le sue proprietà a prescindere dallo studio di f e viceversa, ma vedremo nel Capitolo 6 che in generale è possibile studiare le due cose insieme. Questo tipo di funzioni generatrici è particolarmente adatto a studiare le funzioni aritmetiche moltiplicative, come abbiamo visto all'inizio di questo capitolo, e soprattutto nel Teorema di Eulero 2.3.1. Naturalmente non è l'unico tipo di funzioni generatrici che si possono considerare, ed infatti nel Capitolo 7 vedremo un tipo di funzioni generatrici completamente diverso, adatto ai problemi additivi.

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 6): 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 §2.1 sono del tutto evidenti: il fatto che il prodotto di Dirichlet commuti e sia associativo è immediato. I Teoremi 2.1.9 e 2.2.4 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 6.2.2). È semplice verificare la prima formula di inversione di Möbius 2.1.11: 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 2.2.9 equivale a

$$-\frac{\zeta'}{\zeta}(s) = \big(-\zeta'(s)\big)\frac{1}{\zeta(s)}$$

dato che

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

Ci limitiamo ad osservare che affinché la serie a destra della (2.4.1) converga
𝔈 1 in qualche insieme è necessario e sufficiente che $a_n = O(n^c)$ 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 $\sum_{n\leq x} a_n$.

Esercizi.

𝔈 1. Dimostrare che $\sum_{n\geq 1} a_n n^{-s}$ converge in qualche insieme se e solo se esiste $c\in\mathbb{R}$ tale che $a_n = O(n^c)$, e quindi la serie converge assolutamente per $\sigma > c+1$.

Riferimenti. Si veda il Cap. 17 di Hardy & Wright [57], in particolare i §§6–7.

2.5 Problemi aperti

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 2.2.2 e 2.2.4 abbiamo visto che $E_i(x) = O\big(x^{1/2}\big)$ per $i = 1, 2$. Questi risultati sono stati migliorati ed ora è noto che $E_1(x) = O\big(x^{139/429+\varepsilon}\big)$ e che $E_2(x) = O\big(x^{35/108}\big)$. Hardy ha dimostrato che $E_1(x) = \Omega_{\pm}\big(x^{1/4}\big)$ e lo stesso vale per $E_2(x)$. Per i risultati piú forti (che sono complicati da enunciare) si rimanda ai libri di Ivić [74] e Titchmarsh [137].

Per s, $k \in \mathbb{N}^*$ si definisca $r_{s,k}(n) := |\{(x_1, \dots, x_s) \in \mathbb{N}^s \colon x_1^k + \cdots + x_s^k = n\}|$. Waring nelle *Meditationes Algebraicæ* [144] del 1770 si chiese se dato $k \geq 2$ 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 si sa che

$$g(k) \leq 2^k + \left[\left(\frac{3}{2}\right)^k\right] + \left[\left(\frac{4}{3}\right)^k\right] - 2.$$

Il punto è che il valore di $g(k)$ è enormemente gonfiato dagli interi relativamente piccoli che richiedono un valore di 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 $G(k) \leq k\big(\log k + \log\log k + O(1)\big)$ per $k \to +\infty$. È relativamente facile dimostrare che $G(k) \geq k + 1$.

Riferimenti. Titchmarsh [137] Cap. 13 e relative note, oppure Ivić [74] §13.2, 13.8 e Note. Problema di Waring: Vaughan [141], Ellison [33], Wooley [148].

Capitolo 3

Distribuzione dei Numeri Primi

Questo Capitolo è dedicato principalmente alla dimostrazione del Teorema dei Numeri Primi 3.1.3 facendo uso esclusivamente di tecniche "elementari," e cioè senza l'analisi complessa: questo significa che i risultati che saremo in grado di ottenere sono piú deboli di quelli che dimostreremo nel Capitolo 6, ma è comunque interessante dare una dimostrazione relativamente semplice di fatti importanti.

La prima parte del Capitolo è dedicata ai risultati di Chebyshev e di Mertens, che sono conseguenze quasi immediate del Teorema dei Numeri Primi: evidentemente è importante notare che possono essere dimostrate anche direttamente. Poi passeremo alla dimostrazione elementare del Teorema dei Numeri Primi dovuta a Selberg [134] ed Erdős [35] (1949): la dimostrazione originale di Hadamard e de la Vallée Poussin (che hanno lavorato indipendentemente su una traccia lasciata da Riemann nel 1859 [129]) è del 1896 e nel mezzo secolo fra i due risultati molti matematici si sono sbilanciati nell'affermare che una dimostrazione elementare era impossibile. La recensione di Ingham [72] dei lavori di Selberg ed Erdős spiega dettagliatamente le somiglianze formali fra le due dimostrazioni, quella "elementare" da un lato e quella "analitica" dall'altro.

3.1 Risultati elementari

Definizione 3.1.1 (Funzioni di Chebyshev) *Per $x \geq 1$ poniamo*

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

Vedremo subito nel §3.2 che la funzione $\pi(x)$ è dell'ordine di grandezza di $x/\log x$ (e quindi che l'n-esimo numero primo p_n è dell'ordine di $n \log n$), mentre le funzioni θ e ψ differiscono fra loro di poco (Lemma 3.2.4). Il "peso" $\log p$ con cui contiamo i numeri primi in θ (ed il peso $\Lambda(n)$ con cui contiamo le potenze dei

2	3	5	7	11	13	17	19	23	29	31	37
41	43	47	53	59	61	67	71	73	79	83	89
97	101	103	107	109	113	127	131	137	139	149	151
157	163	167	173	179	181	191	193	197	199	211	223
227	229	233	239	241	251	257	263	269	271	277	281
283	293	307	311	313	317	331	337	347	349	353	359
367	373	379	383	389	397	401	409	419	421	431	433
439	443	449	457	461	463	467	479	487	491	499	503
509	521	523	541	547	557	563	569	571	577	587	593
599	601	607	613	617	619	631	641	643	647	653	659
661	673	677	683	691	701	709	719	727	733	739	743
751	757	761	769	773	787	797	809	811	821	823	827
829	839	853	857	859	863	877	881	883	887	907	911
919	929	937	941	947	953	967	971	977	983	991	997

Figura 3.1: I numeri primi fino a 1000.

primi in ψ) bilancia esattamente la rarefazione dei primi, come dimostra il Teorema di Chebyshev 3.2.2. In definitiva, le tre funzioni $\pi(x)\log x$, $\theta(x)$ e $\psi(x)$ sono "equivalenti," almeno in prima approssimazione. Nel Capitolo 6 spiegheremo perché la funzione ψ, anche se apparentemente artificiale, è in realtà la piú naturale delle tre: per il momento ci limitiamo ad osservare che $\psi(x)$ è il logaritmo del
Æ 1 minimo comune multiplo di tutti gli interi fra 1 ed x.

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 come quelle discusse nel §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 B per un confronto numerico fra le varie approssimazioni proposte. Si consultino anche le Tavole II e III di Rosser & Schoenfeld [131], 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.

Definizione 3.1.2 *Per $x \ge 2$ definiamo la funzione* logaritmo integrale *per mezzo della relazione*

$$\mathrm{li}(x) \stackrel{\mathrm{def}}{=} \lim_{\varepsilon\to 0+} \left\{ \int_{\varepsilon}^{1-\varepsilon} + \int_{1+\varepsilon}^{x} \right\} \frac{\mathrm{d}t}{\log t}. \tag{3.1.1}$$

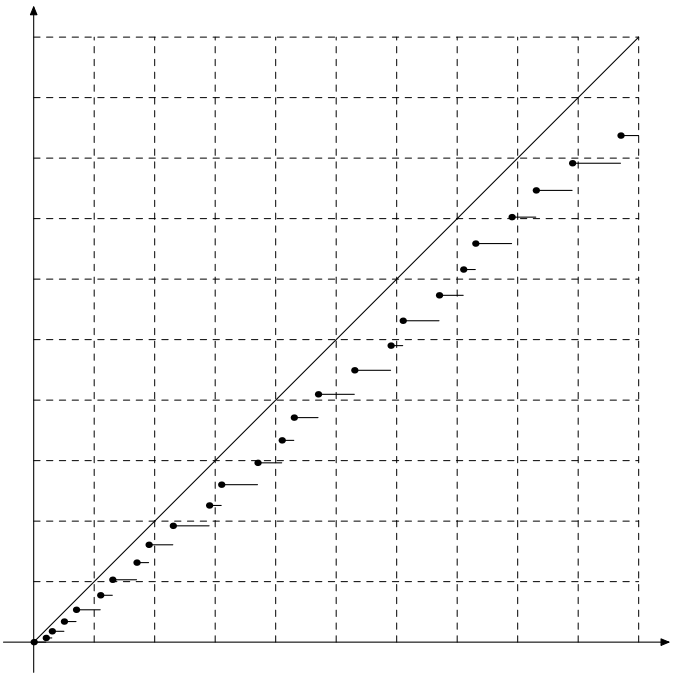


Figura 3.2: Il grafico di $\theta(x)$ e di x per $x \in [0,100]$.

Scopo principale di questo Capitolo è la dimostrazione di una forma debole del seguente risultato, che si chiama Teorema dei Numeri Primi: è stato congetturato da Gauss alla fine del Settecento, ma è stato dimostrato solo un secolo piú tardi.

Teorema 3.1.3 (Hadamard-de la Vallée Poussin) *Esiste una costante $c > 0$ tale che per $x \to +\infty$ si ha*

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

In questo Capitolo ci limiteremo a dimostrare che $\pi(x) \sim \mathrm{li}(x) \sim x/\log x$ quando $x \to +\infty$. Nel Capitolo 6 daremo i punti essenziali della dimostrazione di una versione con termine d'errore $O\big(x\exp\{-c(\log x)^{1/2}\}\big)$, che è leggermente piú debole di quello in 3.1.3. Si vedano i Capitoli 7–18 del libro di Davenport [22]. Per poter confrontare il risultato $\pi(x) \sim x/\log x$ con il Teorema 3.1.3, osserviamo che mediante integrazioni per parti ripetute è facile mostrare che per ogni $n \in \mathbb{N}$ fissato
𝔈 5 si ha

$$\mathrm{li}(x) = \frac{x}{\log x}\sum_{k=0}^{n}\frac{k!}{(\log x)^k} + O_n\left(\frac{x}{(\log x)^{n+2}}\right). \tag{3.1.2}$$

Quindi in questo Capitolo dimostreremo 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 6.

Legendre fu il primo a fare congetture sulla distribuzione dei numeri primi, ed in particolare sull'andamento della funzione π: formulata in termini moderni, la sua congettura prende la forma

$$\pi(x) = \frac{x}{\log x - A + o(1)}, \qquad \text{dove} \qquad A = 1.08366\ldots \tag{3.1.3}$$

Questa congettura può essere scritta in un'altra forma equivalente, e cioè

$$\pi(x) = \frac{x}{\log x} + (A + o(1))\frac{x}{(\log x)^2}.$$

Se il termine con $k = 1$ nello sviluppo (3.1.2) è rilevante, allora A vale 1, e la congettura di Legendre è falsa. In realtà possiamo dimostrare la falsità della congettura di Legendre senza usare neppure il Teorema dei Numeri Primi: ce ne occuperemo alla fine del §3.3.

Gauss invece congetturò la validità del Teorema dei Numeri Primi con termine principale $\mathrm{li}(x)$, ma senza dare indicazioni precise sul termine d'errore.

Il termine d'errore nell'enunciato del Teorema dei Numeri Primi 3.1.3 probabilmente non è ottimale: in effetti si congettura che sia, sostanzialmente, dell'ordine di grandezza della radice quadrata del termine principale. Si tratta della Congettura di Riemann.

Congettura 3.1.4 (Riemann) *Per $x \to +\infty$ si ha*

$$\pi(x) = \mathrm{li}(x) + O\big(x^{1/2}\log x\big).$$

Nei prossimi paragrafi otterremo dei risultati approssimati sempre piú precisi: per la maggior parte sono conseguenze immediate del Teorema dei Numeri Primi, ma noi le useremo come base per la dimostrazione "elementare."

Esercizi.

$\mathfrak{E}$ 1. Dimostrare che $\psi(x) = \log\big[1, 2, \ldots, [x]\big]$.

$\mathfrak{E}$ 2. Dimostrare che se p è primo e $p^\alpha \parallel n!$, allora

$$\alpha = \sum_{r\geq 1}\left[\frac{n}{p^r}\right] \leq \frac{n}{p-1}.$$

$\mathfrak{E}$ 3. Con quante cifre 0 termina la rappresentazione decimale di 1000! ?

$\mathfrak{E}$ 4. Senza usare il Teorema dei Numeri Primi 3.1.3 dimostrare che dato $n \in \mathbb{N}$ è possibile trovare n interi consecutivi non primi.

$\mathfrak{E}$ 5. Dimostrare per induzione la formula (3.1.2).

3.2 I Teoremi di Eulero e di Chebyshev

Teorema 3.2.1 (Eulero) *La serie e il prodotto seguenti sono divergenti:*

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

Dim. Sia $f_x \in \mathfrak{M}^*$ con $f_x(p) := p^{-1}$ se $p \le x$, $f_x(p) := 0$ se $p > x$. In sostanza poniamo $f_x(n) := n^{-1}$ se n non ha fattori primi $> x$, e poniamo $f_x(n) := 0$ in caso contrario. Poiché f_x è completamente moltiplicativa, per il Teorema 2.3.1 si ha

$$P(x) \stackrel{\text{def}}{=} \prod_{p\le x}\left(1-\frac{1}{p}\right)^{-1} = \sum_{n\ge 1} f_x(n) = \sum_{n\in\mathcal{A}(x)} \frac{1}{n},$$

dove

$$\mathcal{A}(x) \stackrel{\text{def}}{=} \{n \in \mathbb{N}^* :\ p \mid n \Rightarrow p \le x\}.$$

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

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

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

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

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. I Teoremi 3.3.4 e 3.3.6 mostrano che le minorazioni ottenute sono dell'ordine di grandezza corretto.

È importante notare che questo risultato di Eulero non solo dimostra che esistono infiniti numeri primi, ma dà anche delle indicazioni numeriche sulla loro densità: infatti notiamo che le serie dei reciproci delle potenze di 2, o la somma dei reciproci dei quadrati perfetti sono entrambe convergenti. Quindi, in un senso non molto preciso, possiamo dire che i numeri primi sono piú numerosi dei quadrati perfetti. Notiamo anche che, per il criterio integrale per la convergenza delle serie (vedi Lemma A.1.3) la minorazione ottenuta nel corso della dimostrazione suggerisce che $p_n \approx n\log n$: infatti

$$\sum_{\substack{n\ge 2\\ n\log n\le x}} \frac{1}{n\log n} \approx \sum_{n=2}^{x/\log x} \frac{1}{n\log n} \approx \log\log x.$$

Teorema 3.2.2 (Chebyshev) *Posto*

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

si ha $\lambda_1 = \lambda_2 = \lambda_3$ *e* $\Lambda_1 = \Lambda_2 = \Lambda_3$.

Dim. Si ha banalmente $\theta(x) \le \psi(x)$ ed inoltre per $x \ge 1$

$$\begin{aligned}\psi(x) &= \sum_{n\le x} \Lambda(n) = \sum_{p^m\le x} \log p = \sum_{p\le x} |\{m\in\mathbb{N}^*:\ p^m\le x\}| \log p \\ &= \sum_{p\le x} \left[\frac{\log x}{\log p}\right] \log p \le \log x \sum_{p\le x} 1 = \pi(x)\log x.\end{aligned}$$

Questo dimostra che $\lambda_2 \le \lambda_3 \le \lambda_1$ e che $\Lambda_2 \le \Lambda_3 \le \Lambda_1$. Inoltre si ha

$$\theta(x) \ge \sum_{y<p\le x} \log p \ge \big(\pi(x) - \pi(y)\big)\log y \tag{3.2.1}$$

per ogni $y \in (1,x]$, da cui ricaviamo $\pi(x) \le \pi(y) + \theta(x)/\log y$ e quindi, ricordando che $\pi(y) \le y$,

$$\frac{\pi(x)\log x}{x} \le \frac{\theta(x)}{x}\frac{\log x}{\log y} + \frac{\pi(y)\log x}{x} \le \frac{\theta(x)}{x}\frac{\log x}{\log y} + \frac{y\log x}{x}. \tag{3.2.2}$$

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

È necessario prendere y abbastanza grande da rendere significativa la minorazione (3.2.1), ma non troppo grande perché non domini il termine all'estrema destra nella (3.2.2). Le condizioni sono $(\log y)/\log x \to 1$ ed $y = o(x/\log x)$ quando $x \to +\infty$. In alternativa, scelto $y = x^\alpha$ con $\alpha < 1$, si ricava $\alpha\lambda_1 \le \lambda_2$ per ogni $\alpha < 1$, e quindi $\lambda_1 \le \lambda_2$.

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 che se esiste il $\lim_{x\to+\infty}\big(\pi(x)\log x\big)/x$ allora valgono entrambi 1: si veda il Corollario 3.3.5.

Teorema 3.2.3 (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 $0 < I_m \leq 4^{-m}$, 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 $\leq 2m+1$. Dunque $I_m \exp\psi(2m+1) \in \mathbb{N}^*$, e quindi $I_m \exp\psi(2m+1) \geq 1$. Da quest'ultima relazione ricaviamo

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

da cui

$$\psi(2m+1) \geq (2m+1)\log 2 - \log 2.$$

Inoltre

$$\frac{\psi(2m+2)}{2m+2} \geq \frac{\psi(2m+1)}{2m+1} \cdot \left(1 - \frac{1}{2m+2}\right)$$

e la prima disuguaglianza segue immediatamente passando al minimo limite.

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

$$\theta(2N+1) - \theta(N+1) \leq \log M < 2N\log 2. \tag{3.2.3}$$

Supponiamo di aver dimostrato che $\theta(n) < 2n\log 2$ per $1 \leq n \leq n_0 - 1$, 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 (3.2.3) e per l'ipotesi induttiva, ed il Teorema segue. □

𝔈 1 Integrando $|k|$ volte per parti, si dimostra facilmente che per $|k| \leq m$ si ha

$$I_m = \frac{m!^2}{(m+k)!(m-k)!} \int_0^1 x^{m+k}(1-x)^{m-k}\,\mathrm{d}x. \tag{3.2.4}$$

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 po-
𝔈 2 linomio $p(x) := x^4(1-2x)^2(1-x)^4$ si ottiene la limitazione $\lambda^* \geq \frac{1}{2}\log 5$, ed è possibile ottenere limitazioni ancora piú precise con altri polinomî, ma *non* che $\lambda^* \geq 1$. Osserviamo che la formula di Stirling (A.3.2) dà la relazione $I_m^{-1} = 2^{2m+1}m^{1/2}\pi^{-1/2}\big(1 + O\big(m^{-1}\big)\big)$, ma questa non dà informazioni piú precise. Infine, $I_m = \mathrm{B}(m+1, m+1)$ dove B è la funzione Beta definita nell'Appendice A.2, e la (3.2.4) segue immediatamente dalle proprietà indicate nell'Appendice.

Lemma 3.2.4 *Per $x \to +\infty$ si ha*

$$\psi(x) - \theta(x) = O\big(x^{1/2}\big).$$

Dim. Per il Teorema 3.2.3 si ha $\theta(x) = O(x)$, e dalla definizione è chiaro che

$$\psi(x) = \theta(x) + \theta\big(x^{1/2}\big) + \theta\big(x^{1/3}\big) + \cdots.$$

Osserviamo che se $m > m_0 := \big[(\log x)/\log 2\big]$ allora $x^{1/m} < x^{(\log 2)/\log x} = 2$ e che $\theta(x) = 0$ per $x < 2$. Quindi possiamo scrivere la differenza $\psi(x) - \theta(x)$ nella forma

$$\theta\big(x^{1/2}\big) + \sum_{m=3}^{m_0} \theta\big(x^{1/m}\big) = O\big(x^{1/2}\big) + O\big(m_0 x^{1/3} \log x\big),$$

e la tesi segue osservando che $m_0 = O(\log x) = O\big(x^{1/6}/\log x\big)$. □

Si noti che il Teorema 3.2.3 implica che $\theta(x) \geq x(\log 2 + o(1))$, e quindi la stima del Lemma 3.2.4 è evidentemente ottimale, a parte per il valore della costante implicita nella notazione $O(\cdot)$. Questo risultato, inoltre, fornisce una dimostrazione alternativa delle uguaglianze $\lambda_2 = \lambda_3$ e $\Lambda_2 = \Lambda_3$, nella notazione del Teorema di Chebyshev 3.2.2.

Corollario 3.2.5 *Si ha $\pi(x) = O(x/\log x)$.*

Questo significa che "quasi tutti" gli interi sono composti, il che è ragionevole perché gli interi grandi hanno una probabilità bassa di essere primi.

Esercizi.

- 𝔈 1. Dimostrare per induzione la formula (3.2.4).
- 𝔈 2. Dimostrare che $\psi(x) \geq \frac{1}{2} x \log 5 + O(1)$ utilizzando il polinomio $f(x) = x^4(1-2x)^2(1-x)^4$ nella dimostrazione del Teorema 3.2.3.
- 𝔈 3. * (Postulato di Bertrand) Dimostrare che $\pi(2x) - \pi(x) > 0$ per ogni $x \geq 2$.

Riferimenti. Teorema di Eulero 3.2.1: Ingham [73], §1.2. Storia del Teorema dei Numeri Primi 3.1.3: Goldstein [42] dà anche una breve descrizione della dimostrazione analitica. Si vedano anche Bateman & Diamond [7], Granville [47], [46]. Congettura di Legendre: Pintz [114]. Per l'andamento numerico delle funzioni π, θ e ψ e la bontà delle varie approssimazioni: Rosser & Schoenfeld [131] e Deléglise & Rivat [23], [24]. La minorazione nel Lemma di Chebyshev 3.2.3 è tratta da Nair [109], [108]. Per ulteriori considerazioni al riguardo, si veda Montgomery [102] Cap. 10. La maggiorazione nello stesso Lemma è quella del Teorema 415 di Hardy & Wright [57]. Si veda anche Ingham [73] §§1.4–1.5.

3.3 Le formule di Mertens

Teorema 3.3.1 (Prima formula di Mertens) *Per $N \to +\infty$ si ha*

$$\sum_{n\le N} \frac{\Lambda(n)}{n} = \log N + O(1). \tag{3.3.1}$$

Dim. Per la formula di Stirling A.3.2 abbiamo $\log N! = N\log N + O(N)$. Scrivendo la fattorizzazione canonica di $N!$ ed utilizzando l'Esercizio 3.1.2, si trova

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

per il Teorema 3.2.3; la tesi segue confrontando le due espressioni per $\log N!$. □

Teorema 3.3.2 (Seconda formula di Mertens) *Per $N \to +\infty$ si ha*

$$\sum_{p\le N} \frac{\log p}{p} = \log N + O(1). \tag{3.3.2}$$

Dim. È una conseguenza immediata della prima formula di Mertens (3.3.1). Infatti

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

e l'ultima serie è convergente. □

Teorema 3.3.3 (Terza formula di Mertens) *Per $N \to +\infty$ si ha*

$$\int_1^N \frac{\psi(t)}{t^2}\,\mathrm{d}t = \log N + O(1). \tag{3.3.3}$$

Dim. Per la formula di sommazione parziale (A.1.3) con $a_n = \Lambda(n)$ e $\phi(t) = t^{-1}$, si ha

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

e il risultato voluto segue dal Teorema 3.2.3 e dalla formula (3.3.1). □

Teorema 3.3.4 (Formula di Mertens per i primi) *Esiste una costante $B \in \mathbb{R}$ tale che per $N \to +\infty$ si ha*

$$\sum_{p \le N} \frac{1}{p} = \log\log N + B + O\big((\log N)^{-1}\big). \tag{3.3.4}$$

Dim. Poniamo $R(N) := \sum_{p \le N} p^{-1} \log p - \log N$. Per la seconda formula di Mertens (3.3.2) si ha $R(N) = O(1)$. Quindi, per la formula di sommazione parziale (A.1.3) con $a_n = (\log n)/n$ se n è primo, e 0 altrimenti, $\phi(t) = (\log t)^{-1}$, otteniamo

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

dove gli integrali impropri convergono poiché $R(N) = O(1)$. □

Corollario 3.3.5 (Chebyshev) *Nella notazione del Teorema 3.2.3, si ha $\lambda^* \le 1 \le \Lambda^*$. Dunque, se esiste il*

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

allora vale 1.

Dim. Sia $\varepsilon > 0$ e sia $N > N_0(\varepsilon)$. Per la formula di sommazione parziale (A.1.3) con $a_n = 1$ se n è primo, e 0 altrimenti, $\phi(t) = t^{-1}$, si ha

$$\sum_{p \le N} \frac{1}{p} = \frac{\pi(N)}{N} + \int_2^N \frac{\pi(t)}{t^2}\,\mathrm{d}t \ge \big(\lambda^* - \varepsilon + o(1)\big) \int_2^N \frac{\mathrm{d}t}{t\log t} \ge \big(\lambda^* - 2\varepsilon\big)\log\log N.$$

Analogamente, la somma qui sopra non supera $(\Lambda^* + 2\varepsilon)\log\log N$, e la tesi segue dal Teorema 3.3.4. □

Teorema 3.3.6 (Mertens) *Per $N \to +\infty$ si ha*

$$\prod_{p \le N} \left(1 - \frac{1}{p}\right) = \frac{\mathrm{e}^{-\gamma}}{\log N} + O\left(\frac{1}{(\log N)^2}\right), \tag{3.3.5}$$

dove γ è la costante di Eulero definita dalla (A.4.1).

Dim. Non è difficile mostrare questo risultato con una costante positiva (non esplicita) al posto di $e^{-\gamma}$. Infatti, dal Teorema 3.3.4 si ha

$$\begin{aligned}\log\prod_{p\le N}\left(1-\frac{1}{p}\right) &= -\sum_{p\le N}\sum_{m\ge 1}\frac{1}{mp^m}\\ &= -\sum_{p\le N}\frac{1}{p}-\sum_{p}\sum_{m\ge 2}\frac{1}{mp^m}+O\left(\sum_{p>N}\sum_{m\ge 2}\frac{1}{mp^m}\right)\\ &= -\log\log N+C+O\big((\log N)^{-1}\big).\end{aligned}$$

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

Usando la terza formula di Mertens (3.3.3), è relativamente semplice dimostrare che la congettura di Legendre (3.1.3) non può essere corretta.

Teorema 3.3.7 *Se esistono A, $B\in\mathbb{R}$ tali che*

$$\pi(x)=A\frac{x}{\log x}+(B+o(1))\frac{x}{(\log x)^2} \tag{3.3.6}$$

per $x\to+\infty$, allora vale la relazione

$$\psi(x),\,\theta(x)=Cx+(D+o(1))\frac{x}{\log x} \tag{3.3.7}$$

con $C=A$ e $D=B-A$. Viceversa, se esistono C, $D\in\mathbb{R}$ tali che valga la (3.3.7) per $x\to+\infty$, allora la (3.3.6) vale con $A=C$ e $B=C+D$. Infine, se vale una qualsiasi fra (3.3.6) e (3.3.7), allora $A=B=C=1$ e $D=0$.

Dim. È chiaro che le due relazioni nella (3.3.7) sono equivalenti a causa del Lemma 3.2.4. Se vale la (3.3.6) allora, per la formula di sommazione parziale (A.1.3) con $a_n=1$ se n è primo, 0 altrimenti, $\phi(t)=\log t$,

$$\begin{aligned}\theta(x)=\sum_{p\le x}\log p &= \pi(x)\log x-\int_2^x\frac{\pi(t)}{t}\,\mathrm{d}t\\ &= Ax+(B+o(1))\frac{x}{\log x}-\int_2^x\left(\frac{A}{\log t}+\frac{B+o(1)}{(\log t)^2}\right)\mathrm{d}t\\ &= Ax+(B-A+o(1))\frac{x}{\log x}.\end{aligned}$$

Viceversa, se vale la (3.3.7) allora, ancora per sommazione parziale con $a_n=1$ se n è primo, 0 altrimenti, $\phi(t)=1/\log t$,

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

$$= C\frac{x}{\log x} + (D+o(1))\frac{x}{(\log x)^2} + \int_2^x \Big(\frac{C}{(\log t)^2} + \frac{D+o(1)}{(\log t)^3}\Big)\,\mathrm{d}t$$
$$= C\frac{x}{\log x} + (C+D+o(1))\frac{x}{(\log x)^2}.$$

Infine, se vale la (3.3.7) allora

$$\int_2^x \frac{\psi(t)}{t^2}\,\mathrm{d}t = \int_2^x \Big(\frac{C}{t} + \frac{D+o(1)}{t\log t}\Big)\,\mathrm{d}t = C\log x + (D+o(1))\log\log x,$$

ed il risultato voluto segue dal confronto fra l'espressione a sinistra e la terza formula di Mertens (3.3.3). □

Le formule di Mertens (3.3.2) e (3.3.4) ed il Teorema di Mertens 3.3.6 danno informazioni sulla "densità" dei numeri primi nella successione dei numeri naturali. Può essere un buon esercizio sulle formule di sommazione del §A.1, dimostrare le formule analoghe in cui somme e prodotti sono estesi a tutti i numeri naturali. L'analoga della (3.3.4) è ovviamente il Teorema A.4.1 con $k=-1$, mentre le altre
𝔈 1 due diventano rispettivamente

$$\sum_{n\le x} \frac{\log n}{n} = \frac{1}{2}(\log x)^2 + O(\log x), \tag{3.3.8}$$

$$\prod_{2\le n\le x}\Big(1-\frac{1}{n}\Big) = \frac{1}{[x]} = \frac{1}{x} + O\Big(\frac{1}{x^2}\Big). \tag{3.3.9}$$

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

$$\pi(x) = \frac{x}{\log x} + \frac{x}{(\log x)^2} + O\Big(\frac{x}{(\log x)^3}\Big), \tag{3.3.10}$$

(*cfr* la (3.3.6) con $A=B=1$) permette di migliorare alcune delle formule di Mertens: infatti, come nel Teorema 3.3.7, da questa deduciamo

$$\theta(x) = \pi(x)\log x - \int_2^x \frac{\pi(t)}{t}\,\mathrm{d}t = x + O\Big(\frac{x}{(\log x)^2}\Big), \tag{3.3.11}$$

e poi, per sommazione parziale (A.1.3) con $a_n = \log n$ se n è primo, 0 altrimenti, $\phi(t) = t^{-1}$, abbiamo

$$\begin{aligned}\sum_{p\le x}\frac{\log p}{p} &= \frac{\theta(x)}{x} + \int_2^x \frac{\theta(t)}{t^2}\,\mathrm{d}t \\ &= 1 + O\big((\log x)^{-2}\big) + \int_2^x \frac{\mathrm{d}t}{t} + \int_2^x \frac{\theta(t)-t}{t^2}\,\mathrm{d}t \\ &= \log x + c + o(1),\end{aligned} \tag{3.3.12}$$

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 (3.3.10) dalla (3.3.11).

È comunque importante sottolineare il fatto che il Teorema dei Numeri Primi nella forma che abbiamo dimostrato è *equivalente* alla (3.3.12).

Esercizi.

℄ 1. Dimostrare le formule (3.3.8)–(3.3.9).

℄ 2. Dimostrare la disuguaglianza $d(n!) \geq n^{\pi(n)}/\exp(\theta(n))$. Utilizzando il Teorema dei Numeri Primi nella forma "debole" (senza termine d'errore), la Formula di Stirling A.3.2 e il Teorema 3.3.7, dimostrare che

$$\limsup_{N\to+\infty} \frac{\log(d(N))(\log\log(d(N)))^2}{\log N} \geq 1.$$

℄ 3. Utilizzando il Teorema dei Numeri Primi e la successione $N_m = p_1 \cdots p_m$, dimostrare che

$$\limsup_{N\to+\infty} \frac{\log(d(N))\log\log(d(N))}{\log N} \geq \log 2.$$

Riferimenti. Teoremi di Mertens (3.3.1)-(3.3.4): Hardy & Wright [57] Teoremi 424, 425, (22.6.1) e Teorema 427, oppure Ingham [73], §1.9. Teorema di Chebyshev 3.3.5: vedi Ingham [73], §1.8 per una dimostrazione alternativa. Teorema 3.3.6: si veda Hardy & Wright [57] Teorema 429, Ingham [73], §1.9. Pintz [114]. Diamond [26] elenca le "equivalenze" elementari delle relazioni fra le funzioni di Chebyshev.

3.4 Le formule di Selberg

Le formule di Selberg sono importanti da punto di vista storico perché, una volta scoperte, permisero quasi istantaneamente a Selberg [134] stesso e ad Erdős [35] di dare una dimostrazione elementare del Teorema dei Numeri Primi 3.1.3, cioè senza fare uso dell'analisi complessa. Si noti che i due addendi nelle formule di Selberg, a posteriori, hanno lo stesso peso $\sim x\log x$.

Per dimostrare le formule di Selberg useremo una variante *ad hoc* della seconda formula di inversione di Möbius 2.1.12.

Lemma 3.4.1 (Iseki–Tatuzawa) *Sia $F\colon [1,+\infty) \to \mathbb{C}$ una funzione qualsiasi e*

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

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 2.1.9 ed il Corollario 2.2.10. □

Teorema 3.4.2 (Selberg) *Per $x\to+\infty$ si hanno le seguenti relazioni equivalenti*

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

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

Dim. Per la formula di sommazione parziale (A.1.3) con $a_n=\Lambda(n)$ e $\phi(t)=\log t$ abbiamo

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

dal Teorema 3.2.3, 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 3.4.1, 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 2.2.9 (oppure dal Metodo dell'Iperbole 2.1.13 con $f=\Lambda$, $F(x)=\psi(x)$, $g=N_0$, $G(x)=[x]$, $y=x$) otteniamo

$$\sum_{n\le x}\psi\left(\frac{x}{n}\right)=\sum_{n\le x}\sum_{nm\le x}\Lambda(m)=\sum_{d\le x}\sum_{m|d}\Lambda(m)=\sum_{d\le x}\log d$$

$$= x\log x - x + O(\log x).$$

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

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

e quindi, in definitiva, $G(x) = O\big(\log^2 x\big)$. Per il Lemma A.4.4 con $k = 2$ ed il Lemma 3.4.1, abbiamo

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

Questo porta alla formula

$$F(x)\log x + \sum_{n\le x} F\left(\frac{x}{n}\right)\Lambda(n) = O(x), \tag{3.4.1}$$

e si ottiene il risultato voluto ricordando che $\psi(x) = O(x)$ per il Teorema 3.2.3. □

Le formule di Selberg 3.4.2 sono alla base della dimostrazione elementare del Teorema dei Numeri Primi 3.1.3. 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 risultato, che implica il Corollario 3.3.5.

Corollario 3.4.3 *Siano λ^* e Λ^* i valori comuni dei limiti nel Teorema 3.2.2. Si ha $\lambda^* + \Lambda^* = 2$.*

Dim. Per definizione, fissato $\varepsilon > 0$ è possibile trovare $x_0 = x_0(\varepsilon)$ tale che $(\lambda^* - \varepsilon)x \le \psi(x) \le (\Lambda^* + \varepsilon)x$ per ogni $x \ge x_0$. Inoltre, per il Teorema 3.2.3, esiste una costante assoluta C tale che $\psi(x) \le Cx$ per ogni $x \ge 1$. Dividiamo la seconda formula di Selberg per $x\log x$, e separiamo nella somma i termini con $n \le x/x_0$ dagli altri, ottenendo

$$\frac{\psi(x)}{x} + \frac{1}{x\log x}\sum_{1\le n\le x/x_0} \psi\left(\frac{x}{n}\right)\Lambda(n) + \frac{1}{x\log x}\sum_{x/x_0<n\le x} \psi\left(\frac{x}{n}\right)\Lambda(n) = 2 + o(1). \tag{3.4.2}$$

Per stimare la prima somma usiamo la prima formula di Mertens (3.3.1):

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

Nella seconda abbiamo

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

Sostituendo in (3.4.2) otteniamo

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

e quindi per $x\ge x_0$ si ha

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

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

Ricaviamo ora un'importante conseguenza delle formule di Selberg: poniamo $R(x):=\psi(x)-x$, cosicché il Teorema dei Numeri Primi è equivalente all'affermazione $R(x)=o(x)$ quando $x\to+\infty$. Sostituendo otteniamo

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

Ricordando la prima formula di Mertens (3.3.1) e semplificando, si ottiene

$$R(x)\log x+\sum_{n\le x}\Lambda(n)R\left(\frac{x}{n}\right)=O(x). \tag{3.4.3}$$

Questa formula è equivalente alla (3.4.1) e sta alla base della dimostrazione che segue, che spezzeremo in varî Lemmi.

Riferimenti. La dimostrazione delle formule di Selberg 3.4.2 per mezzo del Lemma di Iseki–Tatuzawa 3.4.1, è adattata da Chandrasekharan [14], Cap. 1.

3.5 Dimostrazione del Teorema dei Numeri Primi

Lemma 3.5.1 *Si ha*

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

dove

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

Dim. Sostituiamo x/m al posto di x nella (3.4.3) ed otteniamo

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

e quindi si ha

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

per la prima formula di Mertens (3.3.1). Dunque

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

ed il Lemma segue immediatamente prendendo il valore assoluto. □

Lemma 3.5.2 *Si ha*

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

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 3.5.1. Poi approssimiamo quest'ultima somma con l'integrale desiderato.

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

$$\begin{aligned}\big||R(t_1)| - |R(t_0)|\big| &\le \big|R(t_1) - R(t_0)\big| = \big|\psi(t_1) - \psi(t_0) - t_1 + t_0\big| \\ &\le \psi(t_1) - \psi(t_0) + t_1 - t_0 = F(t_1) - F(t_0). \qquad (3.5.1)\end{aligned}$$

Inoltre $F(t) = O(t)$ per il Lemma 3.2.3 e quindi

$$\sum_{n\le x-1} n\left\{F\left(\frac{x}{n}\right) - F\left(\frac{x}{n+1}\right)\right\} = \sum_{n\le x} F\left(\frac{x}{n}\right) - [x]F\left(\frac{x}{[x]}\right)$$
$$= O\left(x\sum_{n\le x}\frac{1}{n}\right) + O(x) = O(x\log x), \qquad (3.5.2)$$

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

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

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

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

Usando la formula di sommazione parziale (A.1.3) con $N = [x]$, dalla (3.5.1) otteniamo

$$\sum_{n\le x} c_n f(n) = \sum_{n\le x} a_n\left|R\left(\frac{x}{n}\right)\right| - 2\sum_{2\le n\le x}\left|R\left(\frac{x}{n}\right)\right|\int_{n-1}^{n}\log t\,\mathrm{d}t \qquad (3.5.3)$$
$$= \sum_{n\le x-1} C(n)\left\{\left|R\left(\frac{x}{n}\right)\right| - \left|R\left(\frac{x}{n+1}\right)\right|\right\} + C(x)\left|R\left(\frac{x}{[x]}\right)\right| \qquad (3.5.4)$$
$$= O\left(\sum_{n\le x-1} n\left\{F\left(\frac{x}{n}\right) - F\left(\frac{x}{n+1}\right)\right\}\right) + O(x) = O(x\log x), \qquad (3.5.5)$$

per la (3.5.2). Infine

$$\left|\left|R\left(\frac{x}{n}\right)\right|\int_{n-1}^{n}\log t\,\mathrm{d}t - \int_{n-1}^{n}\left|R\left(\frac{x}{t}\right)\right|\log t\,\mathrm{d}t\right|$$
$$\le \int_{n-1}^{n}\left|\left|R\left(\frac{x}{n}\right)\right| - \left|R\left(\frac{x}{t}\right)\right|\right|\log t\,\mathrm{d}t$$
$$\le \int_{n-1}^{n}\left\{F\left(\frac{x}{t}\right) - F\left(\frac{x}{n}\right)\right\}\log t\,\mathrm{d}t$$
$$\le (n-1)\left\{F\left(\frac{x}{n-1}\right) - F\left(\frac{x}{n}\right)\right\}. \qquad (3.5.6)$$

Quindi dalle (3.5.2)–(3.5.6) otteniamo

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

$$= O\left(\sum_{2\le n\le x}(n-1)\left\{F\left(\frac{x}{n-1}\right)-F\left(\frac{x}{n}\right)\right\}\right)+O(x\log x)$$
$$= O(x\log x).$$

Questo conclude la dimostrazione del Lemma. □

Lemma 3.5.3 *Posto* $V(\xi) := \mathrm{e}^{-\xi}R(\mathrm{e}^{\xi}) = \mathrm{e}^{-\xi}\psi(\mathrm{e}^{\xi}) - 1$, *si ha*

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

Dim. Combinando i risultati dei Lemmi 3.5.1–3.5.2 si ha

$$|R(x)|\log^2 x \le 2\int_1^x \left|R\left(\frac{x}{t}\right)\right|\log t\,\mathrm{d}t + O(x\log x). \tag{3.5.7}$$

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

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

La disuguaglianza voluta segue sostituendo nella (3.5.7) e dividendo per x. □

Lemma 3.5.4 *Vale la disuguaglianza* $\alpha \le \beta$, *dove*

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

Dim. È chiaro che α e β esistono finiti, poiché $\psi(x) = O(x)$. 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 3.5.3

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

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 $\alpha = \beta$. L'obiettivo, naturalmente, è dimostrare che $\alpha = 0$.

Lemma 3.5.5 *Esiste una costante assoluta $A > 0$ tale che per ogni ξ_1, $\xi_2 \in \mathbb{R}^+$ si ha*

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

Dim. Basta osservare che

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

per la terza formula di Mertens (3.3.3). □

Lemma 3.5.6 *Se $\eta_0 > 0$ e $V(\eta_0) = 0$ allora*

$$\int_0^{\alpha} \left| V(\eta_0 + \tau) \right| d\tau \leq \frac{1}{2}\alpha^2 + O\left(\eta_0^{-1} \right).$$

Dim. Riscriviamo la seconda formula di Selberg 3.4.2 nella forma

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

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:

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

La somma su n ed m è positiva e quindi

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

da cui deduciamo immediatamente

$$\left| R(x_1) \log x_1 - R(x_0) \log x_0 \right| \leq x_1 \log x_1 - x_0 \log x_0 + O(x_1),$$

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

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

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

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

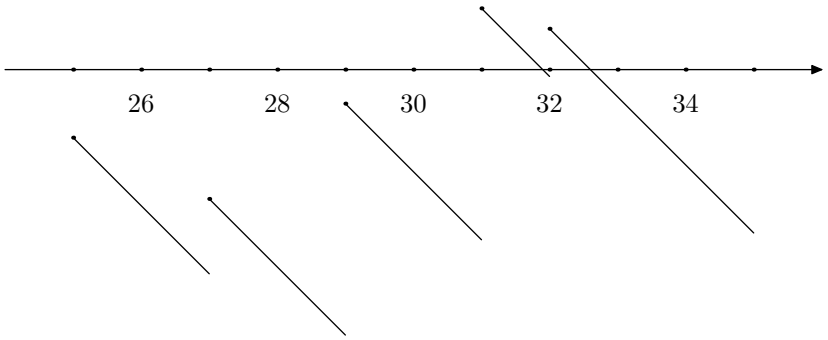


Figura 3.3: Il grafico di $\psi(x)-x$ per $x \in [25,35]$. Il grafico di $V(\xi)$ si può ricavare da questo mediante un cambiamento di variabile, ma il comportamento qualitativo evidentemente è lo stesso.

Quindi si ha

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

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 3.5.4.

Lemma 3.5.7 $\alpha = 0$.

Dim. Detta A la costante nel Lemma 3.5.5, 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 3.3: l'intervallo $[31,34]$ è del primo tipo, mentre l'intervallo $[28,31.5]$ è del secondo tipo.

Primo caso Per ζ sufficientemente grande, per il Lemma 3.5.6 si può scrivere

$$\int_\zeta^{\zeta+\delta} \left|V(\eta)\right| d\eta = \left\{ \int_\zeta^{\eta_0} + \int_{\eta_0}^{\eta_0+\alpha} + \int_{\eta_0+\alpha}^{\zeta+\delta} \right\} \left|V(\eta)\right| d\eta$$

$$\leq \alpha(\eta_0-\zeta)+\frac{1}{2}\alpha^2+\alpha(\zeta+\delta-\eta_0-\alpha)+o(1)$$
$$=\alpha\left(\delta-\frac{1}{2}\alpha\right)+o(1)=\alpha_1\delta+o(1),$$

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

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

per il Lemma 3.5.5. Se invece V non cambia segno, sempre per lo stesso Lemma,

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

In definitiva, stimando banalmente $|V(\eta)|\leq\alpha+o(1)$ su $[\zeta+\delta-\alpha,\zeta+\delta]$, si ha

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

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

$$\int_\zeta^{\zeta+\delta}\bigl|V(\eta)\bigr|\,d\eta\leq\alpha_1\delta+o(1),\tag{3.5.8}$$

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 (3.5.8). Poniamo $M:=\bigl[\xi/\delta\bigr]$. Si ha

$$\int_0^\xi\bigl|V(\eta)\bigr|\,d\eta=\sum_{k=0}^{M-1}\int_{k\delta}^{(k+1)\delta}\bigl|V(\eta)\bigr|\,d\eta+\int_{M\delta}^{\xi}\bigl|V(\eta)\bigr|\,d\eta$$
$$\leq\alpha_1 M\delta+o(M)+O(1)=\alpha_1\xi+o(\xi).$$

Ma questo implica immediatamente che $\beta\leq\alpha_1<\alpha$, in contraddizione con il Lemma 3.5.4. Dunque $\alpha=0$, come si voleva. □

Questo dimostra il Teorema dei Numeri Primi nella forma $\psi(x)\sim x$, ma senza
𝔈 1-2 indicazione della "velocità" di convergenza di $\psi(x)/x$ ad 1.

Esercizi.

$\mathfrak{E}$ 1. Utilizzando il Teorema dei Numeri Primi 3.1.3, dimostrare che

$$\liminf_{n\to+\infty} \frac{p_{n+1}-p_n}{\log p_n} \le 1, \qquad \limsup_{n\to+\infty} \frac{p_{n+1}-p_n}{\log p_n} \ge 1.$$

$\mathfrak{E}$ 2. Dimostrare che per ogni $c>1$ fissato si ha $\pi(cx)-\pi(x) \sim (c-1)x/\log x$.

Riferimenti. Dimostrazione elementare del Teorema dei Numeri Primi 3.1.3: Hardy & Wright [57], Cap. 22. Altre dimostrazioni elementari: Diamond [26], Levinson [93], Daboussi [21] (questa è basata su un'idea totalmente diversa) e Bombieri [9] (questa dà anche stime per il termine d'errore).

3.6 Altri risultati su alcune funzioni aritmetiche

In questo paragrafo poniamo

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

Teorema 3.6.1 *Si ha*

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

Dim. Disponiamo i numeri primi $p_1, p_2, \ldots$, in ordine crescente, poniamo $n_0 := 1$ e per $k \in \mathbb{N}^*$ definiamo $n_k := P(p_k) = \exp\bigl(\theta(p_k)\bigr)$. Qualunque sia $n \in \mathbb{N}^*$, esiste $k = k(n) \in \mathbb{N}$ 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

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

cioè che gli n_k sono punti di minimo locale per questo rapporto, e dunque, *a fortiori*, $\phi(n)n^{-1}\log\log(n) \ge \phi(n_k)n_k^{-1}\log\log(n_k)$. Siano $q_1, q_2, \ldots, q_r$, i fattori primi di n, contati ciascuno una volta sola, e disposti in ordine crescente. La disuguaglianza di sopra è equivalente a

$$\prod_{j=1}^{r}\left(1-\frac{1}{q_j}\right) \ge \prod_{j=1}^{k}\left(1-\frac{1}{p_j}\right).$$

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

$$\prod_{j=1}^{r}\left(1-\frac{1}{q_j}\right) \ge \prod_{j=1}^{r}\left(1-\frac{1}{p_j}\right) \ge \prod_{j=1}^{k}\left(1-\frac{1}{p_j}\right),$$

come si voleva. Osserviamo che per il Teorema di Mertens 3.3.6,

$$\frac{\phi(n_k)}{n_k} = \prod_{j=1}^{k}\left(1-\frac{1}{p_j}\right) = \prod_{p\le p_k}\left(1-\frac{1}{p}\right) = \frac{\mathrm{e}^{-\gamma}}{\log p_k}\big(1+o(1)\big),$$

e cioè $n_k^{-1}\phi(n_k)\log p_k = \mathrm{e}^{-\gamma}\big(1+o(1)\big)$. 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 3.2.3 si ha $c_1 p_k \le \theta(p_k) \le c_2 p_k$ per opportune costanti positive c_1 e c_2 e $k \ge 1$, da cui $\log\log n_k = \log\theta(p_k) = \log p_k + O(1)$. Mettendo insieme queste disuguaglianze, si conclude che quando $n \to +\infty$ si ha

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

che insieme danno la tesi. □

Teorema 3.6.2 *Si ha* $1 \le \omega(n) \le \Omega(n)$ *per ogni* $n \ge 2$ *ed inoltre*

$$\liminf_{n\to+\infty}\omega(n) = \liminf_{n\to+\infty}\Omega(n) = 1,$$

$$\limsup_{n\to+\infty}\frac{\omega(n)\log\log n}{\log n} = 1, \qquad \limsup_{n\to+\infty}\frac{\Omega(n)}{\log n} = \frac{1}{\log 2}.$$

Dim. Le prime affermazioni seguono immediatamente dalle definizioni. Per quanto riguarda l'ultima, poiché 2^k è il piú piccolo intero positivo per cui $\Omega(n) \ge k$, si ha

$$\frac{\Omega\big(2^k\big)}{\log 2^k} = \frac{1}{\log 2} \qquad \text{ed inoltre} \qquad \frac{\Omega(n)}{\log n} \le \frac{k}{\log n} \le \frac{\Omega\big(2^k\big)}{\log 2^k} = \frac{1}{\log 2}$$

per tutti gli $n \in \big[2^k, 2^{k+1}\big)$. Per dimostrare la penultima disuguaglianza useremo il Teorema dei Numeri Primi 3.1.3. 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

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

per il Teorema dei Numeri Primi 3.1.3. Ma $\log P(x) = \theta(x) \sim x$, sempre per lo stesso risultato, e quindi $\log\log P(x) \sim \log x$. Sostituendo nella (3.6) si ha

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

Inoltre la funzione $(\log n)/\log\log n$ è crescente per n grande, e la disuguaglianza voluta segue, come sopra. □

Teorema 3.6.3 *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 (3.3.4) si ha

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

La seconda relazione si dimostra considerando $\sum_{n\le x}\big(\Omega(n)-\omega(n)\big)$. □

Teorema 3.6.4 *Per $N \to +\infty$ si ha*

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

Dim. Per quanto visto sopra, abbiamo

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

L'errore introdotto completando la somma a tutti i $d \ge 1$ è a sua volta $O\big(N^{1/2}\big)$, e la somma infinita risultante vale $\zeta(2)^{-1}$. Il risultato segue immediatamente. □

𝔈 1 Si vedano il Teorema 6.2.2 e gli Esercizi. Abbiamo visto nel Teorema 3.6.1 che ogni tanto la funzione ϕ di Eulero è lontana dal suo valore massimo possibile (che è assunto sui numeri primi). Il prossimo risultato mostra che, in media, $1/\phi(n)$ si comporta come un multiplo di $1/n$: questo significa che, pur esistendo valori eccezionali di n per cui $\phi(n)$ è "piccolo," questi valori di n non sono cosí numerosi da influenzare in modo significativo la media di $1/\phi$.

Teorema 3.6.5 *Per $N \to +\infty$ si ha*

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

Dim. Si verifica immediatamente che $N_1/\phi = (\mu^2/\phi) * N_0$. Il Metodo dell'Iperbole 2.1.13 con $y = x$ dà

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

Per il Teorema 3.6.1 i termini d'errore sono entrambi $O\big((\log N)^2\big)$. Il Teorema 2.3.1 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 con la formula sommazione parziale (A.1.3). □

In queste note non parliamo di algoritmi per la fattorizzazione di interi, né di criteri di primalità: per questo rimandiamo a trattazioni specialistiche come Crandall & Pomerance [20] e Languasco & Zaccagnini [88]. In alcuni di questi algoritmi vi sono delle parti in cui è necessario determinare opportuni interi con specifiche caratteristiche "moltiplicative," come, ad esempio, l'essere privi di fattori primi "grandi" o "piccoli," e ci si chiede, per fare l'analisi della loro complessità, quanto sia difficile trovare numeri con queste proprietà. Rivolgiamo dunque la nostra attenzione all'aspetto "teorico" di questo problema: come sono distribuiti gli interi privi di fattori primi grandi.

Senza alcuna pretesa di completezza, parliamo brevemente della piú importante fra le funzioni enumeratrici degli interi suddetti. Poniamo

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

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

$$\Psi(x,y) = \sum_{\substack{n\le x\\ p\mid n\Rightarrow p\le y}} 1 \le \sum_{\substack{n\le x\\ p\mid n\Rightarrow p\le y}}\left(\frac{x}{n}\right)^{\sigma} \le \sum_{\substack{n\ge 1\\ p\mid n\Rightarrow p\le y}}\left(\frac{x}{n}\right)^{\sigma} = x^{\sigma}\prod_{p\le y}\big(1-p^{-\sigma}\big)^{-1}. \tag{3.6.1}$$

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 pressoché 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 quando $x\to+\infty$ si ha

$$\Psi(x,y) \sim \left(\pi(y)!\prod_{p\le y}\log p\right)^{-1}(\log x)^{\pi(y)}. \tag{3.6.2}$$

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 $p^\sigma = \exp\bigl(\sigma \log p\bigr) = 1 + \sigma \log p + O\bigl(\sigma^2 \log^2 p\bigr)$ e la (3.6.1) dà

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

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

$$\Psi(x,y) \le \left(\frac{\mathrm{e}}{\pi(y)}\right)^{\pi(y)} \Bigl(\prod_{p \le y} \log p\Bigr)^{-1} (\log x)^{\pi(y)} \left\{1 + O\left(\frac{y^2}{\log x \log y}\right)\right\}. \quad (3.6.3)$$

Per la formula di Stirling $n! \sim \sqrt{2\pi n}\bigl(n/\mathrm{e}\bigr)^n$ e quindi la stima (3.6.3) non è molto piú debole della formula asintotica (3.6.2). È importante cercare di estendere questo tipo di stime anche al caso in cui y è piú grande: per esempio, dimostriamo la seguente maggiorazione universale.

Lemma 3.6.6 *Fissato arbitrariamente $A > 0$, per $x \ge 1$ ed $y \ge \mathrm{e}^A$ si ha $\Psi(x,y) = O_A\bigl(x\mathrm{e}^{-Au}\log y\bigr)$, dove $u = (\log x)/\log y$.*

Dim. La dimostrazione si ottiene immediatamente prendendo $\sigma = 1 - A(\log y)^{-1}$ in (3.6.1), usando la stima $p^{1-\sigma} = 1 + O_A((1-\sigma)\log p)$ e le formule di Mertens (3.3.2) e (3.3.4). □

Esercizi.

℈ 1. Dimostrare che

$$\sum_{d \ge y} \frac{\mu(d)}{d^2} = O\bigl(y^{-1}\bigr) \quad \text{e che} \qquad \sum_{d \ge 1} \frac{\mu(d)}{d^2} = \frac{1}{\zeta(2)} = \Bigl(\sum_{d \ge 1} \frac{1}{d^2}\Bigr)^{-1}.$$

℈ 2. Si riprenda l'Esercizio 13 del §2.2 e si dimostri che

$$d(N!) \ge \prod_{p \le N} \frac{N}{p} = N^{\pi(N)} e^{-\theta(N)} = \exp(\pi(N)\log N - \theta(N)) = \exp \int_2^N \frac{\pi(t)}{t}\,\mathrm{d}t.$$

Da questo si deduca che

$$\log(d(N!)) \geq \int_2^N \frac{\pi(t)}{t}\,\mathrm{d}t \geq (1+o(1))\frac{N}{\log N} = (1+o(1))\frac{\log(N!)}{(\log\log(N!))^2}.$$

Riferimenti. La dimostrazione del Teorema 3.6.1 è adattata da Hardy & Wright [57] Teorema 328. Per i Teoremi 3.6.2 e 3.6.3 si veda il §22.10 ed il Teorema 430 di Hardy & Wright [57]. Per la funzione $\Psi(x,y)$ si vedano Hildebrand & Tenenbaum [68] e Tenenbaum & Mendès France [136].

3.7 Grandi intervalli fra numeri primi consecutivi

Usiamo i risultati del paragrafo precedente per dimostrare che, talvolta, due numeri primi consecutivi possono essere piú distanti della "media" prevista dal Teorema dei Numeri Primi. Non daremo per ovvi motivi il risultato piú forte oggi noto, ma vedremo un risultato non banale e, tutto sommato, relativamente elementare. Adattiamo, semplificandola, una costruzione di Erdős e Rankin.

Teorema 3.7.1 *Sia p_n l'n-esimo numero primo; si ha*

$$\limsup_{n\to\infty} \frac{p_{n+1}-p_n}{\log p_n}\cdot\frac{(\log\log\log p_n)^2}{\log\log p_n} = +\infty.$$

Dim. Per $x \geq 1$ poniamo $P(x) := \exp(\theta(x))$ e consideriamo altri tre parametri con le limitazioni $y < w < x < u$. L'idea di base è costruire un intero $z < P(x)$ tale che $\big(z+n, P(x)\big) > 1$ per ogni $n \in [0,u]$. Suddividiamo dunque l'insieme $\mathfrak{P}$ dei numeri primi $p \leq u$ in quattro classi: $\mathfrak{P}_1 := \mathfrak{P}\cap[1,y]$, $\mathfrak{P}_2 := \mathfrak{P}\cap(y,w]$, $\mathfrak{P}_3 := \mathfrak{P}\cap(w,x]$, $\mathfrak{P}_4 := \mathfrak{P}\cap(x,u]$. Per cominciare imponiamo che $z \equiv 0 \bmod p$ per ogni $p \in \mathfrak{P}_2$.

Poniamo $\mathcal{A}_0 := \{n \in [0,u] : \big(z+n, P(x)\big) = 1\}$ ed $N_0 := |\mathcal{A}_0|$. Allora $n \in \mathcal{A}_0$ solo se si verifica una delle condizioni seguenti:

1. n ha tutti i fattori primi $\leq y$; il numero di questi interi è $B_1 := \Psi(u,y)$.
2. n ha un fattore primo $p \in \mathfrak{P}_3 \cup \mathfrak{P}_4$; sia B_2 il numero di questi interi.

Per il Lemma 3.6.6 si ha $B_1 = O_A(u\exp(-A(\log u)/\log y)\log y)$ per $y \geq \mathrm{e}^A$, dove $A > 0$ è arbitrario. Per la formula di Mertens (3.3.4) si ha

$$B_2 \leq \sum_{w\leq p\leq u} \frac{u}{p} \leq u\log\frac{\log u}{\log w}(1+o(1)).$$

Ordiniamo i primi dell'insieme $\mathfrak{P}_1$, scrivendo $p_1 < p_2 < \cdots < p_k$, dove $k = \pi(y)$. Per $i \geq 1$ definiamo induttivamente N_i ed $\mathcal{A}_i$ a partire da N_{i-1} ed $\mathcal{A}_{i-1}$.

Scegliamo $r_i \bmod p_i$ in modo che l'equazione $n \equiv r_i \bmod p_i$ sia risolubile per almeno N_{i-1}/p_i interi $n \in \mathcal{A}_{i-1}$, ed imponiamo $z \equiv -r_i \bmod p_i$. Ora definiamo $\mathcal{A}_i := \{n \in \mathcal{A}_{i-1} : n \not\equiv r_i \bmod p_i\}$, $N_i := |\mathcal{A}_i|$. Quindi

$$N_i \le \left(1 - \frac{1}{p_i}\right) N_{i-1},$$

e per il Teorema di Mertens 3.3.6 si ha

$$N_k \le \prod_{p \le y} \left(1 - \frac{1}{p}\right) N_0 = \frac{\mathrm{e}^{-\gamma}}{\log y} N_0 \, (1 + o(1)).$$

Poniamo per brevità $\mathcal{L} := \log x$. Ora finalmente scegliamo

$$y \stackrel{\text{def}}{=} \exp\Big(\frac{A\mathcal{L}}{\log \mathcal{L}}\Big), \qquad w \stackrel{\text{def}}{=} \frac{x}{\log \mathcal{L}}, \qquad u \stackrel{\text{def}}{=} \delta x \frac{\mathcal{L}}{(\log \mathcal{L})^2},$$

dove $0 < \delta < A\mathrm{e}^{\gamma}$. Da queste definizioni, con semplici calcoli deduciamo che $N_0 \le (\delta + o(1)) x (\log \mathcal{L})^{-1}$ e quindi che, per x sufficientemente grande, si ha

$$N_k \le \mathrm{e}^{-\gamma} A^{-1} \delta \frac{x}{\mathcal{L}} (1 + o(1)) \le \pi(x) - \pi(w).$$

Questo significa che vi sono piú numeri primi $q \in \mathfrak{P}_3$ di quanti elementi vi siano in $\mathcal{A}_k$: se $\mathcal{A}_k = \{n_1, n_2, \ldots, n_j\}$ e $\mathfrak{P}_3 = \{q_1, q_2, \ldots, q_m\}$, per $i = 1, \ldots, j$ poniamo $z \equiv -n_i \bmod q_i$, e per $i = j+1, \ldots, m$ poniamo $z \equiv 0 \bmod q_i$. Tutte le congruenze scritte fin qui sono indipendenti e quindi, per il Teorema Cinese del Resto 1.2.4 ammettono una soluzione simultanea $z^* \in [1, P(x)]$. Per questo z^* si ha $(z^* + n, P(x)) > 1$ per tutti gli $n \in [0, u]$, e quindi nessuno degli interi $z^* + n$ con $n \in [0, u]$ può essere primo.

Consideriamo ora il massimo numero primo $p < z^*$ ed il suo successore p': per quanto abbiamo appena visto si ha $p' > z^* + u$ e quindi, poiché la funzione $t \mapsto (\log\log t)/(\log\log\log t)^2$ è definitivamente crescente, si ha

$$\frac{p' - p}{\log p} \cdot \frac{(\log\log\log p)^2}{\log\log p} \ge \frac{u}{\log P(x)} \cdot \frac{(\log\log\log P(x))^2}{\log\log P(x)} \ge \delta + o(1)$$

per il Teorema dei Numeri Primi 3.1.3, che implica la tesi. □

3.8 Problemi aperti

La domanda piú importante naturalmente riguarda il vero ordine di grandezza di $\pi(x) - \mathrm{li}(x)$. Littlewood [97] ha dimostrato che

$$\pi(x) - \mathrm{li}(x) = \Omega\big(x^{1/2} \log_3 x (\log x)^{-1}\big),$$

mentre secondo la Congettura di Riemann 3.1.4 si dovrebbe avere $\pi(x) = \mathrm{li}(x) + O\big(x^{1/2}\log x\big)$, o, equivalentemente, $\psi(x) = x + O\big(x^{1/2}(\log x)^2\big)$. Sorprendentemente, la Congettura di Riemann 3.1.4 può essere espressa in modo assolutamente elementare come segue: sia

$$H_n \stackrel{\text{def}}{=} \sum_{i=1}^{n} \frac{1}{i}$$

il cosiddetto n-esimo numero armonico. Allora, per ogni $n \geq 1$ si ha

$$\sigma(n) \leq H_n + \exp(H_n)\log(H_n) \tag{3.8.1}$$

se e solo se è vera la Congettura di Riemann. Informalmente, se la Congettura di Riemann fosse falsa, esisterebbe una successione divergente x_j tale che $\pi(x_j) > \mathrm{li}(x_j) + x_j^{1/2+\delta}$, dove $\delta > 0$ è una quantità fissata. Usando i numeri primi in $[1, x_j]$ si potrebbe costruire un intero n_j con un valore $\sigma(n_j)$ piú grande della norma e tale da falsificare, seppur di poco, la (3.8.1). Per i dettagli si veda Lagarias [81].

Il Teorema dei Numeri Primi 3.1.3 suggerisce che

$$\pi(x) - \pi(x-y) \sim \int_{x-y}^{x} \frac{\mathrm{d}t}{\log t}, \tag{3.8.2}$$

almeno quando y non è troppo piccolo rispetto ad x. Heath-Brown [61] 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 $y = (\log x)^A$, per ogni $A > 0$ fissato (Maier [98]), ed anche per funzioni di x che crescono piú rapidamente: i migliori risultati noti (Hildebrand & Maier [67], Friedlander, Granville, Hildebrand & Maier [37]), sono complicati da enunciare. In ogni caso, per $x > 0$ ed $y > 1$ vale la maggiorazione universale detta disuguaglianza di Brun–Titchmarsh (Montgomery & Vaughan [103])

$$\pi(x+y) - \pi(x) \leq \frac{2y}{\log y}.$$

Si confronti con la versione nel Teorema 5.5.2.

In vista del Teorema dei Numeri Primi si deve necessariamente avere

$$\limsup_{n\to+\infty} \frac{p_{n+1} - p_n}{\log p_n} \geq 1.$$

In un certo senso, il valor medio di $p_{n+1} - p_n$ è $\log p_n$. Cramér [19] (vedi anche Granville [46]) 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 noto è quello di Pintz [116]

$$\limsup_{n\to+\infty} \frac{p_{n+1}-p_n}{\log p_n} \frac{(\log_3 p_n)^2}{\log_2 p_n \log_4 p_n} \geq 2e^{\gamma}.$$

Questo si ottiene usando una stima piú forte per la funzione Ψ al posto del Lemma 3.6.6 nella dimostrazione del Teorema 3.7.1, ed una complicata argomentazione combinatoria. Inoltre Baker, Harman & Pintz [6] hanno dimostrato che

$$p_{n+1}-p_n = O\big(p_n^{0.525}\big).$$

Nell'altra direzione ci si chiede se esistano infiniti "primi gemelli" (*cfr* i Capitoli 5 e 7), che implicherebbe la relazione

$$\liminf_{n\to+\infty} \frac{p_{n+1}-p_n}{\log p_n} = 0.$$

Recentemente Goldston, Pintz e Yıldırım hanno annunciato una dimostrazione di quest'ultimo risultato e ne hanno pubblicato su web con Y. Motohashi [43] una versione semplificata. Per alcuni risultati elementari in questa direzione, vedi Languasco & Zaccagnini [90], che contiene anche la dimostrazione di alcuni risultati piú deboli del Teorema 3.7.1, che mostrano l'evoluzione delle idee necessarie.

Capitolo 4

Primi nelle progressioni aritmetiche

Nel Capitolo 3 abbiamo dimostrato che esistono infiniti numeri primi: analizzando le tavole numeriche (si veda ad esempio la Figura 3.1) si notano facilmente alcune regolarità. Per esempio, si nota che circa $\frac{1}{4}$ dei numeri primi sono $\equiv 1 \bmod 10$, e lo stesso vale per i primi congrui rispettivamente a 3, 7 o 9 mod 10. In effetti, a parte i numeri primi 2 e 5, gli altri 166 primi della Figura 3.1 sono cosí ripartiti nelle 4 classi: 40 sono $\equiv 1 \bmod 10$, 42 sono $\equiv 3 \bmod 10$, 46 sono $\equiv 7 \bmod 10$ ed infine 38 sono $\equiv 9 \bmod 10$. È del tutto evidente che vi può essere al massimo un numero primo in ciascuna delle classi di congruenza 0, 2, 4, 5, 6, 8 mod 10, ma non è affatto ovvio che debbano esistere infiniti numeri primi in ciascuna delle altre classi di congruenza, o che debbano essere approssimativamente equiripartiti fra le classi stesse.

In generale, dato il polinomio di primo grado $f(x) = qx+a$, se $d := (a,q) > 1$ allora *tutti* i valori del polinomio sono divisibili per d e quindi al massimo uno di questi può essere primo. Viceversa, se $d = 1$, è naturale chiedersi se f assuma valore primo per infiniti valori interi della variabile x. Abbiamo dimostrato sopra (Teorema 1.7.5) i casi particolari $q = 4$, $a = 1$ e $q = 4$, $a = 3$ con un'argomentazione *ad hoc* che non può essere estesa in generale.

Vedremo che effettivamente il polinomio $f(x) = qx+a$ assume valori primi per infiniti valori di x, in una forma piuttosto forte dal punto di vista quantitativo, analoga al Teorema di Eulero 3.2.1, o meglio alla seconda formula di Mertens (3.3.2) (si veda il Teorema di Dirichlet 4.4.1); in definitiva, in un certo senso preciso, i numeri primi sono, almeno in prima approssimazione, equiripartiti fra le $\phi(q)$ classi di congruenza ammissibili modulo q.

In realtà, il problema è piú generale, e la domanda che ci si pone è la seguente: dato $f \in \mathbb{Z}[x]$, non costante, irriducibile su $\mathbb{Q}$ e senza divisori primi fissi (cioè tale che per ogni numero primo p esiste almeno un intero m tale che $f(m) \not\equiv 0 \bmod p$; ad esempio il polinomio irriducibile $f(x) = x^2+x+2$ assume solo valori pari, ed è primo solo per $x = 0$) è vero che $f(x)$ è primo per infiniti valori della variabile

x? Al momento attuale, purtroppo, non è noto neppure un polinomio di grado 2 o piú per cui questa congettura sia stata dimostrata, anche se l'evidenza teorica e quella numerica sono decisamente a favore della sua verità. Torneremo su questo problema nel Capitolo 5, dove daremo alcuni risultati parziali.

4.1 Caratteri di un gruppo abeliano

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

Definizione 4.1.1 *Sia G un gruppo abeliano. Diciamo che $\chi\colon G \to \mathbb{C}^*$ è un* carattere *di G se χ è un omomorfismo.*

Lemma 4.1.2 *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 $\chi(g) = \mathrm{e}^{2\pi \mathrm{i} k/n}$.*

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

Lemma 4.1.3 *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 4.1.4 *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 4.1.5 *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 4.1.6 *Se G è un gruppo abeliano finito allora $\widehat{G} \simeq G$.*

Dim. G è prodotto diretto di sottogruppi ciclici. □

Definizione 4.1.7 *Il carattere* $\chi_0 \colon G \to \mathbb{C}^*$ *tale che* $\chi_0(g) = 1$ *per ogni* $g \in G$ *si dice* carattere principale.

Teorema 4.1.8 (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 $S := \sum_{g\in G}\chi(g)$. 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 $S := \sum_{\chi\in\widehat{G}}\chi(g)$. 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. □

4.2 Caratteri e funzioni *L* di Dirichlet

Definizione 4.2.1 *Dato* $q \in \mathbb{N}^*$*, e dato* $\chi \in \widehat{\mathbb{Z}_q^*}$*, chiamiamo* carattere di Dirichlet modulo q *la funzione* $f \colon \mathbb{Z} \to \mathbb{C}$ *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
𝔈 1-2 indicare sia il carattere del gruppo $\mathbb{Z}_q^*$, sia la sua estensione a $\mathbb{Z}$.

Definizione 4.2.2 *Si dice* carattere principale *modulo* q *il carattere di Dirichlet* χ_0 *definito da*

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

	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

Tabella 4.1: I caratteri di Dirichlet modulo 3, 5, 8.

Osservazione 4.2.3 *Le relazioni di ortogonalità 4.1.8 permettono di scegliere la progressione aritmetica $n \equiv a \bmod q$, purché $(a,q) = 1$: infatti, per ogni successione (α_n) si ha*

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

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 $\phi(q)$ se $n \equiv a \bmod q$ e 0 altrimenti.

Per $q = 2$ c'è solo il carattere principale χ_0, mentre per $q = 3$, oltre al carattere principale χ_0 mod 3, c'è anche un altro carattere χ_1 mod 3, detto *carattere quadratico*, poiché $\chi_1^2 = \chi_0$. La Tabella 4.1 dà 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 4.1–4.4 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.

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 $\chi_k(x^r) := \mathrm{e}^{2\pi \mathrm{i} rk/(p-1)}$, dove evidentemente χ_0 è il carattere principale. Si osservi inoltre che i caratteri χ_1 mod 3, χ_2 mod 5 e χ_3 mod 7 sono precisamente $\left(\cdot \mid p\right)$ per $p = 3$, 5 e 7. Per ogni primo p, il simbolo di Legendre è un carattere che assume solo valori reali.

Lemma 4.2.4 *Sia χ mod q un carattere non principale, $\Re(\delta) > 0$, $\frac{3}{2} \le x \le y$. Si ha*

$$\sum_{x<n\le y} \frac{\chi(n)}{n^\delta} = O_q\left(x^{-\delta}\right), \qquad \sum_{x<n\le y} \frac{\chi(n)\log n}{n^\delta} = O_q\left(x^{-\delta}\log x\right).$$

	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

Tabella 4.2: I caratteri di Dirichlet modulo 7 (e, a meno di isomorfismi, modulo 9, 14 e 18). Qui ω è una radice sesta primitiva dell'unità, e soddisfa $\omega^2 - \omega + 1 = 0$. Dato che $\mathbb{Z}_7^*$ è generato da 3, è sufficiente conoscere $\chi(3)$ per poter calcolare il valore di χ su tutti gli elementi di $\mathbb{Z}_7^*$.

	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	$-$i	1	i	-1	$-$i
4	1	-1	1	-1	1	-1	1	-1
7	1	$-$i	-1	i	-1	i	1	$-$i
8	1	$-$i	-1	i	1	$-$i	-1	i
11	1	-1	1	-1	-1	1	-1	1
13	1	i	-1	$-$i	-1	$-$i	1	i
14	1	1	1	1	-1	-1	-1	-1

Tabella 4.3: I caratteri modulo 15 (ed anche, a meno di isomorfismi, modulo 16 e 20). Conviene ricordare che $\mathbb{Z}_{15}^* \simeq \mathbb{Z}_2 \times \mathbb{Z}_4$ e quindi $\chi^4 = \chi_0$ per ogni carattere χ.

	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

Tabella 4.4: I caratteri modulo 24. Ricordiamo che $\mathbb{Z}_{24}^* \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, e che ogni elemento soddisfa $x^2 = 1$.

Dim. Per la formula di sommazione parziale (A.1.3) con $a_n = \chi(n)$ e $\phi(t) = t^{-\delta}$, e per le relazioni di ortogonalità 4.1.8

$$\sum_{x<n\le y} \frac{\chi(n)}{n^\delta} = y^{-\delta} \sum_{x<n\le y} \chi(n) + \delta \int_x^y \sum_{x<n\le t} \chi(n) \frac{\mathrm{d}t}{t^{\delta+1}}$$
$$= O_q\left(y^{-\delta}\right) + \delta \int_x^y \frac{O_q(1)}{t^{\delta+1}}\,\mathrm{d}t = O_q\left(y^{-\delta}\right) + O_q\left(x^{-\delta}\right) = O_q\left(x^{-\delta}\right).$$

La seconda disuguaglianza si dimostra in modo analogo. □

Definizione 4.2.5 *Dato un carattere* χ mod q *definiamo la* funzione L di Dirichlet $L(s,\chi)$ *e la* funzione zeta di Riemann $\zeta(s)$ *per mezzo delle relazioni*

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

Teorema 4.2.6 *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 4.2.4 con $\delta := \sigma$. Se $\chi = \chi_0$ suddividiamo l'intervallo $[1,x]$ in $\lfloor x/q \rfloor$ intervalli $[mq+1,(m+1)q)$, oltre, eventualmente, ad un intervallo di lunghezza $< q$. Abbiamo dunque

$$A(x) \stackrel{\text{def}}{=} \sum_{n\le x} \chi_0(n) = \frac{\phi(q)}{q} x + O_q(1),$$

e quindi, per la formula di sommazione parziale (A.1.3) con $\phi(t) = t^{-s}$ ed $a_n = \chi_0(n)$:

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

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

Osservazione 4.2.7 *Preso un carattere di Dirichlet* χ mod q *ed il carattere principale* χ_0 mod q, *e posto* $f(n) = \chi(n)n^{-s}$, $f(n) = \chi_0(n)n^{-s}$ *rispettivamente, per il Prodotto di Eulero* 2.3.1, *per* $\sigma > 1$ *si hanno le rappresentazioni*

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

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* $\chi \ne \chi_0$, *poiché in* $0 < \sigma \le 1$ *la convergenza della serie non è assoluta.*

Osservazione 4.2.8 *La derivata di* $L(s,\chi)$ *è*

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

La serie data converge totalmente in $\sigma \ge 1+\delta$ per ogni $\delta > 0$ fissato (per il Lemma 4.2.4) 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 $\chi \ne \chi_0$ per lo stesso Lemma.

Esercizi.

𝔈 1. Dato $q \in \mathbb{N}^*$, si chiami A la matrice quadrata di ordine $\phi(q)$ dei caratteri modulo q. In altre parole, se $1 = a_1 < a_2 < \cdots < a_{\phi(q)} = q-1$ sono gli interi fra 1 e q primi con q, e $\chi_0, \ldots, \chi_{\phi(q)-1}$ sono i $\phi(q)$ caratteri modulo q, allora $A_{i,j} = \chi_{j-1}(a_i)$. Determinare $|\det(A)|$. Suggerimento: sia $B = A^T$. Allora $|\det(A)|^2 = \det(A)\det(B) = \det(AB)$ ed $AB = \phi(q)I_{\phi(q)}$, dove I_k è la matrice identica k per k.

𝔈 2. * Dimostrare che se $X\colon \mathbb{N}^* \to \mathbb{C}$, $X \in \mathfrak{M}^*$ ha periodo minimo $q > 1$ (cioè è periodica di periodo q, e non è periodica per nessun intero piú piccolo), allora $X(n) = 0$ se $(n,q) > 1$. Suggerimento: se $p \mid q$ e $X(p) \ne 0$, si ha $X(p)X(n+q/p) = X(pn+q) = X(pn) = X(p)X(n)$ ed X ha periodo q/p. Quindi, se $(n,q) > 1$ allora $X(n) = 0$.

Riferimenti. Davenport [22] Capp. 1, 4–6, Apostol [5] Cap. 6.

4.3 Preliminari per il Teorema di Dirichlet

In questo paragrafo vogliamo dimostrare che esistono infiniti primi in ogni progressione aritmetica $a+nq$ con $(a,q)=1$. I Lemmi 4.3.1 e 4.3.4 implicano che $L(1,\chi)\neq 0$ se χ mod q è un carattere non principale. La piú importante conseguenza di questo fatto è che un'opportuna somma contenente χ (si veda l'enunciato del Lemma 4.3.3) è limitata, e da questo segue quasi immediatamente il Teorema di Dirichlet 4.4.1. Per una motivazione differente, si legga il §6.9.1.

Lemma 4.3.1 *Se χ è un carattere reale non principale* mod q*, allora* $L(1,\chi)\neq 0$.

Dim. Consideriamo la funzione aritmetica $F:=\chi * N_0$. Per il Teorema 2.1.4, anche F è una funzione moltiplicativa e si vede molto facilmente che

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

Dunque, in ogni caso

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

Perciò

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

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

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

diciamo. Stimiamo Σ_1 come segue: per i Lemmi A.4.1 e 4.2.4,

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

Inoltre, il Lemma 4.2.4 implica $\Sigma_2=O_q(1)$. In definitiva, abbiamo che $G(x)=2\sqrt{x}L(1,\chi)+O(1)$, e la tesi segue poiché $G(x)\to+\infty$ quando $x\to+\infty$. □

Lemma 4.3.2 *Sia χ un carattere non principale modulo q. Allora si ha*

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

Dim. Ponendo $g(x):=x$, $h(n):=\chi(n)$, ed

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

nella seconda formula di inversione di Möbius 2.1.12, troviamo

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

poiché $|\mu(n)\chi(n)|\le 1$ per ogni n. Se $L(1,\chi)\neq 0$, dividendo membro a membro l'uguaglianza precedente per x ricaviamo

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

e, moltiplicando ambo i membri per $-L'(1,\chi)/L(1,\chi)=O_q(1)$, troviamo la tesi. Se invece $L(1,\chi)=0$, ancora per la seconda formula di Möbius con $g(x):=x\log x$, $h(n):=\chi(n)$,

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

per il Lemma 4.2.4. Quindi, invertendo

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

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 2.1.10. È quindi naturale attendersi che questa quantità sia limitata se $L(1,\chi)\neq 0$, ed illimitata in caso contrario.

Lemma 4.3.3 *Sia χ un carattere non principale modulo q. Si ha*

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

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

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

Quindi, usando i Lemmi 2.2.9 e 4.2.4, si ha

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

per il Lemma A.4.4. Quindi la tesi segue dal Lemma 4.3.2. □

Lemma 4.3.4 *Se χ è un carattere non principale modulo q, allora $L(1,\chi)\neq 0$.*

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

$$\phi(q)\sum_{\substack{p\le x\\ p\equiv 1 \bmod q}}\frac{\log p}{p}=\sum_{\chi \bmod q}\sum_{p\le x}\frac{\chi(p)\log p}{p}$$

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

per i Lemmi 3.3.2 e 4.3.3. 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 4.3.1, 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. □

Riferimenti. I Lemmi 4.3.1–4.3.4 sono i Lemmi 1–4 nel Capitolo 9.8 di Hua [69].

4.4 Il Teorema di Dirichlet

Teorema 4.4.1 (Dirichlet) *Dato $q\in\mathbb{N}^*$, sia $a\in\mathbb{Z}$ un intero tale che $(a,q)=1$. Allora esistono infiniti numeri primi $p\equiv a \bmod q$. Piú precisamente, per $x\to+\infty$ si ha*

$$\sum_{\substack{p\le x\\ p\equiv a \bmod q}} \frac{\log p}{p} = \frac{1}{\phi(q)}\log x + O_{q,a}(1).$$

Dim. Per i Lemmi 4.3.3 e 4.3.4, se $\chi\neq\chi_0$ si ha

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

Per ortogonalità,

$$
\begin{aligned}
\phi(q)\sum_{\substack{p\le x\\ p\equiv a \bmod q}}\frac{\log p}{p} &= \sum_{\chi \bmod q}\overline{\chi}(a)\sum_{p\le x}\chi(p)\frac{\log p}{p}\\
&= \sum_{\substack{p\le x\\ p\nmid q}}\frac{\log p}{p} + \sum_{\substack{\chi \bmod q\\ \chi\neq\chi_0}}\sum_{p\le x}\chi\left(pa^{-1}\right)\frac{\log p}{p}\\
&= \log x + O_{q,a}(1),
\end{aligned}
$$

per la seconda formula di Mertens (3.3.2), 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 [22]. Questo risultato può essere espresso in modo piú pittoresco dicendo che i numeri primi sono (approssimativamente) equidistribuiti nelle progressioni aritmetiche.

Teorema 4.4.2 *Fissato $A > 0$, esiste una costante $C = C(A) > 0$ tale che per $x \to +\infty$ ed uniformemente per $q \leq (\log x)^A$ e per $(a,q) = 1$ si ha*

$$\pi(x;q,a) \stackrel{\text{def}}{=} \sum_{\substack{p \leq x \\ p \equiv a \bmod q}} 1 = \frac{1}{\phi(q)} \operatorname{li}(x) + O_A\left(x \exp\left(-C\sqrt{\log x}\right)\right).$$

Riferimenti. Teorema di Dirichlet 4.4.1: Hua [69], Teorema 8.2 oppure Apostol [5] Cap. 7. Dimostrazione del Teorema dei Numeri Primi nelle Progressioni 4.4.2: Davenport [22] Capp. 8–22. Dimostrazione elementare del Teorema dei Numeri Primi nelle Progressioni Aritmetiche 4.4.2: per le relazioni fra la formula di Selberg generalizzata e la distribuzione dei numeri primi nelle progressioni, si veda Granville [45].

4.5 La disuguaglianza di Pólya–Vinogradov

Definizione 4.5.1 *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 $\chi^* := \chi_0\chi$ si dice* indotto *da χ. Un carattere modulo q che* non è *indotto da altri caratteri modulo qualche divisore proprio 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. Con riferimento alle Tabelle 4.1–4.4, si può notare che il carattere χ_2 mod 8 è indotto da χ_1 mod 4, e che χ_6 mod 15 è indotto da χ_1 mod 3 mentre χ_2, χ_5 e χ_7 mod 15 sono indotti rispettivamente da χ_2, χ_1 e χ_3 mod 5. Infine χ_1 mod 24 è indotto da χ_1 mod 3, χ_2 mod 24 è indotto da χ_1 mod 4, χ_5 e χ_7 sono indotti rispettivamente da χ_1 e χ_3 mod 8 e χ_4 è indotto da un carattere mod 12. Si noti che se χ mod q induce χ^* mod 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 4.2.7. Vediamo subito un risultato che vale solo per i caratteri primitivi.

Lemma 4.5.2 *Sia $\tau(\chi)$ la somma di Gauss*

$$\tau(\chi) \stackrel{\text{def}}{=} \sum_{h \bmod q} \chi(h)\mathrm{e}_q(h).$$

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:

$$\overline{\chi}(n)\tau(\chi)=\sum_{h \bmod q}\chi\big(hn^{-1}\big)\mathrm{e}_q(h)=\sum_{h_1 \bmod q}\chi(h_1)\mathrm{e}_q(nh_1). \tag{4.5.1}$$

𝔈 1 Si può dimostrare, ma noi non lo faremo, che questa relazione vale anche se $(n,q)>1$, perché χ è primitivo. Quindi

$$|\overline{\chi}(n)|^2|\tau(\chi)|^2=\sum_{h_1,h_2 \bmod q}\sum\chi(h_1)\overline{\chi}(h_2)\mathrm{e}_q\big(n(h_1-h_2)\big).$$

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:

$$\begin{aligned}\phi(q)|\tau(\chi)|^2&=\sum_{h_1,h_2 \bmod q}\sum\chi(h_1)\overline{\chi}(h_2)\sum_{n \bmod q}\mathrm{e}_q\big(n(h_1-h_2)\big)\\&=\sum_{h_1,h_2 \bmod q}\sum\chi(h_1)\overline{\chi}(h_2)\begin{cases}q & \text{se } h_1\equiv h_2 \bmod q,\\ 0 & \text{altrimenti,}\end{cases}=q\phi(q).\end{aligned}$$

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 4.1.8). Talvolta è utile avere informazioni piú precise, e queste ci sono fornite dal seguente

Teorema 4.5.3 (Disuguaglianza di Pólya–Vinogradov) *Sia χ un carattere non principale modulo q. Si ha*

$$\sum_{n\le x}\chi(n)\ll q^{1/2}\log q.$$

Dim. Ci limitiamo al caso di χ primitivo. Per la (4.5.1) si ha

$$\begin{aligned}\sum_{n\le x}\chi(n)&=\sum_{n\le x}\frac{1}{\tau(\overline{\chi})}\sum_{h \bmod q}\overline{\chi}(h)\mathrm{e}_q(nh)=\frac{1}{\tau(\overline{\chi})}\sum_{h \bmod q}\overline{\chi}(h)\sum_{n\le x}\mathrm{e}_q(nh)\\&=\frac{1}{\tau(\overline{\chi})}\sum_{\substack{h \bmod q\\(h,q)=1}}\overline{\chi}(h)\frac{\mathrm{e}_q(h)-\mathrm{e}_q\big(h([x]+1)\big)}{1-\mathrm{e}_q(h)}.\end{aligned}$$

Osserviamo che a causa della presenza del fattore $\overline{\chi}(h)$ possiamo aggiungere alla somma su h mod 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 $|1-\mathrm{e}(u)|=2|\sin(\pi u)|$ 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 $f(t):=\big(|\sin(\pi t)|\big)^{-1}$ e $\delta:=q^{-1}$ 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 [22].

Esercizi.

𝔈 1. Dimostrare che se χ è un carattere modulo q ed n è un intero tale che $\chi(n)=0$ allora $\sum_{h \bmod q}\chi(h)\mathrm{e}_q(nh)=0$.

Riferimenti. Disuguaglianza di Pólya–Vinogradov 4.5.3: Davenport [22], Capitolo 23; Apostol [5] Teorema 8.21. Per il valore della costante e per altri problemi legati si veda Hildebrand [66], [65].

4.6 Il Teorema di Gauss–Jacobi

Torniamo brevemente sul problema di rappresentare $n\in\mathbb{N}$ come somma di due quadrati.

Teorema 4.6.1 (Gauss, Jacobi) *Detto χ il carattere non principale modulo 4, per $n\ge 1$ si ha $r_2=4\chi*N_0$, o, in altre parole,*

$$r_2(n)=4\sum_{d|n}\chi(d).$$

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 $r_2(n) = r_2\big(2^\alpha n\big)$ 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 $a \equiv b \equiv 0 \bmod 2$. 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 $\equiv 3 \bmod 4$. 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 $\equiv 1 \bmod 4$, diciamo $n := \prod_{j=1}^k p_j^{\alpha_j}$. 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 $j = 1, \ldots, k$, 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 $d := \prod_{j=1}^k p_j^{\beta_j}$ 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 2.2.2, ed utilizzando il metodo dell'iperbole di Dirichlet 2.1.13 con $y = x^{1/2}$ ed il Lemma 4.2.4, si trova

$$\sum_{n \le x} r_2(n) = 4xL(1,\chi) + O\big(x^{1/2}\big),$$

da cui $L(1,\chi) = \frac{1}{4}\pi$, risultato d'altra parte ovvio poiché

$$L(1,\chi) = \sum_{n \ge 1} \frac{(-1)^n}{2n+1}.$$

Riferimenti. La dimostrazione del Teorema di Gauss-Jacobi 4.6.1 è adattata da Hardy & Wright [57] Teorema 278.

4.7 Problemi aperti

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

$$\psi(x;q,a) \stackrel{\text{def}}{=} \sum_{\substack{n\leq x \\ n\equiv a \bmod q}} \Lambda(n) = \frac{x}{\phi(q)} + O\bigl(x^{1/2}\log^2 x\bigr),$$

(Congettura di Riemann Generalizzata). Inoltre, ci si chiede quale sia la vera uniformità che si può avere nel Teorema dei Numeri Primi nelle Progressioni 4.4.2. 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 [96] ha dimostrato che, detto $P(q,a)$ il piú piccolo numero primo $\equiv a \bmod q$, esiste una costante assoluta $L\geq 1$ tale che $P(q,a)\ll q^L$ per ogni $(a,q)=1$. Heath-Brown [62] e Pomerance [119] hanno dimostrato rispettivamente che $L\leq 5.5$ e che

$$\limsup_{q\to+\infty}\Bigl(\max_{(a,q)=1} P(q,a)\Bigr)\Bigl(q\log q\log_2 q\frac{\log_4 q}{(\log_3 q)^2}\Bigr)^{-1} > 0$$

e se vale la Congettura Generalizzata di Riemann allora

$$\max_{(a,q)=1} P(q,a) = O_\varepsilon\bigl(q^{2+\varepsilon}\bigr).$$

Riferimenti. Davenport [22] Capp. 9–22.

Capitolo 5

Metodi di Crivello

Questo Capitolo è dedicato ai moderni metodi di crivello: il primo e piú noto crivello è senza dubbio quello di Eratostene (II sec. a. C.); si tratta di una procedura che permette di determinare tutti i numeri primi in un certo intervallo $[1,N]$, come illustrato nella Figura 5.1. Questa procedura ispirò Legendre, che scoprí come ottenere una formula per determinare iterativamente $\pi(N)$ a partire dalla conoscenza esplicita di tutti i numeri primi nell'intervallo $\left[1,N^{1/2}\right]$: descriveremo la formula di Legendre nel §5.1, e vedremo che, a parte per l'indubbio interesse storico, questa formula non si presta al calcolo numerico quando N è grande, a causa del numero troppo grande di termini che contiene. In effetti, il calcolo di $\pi(N)$ viene effettuato mediante varianti di questa formula, come brevemente descritto nell'Appendice B.

Per tutto il XIX secolo non vi sono state ulteriori ricerche sui crivelli, ma all'inizio del XX secolo Brun scoprí come rendere il procedimento di Legendre piú generale e piú flessibile. Piú generale perché non è affatto necessario, per il conteggio, dover eliminare gli interi nella classe 0 mod p, ma qualunque classe di congruenza è ugualmente ammissibile. Piú flessibile perché mostrò che, riordinando opportunamente i termini presenti nella sua forma generale della formula di Legendre e trascurando alcuni addendi, si ottengono minorazioni e maggiorazioni per la quantità cercata, sempre piú precise e che coinvolgono un numero di termini decisamente inferiore a quelli necessari nella formula di Legendre. Diamo una descrizione delle idee principali alla base del crivello di Brun nel §5.2.

Si tratta della prima istanza del "crivello piccolo," in cui si prende un insieme finito A di interi, un insieme finito di numeri primi $\mathfrak{P}$ e per ciascuno di questi un numero $\omega(p)$ di classi di resto modulo p, in modo che $\omega(p) < c$ dove c è una costante assoluta. L'obiettivo è determinare (o eventualmente stimare dall'alto e dal basso) il numero di elementi di A che non giacciono in *nessuna* delle classi di resto scelte modulo i primi in $\mathfrak{P}$.

I risultati concreti che otterremo nel §5.3 come applicazione della teoria gene-

rale riguardano i valori primi assunti dai polinomi, maggiorazioni per il numero di numeri primi in un intervallo, per il numero di coppie di "primi gemelli" in un intervallo, per il numero degli interi n per cui $r_2(n) > 0$.

Nel §5.4 vedremo anche le basi della teoria del "crivello grande," per il quale viene a mancare la richiesta di una maggiorazione uniforme per $\omega(p)$. Come applicazione, nel §5.5 vedremo una fondamentale disuguaglianza per il numero di primi in un intervallo (Teorema di Brun–Titchmarsh 5.5.2), una maggiorazione piú precisa per il numero degli interi n per cui $r_2(n) > 0$ e per il numero di primi gemelli.

Il crivello piccolo (almeno nella sua forma elementare descritta qui) è sostanzialmente combinatorio, mentre il crivello grande ha una base analitica e per molti versi è piú potente del crivello piccolo. Per discussioni complete sui crivelli si vedano le monografie di Greaves [48], Halberstam & Richert [50], Halberstam & Roth [51], Harman [59].

5.1 Il principio di inclusione–esclusione e la formula di Legendre

Definizione 5.1.1 *Dati $\mathcal{A} \subseteq \mathbb{N}^*$, $\mathcal{B} \subseteq \mathbb{N}$, $x \geq 1$, d ed $M \in \mathbb{N}^*$ poniamo*

$$\mathcal{S}(\mathcal{A};x;M) \stackrel{\text{def}}{=} \bigl|\{a \in \mathcal{A} \cap [1,x] \colon (a,M) = 1\}\bigr| \qquad \mathcal{B}(x) \stackrel{\text{def}}{=} \mathcal{B} \cap [1,x]$$

$$\mathcal{A}_d \stackrel{\text{def}}{=} \{a \in \mathcal{A} \colon d \mid a\} \qquad P(x) \stackrel{\text{def}}{=} \prod_{p \leq x} p = \exp\theta(x).$$

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: dato che le formule dipendono solo dai fattori primi di M e non dalla loro molteplicità, nel seguito potremo supporre sempre che $\mu(M) \neq 0$.

Teorema 5.1.2 (Principio di Inclusione–Esclusione) *Dato un insieme di numeri naturali $\mathcal{A} \subseteq \mathbb{N}^*$, un numero reale $x \geq 1$ ed un numero naturale $M \in \mathbb{N}^*$ si ha*

$$\mathcal{S}(\mathcal{A};x;M) = \sum_{d \mid M} \mu(d) \bigl|\mathcal{A}_d(x)\bigr|.$$

Dim. Per il Teorema 2.1.9

$$\mathcal{S}(\mathcal{A};x;M) = \sum_{\substack{a \in \mathcal{A}(x) \\ (a,M)=1}} 1 = \sum_{a \in \mathcal{A}(x)} \sum_{d \mid (a,M)} \mu(d)$$

$$= \sum_{d|M} \mu(d) \sum_{\substack{a \in \mathcal{A}(x) \\ d|a}} 1 = \sum_{d|M} \mu(d) \left| \mathcal{A}_d(x) \right|.$$

𝔈 1 Si osservi che il risultato dipende solo dai fattori primi distinti di M. □

Per esempio, prendendo $\mathcal{A} = [1, M] = \mathbb{N}(M)$ ed $x = M$ si ha

$$\mathcal{S}(\mathcal{A}; M; M) = \phi(M) = \sum_{d|M} \mu(d) \frac{M}{d} = (N_1 * \mu)(M),$$

che è una parte del Teorema 2.2.8.

Utilizzando le idee di Eratostene, Legendre scoprí una formula che permette
𝔈 2 di calcolare $\pi(x)$ iterativamente:

$$\pi(x) - \pi\left(x^{1/2}\right) + 1 = \sum_{d|P\left(x^{1/2}\right)} \mu(d) \left[\frac{x}{d}\right]. \tag{5.1.1}$$

La dimostrazione è molto semplice: ci sono esattamente $[x]$ interi $\le x$ (il termine $d = 1$). Ogni primo $p \le x^{1/2}$ divide $\left[x/p\right]$ 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

$$\begin{aligned}
\sum_{d|210} \mu(d) \left[\frac{100}{d}\right] &= \left[\frac{100}{1}\right] - \left(\left[\frac{100}{2}\right] + \left[\frac{100}{3}\right] + \left[\frac{100}{5}\right] + \left[\frac{100}{7}\right]\right) \\
&\quad + \left(\left[\frac{100}{6}\right] + \left[\frac{100}{10}\right] + \left[\frac{100}{14}\right] + \left[\frac{100}{15}\right] + \left[\frac{100}{21}\right] + \left[\frac{100}{35}\right]\right) \\
&\quad - \left(\left[\frac{100}{30}\right] + \left[\frac{100}{42}\right] + \left[\frac{100}{70}\right] + \left[\frac{100}{105}\right]\right) + \left[\frac{100}{210}\right] \\
&= 100 - (50 + 33 + 20 + 14) + (16 + 10 + 7 + 6 + 4 + 2) \\
&\qquad - (3 + 2 + 1 + 0) + 0 \\
&= 100 - 117 + 45 - 6 = 22,
\end{aligned} \tag{5.1.2}$$

ed infatti $\pi(100) - \pi(10) + 1 = 25 - 4 + 1 = 22$. Una dimostrazione altrettanto semplice si può dare utilizzando il Principio di Inclusione–Esclusione 5.1.2 con $\mathcal{A} = \mathbb{N}^*$, $M = P\left(x^{1/2}\right)$, poiché la condizione $(M, a) = 1$ con $a \in \mathbb{N}(x)$ vuol dire che $a = 1$ oppure a è un numero primo $p \in \left(x^{1/2}, x\right]$. Il difetto principale della formula di Legendre è che contiene troppi termini per essere utilizzabile come strumento pratico per il calcolo. Per esempio, consideriamo un parametro reale $z \in \left[2, x^{1/2}\right]$. È evidente che $\{a \in \mathbb{N}(x) \colon \left(a, P(z)\right) = 1\} \supseteq \{p \in (z, x]\}$. Applicando la formula di Legendre otteniamo

$$\pi(x) - \pi(z) \le \mathcal{S}\left(\mathbb{N}^*; x; P(z)\right) = \sum_{d|P(z)} \mu(d) \left[\frac{x}{d}\right]$$

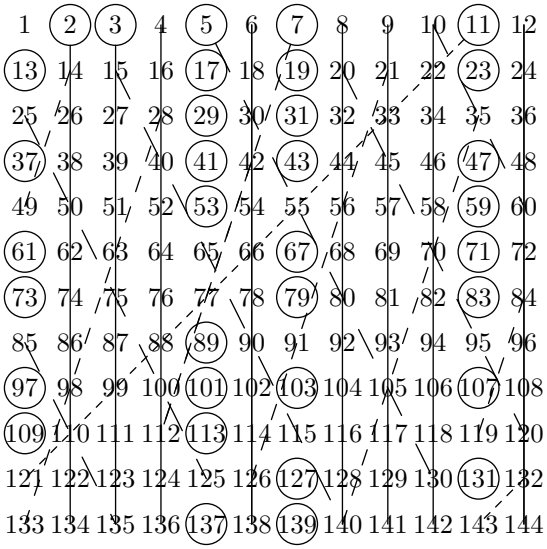


Figura 5.1: Il crivello di Eratostene.

$$\begin{aligned}
&= \sum_{d|P(z)} \mu(d)\frac{x}{d} + O\Big(\sum_{\substack{d|P(z)\\ d\le x}} 1\Big)\\
&= x\prod_{p\le z}\left(1-\frac{1}{p}\right) + O\Big(2^{\pi(z)}\Big)\\
&= \mathrm{e}^{-\gamma}\frac{x}{\log z}\big(1+o(1)\big) + O\Big(2^{2z/\log z}\Big).
\end{aligned}$$

per il Teorema di Mertens 3.3.6 ed il Lemma 2.1.5. Se non vogliamo dimostrare banalità tipo $\pi(x) = O(x)$ (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

$$\pi(x) = O\left(\frac{x}{\log\log x}\right).$$

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.

Esercizi.

𝔈 1. Dimostrare il Principio di Inclusione-Esclusione 5.1.2 utilizzando la formula

$$\Big|\bigcap_{i\in I} B_i\Big| = \sum_{\substack{J\subseteq I\\ J\neq\emptyset}} (-1)^{1+|J|}\Big|\bigcup_{j\in J} B_j\Big|$$

valida qualunque sia l'insieme finito I e qualunque siano gli insiemi finiti B_i, $i \in I$. Suggerimento: Porre $I := \{p\colon\ p \mid M\}$, $B_d := \mathbb{N} \cap [1,x] \setminus \mathcal{A}_d$ ed utilizzare il Teorema 2.1.9.

𝔈 2. Dimostrare la formula di Legendre (5.1.1) utilizzando l'Esercizio 2.1.5 ed osservando che

$$\pi(x) = \pi\bigl(x^{1/2}\bigr) + \sum_{x^{1/2}<p\le x} 1 = \pi\bigl(x^{1/2}\bigr) + \sum_{x^{1/2}<p\le x} \sum_{d\le x/p} \mu(d) \left[\frac{x}{pd}\right].$$

Riferimenti. Principio di Inclusione–Esclusione 5.1.2: si veda anche Hardy & Wright [57] Teorema 260. Formula di Legendre 5.1.1: Halberstam & Richert [50], §1.5 e relative note, o Lehmer [92].

5.2 Il crivello di Brun

Vogliamo modificare il Teorema 5.1.2 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 $\binom{n}{r} := 0$ 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 5.2.1 *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 $m > n$ allora il primo membro vale $(1-1)^{n+1} = 0$. □

Teorema 5.2.2 (Brun) *Dati $\mathcal{A} \subseteq \mathbb{N}^*$, $x \ge 1$, $m \in \mathbb{N}^*$ dispari ed $M \in \mathbb{N}^*$ si ha*

$$\sum_{\substack{d\mid M\\ \omega(d)\le m}} \mu(d) \bigl|\mathcal{A}_d(x)\bigr| \le \mathcal{S}(\mathcal{A};x;M) \le \sum_{\substack{d\mid M\\ \omega(d)<m}} \mu(d) \bigl|\mathcal{A}_d(x)\bigr|. \tag{5.2.1}$$

Dim. Consideriamo gli insiemi

$$\mathfrak{A} \stackrel{\text{def}}{=} \{a \in \mathcal{A}\colon a \le x, (a,M) = 1\} \qquad \text{e} \qquad \mathfrak{B} \stackrel{\text{def}}{=} \{a \in \mathcal{A}\colon a \le x, (a,M) > 1\}$$

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 (5.2.1) esattamente una volta (per $d = 1$). Per gli interi $n \in \mathfrak{B}$ si ha $\delta := (n,M) > 1$, ed n è contato in quegli insiemi $\mathcal{A}_d$ per cui $\omega(d) < m$ e $d \mid \delta$. Per il Lemma 5.2.1, il contributo totale di n alla somma di destra nella (5.2.1) è

$$\sum_{\substack{d\mid\delta \\ \omega(d)<m}} \mu(d) = \sum_{r=0}^{m-1} (-1)^r \binom{\omega(\delta)}{r} = (-1)^{m-1} \binom{\omega(\delta)-1}{m-1} \ge 0,$$

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 5.1.2, poiché allora le due somme nella (5.2.1) sono uguali. Le due somme nella (5.2.1) sono una parte della somma considerata nella 5.1.2: 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 5.1.2. In sostanza, il Teorema 5.2.2 implica che le somme parziali nella 5.1.2, ordinate opportunamente, forniscono alternativamente maggiorazioni e minorazioni di $\mathcal{S}(\mathcal{A};x;M)$, come per esempio l'ultima somma nella (5.1.2).

È chiaro che il Teorema di Brun 5.2.2 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 $g \ge 1$ con primo coefficiente $a_g > 0$, mentre l'intero positivo M tale che $\mu(M) \ne 0$ e l'intero positivo dispari m saranno scelti in modo opportuno nelle applicazioni.

𝔈 1-2 **Lemma 5.2.3** *Poniamo* $\rho(d) := |\{n \bmod d\colon f(n) \equiv 0 \bmod d\}|$. *La funzione* ρ *è moltiplicativa ed inoltre* $\rho(p) \le \min(p,g)$ *per ogni numero primo* p.

Dim. La prima parte segue dal Teorema Cinese del Resto 1.2.4; inoltre in un campo come $\mathbb{Z}_p$ ogni equazione polinomiale ha un numero di radici che non supera il grado. □

Lemma 5.2.4 *Per ogni* $x \ge 1$ *si ha*

$$|\{n \in \mathbb{N}(x)\colon f(n) \equiv 0 \mod d\}| = \rho(d)\left(\frac{x}{d} + O(1)\right).$$

Dim. Poiché $f(n) \equiv f(m) \bmod d$ se $n \equiv m \bmod d$, l'equazione $f(n) \equiv 0 \bmod d$ ha esattamente $\rho(d)$ soluzioni in ogni intervallo di d interi consecutivi. Suddividiamo $[1,x]$ in $\lfloor x/d \rfloor$ intervalli del tipo $[(k-1)d+1, kd]$, piú eventualmente un intervallo di lunghezza $\le d$. In totale $\rho(d)\lfloor x/d \rfloor + O(\rho(d)) = \rho(d)\big(x/d + O(1)\big)$ soluzioni, come si voleva. □

Lemma 5.2.5 *Sia M un intero positivo tale che $\mu(M) \neq 0$. Allora*

$$\sum_{\substack{d \mid M \\ \omega(d) < m}} \rho(d) \le \mathrm{e}\big(g\omega(M)\big)^{m-1}.$$

Dim. Per il Lemma 5.2.3 si ha $\rho(d) \le g^{\omega(d)}$ se $d \mid M$, e quindi

$$\begin{aligned}\sum_{\substack{d \mid M \\ \omega(d) < m}} \rho(d) &\le \sum_{r=0}^{m-1} \sum_{\substack{d \mid M \\ \omega(d) = r}} g^{\omega(d)} = \sum_{r=0}^{m-1} g^r \binom{\omega(M)}{r} \\ &\le g^{m-1} \sum_{r=0}^{m-1} \frac{\omega(M)^r}{r!} \le \mathrm{e}\big(g\omega(M)\big)^{m-1},\end{aligned}$$

poiché $\binom{n}{r} \le n^r (r!)^{-1}$. □

Lemma 5.2.6 *Sia S_r la funzione simmetrica elementare di ordine r dei numeri $\xi_1, \dots, \xi_n \in \mathbb{R}^{0+}$, con $n \ge r$. Si ha*

$$S_r \le \frac{S_1^r}{r!}.$$

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 $|\underline{\alpha}| := \alpha_1 + \cdots + \alpha_n$ e $\underline{\alpha}! := \alpha_1! \cdots \alpha_n!$. Inoltre, per ogni $\underline{x} \in \mathbb{R}^n$ con $\underline{x} = (x_1, \dots, x_n)$ poniamo $\underline{x}^{\underline{\alpha}} := x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. Siano

$$\begin{aligned}\mathfrak{A}_n(r) = \mathfrak{A}(r) &\stackrel{\text{def}}{=} \big\{\underline{\alpha} \in \mathbb{N}^n \colon |\underline{\alpha}| = r\big\} \\ \mathfrak{B}_n(r) = \mathfrak{B}(r) &\stackrel{\text{def}}{=} \big\{\underline{\beta} \in \mathfrak{A}_n(r) \colon \beta_i \in \{0,1\}\big\}.\end{aligned}$$

𝔈 3 Posto $\underline{\xi} := (\xi_1, \dots, \xi_n) \in \big(\mathbb{R}^{0+}\big)^n$, 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 $n \geq r$), cosa che si può dimostrare direttamente senza difficoltà. □

Es 4

Lemma 5.2.7 *Poniamo* $\Sigma(M) := \sum_{p|M} p^{-1}$. *Abbiamo*

$$\sum_{r=m}^{\omega(M)} \sum_{\substack{d|M \\ \omega(d)=r}} \frac{\rho(d)}{d} \leq \sum_{r=m}^{\omega(M)} \left(\frac{eg\Sigma(M)}{r}\right)^r.$$

Dim. Infatti per il Lemma 5.2.3 si ha

$$\sum_{r=m}^{\omega(M)} \sum_{\substack{d|M \\ \omega(d)=r}} \frac{\rho(d)}{d} \leq \sum_{r=m}^{\omega(M)} g^r \sum_{\substack{d|M \\ \omega(d)=r}} \frac{1}{d}. \tag{5.2.2}$$

La somma interna è precisamente la funzione simmetrica elementare di ordine r sui numeri p^{-1}, dove $p \mid M$. Per il Lemma 5.2.6 il secondo membro della (5.2.2) è

$$\leq \sum_{r=m}^{\omega(M)} g^r \frac{S_1^r}{r!} \leq \sum_{r=m}^{\omega(M)} \left(\frac{eg\Sigma(M)}{r}\right)^r,$$

poiché $e^r > r^r(r!)^{-1}$ per $r \geq 1$, per lo sviluppo in serie di e^r. □

Lemma 5.2.8 *Siano* $f \in \mathbb{Z}[x]$ *un polinomio di grado* $g \geq 1$, *con primo coefficiente* $a_g > 0$, m *un intero positivo dispari ed* M *un intero positivo tale che* $\mu(M) \neq 0$. *Sia inoltre* $\mathcal{A} := f(\mathbb{N}) \cap \mathbb{N}^*$. *Per* $x \to +\infty$ *si ha*

$$S(\mathcal{A}; f(x); M) \leq x \prod_{p|M} \left(1 - \frac{\rho(p)}{p}\right) + O\Big(x \sum_{r=m}^{\omega(M)} \left(\frac{eg\Sigma(M)}{r}\right)^r\Big) + O\Big(\big(g\omega(M)\big)^{m-1}\Big).$$

Se m *è pari la disuguaglianza vale con il segno* $\geq$ *al posto di* $\leq$.

Dim. Si osservi che per x sufficientemente grande la condizione $f(n) \le f(x)$ è equivalente ad $n \le x$. Per il Lemma 5.2.4 abbiamo $\big|\mathcal{A}_d \cap [1, f(x)]\big| = \big|\{n \le x\colon\ f(n) \equiv 0 \bmod d\}\big| = \rho(d)xd^{-1} + O(\rho(d))$. Quindi, per il Teorema di Brun 5.2.2 ed il Lemma 2.1.5, si ha

$$\begin{aligned}\mathcal{S}\big(\mathcal{A}; f(x); M\big) &\le x \sum_{\substack{d\mid M\\ \omega(d)<m}} \frac{\mu(d)\rho(d)}{d} + O\Big(\sum_{\substack{d\mid M\\ \omega(d)<m}} \rho(d)\Big)\\ &= x\left\{\prod_{p\mid M}\Big(1-\frac{\rho(p)}{p}\Big) + O\Big(\sum_{r=m}^{\omega(M)} \sum_{\substack{d\mid M\\ \omega(d)=r}} \frac{\rho(d)}{d}\Big)\right\}\\ &\quad + O\Big(\big(g\omega(M)\big)^{m-1}\Big)\end{aligned}$$

ed il risultato voluto segue dai Lemmi 5.2.7 e 5.2.5. □

Per ottenere un risultato piú maneggevole di quest'ultimo, 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 5.2.9 *Siano $f \in \mathbb{Z}[x]$ un polinomio di grado $g \ge 1$, con primo coefficiente $a_g > 0$, $\mathfrak{P}$ un insieme di numeri primi con la proprietà che esiste $\kappa \in \mathbb{R}^+$ tale che*

$$\sum_{p\in\mathfrak{P}(z)} \frac{1}{p} \sim \kappa \log\log z \qquad \text{per } z \to +\infty.$$

Allora per $z := \exp\big(\log x(2(1+\varepsilon)\kappa e g \log\log x)^{-1}\big)$ ed $x \to +\infty$ si ha

$$\big|\{n \le x\colon\ p \mid f(n) \Rightarrow p \notin \mathfrak{P}(z)\}\big| \le x \prod_{p\in\mathfrak{P}(z)}\Big(1-\frac{\rho(p)}{p}\Big) + O_{g,\kappa}\Big(\frac{x}{(\log z)^{2\kappa g}}\Big).$$

Dim. Scegliamo $M = M(z) := \prod_{p\in\mathfrak{P}(z)} p$ e quindi si ha $\Sigma(M) \le (1+\varepsilon)\kappa\log\log z$ e per il Teorema 3.2.3 $\omega(M) \le (2\log 2+\varepsilon)z(\log z)^{-1}$. Inoltre osserviamo che

$$\big|\{n \le x\colon\ p \mid f(n) \Rightarrow p \notin \mathfrak{P}(z)\}\big| \le z + \mathcal{S}\big(\mathcal{A}; f(x); M(z)\big),$$

nella notazione del Lemma 5.2.8. Se $m \ge 2(1+\varepsilon)\kappa e g \log\log z$, il primo termine d'errore è

$$\le x \sum_{r\ge m}\left(\frac{(1+\varepsilon)\kappa e g\log\log z}{m}\right)^r \le x\sum_{r\ge m} 2^{-r} = 2^{1-m}x.$$

Il secondo termine è $\le \exp\{m(\log g + \log\omega(M))\} \le \exp\{m\log z\}$. Scegliendo $m = 2[(1+\varepsilon)\kappa e g\log\log z] + 3$ si vede facilmente che $2^m \ge C(g)(\log z)^{2\kappa g}$ per un'opportuna costante positiva $C(g)$ e che $\exp\{m\log z\} \le x(\log z)^{-2\kappa g}$. Raccogliendo tutte queste stime otteniamo la tesi. □

Corollario 5.2.10 *Sia f come sopra, e $z := \exp\bigl(\log x(8eg\log\log x)^{-1}\bigr)$. Per $x \to +\infty$*

$$\bigl|\{n \le x\colon\ p \mid f(n) \Rightarrow p > z\}\bigr| \le x\prod_{p\le z}\left(1-\frac{\rho(p)}{p}\right) + O_g\left(\frac{x}{(\log z)^{2g}}\right).$$

Dim. Basta prendere $\mathfrak{P}$ l'insieme di tutti i numeri primi e $\kappa = 1$ nel Teorema 5.2.9. □

Si osservi che il significativo miglioramento sulle conseguenze dirette del Principio di Inclusione–Esclusione 5.1.2 (si vedano i risultati nel prossimo paragrafo) dipende essenzialmente dal fatto che prendiamo m relativamente piccolo rispetto ad $\omega(M)$.

Esercizi.

𝔈 1. Dimostrare che la funzione ρ definita nel Lemma 5.2.3 è moltiplicativa.

𝔈 2. Dato $f \in \mathbb{Z}[x]$ poniamo $\phi_f(n) := |\{m \in \mathbb{N}\cap[1,n]\colon\ \bigl(n, f(m)\bigr) = 1\}|$. Dimostrare che $\phi_f \in \mathfrak{M}$ e che se $\rho_f(p) := |\{n \bmod p\colon\ f(n) \equiv 0 \bmod p\}|$, allora

$$\phi_f(n) = n\prod_{p\mid n}\left(1-\frac{\rho_f(p)}{p}\right).$$

𝔈 3. Dimostrare che se $n_i \ge 0$ per $i = 1,\dots,k$, allora il numero $N := (n_1+\cdots+n_k)!/(n_1!n_2!\cdots n_k!)$ è un intero.

𝔈 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 5.2.6 si ha

$$f\bigl(\underline{x}+\underline{\xi}\bigr) = \sum_{r\ge 0}\frac{1}{r!}\sum_{\underline{\alpha}\in\mathfrak{A}(r)} c(\underline{\alpha})\frac{\partial^{|\underline{\alpha}|}f}{\partial x_1^{\alpha_1}\cdots\partial x_n^{\alpha_n}}(\underline{x})\,\underline{\xi}^{\underline{\alpha}}.$$

Riferimenti. Questo paragrafo è ispirato a Landau [85], Parte II, Cap. II. Per la moltiplicatività di ρ, Hardy & Wright [57] Teorema 122. Altri tipi di crivello sono descritti in Halberstam & Richert [50], Halberstam & Roth [51], §§4.1–9, James [75], [76].

5.3 Applicazioni del crivello di Brun

5.3.1 Primi e polinomi

Il Corollario 5.2.10 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 (3.3.2):

$$\sum_{p\le x}\frac{\rho(p)\log p}{p}=\kappa\log x+O_f(1), \tag{5.3.1}$$

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:

$$|\{n\le x:\ p\mid f(n)\Rightarrow p>z\}|\ll\frac{x}{\log z}\prod_p\left(1-\frac{\rho(p)-1}{p-1}\right)\left(1-\frac{1}{p}\right)^{1-\kappa}$$

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.

5.3.2 Maggiorazione del numero di primi in un intervallo

Scegliamo $f(n)=n$, per cui $\rho(d)=1$ per ogni $d\in\mathbb{N}^*$ e

$$\begin{aligned}\pi(x)&\le z+\big|\{n\le x:\ p\mid n\Rightarrow p>z\}\big|\\&\le x\prod_{p\le z}\left(1-\frac{1}{p}\right)+O\left(\frac{x}{(\log z)^2}\right)\ll\frac{x\log\log x}{\log x}\end{aligned}$$

per il Teorema di Mertens 3.3.6. Anche se questo risultato è inferiore a quello ottenuto in modo elementare nel Teorema 3.2.3, 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 Legendre, qui non stimiamo i resti con $O(1)$, ma con $O\big(\rho(d)d^{-1}\big)$, che è molto piú piccolo per d grande.

5.3.3 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 $q\ge1$ e che $1\le a\le q$. Si ha

$$\rho(p)=\begin{cases}1 & \text{se } p\nmid q,\\ 0 & \text{se } p\mid q.\end{cases}$$

Se x è sufficientemente grande rispetto a q, dal Corollario 5.2.10 ricaviamo

$$|\{n \le x\colon qn+a \text{ è primo}\}| \le x \prod_{\substack{p\le z\\ p\nmid q}} \left(1-\frac{1}{p}\right) + O\left(\frac{x}{(\log z)^2}\right) \ll \frac{q}{\phi(q)} \frac{x\log\log x}{\log x}.$$

Non deve stupire la presenza del fattore q a numeratore, in apparente contrasto con il Teorema dei Numeri Primi nelle Progressioni 4.4.2. Infatti

$$\begin{aligned} |\{n \le x\colon qn+a \text{ è primo}\}| &= |\{qn+a \le qx+a\colon qn+a \text{ è primo}\}| \\ &= |\{m \le qx+a\colon m \equiv a \mod q \text{ ed } m \text{ è primo}\}|. \end{aligned}$$

5.3.4 Polinomi di secondo grado

Possiamo utilizzare i risultati precedenti nel caso di polinomi di secondo grado, poiché siamo in grado di determinare esattamente $\rho(p)$ per ogni p primo e quindi di dimostrare direttamente che vale la (5.3.1).

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 $p \ne 2, 3$ si ha $\rho(p) = 1+\left(3 \mid p\right)$. Per la legge di reciprocità quadratica 1.6.4 e per $p > 3$ si ha $\left(3 \mid p\right) = \left(p \mid 3\right)(-1)^{(p-1)/2}$, 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 $\rho(p) = 1+\chi_1(p)$ (per ogni p) e la (5.3.1) segue in questo caso dai Teoremi 3.3.2 e 4.3.3.

Consideriamo poi il polinomio (riducibile) $f(n) = n(n+h)$ (dove $h \in \mathbb{N}^*$): se $2 \nmid h$ si vede direttamente che $|\{n \le x\colon p \mid n(n+h) \Rightarrow p > 2\}| = O_h(1)$. Se invece $2 \mid h$ il Corollario 5.2.10 ci dà immediatamente

$$|\{n \le x\colon p \mid n(n+h) \Rightarrow p > z\}| \le x \prod_{p\le z} \left(1-\frac{\rho(p)}{p}\right) + O\left(\frac{x}{(\log x)^4}\right). \tag{5.3.2}$$

In questo caso il discriminante è $-h^2$ ed abbiamo

$$\rho(p) = \begin{cases} 2 & \text{se } p \nmid h, \\ 1 & \text{se } p \mid h. \end{cases}$$

Per h pari, $h \ne 0$, poniamo

$$\mathfrak{S}(h) \stackrel{\text{def}}{=} 2C_0 \prod_{\substack{p\mid h\\ p>2}} \frac{p-1}{p-2} \qquad \text{dove} \qquad C_0 \stackrel{\text{def}}{=} \prod_{p>2} \left(1-\frac{1}{(p-1)^2}\right). \tag{5.3.3}$$

Se z è sufficientemente grande, si ha

$$\begin{aligned}\prod_{p\le z}\Big(1-\frac{\rho(p)}{p}\Big) &= \prod_{p\mid h}\Big(1-\frac{1}{p}\Big)\prod_{\substack{p\le z\\ p\nmid h}}\Big(1-\frac{2}{p}\Big)\\ &= \frac{1}{2}\prod_{\substack{p\mid h\\ p>2}}\left\{\Big(1-\frac{1}{p}\Big)\Big(1-\frac{2}{p}\Big)^{-1}\right\}\prod_{3\le p\le z}\Big(1-\frac{2}{p}\Big)\\ &= \frac{1}{2}\prod_{\substack{p\mid h\\ p>2}}\Big(\frac{p-1}{p-2}\Big)\prod_{3\le p\le z}\frac{p(p-2)}{(p-1)^2}\prod_{3\le p\le z}\Big(1-\frac{1}{p}\Big)^2\\ &= \mathfrak{S}(h)\big(1+O(z^{-1})\big)\prod_{p\le z}\Big(1-\frac{1}{p}\Big)^2.\end{aligned}$$

In definitiva, prendendo z come nel Corollario 5.2.10, qualunque sia $h\in\mathbb{N}^*$, si ha

$$|\{n\le x\colon p\mid n(n+h)\Rightarrow p>z\}|\le C'\mathfrak{S}(h)\frac{x(\log\log x)^2}{(\log x)^2}, \tag{5.3.4}$$

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 $\pi_h(x) := |\{n\le x\colon n \text{ ed } n+h \text{ sono primi}\}$, 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 formula di sommazione parziale (A.1.3) è facile vedere che la (5.3.4) 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 primi gemelli converge, a differenza della somma dei reciproci di tutti i numeri primi.

5.3.5 Rappresentazioni come somma di quadrati

Il Teorema 5.2.9 implica una forma debole del Teorema di Landau 2.2.3: piú precisamente, utilizzando il Teorema 5.5.3, non è difficile dimostrare che

$$|\{n\le x\colon r_2(n)>0\}|\ll x\left(\frac{\log\log x}{\log x}\right)^{1/2}.$$

Infatti, per il Teorema 1.4.10, se $r_2'(n)>0$ allora n non ha fattori primi $\equiv 3 \bmod 4$ e $4\nmid n$, e si può utilizzare il Teorema 5.2.9 con $\mathfrak{P} := \{2\}\cup\{p\colon p\equiv 3 \bmod 4\}$ poiché la stima richiesta dal Teorema vale con $\kappa=\frac{1}{2}$ per sommazione parziale dal Teorema 4.4.1. Piú avanti otterremo una stima dell'ordine di grandezza corretto.

Esercizi.

$\mathfrak{E}$ 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.

Riferimenti. Il Teorema 2.6 in Halberstam & Richert [50], citato anche nel §5.6, dà risultati uniformi e del corretto ordine di grandezza. Per la (5.3.1) in generale si veda Nagel [107]. Il prodotto infinito converge per il Teorema degli Ideali Primi. Per la definizione generale di discriminante di un polinomio, Childs [15] Parte III, Cap. 15. Per la possibilità di esprimere il simbolo di Legendre tramite opportuni caratteri, Davenport [22] Cap. 5.

5.4 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 5.4.1 *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 della variabile reale x definita da*

$$S(x) \stackrel{\text{def}}{=} \sum_{n=M+1}^{M+N} a_n \mathrm{e}(nx) = \sum_{n=M+1}^{M+N} a_n \mathrm{e}^{2\pi i n x}.$$

Definizione 5.4.2 *Dato un numero reale x poniamo*

$$\|x\| \stackrel{\text{def}}{=} \min_{n\in\mathbb{Z}} |x-n| = \min\bigl\{\{x\}, 1-\{x\}\bigr\}.$$

Dati R numeri reali $x_1, \dots x_R$, diciamo che essi sono δ-ben spaziati *se*

$$\min_{i\neq j} \|x_i - x_j\| \geq \delta > 0.$$

Teorema 5.4.3 *Se i numeri reali $x_1, \dots x_R$ sono δ-ben spaziati, allora*

$$\sum_{j=1}^{R} |S(x_j)|^2 \leq \bigl(N + 2\delta^{-1}\bigr) \sum_{n=M+1}^{M+N} |a_n|^2.$$

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 5.4.4 (Selberg) *Sia $\mathcal{X}$ uno spazio vettoriale su $\mathbb{C}$ con prodotto scalare $(\cdot,\cdot)$, siano $\underline{\xi}_1, \underline{\xi}_2, \dots, \underline{\xi}_R$, $\underline{\phi} \in \mathcal{X} \setminus \{\underline{0}\}$ e sia $\|\underline{\phi}\|_{\mathcal{X}} := (\underline{\phi},\underline{\phi})^{1/2}$. Posto*

$$b_j \stackrel{\text{def}}{=} \sum_{k=1}^{R} |(\underline{\xi}_k, \underline{\xi}_j)|, \qquad \textit{si ha} \qquad \sum_{j=1}^{R} \frac{|(\underline{\phi},\underline{\xi}_j)|^2}{b_j} \le \|\underline{\phi}\|_{\mathcal{X}}^2.$$

Dim. Qualunque siano i numeri complessi $a_1, \dots, a_R$ si ha

$$\begin{aligned}
0 &\le \Big\|\underline{\phi} - \sum_{j=1}^{R} a_j \underline{\xi}_j\Big\|_{\mathcal{X}}^2 \\
&= \|\underline{\phi}\|_{\mathcal{X}}^2 - 2\Re\Big\{\sum_{j=1}^{R} \overline{a}_j (\underline{\phi},\underline{\xi}_j)\Big\} + \sum_{i=1}^{R}\sum_{j=1}^{R} a_i \overline{a}_j (\underline{\xi}_i,\underline{\xi}_j) \\
&\le \|\underline{\phi}\|_{\mathcal{X}}^2 - 2\Re\Big\{\sum_{j=1}^{R} \overline{a}_j (\underline{\phi},\underline{\xi}_j)\Big\} + \frac{1}{2}\sum_{i=1}^{R}\sum_{j=1}^{R} (|a_i|^2 + |a_j|^2)|(\underline{\xi}_i,\underline{\xi}_j)| \\
&= \|\underline{\phi}\|_{\mathcal{X}}^2 - 2\Re\Big\{\sum_{j=1}^{R} \overline{a}_j (\underline{\phi},\underline{\xi}_j)\Big\} + \sum_{i=1}^{R}\sum_{j=1}^{R} |a_j|^2 |(\underline{\xi}_i,\underline{\xi}_j)|,
\end{aligned}$$

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 $a_j := (\underline{\phi},\underline{\xi}_j) b_j^{-1}$ dà il risultato voluto. □

Dim. del Teorema 5.4.3. Sia $\mathcal{X} := \ell^2(\mathbb{Z})$, lo spazio (di Hilbert) delle successioni in $\mathbb{Z}$ di quadrato sommabile, munito del prodotto scalare

$$(\underline{\alpha},\underline{\beta}) \stackrel{\text{def}}{=} \sum_{n\in\mathbb{Z}} \alpha_n \overline{\beta}_n, \qquad \text{dove} \qquad \underline{\alpha} \stackrel{\text{def}}{=} (\alpha_n)_{n\in\mathbb{Z}},\ \underline{\beta} \stackrel{\text{def}}{=} (\beta_n)_{n\in\mathbb{Z}}.$$

Il nostro primo obiettivo è la disuguaglianza

$$\sum_{j=1}^{R} |S(x_j)|^2 \le \big(2N + 1 + 2\delta^{-1}\big) \sum_{n=-N}^{N} |a_n|^2, \tag{5.4.1}$$

dove

$$S(x) \stackrel{\text{def}}{=} \sum_{n=-N}^{N} a_n \mathrm{e}(nx).$$

Nel Lemma di Selberg 5.4.4 prendiamo $\underline{\phi} := (\phi_n)_{n\in\mathbb{Z}}$, $\underline{\xi}_j := (\xi(j)_n)_{n\in\mathbb{Z}}$, dove

$$\phi_n \stackrel{\text{def}}{=} \begin{cases} a_n & \text{se } |n| \le N, \\ 0 & \text{altrimenti;} \end{cases}$$

e

$$\xi(j)_n \stackrel{\text{def}}{=} \begin{cases} \mathrm{e}\big(-nx_j\big) & \text{se } |n| \le N, \\ \mathrm{e}\big(-nx_j\big)\big((N+L-|n|)/L\big)^{1/2} & \text{se } N < |n| \le N+L, \\ 0 & \text{altrimenti,} \end{cases}$$

ed L è un intero che sceglieremo piú avanti. Evidentemente

$$\|\underline{\phi}\|_X^2 = \sum_{n=-N}^{N} |a_n|^2, \qquad (\underline{\phi}, \underline{\xi}_j) = \sum_{n=-N}^{N} a_n \,\mathrm{e}(nx_j) = S(x_j).$$

Inoltre $(\underline{\xi}_i, \underline{\xi}_i) = 2N+L$, mentre, utilizzando le identità

$$\sum_{n=-N}^{N} \mathrm{e}(n\alpha) = \frac{\sin\big((2N+1)\pi\alpha\big)}{\sin(\pi\alpha)},$$

$$\sum_{n=-N}^{N} (N-|n|)\mathrm{e}(n\alpha) = \Big|\sum_{n=1}^{N} \mathrm{e}(n\alpha)\Big|^2 = \left(\frac{\sin(N\pi\alpha)}{\sin(\pi\alpha)}\right)^2$$

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

$$|(\underline{\xi}_i, \underline{\xi}_j)| \le \frac{1}{L\sin^2\big(\pi(x_i-x_j)\big)}.$$

Inoltre per $|\alpha| \le \frac{1}{2}$ si ha $|\sin(\pi\alpha)| \ge 2|\alpha|$, 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

$$\begin{aligned} \sum_{j=1}^{R} |(\underline{\xi}_i, \underline{\xi}_j)| &\le 2N+L+\sum_{j\neq i} \frac{1}{L\sin^2\big(\pi(x_i-x_j)\big)} \\ &\le 2N+L+\sum_{j\neq i} \frac{1}{4L\|x_i-x_j\|^2} \\ &\le 2N+L+\frac{1}{4L}\sum_{n\ge 1} \frac{1}{(n\delta)^2} |\{j\colon \|x_i-x_j\| \in [n\delta, (n+1)\delta)\}| \\ &\le 2N+L+\frac{1}{4L\delta^2}\sum_{n\ge 1}\frac{2}{n^2} \\ &\le 2N+L+\frac{1}{L\delta^2}. \end{aligned}$$

Scegliendo $L := \lfloor \delta^{-1} \rfloor + 1$ si ottiene la (5.4.1). 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 $[M+1, M+N]$. □

Prima di passare alle applicazioni aritmetiche, facciamo due osservazioni a proposito della funzione $N + 2\delta^{-1}$ che compare a secondo membro nell'enunciato del Teorema 5.4.3. Per prima cosa, notiamo che per la disuguaglianza di Cauchy–Schwarz, se $R = 1$ si ha

$$\Big| \sum_{n=M+1}^{M+N} a_n \mathrm{e}(nx) \Big|^2 \leq \sum_{n=M+1}^{M+N} 1 \sum_{n=M+1}^{M+N} |a_n|^2 = N \sum_{n=M+1}^{M+N} |a_n|^2.$$

Inoltre, dato che $(x_i, x_i + \delta) \cap (x_j, x_j + \delta) = \emptyset$ se $i \neq j$, la quantità

$$\sum_{j=1}^{R} \delta |S(x_j)|^2$$

è una *somma di Cauchy* per la funzione $|S(x)|^2$ sull'intervallo $[0,1]$ e quindi

$$\delta \sum_{j=1}^{R} |S(x_j)|^2 \asymp \int_0^1 |S(x)|^2 \, \mathrm{d}x = \sum_{n=M+1}^{M+N} |a_n|^2.$$

Dunque la funzione $N + 2\delta^{-1}$ è pressoché ottimale.

Definizione 5.4.5 *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 $\omega(p) := |\Omega_p|$. Dato $\mathcal{A} \subseteq \mathbb{N}^*$ poniamo*

$$\mathcal{S}_0(\mathcal{A}; \mathfrak{P}) = \mathcal{S}_0(\mathcal{A}; \mathfrak{P}; \{\Omega_p\}) \stackrel{\text{def}}{=} \{a \in \mathcal{A} \colon a \bmod p \notin \Omega_p \, \forall p \in \mathfrak{P}\}.$$
$$\mathcal{S}(\mathcal{A}; \mathfrak{P}) = \mathcal{S}(\mathcal{A}; \mathfrak{P}; \{\Omega_p\}) \stackrel{\text{def}}{=} \big|\mathcal{S}_0(\mathcal{A}; \mathfrak{P}; \{\Omega_p\})\big|.$$

Definizione 5.4.6 *Dato $Q \geq 1$, l'insieme delle* frazioni di Farey *è definito da*

$$\mathcal{F} = \mathcal{F}(Q) \stackrel{\text{def}}{=} \Big\{ \frac{a}{q} \colon q \leq Q, \, 1 \leq a \leq q, \, (a,q) = 1 \Big\}.$$

Osservazione 5.4.7 *L'insieme $\mathcal{F}(Q)$ è Q^{-2}-ben spaziato; infatti, dati a_1/q_1 e $a_2/q_2 \in \mathcal{F}(Q)$, se essi sono distinti si ha*

$$\left| \frac{a_1}{q_1} - \frac{a_2}{q_2} \right| = \frac{|a_1 q_2 - a_2 q_1|}{q_1 q_2} \geq \frac{1}{q_1 q_2} \geq \frac{1}{Q^2}. \tag{5.4.2}$$

Teorema 5.4.8 *Dati M, $N \in \mathbb{N}^*$, un insieme non vuoto di numeri primi $\mathfrak{P}$, siano $\mathcal{A} := [M+1, M+N] \cap \mathbb{N}$ e $\mathcal{B} = \mathcal{B}(\mathfrak{P}) := \{n \in \mathbb{N}^* : p \mid n \Rightarrow p \in \mathfrak{P}\}$. 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 $\Omega_p := \emptyset$ per $p \notin \mathfrak{P}$, si può sempre supporre che $\mathfrak{P}$ sia l'insieme di tutti i numeri primi. Poniamo $a_n := 0$ se $n \notin \mathcal{S}_0(\mathcal{A}, \mathfrak{P})$ e

$$S(x) \stackrel{\text{def}}{=} \sum_{n=M+1}^{M+N} a_n \mathrm{e}(nx), \qquad J(q) \stackrel{\text{def}}{=} \prod_{p \mid q} \frac{\omega(p)}{p - \omega(p)}.$$

Si osservi che J è moltiplicativa. Per il Teorema 5.4.3 e per la (5.4.2) con $\delta = Q^{-2}$ è sufficiente dimostrare la disuguaglianza

$$\Big| \sum_{n=M+1}^{M+N} a_n \Big|^2 \mu^2(q) J(q) = |S(0)|^2 \mu^2(q) J(q) \le \sum_{a \bmod q}^{*} \Big| S\Big(\frac{a}{q}\Big) \Big|^2, \tag{5.4.3}$$

dove $\sum^*$ indica che la somma è fatta solo sugli elementi di $\mathbb{Z}_q^*$. Infatti la disuguaglianza cercata segue prendendo $a_n := 1$ per $n \in \mathcal{S}_0(\mathcal{A}, \mathfrak{P})$, e poi sommando su q, poiché in questo modo si ottiene

$$|S(0)|^2 L = \sum_{\substack{q \le Q \\ q \in \mathcal{B}}} |S(0)|^2 \mu^2(q) J(q) \le \sum_{\substack{q \le Q \\ q \in \mathcal{B}}} \sum_{a \bmod q}^{*} \Big| S\Big(\frac{a}{q}\Big) \Big|^2 \le (N + 2Q^2) |S(0)|.$$

Evidentemente è sufficiente dimostrare la (5.4.3) 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 $a_n \mathrm{e}(n\beta)$ si ottiene la disuguaglianza

$$|S(\beta)|^2 J(q) \le \sum_{a \bmod q}^{*} \Big| S\Big(\frac{a}{q} + \beta\Big) \Big|^2. \tag{5.4.4}$$

Supponiamo dunque di aver dimostrato la (5.4.3) 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 (5.4.4) si ha

$$\sum_{a \bmod q_1 q_2}^{*} \Big| S\Big(\frac{a}{q_1 q_2}\Big) \Big|^2 = \sum_{a_1 \bmod q_1}^{*} \sum_{a_2 \bmod q_2}^{*} \Big| S\Big(\frac{a_1}{q_1} + \frac{a_2}{q_2}\Big) \Big|^2$$

$$\geq J(q_2) \sum_{a_1 \bmod q_1}^{*} \left|S\Big(\frac{a_1}{q_1}\Big)\right|^2 \geq J(q_1)J(q_2)|S(0)|^2,$$

cioè la (5.4.3) 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

$$\begin{aligned}\sum_{a=1}^{p-1}\left|S\Big(\frac{a}{p}\Big)\right|^2 &= \sum_{a=1}^{p-1}\Big|\sum_{n=M+1}^{M+N} a_n \mathrm{e}\Big(\frac{a}{p}n\Big)\Big|^2 = \sum_{a=1}^{p-1}\sum_{n,m=M+1}^{M+N} a_n\overline{a}_m \mathrm{e}\Big(\frac{a}{p}(n-m)\Big)\\ &= \sum_{n,m=M+1}^{M+N} a_n\overline{a}_m \sum_{a=1}^{p-1}\mathrm{e}\Big(\frac{a}{p}(n-m)\Big)\\ &= p\sum_{a=1}^{p}|S(p,a)|^2 - |S(0)|^2. \qquad (5.4.5)\end{aligned}$$

D'altra parte, per la disuguaglianza di Cauchy, poiché $S(p,a) = 0$ se $a \in \Omega_p$,

$$|S(0)|^2 = \Big|\sum_{a=1}^{p} S(p,a)\Big|^2 \leq \big(p - \omega(p)\big)\sum_{a=1}^{p}|S(p,a)|^2,$$

e si ottiene quanto voluto dividendo per $p - \omega(p)$ e sostituendo nella (5.4.5). □

Riferimenti. Questo paragrafo è un adattamento del §3 di Bombieri [10]. Si vedano anche il §27 di Davenport [22], i Capp. 2–5 di Montgomery [100], il §4.10 di Halberstam & Roth [51], i Capp. 7, 8, 18, 19 di Huxley [71] e Montgomery [101].

5.5 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 Teorema di Landau 2.2.3 e la terza una maggiorazione per il numero dei primi gemelli.

𝔈 1-2

Lemma 5.5.1 *Se $k \in \mathbb{N}^*$ e $Q \geq 1$ allora*

$$\frac{k}{\phi(k)} \sum_{\substack{q \leq Q \\ (q,k)=1}} \frac{\mu^2(q)}{\phi(q)} > \log Q.$$

Dim. È sufficiente dimostrare che

$$\frac{k}{\phi(k)} \sum_{\substack{q\le Q\\(q,k)=1}} \frac{\mu^2(q)}{\phi(q)} \ge \sum_{n\le Q} \frac{1}{n} > \int_1^Q \frac{\mathrm{d}t}{t} = \log Q.$$

Per il Teorema 2.2.8 si ha

$$\frac{k}{\phi(k)} \sum_{\substack{q\le Q\\(q,k)=1}} \frac{\mu^2(q)}{\phi(q)} = \sum_{\substack{q\le Q\\(q,k)=1}} \frac{\mu^2(q)}{q} \prod_{p\mid q} \left(1+\frac{1}{p}+\frac{1}{p^2}+\dots\right) \times \prod_{p\mid k} \left(1+\frac{1}{p}+\frac{1}{p^2}+\dots\right).$$

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 2.3.1) 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 $(n_1,n_2)=(n_1,k)=1$; quindi n compare nella prima somma qui sopra quando $q=\ker(n_1)\le Q$ ed $m=nq^{-1}$. □

Teorema 5.5.2 (Brun-Titchmarsh) *Per ogni $q\in\mathbb{N}^*$, $a\in\mathbb{Z}$ con $(a,q)=1$, $M>1$, $N>3q$ si ha*

$$\pi(M+N;q,a)-\pi(M;q,a) = \sum_{\substack{p\in(M,M+N]\\ p\equiv a \bmod q}} 1 \le \frac{2N}{\phi(q)\log(N/q)} \left(1+O\left(\frac{\log\log(N/q)}{\log(N/q)}\right)\right),$$

dove la costante in $O(\cdot)$ è assoluta.

Dim. Possiamo evidentemente supporre che $1\le a\le q$. Prendiamo

$$\mathcal{A} \stackrel{\text{def}}{=} \left[\frac{M+1-a}{q}, \frac{M+N-a}{q}\right]\cap\mathbb{N},$$
$$\mathcal{P} \stackrel{\text{def}}{=} \{p\le Q\colon p\nmid q\},$$

$$\Omega_p \stackrel{\text{def}}{=} \{-aq^{-1} \bmod p\} \qquad \text{per } p \in \mathfrak{P},$$

da cui $|\mathcal{A}| \le 1 + N/q$. Dunque $\mathcal{B} \supseteq \{n \le Q\colon (n,q) = 1\}$ e $\omega(p) = 1$ per ogni $p \in \mathfrak{P}$. Se $r \equiv a \bmod q$ è un numero primo $> Q$ allora $p \nmid r$ per ogni primo $p \in \mathfrak{P}$; in altre parole $n := (r-a)/q \notin \Omega_p$ per ogni primo $p \in \mathfrak{P}$ e quindi $n \in \mathcal{S}_0(\mathcal{A}, \mathfrak{P})$, da cui

$$\pi(M+N;q,a) - \pi(M;q,a) \le \mathcal{S}(\mathcal{A},\mathfrak{P}) + Q. \tag{5.5.1}$$

Dal Teorema 5.4.8 deduciamo

$$\mathcal{S}(\mathcal{A},\mathfrak{P}) \le \frac{N/q + 1 + 2Q^2}{L}$$

dove

$$L \stackrel{\text{def}}{=} \sum_{n \in \mathcal{B} \cap [1,Q]} \mu^2(n) \prod_{p \mid n} \frac{1}{p-1} = \sum_{\substack{n \le Q \\ (n,q)=1}} \frac{\mu^2(n)}{\phi(n)}.$$

Per il Lemma 5.5.1 si ha $\dfrac{q}{\phi(q)} L > \log Q$ e la (5.5.1) dà

$$\pi(M+N;q,a) - \pi(M;q,a) \le \frac{N + q + 2qQ^2}{\phi(q)\log Q} + Q,$$

ed il risultato cercato segue prendendo $Q := (N/q)^{1/2} \big(\log(N/q)\big)^{-1}$. □

Teorema 5.5.3 *Poniamo* $\mathfrak{P}(x;q,a) := \{p \le x\colon p \equiv a \bmod q\}$. *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*

$$\prod_{p \in \mathfrak{P}(x;q,a)} \left(1 - \frac{1}{p}\right) = \frac{C(q,a)}{(\log x)^{1/\phi(q)}} \left(1 + O_{q,a}\left(\frac{1}{\log x}\right)\right).$$

Dim. Procediamo come nella dimostrazione del Teorema di Mertens 3.3.6, omettendo qualche dettaglio: per sommazione parziale dal Teorema 4.4.1 otteniamo

$$\sum_{\substack{p \le x \\ p \equiv a \bmod q}} \frac{1}{p} = \frac{1}{\phi(q)} \log\log x + C_1(q,a) + O\big((\log x)^{-1}\big).$$

Inoltre

$$\sum_{\substack{p \le x \\ p \equiv a \bmod q}} \log\left(1 - \frac{1}{p}\right) = -\sum_{\substack{p \le x \\ p \equiv a \bmod q}} \frac{1}{p} + \sum_{p \equiv a \bmod q} \left(\log\left(1 - \frac{1}{p}\right) + \frac{1}{p}\right) + O\left(\frac{1}{x}\right).$$

Il risultato desiderato segue ora passando all'esponenziale. □

Teorema 5.5.4 *Si ha*

$$|\{n \le N\colon r_2(n) > 0\}| \ll \frac{N}{(\log N)^{1/2}}.$$

Dim. Poniamo $r_2'(n) := |\{(a,b) \in \mathbb{Z}^2\colon a^2+b^2 = n \text{ e } (a,b)=1\}|$, 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 $\equiv 3 \bmod 4$ e $4 \nmid n$. Utilizziamo il Teorema 5.4.8 con $\mathcal{A} := [1,N] \cap \mathbb{N}$, $\mathfrak{P} := \{2\} \cup \mathfrak{P}(Q;4,3)$, ed $\Omega_p := \{0\}$ per ogni $p \in \mathfrak{P}$. Si ha quindi

$$|\{n \le N\colon (n,2)=1, r_2'(n) > 0\}| \le \frac{N+2Q^2}{L}$$

dove

$$L \stackrel{\text{def}}{=} \sum_{q \in \mathcal{B}(\mathfrak{P}) \cap [1,Q]} \frac{\mu^2(q)}{\phi(q)}.$$

Se poniamo $k = k(Q) := \prod p$, 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 5.5.1 otteniamo

$$L = \sum_{\substack{q \le Q \\ (q,k)=1}} \frac{\mu^2(q)}{\phi(q)} > \frac{\phi(k)}{k} \log Q = \log Q \prod_{\substack{p \le Q \\ p \equiv 1 \bmod 4}} \left(1 - \frac{1}{p}\right).$$

Per il Lemma 5.5.3 si ha $L \ge \big(C(4,1)+o(1)\big)\big(\log Q\big)^{1/2}$ e la scelta $Q := N^{1/2}$ ci dà quindi

$$|\{n \le N\colon (n,2)=1, r_2'(n) > 0\}| \ll \frac{N}{(\log N)^{1/2}}. \tag{5.5.2}$$

Infine osserviamo che

$$\big|\{n \le N\colon r_2(n) > 0\}\big| \le 2 \sum_{m \le N^{1/2}} \big|\big\{n \le Nm^{-2}\colon (n,2)=1, r_2'(n) > 0\big\}\big|.$$

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 (5.5.2). In definitiva

$$\big|\{n \le N\colon r_2(n) > 0\}\big| \ll \sum_{m \le N^{1/3}} \frac{N}{m^2\big(\log\big(Nm^{-2}\big)\big)^{1/2}} + \sum_{N^{1/3} < m \le N^{1/2}} \frac{N}{m^2}.$$

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 $\ll N \cdot N^{-1/3} \ll N^{2/3}$. La tesi segue immediatamente. □

Lemma 5.5.5 *Dato $h \in \mathbb{N}^*$, per $Q \to +\infty$ si ha*

$$\begin{aligned} D_h(Q) &\stackrel{\text{def}}{=} \sum_{\substack{q \le Q \\ (q,h)=1}} d(q) \\ &= \left\{ \frac{\phi(h)}{h} \right\}^2 Q \left(\log Q + 2\gamma - 1 + 2 \sum_{p \mid h} \frac{\log p}{p-1} \right) + O\Big(Q^{1/2} d(h) \Big). \end{aligned}$$

Dim. Per il Teorema 2.2.5 possiamo ovviamente supporre che $h > 1$ e che $\mu(h) \neq 0$ (cioè che $h = \ker(h)$). Poniamo $\mathcal{B} = \mathcal{B}(h) := \{n \in \mathbb{N}^* : \ \ker(n) \mid h\}$, e definiamo la funzione aritmetica d_h come segue: $d_h(n) = d(n)$ se $n \in \mathcal{B}$, e 0 altrimenti. Poiché ogni $q \ge 1$ può essere scritto in modo unico come rq', con $r \in \mathcal{B}$, $(h, q') = 1$, si ha evidentemente

$$D(Q) \stackrel{\text{def}}{=} D_1(Q) = \sum_{r \in \mathcal{B}} d(r) D_h\left(\frac{Q}{r} \right) = \sum_{r \ge 1} d_h(r) D_h\left(\frac{Q}{r} \right),$$

e quindi per la seconda formula di inversione di Möbius 2.1.12 ed il Teorema 2.2.5 si ha

$$\begin{aligned} D_h(Q) &= \sum_{r \ge 1} d_h^{-1}(r) D\left(\frac{Q}{r} \right) \\ &= \sum_{r \in \mathcal{B}} \mu * \mu(r) \left\{ \frac{Q}{r} \log \frac{Q}{r} + c \frac{Q}{r} + O\Big(Q^{1/2} r^{-1/2} \Big) \right\}, \end{aligned}$$

dove abbiamo scritto per brevità $c := 2\gamma - 1$; inoltre $d^{-1} = (N_0 * N_0)^{-1} = \mu * \mu$. Poiché $\mu * \mu\big(p^\alpha\big) = 0$ per ogni p, se $\alpha \ge 3$, gli unici addendi non nulli nelle somme che seguono sono quelli per cui $r \mid h^2$. Dunque per il Teorema 2.1.5 abbiamo

$$\sum_{r \in \mathcal{B}} \mu * \mu(r) \frac{1}{r} = \prod_{p \mid h} \left\{ 1 + \mu * \mu(p) \frac{1}{p} + \mu * \mu\big(p^2\big) \frac{1}{p^2} \right\} = \left\{ \frac{\phi(h)}{h} \right\}^2.$$

Inoltre si dimostra facilmente per induzione sul numero di fattori primi di h che

$$\sum_{r \mid h^2} \mu * \mu(r) \frac{\log r}{r} = -2 \left\{ \frac{\phi(h)}{h} \right\}^2 \sum_{p \mid h} \frac{\log p}{p-1}.$$

Infine, sempre per il Teorema 2.1.5

$$\sum_{r \mid h^2} \big| \mu * \mu(r) \big| r^{-1/2} = \prod_{p \mid h} \left(1 + \frac{1}{p^{1/2}} \right)^2 \le 8 d(h),$$

che conclude la dimostrazione. □

Teorema 5.5.6 *Sia $h \in \mathbb{N}^*$ un numero pari. Per $x \to +\infty$ si ha*

$$|\{p \le x\colon\ p+h \text{ è primo}\}| \ll_h \frac{x}{(\log x)^2}.$$

Dim. Prendiamo $\mathcal{A} := [1,x] \cap \mathbb{N}$, e per $p \le Q$ poniamo $\Omega_p := \{0,\ -h \bmod p\}$. Evidentemente $\omega(p) = 2$ se $p \nmid h$, $\omega(p) = 1$ se $p \mid h$. Quindi abbiamo

$$\begin{aligned} L &\overset{\text{def}}{=} \sum_{q\le Q} \mu(q)^2 \prod_{p\mid q} \frac{\omega(p)}{p-\omega(p)} = \sum_{q\le Q} \mu(q)^2 \prod_{p\mid q} \left\{ \frac{\omega(p)}{p} + \frac{\omega(p)^2}{p^2} + \cdots \right\} \\ &= \sum_{\substack{q\ge 1 \\ \ker(q)\le Q}} \frac{1}{q} \prod_{p^\alpha \| q} \omega(p)^\alpha \ge \sum_{\substack{q\le Q \\ (q,h)=1}} \frac{2^{\Omega(q)}}{q} \ge \sum_{\substack{q\le Q \\ (q,h)=1}} \frac{d(q)}{q}, \end{aligned}$$

dove $\Omega(q)$ è il numero totale dei fattori primi di q, poiché $d\big(p^\alpha\big) = \alpha+1 \le 2^\alpha$ e $2^\Omega \in \mathfrak{M}^*$. Per sommazione parziale dal Lemma 5.5.5 si ha infine $L \ge \frac{1}{2}\phi^2(h)h^{-2}(\log Q)^2 + O_h(\log Q)$, ed il Teorema segue prendendo $Q := x^{1/2}$. □

Con tecniche piú raffinate (quelle accennate nel Capitolo 6) è possibile dare una stima che fornisce la "giusta" dipendenza da h come nella (5.3.4).

Esercizi.

𝔈 1. Posto $\Omega_2 := \emptyset$, $\Omega_p := \{n \bmod p\colon \big(n \mid p\big) = -1\}$ per $p > 2$, dimostrare che $|\{n \le x\colon n = m^2\}| = O\big(x^{1/2}\big)$ per mezzo del Teorema 5.4.8.

𝔈 2. * Fissato $h \in \mathbb{N}^*$ e posto $\Omega_p := \{0\}$ se $p \mid h$, $\Omega_p := \emptyset$ altrimenti, dimostrare che $|\{n \le x\colon (n,h) = 1\}| \le \phi(h)x/h + 2h\phi(h)$. Se $\mu(h) \ne 0$, posto invece $\Omega_p := \mathbb{Z}_p \setminus \{0\}$ se $p \mid h$, $\Omega_p := \emptyset$ altrimenti, dimostrare che $|\{n \le x\colon h \mid n\}| \le x/h + 2h$. Suggerimento: per stimare L scegliere $Q = h$ ed usare il Lemma 2.1.5.

Riferimenti. La dimostrazione del Teorema di Brun–Titchmarsh 5.5.2 è adattata dal §3 di Bombieri [10].

5.6 Problemi aperti

Il Teorema di Dirichlet 4.4.1 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 4.4.2). 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 $\rho(p) < p$ 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 5.2.10 asserisce che

$$\begin{aligned}|\{n \le x\colon \big(f(n), P(z)\big) = 1\}| = x \prod_{p \le z} \left(1 - \frac{\rho(p)}{p}\right) \times \\ \times \Big(1 + O\big(\exp\big\{-u\big(\log u - \log_2 3u - \log \deg(f) - 2\big)\big\}\big) \\ + O_{\deg(f)}\Big(\exp\{-(\log x)^{1/2}\}\Big)\Big)\end{aligned}$$

purché $\rho(p) < p$ per ogni primo p (questo significa che f non ha divisori primi fissi; si noti che per il Lemma 5.2.3 $\rho(p) \le \deg(f)$ e quindi questa è una condizione che può essere verificata in un numero finito di passi) ed $u := \log x (\log z)^{-1} \ge 1$. Recentemente Friedlander & Iwaniec [38] hanno dimostrato che $a^2 + b^4$ assume valore primo il numero "atteso" di volte. Heath-Brown [63] ha dimostrato un risultato analogo per $a^3 + 2b^3$.

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 [54] hanno congetturato che

$$\pi_h(x) \sim \mathfrak{S}(h) \frac{x}{(\log x)^2}. \tag{5.6.1}$$

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 $n \ge 6$ 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 $p_1 \ne p_2$), Hardy & Littlewood [54] hanno congetturato che

$$r(n) \sim \mathfrak{S}(n) \frac{n}{(\log n)^2}. \tag{5.6.2}$$

Vinogradov [142] ha dimostrato nel 1937 che per n dispari sufficientemente grande l'equazione $n = p_1 + p_2 + p_3$ ha soluzione. Ramaré [127] ha dimostrato che l'equazione $n = p_1 + p_2 + \cdots + p_r$ ha soluzione per ogni $n > 1$ con $r \le 7$. Montgomery & Vaughan [104] hanno dimostrato che esiste $\delta > 0$ tale che

$$|\{n \le x\colon n \text{ è pari ed } r(n) = 0\}| \ll x^{1-\delta}.$$

[1]

[1] FIXME: Semplificare la dimostrazione del Teorema 5.4.8. Ottenere la costante giusta nel Teorema 5.5.6.

Capitolo 6

Introduzione alla Teoria Analitica dei Numeri

La Teoria Analitica dei Numeri nasce con la dimostrazione di Eulero del fatto che esistono infiniti numeri primi, che abbiamo riprodotto nel Teorema 3.2.1. Qui daremo solo qualche breve cenno ai risultati principali, senza alcuna pretesa di completezza anche nelle dimostrazioni. Supporremo qualche conoscenza della teoria delle funzioni olomorfe: si veda anche l'Appendice §A.2. Da qui in poi $s := \sigma + it$ è una variabile complessa con parte reale $\sigma = \Re(s)$ e parte immaginaria $t = \Im(s)$. Useremo le notazioni non standard $\mathcal{S}(\alpha)$ per indicare il semipiano $\{s \in \mathbb{C}\colon \Re(s) > \alpha\}$, $\mathcal{S}^-(\alpha)$ per il semipiano $\{s \in \mathbb{C}\colon \Re(s) < \alpha\}$, e $\mathcal{D}(R)$ per il disco chiuso di centro l'origine e raggio $R > 0$.

6.1 Il programma di Riemann

Riemann ha lasciato un solo, breve lavoro in Teoria dei Numeri [129] nel quale ha dimostrato, fra le altre cose, l'*equazione funzionale* per la funzione ζ che ne fornisce il prolungamento analitico a tutto il piano complesso privato del punto $s = 1$, e fatto molte affermazioni solo parzialmente giustificate: queste sono state tutte dimostrate nei successivi 40 anni circa. Quella che è nota come *Congettura di Riemann* 3.1.4 è stata enunciata semplicemente come "molto probabile," e questo fa ritenere che Riemann avesse dimostrazioni rigorose di tutte le altre affermazioni, e che non le abbia incluse nell'articolo citato sopra per brevità.

L'obiettivo indicato all'inizio del suo articolo era quello di dimostrare una *formula esplicita* che leghi la funzione π agli zeri della funzione zeta: daremo questa formula (6.7.3), senza dimostrazione, piú avanti. Oggi si preferisce ottenere una formula esplicita per la funzione ψ di Chebyshev, perché questa risulta piú semplice da utilizzare: è quello che faremo anche qui.

Vediamo ora gli ingredienti fondamentali della dimostrazione classica del Teorema dei Numeri Primi. Possiamo rissumerne i punti fondamentali come segue:

1. Dimostrazione dell'identità fondamentale, valida per $s \in \mathcal{S}(1)$,
$$\zeta(s) \stackrel{\text{def}}{=} \sum_{n\geq 1} \frac{1}{n^s} = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}$$
dove il prodotto è esteso a tutti e soli i numeri primi.
2. Equazione funzionale e prolungamento analitico della funzione ζ.
3. Espressione di ζ come *prodotto di Weierstrass* sugli zeri, e stima del numero degli zeri di ζ nella *striscia critica* $0 < \sigma < 1$.
4. Determinazione di una *regione libera da zeri*.
5. Espressione di $\psi(x)$ mediante un opportuno integrale complesso su un cammino illimitato contenuto nel semipiano $\mathcal{S}(1)$.
6. Deformazione del cammino di integrazione: connessione fra ψ e gli zeri della funzione ζ (la *formula esplicita*).

Queste sono le "tappe" che portano alla dimostrazione del Teorema dei Numeri Primi. Le parti piú complesse sono la dimostrazione dell'equazione funzionale, la formula esplicita e la determinazione della regione libera da zeri. Non daremo proprio tutti i dettagli, ma cercheremo di indicare almeno i punti fondamentali della dimostrazione di ciascuna parte del nostro programma.

Riferimenti. L'articolo originale di Riemann [129] è riprodotto, tradotto in inglese, nelle ultime pagine di Edwards [31], il cui primo capitolo è interamente dedicato ad un'analisi estremamente puntuale e dettagliata di tutti gli aspetti lasciati aperti o non sufficientemente spiegati da Riemann. Gli altri capitoli sono dedicati agli sviluppi successivi, in grandissima parte motivati dagli spunti presenti nell'articolo di Riemann. In nessuno degli altri libri interamente dedicati alla funzione ζ (Ivić [74], Titchmarsh [137]) si può trovare qualcosa di analogo.

6.2 L'equazione funzionale della funzione zeta

In questo paragrafo dimostreremo che la funzione ζ soddisfa un'equazione funzionale che permette di ricavare le sue caratteristiche nel sempiano $\mathcal{S}^-(\frac{1}{2})$ conoscendole nel semipiano $\mathcal{S}(\frac{1}{2})$. Dato che le caratteristiche piú importanti di ζ nel semipiano $\mathcal{S}(1)$ sono note, mediante la trasformazione $s \to 1-s$ possiamo ricavare le proprietà di ζ in $\mathcal{S}^-(0)$: si veda la Figura 6.2. Resta fuori da questo discorso

la striscia $0 \leq \sigma \leq 1$, che viene detta *striscia critica*. Vedremo oltre che per quello che riguarda la distribuzione dei numeri primi, ciò che conta è il numero e la posizione degli zeri della funzione ζ in questa regione.

Notiamo anche che la funzione zeta soddisfa la relazione $\zeta(\bar{s}) = \overline{\zeta(s)}$ (principio di riflessione) perché dalla definizione come serie di Dirichlet è chiaro che ζ è reale sull'asse reale. Questo comporta, in particolare, che eventuali zeri ρ non reali vengano a coppie ρ e $\bar{\rho}$.

Teorema 6.2.1 (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 $\mathcal{S}(1)$ e rappresentano la stessa funzione olomorfa, detta funzione ζ di Riemann. La funzione ζ ha un prolungamento meromorfo ad $\mathcal{S}(0)$, e nel punto $s = 1$ ha un polo semplice con residuo 1.

Dim. Sia K un compatto contenuto nel semipiano $\mathcal{S}(1)$: per la continuità dell'applicazione $s \mapsto \Re(s)$, esiste $s_0 \in K$ in cui questa assume valore minimo, ed evidentemente $\sigma_0 = \Re(s_0) > 1$. La convergenza totale della somma e del prodotto è una conseguenza immediata delle disuguaglianze

$$\left|\sum_{n\geq 1} \frac{1}{n^s}\right| \leq \sum_{n\geq 1} \left|\frac{1}{n^s}\right| = \sum_{n\geq 1} \frac{1}{n^\sigma} = \zeta(\sigma) \leq \zeta(\sigma_0).$$

La rappresentazione come prodotto di Eulero segue immediatamente dal Teorema 2.3.1, poiché $N_{-s} \in \mathfrak{M}^*$. Preso poi un numero reale $x > 1$, per la formula di sommazione parziale (A.1.3), nel semipiano $\mathcal{S}(1)$ 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,

$$\zeta(s) = \lim_{x\to+\infty} \sum_{n\leq x} \frac{1}{n^s} = \frac{s}{s-1} - s\int_1^{+\infty} \frac{\{t\}}{t^{s+1}}\,\mathrm{d}t. \tag{6.2.1}$$

Quest'ultima formula fornisce il prolungamento analitico di ζ al semipiano $\mathcal{S}(0)$, privato del punto $s = 1$, in quanto l'integrale è totalmente convergente in ogni compatto contenuto in $\mathcal{S}(0)$, ed è anche chiaro che ζ ha un polo semplice con residuo 1 in $s = 1$. □

Osserviamo che, ricordando la definizione della costante di Eulero data nella (A.4.1), si verifica immediatamente che

$$\lim_{s\to 1}\left(\zeta(s)-\frac{1}{s-1}\right)=1-\int_1^{+\infty}\frac{\{t\}}{t^2}\,\mathrm{d}t=\gamma. \tag{6.2.2}$$

L'esistenza di un prolungamento meromorfo al semipiano $\mathcal{S}(0)$ può essere dimostrata osservando che

$$(1-2^{1-s})\zeta(s)=\sum_{n\geq 1}\frac{1}{n^s}-2\sum_{n\geq 1}\frac{1}{(2n)^s}=\sum_{n\geq 1}\frac{1}{n^s}-2\sum_{\substack{n\geq 1\\ 2|n}}\frac{1}{n^s}=\sum_{n\geq 1}\frac{(-1)^{n+1}}{n^s}. \tag{6.2.3}$$

Quest'ultima serie converge nel semipiano dato: si proceda come nella dimostrazione del Teorema 4.2.6, osservando che la funzione periodica $f(n)=(-1)^{n+1}$ si comporta essenzialmente come un carattere di Dirichlet non principale, nel senso che la somma dei suoi valori su un intervallo di interi consecutivi è limitata. Quindi ζ è prolungabile: il vantaggio della relazione (6.2.3) sulla (6.2.1) sta forse nel non avere una funzione integrale meno naturale della serie di Dirichlet, ma, viceversa, la formula (6.2.1) esibisce direttamente il polo semplice. L'esistenza del polo semplice con residuo 1 può essere dedotta anche dalla (6.2.3) osservando che vicino ad $s=1$ si ha $1-2^{1-s}=(s-1)\log 2+o(|s-1|)$ mentre la serie all'estrema destra della (6.2.3), valutata in $s=1$, vale $\log 2$. In entrambi i casi, il prolungamento analitico dato è, parafrasando Riemann, una formula che vale per un insieme piú grande di valori di s piuttosto che una serie di potenze con raggio di convergenza piú grande.

Teorema 6.2.2 *Nel semipiano $\mathcal{S}(1)$ 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 nello stesso semipiano S.

Dim. La convergenza uniforme di serie e prodotto nel semipiano $\mathcal{S}(1)$ si dimostrano esattamente come sopra, dato che $|\mu(n)|\leq 1$ per ogni $n\in\mathbb{N}^*$. Inoltre è chiaro dal Teorema 6.2.1 che il prodotto vale $1/\zeta(s)$. □

Corollario 6.2.3 $\zeta(s)\neq 0$ *per tutti gli s nel semipiano $\mathcal{S}(1)$.*

Dim. La convergenza assoluta della serie $g(s):=\sum_n\mu(n)n^{-s}$ 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 $\mathcal{S}(1)$ comporterebbe un polo di $1/\zeta$. Ci si può anche basare sulla seconda dimostrazione del Teorema 2.3.1 con $f(n) = n^{-s}$: la (2.3.3) e la (2.3.4) con $x = 1 + \big(2/(\sigma-1)\big)^{1/(\sigma-1)}$ implicano

$$\left|\zeta(s)\prod_{p\le x}\left(1-\frac{1}{p^s}\right)-1\right| \le \sum_{n>x}\frac{1}{n^\sigma} \le \int_{x-1}^{+\infty}\frac{\mathrm{d}t}{t^\sigma} = \frac{1}{\sigma-1}(x-1)^{1-\sigma} < 1,$$

e questo dà una contraddizione se $\zeta(s) = 0$. □

Teorema 6.2.4 (Riemann) *La funzione ξ definita da*

$$\xi(s) \stackrel{\text{def}}{=} \frac{1}{2}s(s-1)\pi^{-s/2}\Gamma\left(\frac{1}{2}s\right)\zeta(s), \tag{6.2.4}$$

è olomorfa su $\mathbb{C}$, non ha zeri in $\mathcal{S}(1)\cup\mathcal{S}^-(0)$, e soddisfa l'equazione funzionale

$$\xi(s) = \xi(1-s). \tag{6.2.5}$$

La (6.2.5) fornisce dunque il prolungamento analitico di ζ a $\mathbb{C}\setminus\{1\}$.

Dim. Diamo una dimostrazione senza troppi dettagli: in $\mathcal{S}(1)$ e per $n \in \mathbb{N}^*$

$$\Gamma(s) = \int_0^{+\infty} t^{s-1}\mathrm{e}^{-t}\,\mathrm{d}t = n^s\int_0^{+\infty} x^{s-1}\mathrm{e}^{-nx}\,\mathrm{d}x$$

e quindi in $\mathcal{S}(1)$ si ha

$$\zeta(s)\Gamma(s) = \sum_{n\ge1}\Gamma(s)n^{-s} = \int_0^{+\infty}\frac{x^{s-1}}{\mathrm{e}^x-1}\,\mathrm{d}x. \tag{6.2.6}$$

Consideriamo l'integrale

$$I(s) \stackrel{\text{def}}{=} \frac{1}{2\pi\mathrm{i}}\int_\gamma \frac{z^{s-1}}{\mathrm{e}^{-z}-1}\,\mathrm{d}z \tag{6.2.7}$$

dove γ è il cammino nella Figura 6.1, nella quale è sottinteso che le semirette indicate con A e C giacciono entrambe sull'asse reale negativo, e che il raggio della circonferenza è $\rho < 2\pi$. Inoltre definiamo $z^s := \exp\big(s\log z\big)$ dove $|\arg(z)| \le \pi$. Si può far vedere che la (6.2.7) definisce una funzione analitica di s il cui valore è indipendente da ρ, e che per $\rho \to 0+$ l'integrale sulla circonferenza tende a 0; combinando i due integrali sulle semirette A e C mediante i cambiamenti di variabile $z := r\mathrm{e}^{-\pi\mathrm{i}}$, $z := r\mathrm{e}^{\pi\mathrm{i}}$ rispettivamente, si trova

$$\pi I(s) = \sin(\pi s)\Gamma(s)\zeta(s) \qquad \text{da cui} \qquad \zeta(s) = \Gamma(1-s)I(s). \tag{6.2.8}$$

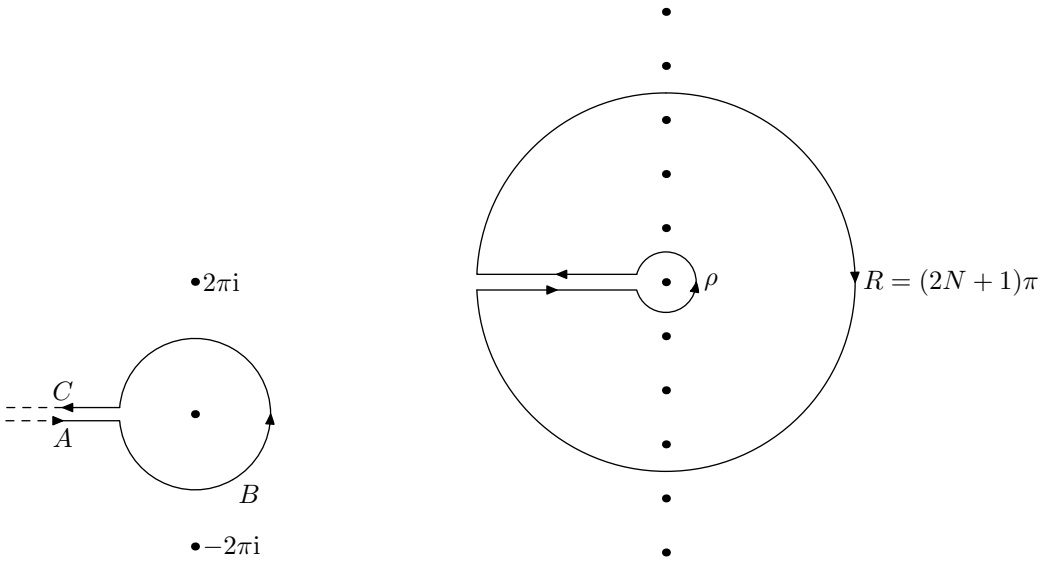


Figura 6.1: I cammini di integrazione nel Teorema 6.2.4.

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 in $\mathcal{S}^-(0)$. Consideriamo la funzione

$$I_N(s) \stackrel{\text{def}}{=} \frac{1}{2\pi\mathrm{i}} \int_{C(N)} \frac{z^{s-1}}{\mathrm{e}^{-z}-1}\,\mathrm{d}z$$

dove $C(N)$ è il cammino nella Figura 6.1, con convenzioni simili a quelle sopra, e la circonferenza esterna ha raggio $R = (2N+1)\pi$, con $N \in \mathbb{N}$. Si può dimostrare che per $N \to +\infty$ l'integrale sulla circonferenza esterna tende a 0; per il Teorema di Cauchy abbiamo dunque

$$\begin{aligned} I_N(s) &= \sum_{n=1}^{N} \left((2\pi\mathrm{i}n)^{s-1} + (-2\pi\mathrm{i}n)^{s-1} \right) \\ &= \sum_{n=1}^{N} (2n\pi)^{s-1} 2\cos\left(\frac{1}{2}\pi(s-1)\right) = 2(2\pi)^{s-1}\sin\left(\frac{1}{2}\pi s\right) \sum_{n=1}^{N} n^{s-1} \\ &\to 2(2\pi)^{s-1}\sin\left(\frac{1}{2}\pi s\right)\zeta(1-s) \end{aligned} \tag{6.2.9}$$

per $N \to +\infty$. Ma per $N \to +\infty$ si ha anche $I_N(s) \to I(s)$ e confrontando le due espressioni (6.2.8) e (6.2.9) si ottiene l'equazione funzionale nella forma asimmetrica

$$\zeta(s) = \frac{(2\pi)^s \sin\left(\frac{1}{2}\pi s\right)}{\sin(\pi s)\Gamma(s)}\zeta(1-s) = \frac{(2\pi)^s}{2\cos\left(\frac{1}{2}\pi s\right)\Gamma(s)}\zeta(1-s).$$

Per ottenere la forma dell'enunciato si usano le proprietà della funzione Γ: in particolare, sostituendo al posto di $\Gamma(s)$ il valore fornito dalla (A.2.5) si ottiene

$$\zeta(s) = \pi^{s+1/2} \frac{\Gamma\left(\frac{1}{2} - \frac{1}{2}s\right)}{\Gamma\left(\frac{1}{2}s\right)} \zeta(1-s)$$

dopo alcune semplificazioni, e da questa deduciamo

$$\zeta(s)\Gamma\left(\frac{1}{2}s\right)\pi^{-s/2} = \pi^{-s/2+1/2}\Gamma\left(\frac{1}{2} - \frac{1}{2}s\right)\zeta(1-s),$$

e l'equazione funzionale segue immediatamente moltiplicando per $\frac{1}{2}s(s-1)$. □

La Figura 6.2 illustra alcune conseguenze dell'equazione funzionale: il valore della funzione ζ in s può essere utilizzato per ottenere il valore in $1-s$. In particolare, se ρ è uno zero nella striscia critica, allora anche $1-\rho$ è uno zero, ed è nella striscia critica. Inoltre, a causa della relazione $\zeta(\overline{s}) = \overline{\zeta(s)}$, anche $\overline{\rho}$ è uno zero, e, di nuovo per l'equazione funzionale, c'è uno zero anche in $1-\overline{\rho}$.

Corollario 6.2.5 *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 $s = -2n$, con $n \in \mathbb{N}^*$. Nella striscia $0 < \sigma < 1$ ha gli stessi zeri di ξ, detti zeri non banali. Inoltre, dalle (6.2.6) e (6.2.8) 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* Ɛ 1 *di Bernoulli definiti nell'Appendice A.4. Dunque $\zeta(2n)\pi^{-2n} \in \mathbb{Q}$.*

Esercizi.

Ɛ 1. Dimostrare che per ogni $n \in \mathbb{N}^*$ si ha $\zeta(2n)\pi^{-2n} \in \mathbb{Q}^+$. In particolare, $\zeta(2) = \pi^2/6$, $\zeta(4) = \pi^4/90$ e $\zeta(6) = \pi^6/945$. 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.

Ɛ 2. Dimostrare che $\sum_{n \leq x} \log^2 n = x(\log^2 x - 2\log x + 2) + O\big((\log x)^2\big)$. Suggerimento: usare la formula di Euler-McLaurin A.1.2.

Ɛ 3. * (Ingham) Dimostrare che in $\mathcal{S}(1)$ 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 3.4.2. Usando anche alcuni degli esercizi precedenti, dimostrare che esistono costanti a, b, $c \in \mathbb{R}$ tali che in $\mathcal{S}(1)$ si ha $\zeta''(s) = a\zeta(s)^3 + b\zeta(s)^2 + c\zeta(s) + \sum_{n \geq 1} a_n n^{-s}$

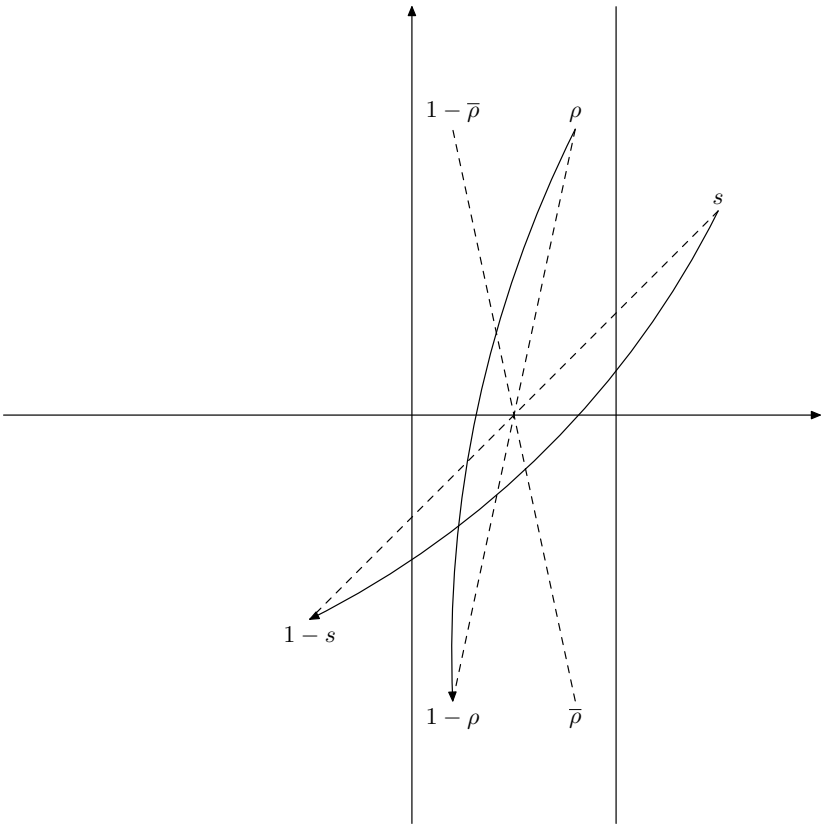


Figura 6.2: Conseguenze dell'equazione funzionale.

dove $\sum_{n\le x} a_n = O(x^{\alpha})$ per qualche $\alpha < 1$. Utilizzare tutti questi risultati per dimostrare le formule di Selberg del Teorema 3.4.2. In un certo senso, si può dire che la dimostrazione elementare data nel Capitolo 3 "corrisponde" a dimostrare queste relazioni senza usare l'analisi complessa.

Riferimenti. Teoria delle funzioni olomorfe: Ahlfors [2], Titchmarsh [138] oppure Whittaker & Watson [146]. Prolungamento analitico ed equazione funzionale: Davenport [22] Cap. 8, Ingham [73] §3.2 o Titchmarsh [137] Cap. 2, dove ne sono riportate ben sette dimostrazioni, oppure Titchmarsh [138] §§4.43–4.45. L'equazione funzionale è stata scoperta da Eulero: si vedano i §§2.2-2.3 di Hardy [52]. Prodotto infinito: Ingham [73] §3.8.

6.3 Distribuzione degli zeri della funzione zeta

Dato il polinomio $f(z) = a_n z^n + \cdots + a_0$ con $a_0 \neq 0$, $a_n \neq 0$, e con le radici λ_1, $\ldots$, λ_n ripetute ciascuna secondo la propria molteplicità, è un fatto elementare che

$f = g$ dove

$$g(z) = a_0\Big(1 - \frac{z}{\lambda_1}\Big)\cdots\Big(1 - \frac{z}{\lambda_n}\Big), \tag{6.3.1}$$

perché f e g sono polinomî dello stesso grado, con stesse radici e termine noto.

Se invece f è una funzione olomorfa qualsiasi, il prodotto corrispondente alla (6.3.1) potrebbe contenere infiniti fattori, e non è quindi detto che debba essere convergente, oppure potrebbe essere vuoto e dunque non avere nulla a che fare con f. Potremmo dire, approssimativamente, che la convergenza del prodotto dipende dalla "densità" degli zeri di f. Per una classe importante di funzioni (le cosiddette *funzioni intere di ordine finito*) gli zeri non possono essere troppo densi in un senso quantitativamente preciso che dipende dalla formula di Jensen (6.3.4), e quindi è possibile dimostrare il risultato che corrisponde alla fattorizzazione (6.3.1). Torneremo su questo argomento alla fine del paragrafo.

Teorema 6.3.1 (Prodotto infinito) *La funzione ξ ha un'infinità di zeri $\rho := \beta + i\gamma$ 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*

$$\xi(s) = e^{A+Bs}\prod_{\rho}\Big(1 - \frac{s}{\rho}\Big)e^{s/\rho} \stackrel{\text{def}}{=} e^{A+Bs}\lim_{T\to+\infty}\prod_{|\rho|<T}\Big(1 - \frac{s}{\rho}\Big)e^{s/\rho}, \tag{6.3.2}$$

dove il prodotto converge per tutti gli $s \in \mathbb{C}$, e ρ indica il generico zero non banale di ζ.

L'esistenza della fattorizzazione data nell'enunciato (il cosiddetto prodotto di Weierstrass sugli zeri) dipende dalla teoria generale delle funzioni intere di ordine finito, della quale ricordiamo brevemente qualche rudimento. Definiamo *ordine* della funzione intera f l'estremo inferiore dei numeri reali positivi μ tali che

$$f(z) = O_\mu\big(\exp\big(|z|^\mu\big)\big). \tag{6.3.3}$$

Chiamiamo $n(R)$ il numero degli zeri ρ della funzione olomorfa f, contati ciascuno con la rispettiva molteplicità, tali che $|\rho| \le R$. 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 $\mathcal{D}(R)$ con centro nell'origine e raggio $R > 0$.

Lemma 6.3.2 (Formula di Jensen) *Sia $f\colon \mathcal{D}(R) \to \mathbb{C}$ una funzione olomorfa tale che $f(0) \neq 0$ e priva di zeri su $\{|z| = R\} = \partial\mathcal{D}(R)$. Siano $0 < \rho_1 \le \rho_2 \le \cdots \le \rho_n$ i moduli degli zeri di f in questo cerchio, ripetuti secondo la rispettiva molteplicità. Si ha dunque*

$$\frac{1}{2\pi}\int_0^{2\pi}\log\left|\frac{f(Re^{i\theta})}{f(0)}\right|d\theta = \log\frac{R^n}{\rho_1\cdots\rho_n} = \int_0^R\frac{n(t)}{t}\,dt. \tag{6.3.4}$$

Non è difficile dare una dimostrazione di questo Lemma osservando che se vale separatamente per f e per g, è immediato che valga per $f \cdot g$ a causa dell'additività delle espressioni nella (6.3.4). Dunque è sufficiente dimostrare che vale per funzioni che non hanno zeri in $\mathcal{D}(R)$ e per funzioni del tipo $\phi(z) = z - \alpha$ con $0 < |\alpha| < R$. La prima parte è una conseguenza immediata della formula di Cauchy, poiché, se f è olomorfa e non nulla in $\mathcal{D}(R)$, allora anche $\log f$ è olomorfa nello stesso insieme. In questo caso, tutti i membri della (6.3.4) valgono 0. Per quanto riguarda la seconda parte, basta osservare che la funzione $g(z) = \phi(z)(R^2 - \overline{\alpha}z)/(R(z-\alpha))$ evidentemente è olomorfa e non nulla in $\mathcal{D}(R)$, e
ℭ 1 quindi si può usare la prima parte. Inoltre, $|g(z)| = |\phi(z)|$ su $|z| = R$. L'uguaglianza a destra nella (6.3.4) si dimostra osservando che lo zero ρ_k contribuisce positivamente all'integrale solo sull'intervallo $[\rho_k, R]$, e in questo intervallo fornisce una quantità $\log(R/\rho_k)$.

Sia $n(R)$ il numero di zeri che la funzione intera f ha all'interno del cerchio $\mathcal{D}(R)$, ed α l'ordine di f. Per R grande, il primo membro della formula di Jensen (6.3.4) è $O_\varepsilon(R^{\alpha+\varepsilon})$. Dato che $n(R)$ è monotona crescente, si ha

$$n(R) = n(R) \int_R^{eR} \frac{1}{t}\,dt \le \int_R^{eR} \frac{n(t)}{t}\,dt = O_\varepsilon\left(R^{\alpha+\varepsilon}\right),$$

e, in definitiva, che $n(R) = O_\varepsilon(R^{\alpha+\varepsilon})$. Da questo si deduce immediatamente che

$$\sum_\rho |\rho|^{-\alpha-\varepsilon} \tag{6.3.5}$$

converge, dove ρ indica il generico zero della funzione f, supponendo che $f(0) \neq 0$. Infatti, per la formula di sommazione parziale, si ha

$$\sum_{|\rho_n| \le R} \frac{1}{\rho_n^{\alpha+\varepsilon}} = \frac{n(R)}{R^{\alpha+\varepsilon}} + (\alpha+\varepsilon) \int_0^R \frac{n(t)}{t^{\alpha+\varepsilon+1}}\,dt.$$

Ma $n(t) = O_\varepsilon\left(t^{\alpha+\varepsilon/2}\right)$, e quindi quest'ultimo integrale è convergente.

Dimostrazione del Teorema 6.3.1. 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 (6.2.1), 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" in modulo solo in prossimità dell'asse reale.

Questo significa che la (6.3.3) 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 (6.3.5) diverge per $\varepsilon = 0$, e questo può accadere solo se ξ (e dunque ζ) ha infiniti zeri. L'equazione funzionale ed il Lemma 6.2.3 implicano che questi zeri sono

nella striscia $0 \leq \sigma \leq 1$. 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 parte immaginaria positiva minima è ≈ 14.13. □

In generale, sia f una funzione intera di ordine α: dalla (6.3.5) sappiamo che gli zeri di f non sono troppo densi, e da questo vogliamo dedurre che è possibile dare ad f una fattorizzazione simile a quella valida per i polinomî che abbiamo visto in (6.3.1). Come possiamo garantire che il

$$\lim_{T\to+\infty} \prod_{|\rho|<T} \left(1 - \frac{s}{\rho}\right)$$

esista finito? Una possibilità è quella di "correggere" ciascun fattore $1 - s/\rho$ mediante un opportuno esponenziale: piú precisamente, consideriamo la quantità

$$p_\rho(s) \stackrel{\text{def}}{=} \left(1 - \frac{s}{\rho}\right) \exp\left(\frac{s}{\rho} + \frac{s^2}{2\rho^2} + \cdots + \frac{s^n}{n\rho^n}\right),$$

dove n è un intero fissato che sceglieremo dopo. Si ha banalmente che

$$\log p_\rho(s) = -\sum_{m\geq 1} \frac{s^m}{m\rho^m} + \frac{s}{\rho} + \frac{s^2}{2\rho^2} + \cdots + \frac{s^n}{n\rho^n} = -\sum_{m>n} \frac{s^m}{m\rho^m} = O\left(\frac{|s|^{n+1}}{|\rho|^{n+1}}\right),$$

per la formula di Taylor con resto per la funzione $\log(1-z)$. Se scegliamo n in modo che $n+1 > \alpha$, la (6.3.5) garantisce che

$$\lim_{T\to+\infty} \sum_{|\rho|<T} \log p_\rho(s)$$

sia uniformemente convergente in ogni compatto fissato che non contiene nessuno degli zeri di f, e quindi che il *prodotto di Weierstrass* sugli zeri di f definito da

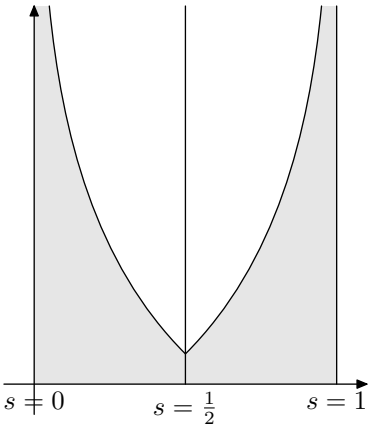
$$P_f(s) \stackrel{\text{def}}{=} \prod_\rho p_\rho(s)$$

sia a sua volta convergente ad una funzione olomorfa. Osserviamo che il prodotto potrebbe essere vuoto, se f non ha zeri, ma si può dimostrare che $g(s) := f(s)/P_f(s)$ è una funzione olomorfa priva di zeri, di ordine α, ed è relativamente facile dedurne che g è l'esponenziale di un polinomio di grado al piú α. Per i dettagli si veda Titchmarsh [138] §8.24.

Nel caso della funzione ξ abbiamo $\alpha = 1$, e quindi il fattore $e^{s/\rho}$ è sufficiente a garantire la convergenza del prodotto infinito.

Esercizi.

𝔈 1. Si completi la dimostrazione della formula di Jensen (6.3.4). Si dimostri che se $|z| = R$ allora $|(R^2 - \overline{\alpha}z)/(R(z-\alpha))| = 1$ moltiplicando per $\overline{z}/R$.



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 6.3: La regione libera da zeri.

6.4 La regione libera da zeri

La formula esplicita nella forma troncata del Teorema 6.5.3 ci darà la dipendenza del termine d'errore nel Teorema dei Numeri Primi dalla posizione e dal numero degli zeri di zeta. Come vedremo piú dettagliatamente nel prossimo paragrafo, per poter avere una buona stima per il termine d'errore è necessario che gli addendi della somma sugli zeri non siano individualmente troppo grandi. Se per un qualche zero $\rho = \beta + i\gamma$, la parte reale β fosse molto vicina ad 1, il suo contributo (sommato a quello del coniugato $\beta - i\gamma$) alla somma in questione sarebbe

$$-\frac{x^{\beta+i\gamma}}{\beta+i\gamma} - \frac{x^{\beta-i\gamma}}{\beta-i\gamma} = -\frac{x^{\beta}}{\beta^2+\gamma^2} \cdot \left((\beta - i\gamma)x^{i\gamma} + (\beta + i\gamma)x^{-i\gamma} \right). \tag{6.4.1}$$

Per quel che ne sappiamo, i due termini "oscillanti" $x^{i\gamma}$ ed il suo coniugato potrebbero talvolta "coalizzarsi" e far sí che il termine in (6.4.1) sia cosí grande da cancellare in parte il termine x nella formula esplicita che vorremmo essere il termine dominante. In altre parole, la quantità in (6.4.1) potrebbe essere frequentemente cosí grande da far sí che

$$\liminf_{x\to+\infty} \frac{\psi(x)}{x} < 1 \qquad \limsup_{x\to+\infty} \frac{\psi(x)}{x} > 1.$$

In effetti, dimostreremo che eventuali zeri con β molto vicino ad 1, sempre ammesso che esistano, hanno γ molto grande, e, in definitiva, il contributo di ciascuno zero non è tale da influenzare il termine principale della formula esplicita.

Lemma 6.4.1 *In $\mathcal{S}(1)$ valgono le identità*

$$\log\zeta(s) = -\sum_p \log\left(1 - \frac{1}{p^s}\right) = \sum_p \sum_{m\geq 1} \frac{1}{mp^{ms}} \qquad e \qquad -\frac{\zeta'}{\zeta}(s) = \sum_{n\geq 1} \frac{\Lambda(n)}{n^s}.$$

Dim. La prima relazione segue dall'identità nell'enunciato del Teorema di Eulero–Riemann 6.2.1 e dalla formula di Taylor per $\log(1-x)$. Derivando membro a membro la seconda uguaglianza si trova

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

come si voleva. □

Lemma 6.4.2 *Esiste un numero complesso C tale che*

$$-\frac{\zeta'}{\zeta}(s) = \frac{1}{s-1} + C + \frac{1}{2}\frac{\Gamma'}{\Gamma}\left(\frac{1}{2}s+1\right) - \sum_\rho \left(\frac{1}{s-\rho}+\frac{1}{\rho}\right)$$

per tutti gli s complessi diversi da zeri o poli di ζ.

Dim. Osserviamo che una forma equivalente della definizione della funzione ξ è $\xi(s) = (s-1)\pi^{-s/2}\Gamma\left(\frac{1}{2}s+1\right)\zeta(s)$. Da questa deduciamo immediatamente che

$$\frac{\mathrm{d}}{\mathrm{d}s}\log\xi(s) = \frac{1}{s-1} - \frac{1}{2}\log\pi + \frac{1}{2}\frac{\Gamma'}{\Gamma}\left(\frac{1}{2}s+1\right) + \frac{\zeta'}{\zeta}(s).$$

D'altra parte, dal Teorema 6.3.1 deduciamo

$$\frac{\mathrm{d}}{\mathrm{d}s}\log\xi(s) = B + \sum_\rho \left(\frac{1}{s-\rho}+\frac{1}{\rho}\right),$$

e la tesi segue immediatamente. □

Teorema 6.4.3 *Esiste una costante $c \in \mathbb{R}^+$ tale che per ogni zero non banale di zeta $\rho = \beta + i\gamma$ si ha*

$$\beta < 1 - \frac{c}{\log|\gamma|}.$$

Dim. Partiamo da un'osservazione di Mertens: per ogni $\theta \in \mathbb{R}$ si ha

$$2(1+\cos\theta)^2 = 3 + 4\cos\theta + \cos(2\theta) \geq 0. \tag{6.4.2}$$

Inoltre, nella regione $\mathcal{S}(1)$, per il Lemma 6.4.1 si ha

$$\Re\log\zeta(\sigma+it) = \sum_p \sum_{m\geq 1} \frac{\cos\left(t\log p^m\right)}{mp^{m\sigma}}.$$

Usiamo quest'ultima formula con $s=\sigma$, $s=\sigma+it$ ed $s=\sigma+2it$, ottenendo

$$3\log\zeta(\sigma)+4\Re\log\zeta(\sigma+it)+\Re\log\zeta(\sigma+2it)\geq 0,$$

da cui, passando all'esponenziale,

$$\zeta^3(\sigma)\left|\zeta^4(\sigma+it)\zeta(\sigma+2it)\right|\geq 1. \tag{6.4.3}$$

Poiché per $\sigma\to 1+$ si ha che $\zeta(\sigma)\sim(\sigma-1)^{-1}$ e che $\zeta(\sigma+2it)$ resta limitata, se $1+it$ fosse uno zero di ζ il primo membro della (6.4.3) sarebbe infinitesimo, una contraddizione.

Questo ragionamento può essere esteso per dare il risultato dell'enunciato, ma conviene considerare ζ'/ζ invece di $\log\zeta$ per evitare problemi di prolungamento analitico. Prendiamo la regione $S=\{s\in\mathbb{C}\colon 1\leq\sigma\leq 2,\ t\geq 2\}$: per il Lemma 6.4.1 abbiamo

$$-\Re\frac{\zeta'}{\zeta}(s)=\sum_{n\geq 1}\frac{\Lambda(n)}{n^\sigma}\cos(t\log n).$$

La relazione (6.4.2) dunque implica per $s=\sigma+it\in S$

$$-3\frac{\zeta'}{\zeta}(\sigma)+4\left(-\Re\frac{\zeta'}{\zeta}(\sigma+it)\right)+\left(-\Re\frac{\zeta'}{\zeta}(\sigma+2it)\right)\geq 0. \tag{6.4.4}$$

Da qui in poi, A_j indicheranno opportune costanti positive. Per quanto riguarda il primo addendo, il polo semplice di ζ in $s=1$ implica che nella regione S si ha

$$-\frac{\zeta'}{\zeta}(\sigma)=\frac{1}{\sigma-1}+O(1)\qquad\text{e quindi}\qquad -\frac{\zeta'}{\zeta}(\sigma)<\frac{1}{\sigma-1}+A_1.$$

Consideriamo ora il Lemma 6.4.2: i primi tre termini in valore assoluto sono maggiorati da $A_2\log t$. Inoltre, un rapido calcolo mostra che nella stessa regione si ha $\Re\left(\rho^{-1}+(s-\rho)^{-1}\right)>0$ per ogni zero non banale. Scegliamo dunque uno di questi zeri $\rho_0=\beta_0+i\gamma_0$ e $t=\gamma_0$: in definitiva abbiamo le disuguaglianze

$$-\Re\frac{\zeta'}{\zeta}(\sigma+i|\gamma_0|)<A_3\log|\gamma_0|-\frac{1}{\sigma-\beta_0},\qquad -\Re\frac{\zeta'}{\zeta}(\sigma+2i|\gamma_0|)<A_4\log|\gamma_0|.$$

Sostituendo nella (6.4.4) ricaviamo, per un $A>0$ opportuno, la disuguaglianza

$$\frac{4}{\sigma-\beta_0}<\frac{3}{\sigma-1}+A\log|\gamma_0|,$$

e scegliendo infine $\sigma=1+(2A\log|\gamma_0|)^{-1}$ si ottiene la tesi con $c=(14A)^{-1}$. □

Il prossimo risultato è un corollario del Lemma 6.4.2.

Lemma 6.4.4 *Per τ sufficientemente grande, se sul segmento $-1 \leq \sigma \leq 2$, $t = \tau$ non vi sono zeri della funzione ζ, allora si ha*

$$\frac{\zeta'}{\zeta}(\sigma + i\tau) = \sum_{\substack{\rho \\ |\tau - \gamma| < 1}} \frac{1}{\sigma + i\tau - \rho} + O(\log \tau).$$

Inoltre, il numero di addendi nella somma è $O(\log \tau)$.

Teorema 6.4.5 (Riemann-von Mangoldt) *Per $T \to +\infty$ si ha*

$$\begin{aligned} N(T) &\stackrel{\text{def}}{=} \left|\{\rho = \beta + i\gamma \colon \zeta(\rho) = 0, \beta \in [0,1], \gamma \in [0,T]\}\right| \\ &= \frac{T}{2\pi} \log \frac{T}{2\pi} - \frac{T}{2\pi} + O(\log T). \end{aligned}$$

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 $s_1 = 2$, $s_2 = 2 + iT$, $s_3 = -1 + iT$, $s_4 = -1$. Dato che ξ è reale e non nulla sul segmento $[-1,2]$ non c'è variazione dell'argomento. Inoltre, per l'equazione funzionale 6.2.4, 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 $s_5 = \frac{1}{2} + iT$. Esaminiamo separatamente i fattori che compaiono nella Definizione (6.2.4) di ξ, che scriviamo come $\xi(s) = (s-1)\pi^{-s/2}\Gamma\left(\frac{1}{2}s + 1\right)\zeta(s)$. Per la formula di Stirling generalizzata (A.2.2) per la funzione Γ di Eulero abbiamo

$$\begin{aligned} \Delta_{L(T)} \arg(s-1) &= \frac{1}{2}\pi + O\left(T^{-1}\right), \\ \Delta_{L(T)} \arg \pi^{-s/2} &= -\frac{1}{2} T \log \pi, \\ \Delta_{L(T)} \arg \Gamma\left(\frac{1}{2}s + 1\right) &= \frac{1}{2} T \log \frac{1}{2} T - \frac{1}{2} T + \frac{3}{8}\pi + O\left(T^{-1}\right). \end{aligned}$$

Per ottenere la tesi resta da dimostrare che $\Delta_{L(T)} \arg \zeta(s) = O(\log T)$. Dato che ζ è reale e positiva in $s = 2$ e non nulla in $\mathcal{S}(1)$, la variazione dell'argomento

sul tratto verticale è limitata. Ricordiamo che per una funzione olomorfa f la variazione dell'argomento di f tra i punti $\frac{1}{2}+\mathrm{i}T$ e $2+\mathrm{i}T$ è data da

$$\Delta\arg(f)=\Delta(\Im(\log(f)))=\int_{1/2}^{2}\Im\Big(\frac{f'}{f}(\sigma+\mathrm{i}T)\Big)\,\mathrm{d}\sigma. \tag{6.4.5}$$

Dobbiamo dunque trovare una stima per $\Im\big(\zeta'(s)/\zeta(s)\big)$ sul segmento di estremi $\frac{1}{2}+\mathrm{i}T$ e $2+\mathrm{i}T$. Il Lemma 6.4.4 implica che

$$\begin{aligned}\Delta_{L(T)}\arg\zeta(s)&=-\int_{1/2}^{2}\Im\Big(\frac{\zeta'}{\zeta}(\sigma+\mathrm{i}T)\Big)\,\mathrm{d}\sigma+O(1)\\&=-\sum_{\substack{\rho\\|T-\gamma|<1}}\int_{1/2}^{2}\Im\Big(\frac{1}{\sigma+\mathrm{i}T-\rho}\Big)\,\mathrm{d}\sigma+O(\log T)\\&=-\sum_{\substack{\rho\\|T-\gamma|<1}}\Delta_{L(T)}\arg(\sigma+\mathrm{i}T-\rho)+O(\log T).\end{aligned}$$

La dimostrazione si conclude, poiché per la (6.4.5) si ha $\Delta_{L(T)}\arg(\sigma+\mathrm{i}T-\rho)\le\pi$ per ciascuno degli zeri nell'ultima somma, e, sempre per il Lemma 6.4.4, la somma in questione ha $O(\log T)$ addendi. □

Riferimenti. Teorema 6.4.3: Davenport [22] Cap. 13, Ingham [73] §3.9 o Titchmarsh [137], §6.19. Teorema 6.4.5: Davenport [22] Cap. 15, Ingham [73] §4.2.

6.5 La formula esplicita: legame fra psi e zeta

Ora vedremo come ci sia una stretta relazione fra la funzione ψ e la *derivata logaritmica* della funzione ζ, e cioè ζ'/ζ, esprimendo ψ in termini di un integrale improprio sulla retta dei numeri complessi di parte reale $c>1$ fissata, come si vede dalla relazione (6.5.1). Una volta trovata questa relazione integrale, che può essere invertita come mostra la (6.7.1), vorremo deformare il cammino di integrazione come indicato nella Figura 6.4 per poter prendere il contributo del polo semplice di ordine 1 che ζ'/ζ ha in $s=1$. Naturalmente dovremo tenere conto di eventuali altri zeri che la funzione ζ possa avere all'interno del cammino deformato, perché anche questi daranno un contributo all'integrale in questione, e dovremo anche scegliere opportunamente il cammino in modo da evitare questi zeri. Per il Teorema di Cauchy, l'integrale originario (6.5.1) e quello sul cammino deformato differiscono per il valore del residuo della funzione integranda ai poli, moltiplicato per $2\pi\mathrm{i}$: sappiamo già che ζ ha un polo semplice con residuo 1 in $s=1$ (e quindi anche $-\zeta'/\zeta$ ha un polo semplice con residuo 1 nello stesso punto). Dunque, il contributo della funzione integranda nel punto $s=1$ vale x, e questo è

il termine principale atteso per $\psi(x)$. La funzione integranda ha un polo semplice in $s=0$, con residuo $-\zeta'(0)/\zeta(0)$, ed ha poli in tutti gli zeri di zeta nella porzione di striscia critica di parte immaginaria compresa fra $-T$ e T. Se per semplicità supponiamo che questi zeri siano semplici, vediamo subito che il contributo di ciascuno di questi vale $-x^\rho/\rho$. Inoltre vi sono i poli negli *zeri banali* $s=-2$, $s=-4$, …, $s=-2N$. Non resta quindi che valutare il contributo dei due tratti orizzontali e del tratto verticale sulla retta $\sigma=-2N-1$.

A questo punto vogliamo portare a termine il programma esposto all'inizio del paragrafo precedente: una volta ottenuta la relazione del Lemma 6.5.1, deformiamo il cammino di integrazione in modo da "sostituire" il tratto della retta $\sigma=c$ per cui $t\in[-T,T]$ con una spezzata costituita dal segmento di estremi $c-\mathrm{i}T$ e $-2N-1-\mathrm{i}T$, dal segmento di estremi $-2N-1-\mathrm{i}T$ e $-2N-1+\mathrm{i}T$ e dal segmento di estremi $-2N-1+\mathrm{i}T$ e $c+\mathrm{i}T$. Il tratto verticale non passa per nessuno zero della funzione ζ, poiché questa nel semipiano $\sigma<0$ si annulla solo in $s=-2$, -4, -6, …, mentre i tratti orizzontali devono evitare gli eventuali zeri di ζ nella striscia critica. Abbiamo dimostrato che ζ ha infiniti zeri in questa striscia (il Teorema di Riemann–von Mangoldt 6.4.5), ma ovviamente, essendo meromorfa, ne ha un numero finito in ogni insieme limitato, e quindi, a meno di modificare T di una quantità limitata, è certamente possibile scegliere il cammino richiesto.

Lemma 6.5.1 (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 6.5.2 (Riemann–von Mangoldt) *Per $x>1$ vale la* formula esplicita*:*

$$\psi_0(x)=x-\sum_\rho\frac{x^\rho}{\rho}-\frac{\zeta'(0)}{\zeta(0)}-\frac{1}{2}\log\bigl(1-x^{-2}\bigr),$$

dove la somma deve essere intesa in senso simmetrico (i termini provenienti da ρ e da $\overline{\rho}$ devono essere presi insieme), e $\psi_0(x)$ è la media dei valori di ψ a destra ed a sinistra di x,

$$\psi_0(x)\stackrel{\text{def}}{=}\lim_{\varepsilon\to0+}\frac{1}{2}\bigl(\psi(x+\varepsilon)+\psi(x-\varepsilon)\bigr).$$

Dim. È un'applicazione (non banale) della formula di Perron: infatti per $c > 1$ si ha

$$\psi_0(x) = \frac{1}{2\pi i}\int_{(c)} -\frac{\zeta'}{\zeta}(s)\frac{x^s}{s}\,ds. \tag{6.5.1}$$

Il risultato si ottiene modificando in modo opportuno il cammino di integrazione come descritto all'inizio del paragrafo. Per portare a termine la dimostrazione sono necessarie informazioni su $|\zeta'/\zeta(s)|$ sui tratti orizzontali e su quello verticale a sinistra nella Figura 6.4, che qui omettiamo per brevità. □

Utilizzando una forma troncata della formula di Perron, possiamo ottenere la seguente forma approssimata della formula esplicita, piú utile nelle applicazioni: in sostanza la dimostrazione è analoga a quella del Teorema 6.5.2, ma non si fa tendere T a $+\infty$.

Teorema 6.5.3 (Formula esplicita troncata) *Per $x > 1$ intero e $T > 1$ si ha*

$$\psi(x) = x - \sum_{|\gamma|\le T}\frac{x^\rho}{\rho} + O\Big(\frac{x}{T}\big(\log xT\big)^2\Big). \tag{6.5.2}$$

Si noti che questa formula suggerisce che una condizione necessaria e sufficiente per avere $\psi(x) \sim x$ sia $\beta = \Re(\rho) < 1$ per ogni zero $\rho = \beta + i\gamma$ di ζ.

Riferimenti. Formula di Perron 6.5.1: Davenport [22], Cap. 17, Ingham [73], §4.5 o Titchmarsh [137], Lemma 3.12. Formula esplicita 6.5.3: Davenport [22], Cap. 17 o Ingham [73], §4.6.

6.6 Dimostrazione del Teorema dei Numeri Primi

Riassumiamo brevemente la strategia seguita per dimostrare il Teorema dei Numeri Primi nella forma 3.1.3: utilizzando l'equazione funzionale e le proprietà della funzione Γ di Eulero si ottiene una rappresentazione di $-\zeta'/\zeta$ che dà la formula esplicita 6.5.3 nella forma approssimata, per mezzo della formula di Perron. Poi, utilizziamo la regione libera da zeri del Teorema 6.4.3 per stimare il contributo degli zeri non banali alla formula esplicita, e quindi per ottenere il resto dato dal Teorema 3.1.3.

Dalla formula esplicita del Teorema 6.5.3 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 $\rho = \beta + i\gamma$ per il generico zero non banale di zeta. Si ricordi che gli zeri sono disposti simmetricamente rispetto all'asse

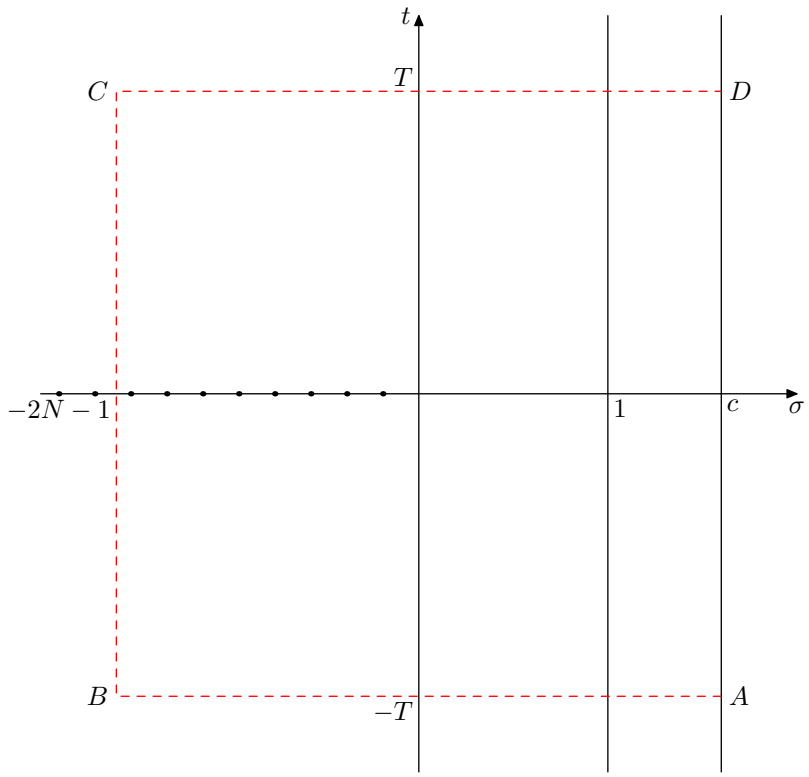


Figura 6.4: Il cammino di integrazione che si usa per dimostrare la forma troncata della fomula esplicita. I tratti orizzontali del cammino deformato devono evitare gli zeri di ζ in $0 < \sigma < 1$, mentre il tratto verticale deve evitare gli zeri banali $s = -2n$, indicati sull'asse reale negativo, e quindi è possibile scegliere un segmento della retta $\sigma = -2N - 1$. In un secondo tempo si fa tendere N a $+\infty$.

reale. Il massimo può essere stimato usando la regione libera da zeri fornita dal Teorema 6.4.3, mentre per la somma utilizziamo la stima per il numero degli zeri della funzione zeta con parte immaginaria $|\gamma| \leq T$ data dal Teorema 6.4.5, con la sommazione parziale nella forma piú generale. In definitiva, possiamo scrivere

$$\psi(x) - x \ll x(\log T)^2 \exp\left\{-c\frac{\log x}{\log T}\right\} + \frac{x}{T}\big(\log xT\big)^2. \tag{6.6.1}$$

Ora scegliamo T come funzione di x in modo che

$$\frac{1}{T} \approx \exp\left\{-c\frac{\log x}{\log T}\right\}$$

per far pesare allo stesso modo i due termini a destra nella (6.6.1). Prendiamo dunque $(\log T)^2 = \log x$: sostituendo e semplificando si trova infine

$$\psi(x) - x \ll x\exp\{-c_1(\log x)^{1/2}\}, \tag{6.6.2}$$

dove c_1 è un'opportuna costante positiva. Per ottenere il risultato che riguarda $\pi(x)$, conviene ricordare che per il Lemma 3.2.4 si ha $\theta(x) = \psi(x) + O\big(x^{1/2}\big)$. Per sommazione parziale ed integrazione per parti, si ottiene

$$\pi(x) = \mathrm{li}(x) + O\Big(x\exp\{-c''(\log x)^{1/2}\}\Big),$$

che è molto piú forte del risultato ottenuto nel Capitolo 3.

Riferimenti. Dimostrazione del Teorema dei Numeri Primi: Davenport [22], Cap. 18. Per un'accurata descrizione delle relazioni fra la dimostrazione elementare e quella analitica, si veda la recensione di Ingham [72] degli articoli originali di Selberg e di Erdős. Si vedano anche i Capp. 1–4 di Hardy [53] 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 [64]. Un'altra dimostrazione analitica si trova in Wiener [147] §17, o in Rudin [132] §§9.8–9.12. Gerig [41] 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 $\mathcal{S}(1)$. Una semplice dimostrazione analitica si trova in Newman [112]. Per la dimostrazione corrispondente del Teorema 4.4.2, si veda Elstrodt [34]. Si veda anche Ingham [73] Cap. 2.

6.7 La congettura di Riemann

Teorema 6.7.1 *Sia* $\Theta := \sup\{\beta\colon \rho = \beta + i\gamma \text{ è uno zero di } \zeta\}$. *La congettura di Riemann* 3.1.4 *è equivalente a* $\Theta = \frac{1}{2}$.

Dim. Posto $R(x) := \psi(x) - x$, con la formula di sommazione parziale si trova la rappresentazione

$$-\frac{\zeta'}{\zeta}(s) = s\int_1^{+\infty} \frac{\psi(x)}{x^{s+1}}\,\mathrm{d}s = \frac{s}{s-1} + s\int_1^{+\infty} \frac{R(x)}{x^{s+1}}\,\mathrm{d}s, \tag{6.7.1}$$

inizialmente in $\mathcal{S}(1)$. Ma se $R(x) \ll x^{1/2}(\log x)^2$, l'ultimo integrale è uniformemente convergente in $\sigma \geq \frac{1}{2} + \delta$ per ogni $\delta > 0$, e quindi il secondo membro definisce una funzione analitica in $\mathcal{S}(\frac{1}{2})$ privato del punto $s = 1$. Per prolungamento analitico, l'unica singolarità della funzione a primo membro in $\mathcal{S}(\frac{1}{2})$ 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 (6.5.1) e (6.7.1) rappresentano una coppia trasformata e 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 π:

$$\log\zeta(s) = s\int_1^{+\infty} \frac{\Pi(t)}{t^{s+1}}\,\mathrm{d}t \qquad \Pi_0(x) = \frac{1}{2\pi\mathrm{i}}\int_{(c)} \log\zeta(s)\frac{x^s}{s}\,\mathrm{d}s \tag{6.7.2}$$

dove

$$\Pi(x) \stackrel{\text{def}}{=} \pi(x) + \frac{1}{2}\pi\big(x^{1/2}\big) + \frac{1}{3}\pi\big(x^{1/3}\big) + \cdots$$

e Π_0 è la regolarizzata di Π definita come ψ_0 a partire da ψ (cfr l'enunciato del Teorema 6.5.2). 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.

La *formula esplicita* originale di Riemann è la seguente:

$$\Pi_0(x) = \mathrm{li}(x) - \sum_{\substack{\rho=\beta+\mathrm{i}\gamma\\ \gamma>0}} \big(\mathrm{li}(x^\rho) + \mathrm{li}(x^{1-\rho})\big) + \int_x^{+\infty} \frac{\mathrm{d}t}{(t^2-1)t\log t} + \log\xi(0). \tag{6.7.3}$$

La dimostrazione di Riemann è piuttosto diversa da quella che abbiamo dato qui per ψ: si tratta in sostanza di utilizzare la formula a destra nella (6.7.2), ricavando ζ dalla definizione di ξ (6.2.4) e di utilizzare una forma del prodotto di Weierstrass per ξ (6.3.2). Non si può integrare termine a termine perché gli integrali risultanti sono divergenti: Riemann dunque integra per parti una volta la (6.7.2) e poi sostituisce. Il termine $\mathrm{li}(x)$ proviene da $\log(s-1)$ mentre i termini che contengono gli zeri provengono dai logaritmi dei relativi fattori nel prodotto di Weierstrass. La parte piú difficile della dimostrazione è la giustificazione della possibilità di scambiare la somma (infinita) sugli zeri di zeta con l'integrazione impropria in (6.7.2). La formula esplicita per π si ottiene da questa usando la Seconda Formula di Inversione di Möbius 2.1.12.

Riferimenti. Congettura di Riemann 3.1.4 e sue conseguenze: Davenport [22] Cap. 18, Ingham [73] §§4.8–4.9, Titchmarsh [137] Cap. 14, oppure Conrey [17]. Per una vasta panoramica su analoghe congetture in situazioni diverse si veda Bombieri [11]. Dimostrazione della formula esplicita di Riemann: Edwards [31], Cap. 1. Risultati aggiornati relativi al calcolo numerico degli zeri di ζ si trovano all'indirizzo `http://numbers.computation.free.fr/Constants/Miscellaneous/zetazeroscompute.html`

6.8 Una famosa affermazione di Eulero

Eulero affermò che

$$\sum_{n\geq 1}\frac{\mu(n)}{n}=0. \tag{6.8.1}$$

La dimostrazione, formalmente, consiste nell'usare il Teorema 6.2.2 anche per $s=1$, e quindi nel dire che il primo membro della (6.8.1) vale $1/\zeta(1)=0$. Dato che la serie in questione non è assolutamente convergente, questa argomentazione suggerisce la validità della relazione (6.8.1) senza dimostrarla. La nostra dimostrazione necessita di una versione piú accurata della Prima formula di Mertens (3.3.1) per la quale ci serve la forma precisa del termine di resto nel Teorema dei Numeri Primi 3.1.3. Per semplicità, per $c\in\mathbb{R}^+$ poniamo $\varepsilon_c(x)=\exp\bigl(-c\sqrt{\log x}\bigr)$.

Teorema 6.8.1 *Esiste un numero reale C tale che per $x\to+\infty$ si ha*

$$S(x)\stackrel{\text{def}}{=}\sum_{n\leq x}\frac{\Lambda(n)}{n}=\log x+C+R_1(x), \tag{6.8.2}$$

con $R_1(x)=O\bigl(\varepsilon_{c_1}(x)\sqrt{\log x}\bigr)$, dove c_1 è la costante nella (6.6.2).

Dim. Sia $R(x):=\psi(x)-x$. Procedendo come nella dimostrazione del Teorema 3.3.4, si ricava che la (6.8.2) vale con un'opportuna costante C ed

$$R_1(x)=\frac{R(x)}{x}-\int_x^{+\infty}\frac{R(t)}{t^2}\,\mathrm{d}t\ll\varepsilon_{c_1}(x)+\int_x^{+\infty}\frac{\varepsilon_{c_1}(t)}{t}\,\mathrm{d}t.$$

Il primo termine può essere assorbito nell'errore. Eseguiamo il cambiamento di variabile $u=(\log t)^{1/2}$, e poniamo $X=(\log x)^{1/2}$. Abbiamo dunque

$$\int_x^{+\infty}\frac{\varepsilon_{c_1}(t)}{t}\,\mathrm{d}t=2\int_X^{+\infty}u\mathrm{e}^{-c_1u}\,\mathrm{d}u=\Bigl[-\frac{2}{c_1^2}(c_1u+1)\mathrm{e}^{-c_1u}\Bigr]_X^{+\infty}\ll\varepsilon_{c_1}(x)\sqrt{\log x},$$

come si voleva. □

Avremo anche bisogno di una relazione che coinvolge la funzione S definita nella formula (6.8.2). Per ogni $x\geq 1$ si ha

$$\sum_{n\leq x}\frac{\mu(n)}{n}\Bigl(S\Bigl(\frac{x}{n}\Bigr)+\log n\Bigr)=0. \tag{6.8.3}$$

Per la dimostrazione, basta osservare che il Teorema 2.1.13 con $f=\mu\cdot N_{-1}$, $g=\Lambda\cdot N_{-1}$ ed $y=1$, ed il Corollario 2.2.10, implicano che

$$\sum_{n\leq x}\frac{\mu(n)}{n}S\Bigl(\frac{x}{n}\Bigr)=\sum_{n\leq x}\frac{1}{n}(\mu*\Lambda)(n)=-\sum_{n\leq x}\frac{1}{n}(\mu\cdot L)(n),$$

come si voleva. Dalla relazione (6.8.3) si ricava che per x abbastanza grande si ha

$$\sum_{n\le x}\frac{\mu(n)}{n}=-\frac{1}{\log x+C}\sum_{n\le x}\frac{\mu(n)}{n}R_1\Big(\frac{x}{n}\Big)\ll(\log x)^{-1}\sum_{n\le x}\frac{1}{n}\varepsilon_{c_1}\Big(\frac{x}{n}\Big)\sqrt{\log\frac{x}{n}},$$

dove R_1 è definito nella (6.8.2). Dimostreremo che la somma all'estrema destra qui sopra è limitata, e questo è sufficiente a completare la dimostrazione della formula di Eulero (6.8.1), con in piú un'indicazione della velocità di convergenza a 0. Per ottenere questo risultato, osserviamo che vale la disuguaglianza banale

$$\sum_{n\in[x,y]}\frac{1}{n}\le\frac{1}{x}+\int_x^y\frac{\mathrm{d}t}{t}=\frac{1}{x}+\log\frac{y}{x}.$$

Suddividiamo l'intervallo di somma per n in intervalli $I_k=[X_k,X_{k+1}]$ dove $X_k=x\exp(-k^2)$, sui quali la funzione $\varepsilon_{c_1}(x/n)$ è sostanzialmente costante:

$$\begin{aligned}\sum_{n\le x}\frac{1}{n}\varepsilon_{c_1}\Big(\frac{x}{n}\Big)\sqrt{\log\frac{x}{n}}&\le\sum_{k\ge0}\sum_{\substack{n\ge1\\n\in I_k}}\frac{1}{n}\varepsilon_{c_1}\Big(\frac{x}{n}\Big)\sqrt{\log\frac{x}{n}}\le\sum_{k\ge0}\varepsilon_{c_1}\big(\mathrm{e}^{k^2}\big)(k+1)\sum_{\substack{n\ge1\\n\in I_k}}\frac{1}{n}\\&\le\sum_{k\ge0}\mathrm{e}^{-c_1k}(k+1)\Big(1+\log\frac{x}{\exp(k^2)}-\log\frac{x}{\exp((k+1)^2)}\Big)\\&\le\sum_{k\ge0}\mathrm{e}^{-c_1k}(k+1)(1+2k+1),\end{aligned}$$

che è evidentemente una quantità limitata. Si noti che per dimostrare la tesi sarebbe sufficiente avere $R(x)=O\big(x(\log x)^{-2-\varepsilon}\big)$ in modo che $R_1(x)=O\big((\log x)^{-1-\varepsilon}\big)$.

Concludiamo questo paragrafo osservando che è possibile determinare il valore della costante C nel Teorema 6.8.1: infatti, lo stesso ragionamento che porta all'uguaglianza (6.5.1) implica che

$$\sum_{n\le x}\frac{\Lambda(n)}{n}=\frac{1}{2\pi\mathrm{i}}\int_{(c)}-\frac{\zeta'}{\zeta}(s+1)\frac{x^s}{s}\,\mathrm{d}s,$$

se $x>1$ non è intero. La funzione integranda è regolare in $\mathcal{S}(0)$, ed ha un polo doppio in $s=0$, con residuo $\log x-\gamma$. Infatti, dal Teorema 6.2.1 e dalla (6.2.2) sappiamo che $\zeta(s+1)=s^{-1}+\gamma+O(|s|)$ in un intorno di $s=0$, da cui deduciamo (usando l'analiticità) $\zeta'(s+1)=-s^{-2}+O(1)$, e quindi

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

mentre $x^s=1+s\log x+O\big(|s|^2\big)$. Ripetendo, *mutatis mutandis*, la dimostrazione dei Teorema dei Numeri Primi, si dimostra che i termini provenienti dagli altri poli della funzione integranda contribuiscono quantità infinitesime (quando $x\to+\infty$), e quindi la costante C vale $-\gamma$. In sostanza, l'analoga della somma sugli zeri nella formula esplicita troncata contiene termini del tipo $x^{\rho-1}\rho^{-1}$.

6.9 Considerazioni finali

6.9.1 Ancora sul Teorema di Dirichlet

Vogliamo motivare brevemente la dimostrazione del Teorema di Dirichlet data nel Capitolo 4, ed in particolare il fatto che l'obiettivo principale della dimostrazione è $L(s,\chi)\neq 0$ per ogni carattere non principale χ. La dimostrazione di Eulero del fatto che esistono infiniti numeri primi può essere riscritta cosí: per il Lemma 6.4.1, in $\mathcal{S}(1)$ si ha

$$\log\zeta(s)=\sum_{m\geq 1}\sum_{p}\frac{1}{mp^{ms}}=\sum_{p}\frac{1}{p^s}+\sum_{m\geq 2}\sum_{p}\frac{1}{mp^{ms}}=f(s)+O(1),$$

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. Analogamente,

$$\log L(s,\chi)=f(s,\chi)+O_q(1),\qquad \text{dove}\qquad f(s,\chi)\stackrel{\text{def}}{=}\sum_{p}\frac{\chi(p)}{p^s}.$$

Inoltre $L(s,\chi_0)=\zeta(s)\prod_{p|q}(1-p^{-s})$ e quindi $f(s,\chi_0)=f(s)+O_q(1)$. Per ortogonalità

$$\sum_{p\equiv a \bmod q}\frac{1}{p^s}=\frac{1}{\phi(q)}\sum_{\chi \bmod q}\overline{\chi}(a)\log L(s,\chi)+O_q(1). \tag{6.9.1}$$

Quindi, se $L(1,\chi)\neq 0$ per $\chi\neq\chi_0$, allora $\log L(s,\chi)$ è una funzione limitata in un intorno di $s=1$, ed il Teorema di Dirichlet segue dalla (6.9.1).

6.9.2 Distribuzione degli zeri e termine d'errore

Si può dimostrare che il Teorema dei Numeri Primi nella forma che abbiamo dimostrato nel Capitolo 3 (cioè la relazione $\pi(x)\sim x(\log x)^{-1}$) è equivalente all'affermazione $\zeta(1+it)\neq 0$ 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 [9] ha studiato la relazione fra una forma generalizzata delle formule di Selberg (3.4.2) ed il termine d'errore nel Teorema dei Numeri Primi che si può ottenere elementarmente. Pintz [115] 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

$$M(x)\stackrel{\text{def}}{=}\max\{|\pi(t)-\operatorname{li}(t)|:\ t\in[2,x]\}.$$

In effetti, si ha che

$$\log\frac{x}{M(x)}\sim\min_{\rho=\beta+i\gamma}\{(1-\beta)\log x+\log|\gamma|\},$$

quando $x \to +\infty$. Per esempio, se $\pi(x) = \mathrm{li}(x) + O\big(x\exp(-(\log x)^b)\big)$ 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 $\rho = \beta + i\gamma$ 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 $R(x) \ll x\exp\big(-c'(\log x)^{1/(\theta+1)}\big)$ per il termine d'errore si può dimostrare scegliendo $(\log T)^{\theta+1} = \log x$ nella (6.6.1).

Un calcolo molto semplice mostra che se $\pi(x) = \mathrm{li}(x) + O\big(x^\Theta\big)$, 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 $\rho_0 = \beta_0 + i\gamma_0$ 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 $\beta_0 \leq \Theta$.

Riferimenti. Davenport [22] Capp. 1 e 4.

6.10 The Zeta Function Song

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 Cramér,
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

André 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 6.4.5.

2. Sia $N_0(T) := \left|\{\rho = \frac{1}{2} + i\gamma\colon\ \zeta(\rho) = 0,\ \gamma \in [0,T]\}\right|$ 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 6.7.1.

4. Per $\sigma \in \mathbb{R}$ si ponga $\mu(\sigma) = \inf\{\alpha \in \mathbb{R}\colon\ |\zeta(\sigma + it)| \ll |t|^\alpha \text{ per } |t| \to +\infty\}$. La teoria generale delle serie di Dirichlet implica che μ è convessa, e la (6.2.1) 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 6.5.3.

6. 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.

6.11 Problemi aperti

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 §6.7, si abbia $\Theta<1$. Questo risultato sarebbe probabilmente il piú importante degli ultimi 150 anni. Una congettura piú debole di quella di Riemann, ma che avrebbe importanti conseguenze per le applicazioni, è l'Ipotesi di Densità: posto

$$N(\sigma,T)\stackrel{\text{def}}{=}\big|\{\rho=\beta+i\gamma\colon\ \zeta(\rho)=0,\beta\geq\sigma,|\gamma|\leq T\}\big|,$$

si congettura che $N(\sigma,T)\ll T^{2(1-\sigma)+\varepsilon}$ uniformemente per $\frac{1}{2}\leq\sigma\leq 1$. Bourgain [12] ha 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 (3.8.2) 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.

Capitolo 7

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 (5.6.1) e (5.6.2), nonché le argomentazioni che conducono alla (5.3.4) ed al Teorema 5.5.6.

7.1 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 $\mathbb{N}$, $\mathcal{A}_1, \ldots, \mathcal{A}_s$, non necessariamente distinti, dove $s \in \mathbb{N}$ è almeno 2. Il problema consiste nel determinare il numero di soluzioni dell'equazione

$$n = a_1 + a_2 + \cdots + a_s \tag{7.1.1}$$

dove $n \in \mathbb{N}$ è dato, e $a_j \in \mathcal{A}_j$ per $j = 1, \ldots, s$, 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 (7.1.1) ha soluzione per ogni $n \in \mathbb{N}$, oppure il minimo s per cui l'equazione (7.1.1) 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 (7.1.1) abbia una soluzione.

Il metodo per affrontare i problemi additivi che vedremo ha la sua origine in un articolo del 1918 di Hardy & Ramanujan [56] sulle partizioni, ma dato il numero di problemi affrontati e risolti in questo modo da Hardy & Littlewood

[54], [55] 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 studiare il numero delle "rappresentazioni" di n nella forma $a_1 + a_2$ con $a_j \in \mathcal{A}$, $j = 1$, 2, poiché, presumibilmente, questo numero è grande e ci aspettiamo che sia piú facile determinarne una minorazione. Poniamo quindi

$$r_2(n) \stackrel{\text{def}}{=} \big|\{(a_1, a_2) \in \mathcal{A} \times \mathcal{A} \colon n = a_1 + a_2\}\big|,$$

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 $r_s(n) := \big|\{(a_1, \dots, a_s) \in \mathcal{A}^s \colon n = a_1 + \cdots + a_s\}\big|$. Per il Teorema di Cauchy, per $\rho < 1$ si ha quindi

$$r_2(n) = \frac{1}{2\pi \mathrm{i}} \oint_{\gamma(\rho)} \frac{f^2(z)}{z^{n+1}} \, \mathrm{d}z, \tag{7.1.2}$$

dove $\gamma(\rho)$ 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 (7.1.2) 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 $r_k(n) := \big|\{(a_1, \dots, a_k) \in \mathbb{N}^k \colon n = a_1 + \cdots + a_k\}\big|$. Naturalmente è possibile dimostrare direttamente che $r_k(n) = \binom{n+k-1}{k-1}$. In questo caso $\mathcal{A} = \mathbb{N}$ e dunque $f(z) = \sum_{n=0}^{+\infty} z^n = (1-z)^{-1}$. Quindi, per $\rho < 1$,

$$r_k(n) = \frac{1}{2\pi \mathrm{i}} \oint_{\gamma(\rho)} \frac{\mathrm{d}z}{(1-z)^k z^{n+1}}. \tag{7.1.3}$$

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 (7.1.3): infatti, poiché $\rho < 1$, 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 (7.1.3) e scambiare l'integrale con la serie:

$$\begin{aligned} r_k(n) &= \frac{1}{2\pi i} \sum_{m=0}^{+\infty} \binom{-k}{m}(-1)^m \oint_{\gamma(\rho)} z^{m-n-1}\,dz \\ &= \frac{1}{2\pi i} \sum_{m=0}^{+\infty} (-1)^m \binom{-k}{m} \begin{cases} 2\pi i & \text{se } m = n, \\ 0 & \text{altrimenti,} \end{cases} = (-1)^n \binom{-k}{n}, \end{aligned}$$

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 $\gamma(\rho)$ a parte un piccolo arco vicino al punto $z = \rho$, il quale dà il contributo principale all'integrale nella (7.1.3).

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 $g(z) = \sum_{m=0}^{+\infty} z^{2m+1} = z/(1-z^2)$, 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 $m \le n$: dunque si può introdurre la funzione

$$f_N(z) \stackrel{\text{def}}{=} \sum_{m=0}^{N} z^m = \frac{1-z^{N+1}}{1-z} \tag{7.1.4}$$

(l'ultima uguaglianza è valida per $z \neq 1$). Per $n \leq N$, il Teorema di Cauchy dà

$$r_k(n) = \frac{1}{2\pi \mathrm{i}} \oint_{\gamma(1)} \frac{f_N^k(z)}{z^{n+1}} \, \mathrm{d}z. \tag{7.1.5}$$

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 $\mathrm{e}(x) := \mathrm{e}^{2\pi \mathrm{i} x}$ e facciamo il cambiamento di variabile $z = \mathrm{e}(\alpha)$ nella (7.1.5):

$$r_k(n) = \int_0^1 f_N^k\big(\mathrm{e}(\alpha)\big) \, \mathrm{e}(-n\alpha) \, \mathrm{d}\alpha. \tag{7.1.6}$$

Questa è anche la formula che dà l'n-esimo coefficiente di Fourier della funzione $f_N^k\big(\mathrm{e}(\alpha)\big)$, per l'ortogonalità della funzione esponenziale complessa. Per futura comodità poniamo $T_N(\alpha) = T(\alpha) := f_N\big(\mathrm{e}(\alpha)\big)$; per la (7.1.4) si ha quindi

$$\begin{aligned} T_N(\alpha) &\stackrel{\text{def}}{=} \sum_{m=0}^{N} \mathrm{e}(m\alpha) \\ &= \begin{cases} \dfrac{1-\mathrm{e}\big((N+1)\alpha\big)}{1-\mathrm{e}(\alpha)} = \mathrm{e}\big(\tfrac{1}{2}N\alpha\big) \dfrac{\sin(\pi(N+1)\alpha)}{\sin(\pi\alpha)} & \text{se } \alpha \notin \mathbb{Z}; \\ N+1 & \text{se } \alpha \in \mathbb{Z}. \end{cases} \end{aligned} \tag{7.1.7}$$

Si veda la Figura 7.2 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 (7.1.7) si ricava facilmente che

$$|T_N(\alpha)| \leq \min\left(N+1, \frac{1}{|\sin(\pi\alpha)|}\right) \leq \min\big(N+1, \|\alpha\|^{-1}\big) \tag{7.1.8}$$

poiché T è periodica di periodo 1 ed inoltre $\alpha \leq \sin(\pi\alpha)$ per $\alpha \in \big(0, \frac{1}{2}\big]$. 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 (7.1.6): infatti, se $\delta \geq 1/N$ e $k \geq 2$ abbiamo

$$\left| \int_\delta^{1-\delta} T_N^k(\alpha) \mathrm{e}(-n\alpha) \, \mathrm{d}\alpha \right| \leq \int_\delta^{1-\delta} |T_N^k(\alpha)| \, \mathrm{d}\alpha \leq \int_\delta^{1-\delta} \frac{\mathrm{d}\alpha}{\|\alpha\|^k} \leq \frac{2}{k-1} \delta^{1-k} \tag{7.1.9}$$

e questo è $o\big(N^{k-1}\big)$ 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 (7.1.6) 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 (7.1.6) ed (7.1.9) si ha

$$\begin{aligned} r_2(N) &= \int_0^1 \Big(\frac{\sin\big(\pi(N+1)\alpha\big)}{\sin(\pi\alpha)}\Big)^2 \mathrm{d}\alpha \\ &= 2\int_0^\delta \Big(\frac{\sin\big(\pi(N+1)\alpha\big)}{\sin(\pi\alpha)}\Big)^2 \mathrm{d}\alpha + o(N), \end{aligned} \tag{7.1.10}$$

perché la funzione integranda è periodica di periodo 1 (se ne veda la definizione). Suddividiamo l'intervallo $[0,\delta]$ negli intervalli $I_h := [\delta_h, \delta_{h+1}]$, per $h = 0, \ldots,$ dove abbiamo posto $\delta_h := h/(N+1)$. Stimando l'integrale su 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 (7.1.10) vale $N + o(N)$.

Riferimenti. Il riferimento classico per il metodo del cerchio è la monografia di Vaughan [141]: in particolare, per quanto riguarda questo paragrafo si veda il Cap. 1. Si vedano anche Hardy [53] Cap. 8 (in particolare i §§8.1–8.7) e James [76] §5. La genesi dell'idea di studiare il comportamento della funzione generatrice in prossimità di diverse singolarità è esposta molto chiaramente in Hardy & Ramanujan [56] (in particolare i §§1.2–1.5) ed in Hardy [53] Cap. 8 (in particolare i §§8.6–8.7). Per il problema di Waring si vedano Hardy & Wright [57] Capp. 20–21 per un'introduzione, e Vaughan [141] per uno studio piú approfondito). Per la relazione fra serie di Laurent e serie di Fourier vedi Titchmarsh [138] §13.12. Si veda anche il survey di Kumchev & Tolev [80].

7.2 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, $\ldots$, indicano sempre numeri primi. Ci interessa il numero di rappresentazioni di n come somma di due primi

$$r_2(n) \stackrel{\text{def}}{=} \big|\{(p_1,p_2) \in \mathfrak{P}\times\mathfrak{P} : n = p_1 + p_2\}\big|,$$

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 $p_1 \neq p_2$. Per il momento non facciamo l'ipotesi che n sia pari. Prendiamo un intero grande N e poniamo

$$V(\alpha) = V_N(\alpha) \stackrel{\text{def}}{=} \sum_{p\le N} \mathrm{e}(p\alpha).$$

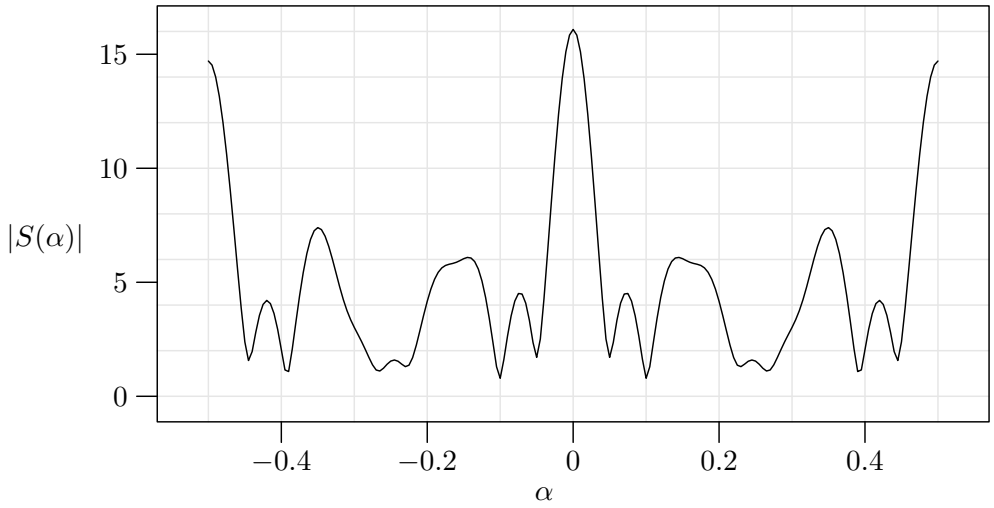


Figura 7.1: Il grafico della funzione $|S_{20}(\alpha)|$ nel quale si notano molto bene i picchi in prossimità dei valori razionali di $\alpha = 0, \frac{1}{2}, \frac{1}{3}, \frac{2}{3}, \frac{1}{6}, \frac{5}{6}$, mentre in $\alpha = \frac{1}{4}, \frac{3}{4}$ non c'è picco poiché $\mu(4) = 0$.

Per l'ortogonalità della funzione esponenziale complessa, per $n \le N$ si ha

$$\int_0^1 V(\alpha)^2 \mathrm{e}(-n\alpha)\,\mathrm{d}\alpha = \sum_{p_1\le N}\sum_{p_2\le N}\int_0^1 \mathrm{e}\big((p_1+p_2-n)\alpha\big)\,\mathrm{d}\alpha = r_2(n). \qquad (7.2.1)$$

Di nuovo, questa è la formula che dà l'n-esimo coefficiente di Fourier della funzione $V(\alpha)^2$ (cfr la (7.1.6)), 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 $x \mapsto \mathrm{e}^{2\pi i x}$) in sotto-intervalli centrati approssimativamente sui numeri razionali con denominatore $q \le Q$, dove $Q = Q(N)$ è un parametro: questa si chiama dissezione di Farey di ordine Q (vedi la Definizione 5.4.6). Gli intervalli corrispondenti ai numeri razionali con denominatore $q \le P$ (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 [54, 55] 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 7.1). Sfruttando il contributo di questi picchi, e trascurando i termini d'errore, Hardy & Littlewood ritrovarono le formule asintotiche espresse nelle Congetture (5.6.1) e (5.6.2).

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

$$S(\alpha) = S_N(\alpha) \stackrel{\text{def}}{=} \sum_{p\le N} \log p\, \mathrm{e}(p\alpha) \qquad \text{e} \qquad \theta(N;q,a) \stackrel{\text{def}}{=} \sum_{\substack{p\le N\\ p\equiv a \bmod q}} \log p.$$

Per il Teorema dei Numeri Primi nelle progressioni aritmetiche 4.4.2 si ha

$$\theta(N;q,a) = \frac{N}{\phi(q)} + E_1(N;q,a)$$

dove

$$E_1(N;q,a) = O_A\Big(N\exp\{-C(A)\sqrt{\log N}\}\Big),$$

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 (7.2.1), per $n \le N$ si ha

$$R_2(n) = \int_0^1 S(\alpha)^2 \mathrm{e}(-n\alpha)\,\mathrm{d}\alpha. \tag{7.2.2}$$

Calcoliamo S su un razionale a/q, quando $1 \le a \le q$ ed $(a,q)=1$:

$$\begin{aligned} S\left(\frac{a}{q}\right) &= \sum_{h=1}^{q} \sum_{\substack{p\le N\\ p\equiv h \bmod q}} \log p\, \mathrm{e}\big(p\tfrac{a}{q}\big) = \sum_{h=1}^{q} \mathrm{e}\big(h\tfrac{a}{q}\big) \sum_{\substack{p\le N\\ p\equiv h \bmod q}} \log p \\ &= \sum_{h=1}^{q} \mathrm{e}\big(h\tfrac{a}{q}\big)\theta(N;q,h) = \sum_{h=1}^{q}{}^{*} \mathrm{e}\big(h\tfrac{a}{q}\big)\theta(N;q,h) + O(\log q), \end{aligned} \tag{7.2.3}$$

dove * significa che alla somma abbiamo aggiunto la condizione supplementare $(h,q)=1$. Nel penultimo passaggio abbiamo ripartito i numeri primi nelle classi $h \bmod q$, e poi abbiamo sfruttato il fatto che le progressioni relative ad un h con $(h,q)>1$ contengono al piú un numero primo, che risulta essere un fattore primo di q. Per il Teorema 2.2.11 e per la (7.2.3) abbiamo dunque

$$S\left(\frac{a}{q}\right) = \frac{N}{\phi(q)} \sum_{h=1}^{q}{}^{*} \mathrm{e}\big(h\tfrac{a}{q}\big) + \sum_{h=1}^{q}{}^{*} \mathrm{e}\big(h\tfrac{a}{q}\big) E_1(N;q,h) + O(\log q)$$

$$= \frac{\mu(q)}{\phi(q)} N + \sum_{h=1}^{q}{}^{*} \mathrm{e}\left(h\tfrac{a}{q}\right) E_1(N;q,h) + O(\log q), \tag{7.2.4}$$

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 $\left|S(a/q)\right|$ decresce essenzialmente come q^{-1}. Poiché S è una funzione continua, ci si aspetta che $|S|$ sia grande in un intorno di 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 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 $S(a/q)$ ad $S(\alpha)$, dove α appartiene all'arco che contiene a/q.

Lemma 7.2.1 *Scelta arbitrariamente la costante $A > 0$, esiste una costante positiva $C = C(A)$ tale che per $1 \le a \le q \le P := (\log N)^A$, con $(a,q) = 1$ e per $|\eta| \le PN^{-1}$ si ha*

$$S\left(\frac{a}{q} + \eta\right) = \frac{\mu(q)}{\phi(q)} T(\eta) + E_2(N;q,a,\eta) \tag{7.2.5}$$

dove

$$E_2(N;q,a,\eta) = O_A\left(N \exp\{-C(A)\sqrt{\log N}\}\right).$$

Dim. Questo è il Lemma 3.1 di Vaughan [141]. Gli ingredienti fondamentali sono il Teorema dei Numeri Primi nelle progressioni aritmetiche 4.4.2, la formula di sommazione parziale, la (7.2.4) ed il Teorema 2.2.11. □

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 $\mathfrak{M}(q,a) := \left[\frac{a}{q} - \frac{P}{N}, \frac{a}{q} + \frac{P}{N}\right]$ l'arco principale relativo al numero razionale a/q, e scriviamo

$$\mathfrak{M} \overset{\text{def}}{=} \bigcup_{q \le P} \bigcup_{a=1}^{q}{}^{*} \mathfrak{M}(q,a) \qquad \text{e} \qquad \mathfrak{m} \overset{\text{def}}{=} \left[PN^{-1}, 1 + PN^{-1}\right] \setminus \mathfrak{M},$$

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 $\left[PN^{-1}, 1 + PN^{-1}\right]$ 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 (7.2.2) abbiamo

$$\begin{aligned} R_2(n) &= \int_0^1 S(\alpha)^2 \mathrm{e}(-n\alpha)\,\mathrm{d}\alpha = \left(\int_{\mathfrak{M}} + \int_{\mathfrak{m}}\right) S(\alpha)^2 \mathrm{e}(-n\alpha)\,\mathrm{d}\alpha \\ &= \sum_{q\le P} \sideset{}{^*}\sum_{a=1}^{q} \int_{-PN^{-1}}^{PN^{-1}} S\left(\frac{a}{q}+\eta\right)^2 \mathrm{e}\left(-n\left(\tfrac{a}{q}+\eta\right)\right)\,\mathrm{d}\eta \\ &\qquad + \int_{\mathfrak{m}} S(\alpha)^2 \mathrm{e}(-n\alpha)\,\mathrm{d}\alpha \\ &= R_{\mathfrak{M}}(n) + R_{\mathfrak{m}}(n), \end{aligned}$$

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 (7.2.5) abbiamo

$$\begin{aligned} R_{\mathfrak{M}}(n) &\approx \sum_{q\le P} \sideset{}{^*}\sum_{a=1}^{q} \int_{-PN^{-1}}^{PN^{-1}} \frac{\mu(q)^2}{\phi(q)^2} T(\eta)^2 \mathrm{e}\left(-n\left(\tfrac{a}{q}+\eta\right)\right)\,\mathrm{d}\eta \\ &= \sum_{q\le P} \frac{\mu(q)^2}{\phi(q)^2} \sideset{}{^*}\sum_{a=1}^{q} \mathrm{e}\left(-n\tfrac{a}{q}\right) \int_{-PN^{-1}}^{PN^{-1}} T(\eta)^2 \mathrm{e}(-n\eta)\,\mathrm{d}\eta. \end{aligned} \tag{7.2.6}$$

Se estendiamo l'integrale a tutto l'intervallo $[0,1]$ troviamo

$$\int_0^1 T(\eta)^2 \mathrm{e}(-n\eta)\,\mathrm{d}\eta = \sum_{\substack{m_1+m_2=n \\ m_1\ge 0, m_2\ge 0}} 1 = n+1 \sim n. \tag{7.2.7}$$

Dunque, si può pensare che $R_2(n)$ sia ben approssimato da

$$R_{\mathfrak{M}}(n) \approx n \sum_{q\le P} \frac{\mu(q)^2}{\phi(q)^2} \sideset{}{^*}\sum_{a=1}^{q} \mathrm{e}\left(-n\tfrac{a}{q}\right) = n \sum_{q\le P} \frac{\mu(q)^2}{\phi(q)^2} c_q(n). \tag{7.2.8}$$

Per il Teorema 2.2.11 la (7.2.8) diventa

$$\begin{aligned} R_{\mathfrak{M}}(n) &\approx n \sum_{q\le P} \frac{\mu(q)^2}{\phi(q)^2} \mu\left(\frac{q}{(q,n)}\right) \frac{\phi(q)}{\phi\big(q/(q,n)\big)} \\ &= n \sum_{q\le P} \frac{\mu(q)^2}{\phi(q)} \frac{\mu\big(q/(q,n)\big)}{\phi\big(q/(q,n)\big)}. \end{aligned}$$

Ora estendiamo la somma a tutti gli interi $q \ge 1$ (commettendo un errore stimabile in modo preciso): osserviamo che l'addendo della somma è una funzione

moltiplicativa di q e quindi per il Lemma 2.1.5 e per il Teorema 2.3.1 abbiamo

$$\begin{aligned} R_{\mathfrak{M}}(n) &\approx n \sum_{q\le P} \frac{\mu(q)^2}{\phi(q)} \frac{\mu\big(q/(q,n)\big)}{\phi\big(q/(q,n)\big)} \\ &\approx n \sum_{q\ge 1} \frac{\mu(q)^2}{\phi(q)} \frac{\mu\big(q/(q,n)\big)}{\phi\big(q/(q,n)\big)} = n \prod_p \big(1+f_n(p)\big) \end{aligned} \tag{7.2.9}$$

dove il prodotto è esteso a tutti i numeri primi ed

$$f_n(p) \stackrel{\text{def}}{=} \frac{\mu(p)^2}{\phi(p)} \frac{\mu\big(p/(p,n)\big)}{\phi\big(p/(p,n)\big)} = \begin{cases} \dfrac{1}{p-1} & \text{se } p \mid n, \\ -\dfrac{1}{(p-1)^2} & \text{se } p \nmid n. \end{cases}$$

Se n è dispari il fattore $1+f_n(2)$ vale 0, e quindi la (7.2.9) 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 (7.2.9) deve essere inteso nel senso che $R_2(n)=o(n)$. Viceversa, se n è pari possiamo trasformare la (7.2.9) 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 (5.3.3). La serie singolare tiene conto delle irregolarità di $R_2(n)/n$ che sono, in effetti, di natura aritmetica. 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 5.5.6 (cfr la (5.6.2)) 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.

Riferimenti. Posto $\mathcal{E}(N) := \{2n \le N : r_2(2n)=0\}$, nel §3.2 di Vaughan [141] si dimostra che per ogni $A>0$ si ha $|\mathcal{E}(N)| = O_A\big(N(\log N)^{-A}\big)$. Un'applicazione del metodo del

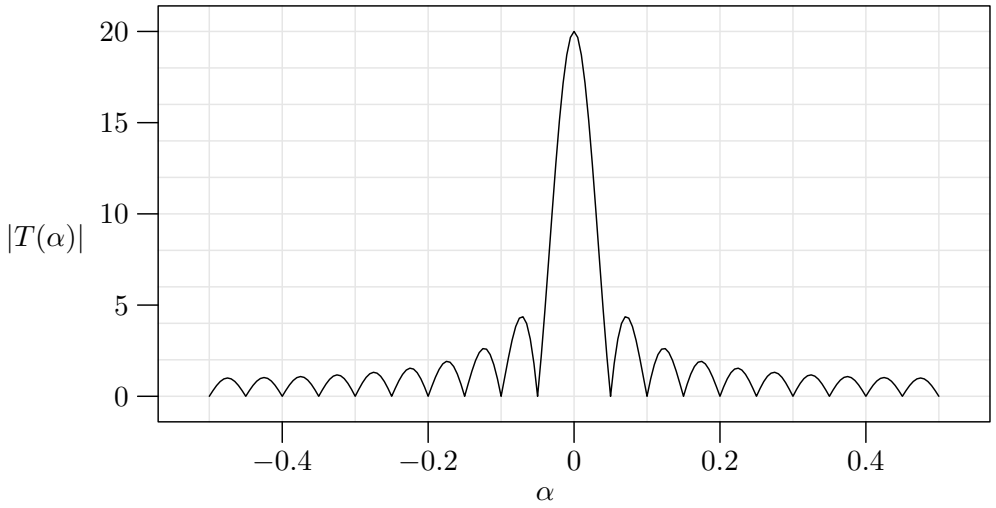


Figura 7.2: Il grafico della funzione $|T_{20}(\alpha)|$ nel quale si nota molto bene che questa funzione ha un grosso picco in prossimità dei valori interi di α, ed è altrimenti molto piccola.

cerchio a diversi problemi legati alla congettura di Goldbach si può trovare in Languasco [87], mentre in Zaccagnini [149] 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 Hardy & Wright [57] §22.20. Le congetture di cui si parla in questo Capitolo ed in Zaccagnini [150] sono inquadrate nel contesto generale della congettura di Schinzel & Sierpiński nell'introduzione di Halberstam & Richert [50]; si vedano le Note relative per la versione quantitativa di Bateman & Horn (vedi anche Zaccagnini [150], 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 Halberstam & Richert [50]. Per altre strategie per la dimostrazione della congettura di Goldbach si veda Ribenboim [128] §4.VI, e per ulteriori riferimenti Guy [49] §C.1.

7.3 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 (7.2.6) alla (7.2.7) può essere giustificata ricordando che per la (7.1.8) si ha $|T(\alpha)| \leq \min\bigl(N+1, \|\alpha\|^{-1}\bigr)$: la Figura 7.2 mostra che $T(\alpha)$ decade molto rapidamente allontanandosi dai valori interi di α. L'errore commesso nella (7.2.9) 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.

7.3.1 Approssimazione della funzione theta di Chebyshev

L'approssimazione di θ fornita dal Teorema dei Numeri Primi nelle progressioni aritmetiche 4.4.2 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 $\theta(N;q,a)-N/\phi(q)$ dipende essenzialmente da una somma i cui addendi sono del tipo $N^\rho/(\phi(q)\rho)$, dove ρ indica il generico zero complesso di opportune funzioni L di Dirichlet. Nel caso piú semplice, quando $q=a=1$, la formula esplicita 6.5.3 implica che per $T\le N$

$$\theta(N)=N-\sum_{\substack{\rho\in\mathbb{C}\text{ t. c. }\zeta(\rho)=0\\ \rho=\beta+i\gamma,\\ |\gamma|\le T}}\frac{N^\rho}{\rho}+O\left(\frac{N}{T}(\log N)^2+\sqrt{N}\log N\right) \tag{7.3.1}$$

dove $\rho=\beta+i\gamma$ 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 (7.1.7), conviene prendere come approssimazione di $S\left(\frac{a}{q}+\eta\right)$ la funzione

$$K(\eta)\stackrel{\text{def}}{=}\sum_{n\le N}\left(1-\sum_{|\gamma|\le T}n^{\rho-1}\right)e(n\eta)$$

dove il coefficiente di $e(n\eta)$ è la derivata rispetto ad N dei primi due termini nella (7.3.1), calcolata in n (poiché se f è regolare $\sum f(n)\sim\int f(t)\,dt$). 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 $\rho=\beta+i\gamma$ della funzione ζ con $\gamma\neq0$ sono uguali ad $\frac12$ (Congettura di Riemann 3.1.4): se cosí è, allora si ha la buona approssimazione $\theta(N)=N+O\left(N^{1/2}(\log N)^2\right)$ che è equivalente alla 3.1.4. 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 $q\le N$ si avrebbe anche la stima

$$\theta(N;q,a)=\frac{N}{\phi(q)}+O\left(N^{1/2}(\log N)^2\right). \tag{7.3.2}$$

Si osservi che le stime 3.1.4 e (7.3.2) 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 (7.3.2). 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 4.4.2. Il contributo di questo eventuale zero sarebbe $\pm N^{\beta}/(\phi(q)\beta)$, e cioè molto prossimo al "termine principale" $N/\phi(q)$, 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 $R_2(n)$.

7.3.2 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 3.1.3 si ha

$$\sum_{n\le N}\left|\int_{\mathfrak{m}} S(\alpha)^2 e(-n\alpha)\,d\alpha\right|^2 \le \int_{\mathfrak{m}} |S(\alpha)|^4\,d\alpha \le \sup_{\alpha\in\mathfrak{m}} |S(\alpha)|^2 \int_0^1 |S(\alpha)|^2\,d\alpha$$
$$= O\left(N\log N \sup_{\alpha\in\mathfrak{m}} |S(\alpha)|^2\right).$$

Dalla (7.2.4) 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 7.3.1 *Per $1 \le a \le q \le N$, $(a,q) = 1$ ed $|\eta| \le q^{-2}$ si ha*

$$S\left(\frac{a}{q}+\eta\right) \ll (\log N)^4\left(Nq^{-1/2} + N^{4/5} + N^{1/2}q^{1/2}\right).$$

Per mezzo di questo Lemma, in effetti si riesce a dimostrare che

$$\sum_{n\le N} |R_{\mathfrak{m}}(n)|^2 = \sum_{n\le N}\left|\int_{\mathfrak{m}} S(\alpha)^2 e(-n\alpha)\,d\alpha\right|^2 = O\left(N^3(\log N)^9 P^{-1}\right) \qquad (7.3.3)$$

e questo dice che, per la "maggioranza" degli interi $n \in [1,N]$ si ha $|R_{\mathfrak{m}}(n)| = O\left(NP^{-1/3}\right)$, che ha ordine di grandezza minore del contributo degli archi principali dato dalla (7.2.9).

Riferimenti. La (7.3.2) è in Davenport [22] Cap. 20. Il Lemma 7.3.1 è il Teorema 3.1 di Vaughan [141]. Per la (7.3.3) vedi Davenport [22] 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 (Halberstam & Richert [50] Cap. 10). Una dimostrazione relativamente semplice di questo fatto (ma con 4 al posto di 2) si trova nel §9 di [10].

7.4 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 $\mathcal{E}(N) := \{n \le N : n \text{ è pari e } R_2(n) = 0\}$, dimostreremo che dato $B > 0$ si ha $|\mathcal{E}(N)| = O_B\big(N(\log N)^{-B}\big)$. Questa è una conseguenza immediata del

Teorema 7.4.1 *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

$$R_{\mathfrak{M}}(n) = n\mathfrak{S}(n,P) + O_A\big(n(\log n)P^{-1}\big) \tag{7.4.1}$$

usando il Lemma 7.2.1 e le (7.1.8), (7.2.6)–(7.2.7), dove

$$\mathfrak{S}(n,P) \stackrel{\text{def}}{=} \sum_{q\le P} \frac{\mu(q)^2}{\phi(q)^2} c_q(n). \tag{7.4.2}$$

Per il Teorema 2.3.1, sfruttando anche il Teorema 2.2.11 ed alcune stime elementari che riguardano la funzione ϕ di Eulero, si trova che

$$\sum_{n\le N} \big|\mathfrak{S}(n,P) - \mathfrak{S}(n)\big|^2 \ll N(\log N)^2 P^{-1}. \tag{7.4.3}$$

Ricordiamo la disuguaglianza elementare $|a+b+c|^2 \le 3\big(|a|^2+|b|^2+|c|^2\big)$. Abbiamo

$$\begin{aligned}\sum_{n\le N} \big|R_2(n) - n\mathfrak{S}(n)\big|^2 &\ll \sum_{n\le N} \big|R_{\mathfrak{M}}(n) - n\mathfrak{S}(n,P)\big|^2 \\ &\quad + \sum_{n\le N} \big|n\mathfrak{S}(n,P) - n\mathfrak{S}(n)\big|^2 + \sum_{n\le N} \big|R_{\mathfrak{m}}(n)\big|^2 \\ &\ll N^3(\log N)^{2-2A} + N^3(\log N)^{2-A} + N^3(\log N)^{9-A}\end{aligned}$$

$$\ll N^3(\log N)^{9-A}$$

per le (7.3.3), (7.4.1)–(7.4.3). Scegliendo ora $A \geq B+9$ si ottiene la tesi. □

Infine, sia $\mathcal{E}'(N) := \{n \in [\frac{1}{2}N, N] : n \text{ è pari e } R_2(2n) = 0\} = \mathcal{E}(N) \cap [\frac{1}{2}N, N]$. Dato che per la (5.3.3) $\mathfrak{S}(n) \geq 2C_0$ quando n è pari, si ha

$$\begin{aligned}\sum_{n\leq N} \big|R_2(n) - n\mathfrak{S}(n)\big|^2 &\geq \sum_{\substack{n\leq N, 2|n\\ R_2(n)=0}} |2C_0 n|^2 \geq \sum_{\substack{N/2\leq n\leq N, 2|n\\ R_2(n)=0}} |2C_0 n|^2 \\ &\geq \frac{1}{2}C_0^2 \big|\mathcal{E}'(N)\big| N^2,\end{aligned}$$

e quindi $|\mathcal{E}'(N)| = O_B\big(N(\log N)^{-B}\big)$ per ogni $B > 0$. Il risultato relativo ad $\mathcal{E}(N)$ segue decomponendo l'intervallo $[1, N]$ in $O(\log N)$ intervalli del tipo $[\frac{1}{2}M, M]$.

7.5 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

$$R_3(n) \stackrel{\text{def}}{=} \sum_{p_1+p_2+p_3=n} \log p_1 \log p_2 \log p_3 = \int_0^1 S(\alpha)^3 \mathrm{e}(-n\alpha)\,\mathrm{d}\alpha$$

se $n \leq N$. 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

$$R_3(n) = \frac{1}{2}n^2\mathfrak{S}_3(n) + O_A\Big(n^2(\log n)^{-A}\Big), \tag{7.5.1}$$

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 7.3.1, per $n \leq N$ e $q > P$ si ha

$$\Big|\int_{\mathfrak{m}} S(\alpha)^3 \mathrm{e}(-n\alpha)\,\mathrm{d}\alpha\Big| \leq \sup_{\alpha\in\mathfrak{m}} |S(\alpha)| \int_0^1 |S(\alpha)|^2\,\mathrm{d}\alpha = O\Big(n^2(\log n)^4 P^{-1/2}\Big). \tag{7.5.2}$$

Deshouillers, Effinger, te Riele & Zinoviev [25] hanno dimostrato che se è vera la Congettura di Riemann Generalizzata allora *tutti* gli interi dispari $n \geq 7$ 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:

$$\theta_N(n) \stackrel{\text{def}}{=} \sum_{\substack{p_2 \leq N \\ p_2 - p_1 = n}} \log p_1 \log p_2 = \int_0^1 |S(\alpha)|^2 \mathrm{e}(-n\alpha)\, \mathrm{d}\alpha,$$

come si vede con un breve calcolo. Questo mostra che i due problemi sono strettamente legati e della stessa difficoltà.

Riferimenti. Per la (7.5.2) vedi Davenport [22] Cap. 26. Problema ternario di Goldbach: [22] Cap. 26, [141] §3.1. La relazione (7.5.1) è giustificata euristicamente in Zaccagnini [150], 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 [25]. [22] Capp. 7–18, oppure Ivić [74] Capp. 11–12. Si veda `http://www.ieeta.pt/~tos/goldbach.html` per dei risultati numerici. Halberstam & Richert [50] Teorema 2.6. Per $\pi_h(x)$ si veda l'argomentazione euristica nel §22.20 di Hardy & Wright [57], e la maggiorazione del Teorema 3.11 di Halberstam & Richert [50]. Altre argomentazioni euristiche diverse si trovano in Pólya [118] ed in Hardy & Littlewood [54]. Problema di Goldbach: Hardy & Littlewood [54]. Per il Teorema di Vinogradov: [22] Cap. 26, oppure [141] Cap. 3. Ramaré [127], Montgomery & Vaughan [104], Pintz [117].

Appendice A

Appendice

Qui raccogliamo alcuni risultati non direttamente legati alla distribuzione dei numeri primi, ma di evidente importanza per la teoria svolta nel testo. In particolare, ci occupiamo di "formule di sommazione" che permettono di trasformare somme in altre somme o integrali, ed alcune applicazioni.

A.1 Formule di sommazione

Teorema A.1.1 (Formula di Abel) *Data una successione strettamente crescente di numeri reali e positivi* $(\lambda_n)_{n\geq 1}$ *tali che* $\lim_{n\to+\infty}\lambda_n = +\infty$*, una successione di numeri complessi* $(a_n)_{n\geq 1}$ *ed una funzione qualsiasi* $\phi\colon \mathbb{R}^{0+}\to\mathbb{C}$*, sia*

$$A(x) \stackrel{\text{def}}{=} \sum_{\lambda_n\leq x} a_n.$$

Per $N\in\mathbb{N}^*$ *si ha*

$$\sum_{1\leq n\leq N} a_n\phi\big(\lambda_n\big) = A\big(\lambda_N\big)\phi\big(\lambda_N\big) - \sum_{n=1}^{N-1} A\big(\lambda_n\big)\Big(\phi\big(\lambda_{n+1}\big)-\phi\big(\lambda_n\big)\Big).$$

Se inoltre $\phi\in\mathcal{C}^1\big(\mathbb{R}^+\big)$ *ed* $x\geq\lambda_1$ *allora*

$$\sum_{\lambda_n\leq x} a_n\phi\big(\lambda_n\big) = A(x)\phi(x) - \int_{\lambda_1}^{x} A(t)\phi'(t)\,\mathrm{d}t. \tag{A.1.1}$$

Dim. Poniamo formalmente $A\big(\lambda_0\big) := 0$ per comodità. Si ha

$$\sum_{n=1}^{N} a_n\phi\big(\lambda_n\big) = \sum_{n=1}^{N}\big[A\big(\lambda_n\big) - A\big(\lambda_{n-1}\big)\big]\phi\big(\lambda_n\big)$$

$$= A\big(\lambda_N\big)\phi\big(\lambda_N\big) - \sum_{n=1}^{N-1} A\big(\lambda_n\big)\Big(\phi\big(\lambda_{n+1}\big) - \phi\big(\lambda_n\big)\Big). \tag{A.1.2}$$

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.1.2) come

$$\sum_{n=1}^{N-1} A\big(\lambda_n\big) \int_{\lambda_n}^{\lambda_{n+1}} \phi'(t)\,\mathrm{d}t = \sum_{n=1}^{N-1} \int_{\lambda_n}^{\lambda_{n+1}} A(t)\phi'(t)\,\mathrm{d}t = \int_{\lambda_1}^{\lambda_N} A(t)\phi'(t)\,\mathrm{d}t,$$

poiché A è costante in ciascun intervallo $(\lambda_n, \lambda_{n+1})$; dato che A è costante anche in $[\lambda_N, x)$, il primo termine è

$$A\big(\lambda_N\big)\phi\big(\lambda_N\big) = A(x)\phi(x) - \int_{\lambda_N}^{x} A(t)\phi'(t)\,\mathrm{d}t,$$

il che conclude la dimostrazione. □

Quando nel testo parliamo della "formula di sommazione parziale" ci riferiamo quasi sempre al caso $\lambda_n = n$ della (A.1.1):

$$\sum_{n\le x} a_n\phi(n) = A(x)\phi(x) - \int_1^x A(t)\phi'(t)\,\mathrm{d}t. \tag{A.1.3}$$

Teorema A.1.2 (Formula di Euler-McLaurin) *Sia $f\colon (x,y] \to \mathbb{C}$ una qualunque funzione derivabile. Si ha*

$$\sum_{x<n\le y} f(n) = \int_x^y f(t)\,\mathrm{d}t + \int_x^y \{t\}f'(t)\,\mathrm{d}t - \{y\}f(y) + \{x\}f(x).$$

Possiamo pensare a questo risultato come ad uno sviluppo in "termine principale," "termine secondario" e "termine di resto." Possiamo anche vederlo come un'approssimazione di un integrale mediante opportune somme di Riemann. Nelle applicazioni spesso si sviluppa $\{t\}$ in serie di Fourier e poi si integra termine a termine.

Dim. Si può facilmente dare una dimostrazione che sfrutta la precedente formula
𝔈 1 di sommazione parziale (A.1.3). Qui diamo una dimostrazione alternativa: se $m \in \mathbb{Z}$ e $t \in (m, m+1)$, si ha $\{t\} = t - [t] = t - m$ dove m è costante e quindi

$$\frac{\mathrm{d}}{\mathrm{d}t}\big(\{t\}f(t)\big) = \{t\}f'(t) + f(t). \tag{A.1.4}$$

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.1.4) 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*

$$\sum_{n\le x} f(n) = \int_1^x f(t)\,\mathrm{d}t + E + O(f(x)).$$

Dim. Poniamo $E_n := f(n) - \int_n^{n+1} f(t)\,\mathrm{d}t$. Poiché f è decrescente si ha che $0 \le E_n \le f(n) - f(n+1)$. Per induzione si verifica immediatamente che

$$0 \le \sum_{h\le n\le k} E_n \le f(h) - f(k+1). \tag{A.1.5}$$

Dunque, la serie $E := \sum_{n\ge 1} E_n$ è convergente ed inoltre $E \le f(1)$. Quindi

$$\begin{aligned}\sum_{n\le x} f(n) - \int_1^x f(t)\,\mathrm{d}t &= \sum_{n\le x}\left(f(n) - \int_n^{n+1} f(t)\,\mathrm{d}t\right) + \int_x^{[x]+1} f(t)\,\mathrm{d}t \\ &= \sum_{n\le x} E_n + O(f(x)) \\ &= E + O\left(\sum_{n\ge [x]+1} E_n\right) + O(f(x)),\end{aligned}$$

e la tesi segue dalla (A.1.5) 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

$$\sum_{2\le n\le N} \frac{1}{\log n} = \mathrm{li}(N) + C + O\big((\log N)^{-1}\big),$$

per un'opportuna costante positiva C. Tenendo presente il Teorema dei Numeri Primi 3.1.3, questa relazione viene talvolta espressa dicendo che la "probabilità" che un intero $n \ge 3$ sia primo è $(\log n)^{-1}$.

Esercizi.

ℭ 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 $\sum_{x<n\le t} 1 = [t] - [x] = t - x - \{t\} + \{x\}$, e poi integrare per parti la funzione $t f'(t)$.

Riferimenti. Formula di sommazione parziale A.1.1: si veda la dimostrazione del Teorema 4.2 di Apostol [5]. Formula di Euler-McLaurin A.1.2: Apostol [5], Teorema 3.1; sue generalizzazioni in Hardy [52], Cap. 13. Lemma A.1.3: Chandrasekharan [13], Teorema 7, Cap. VI.

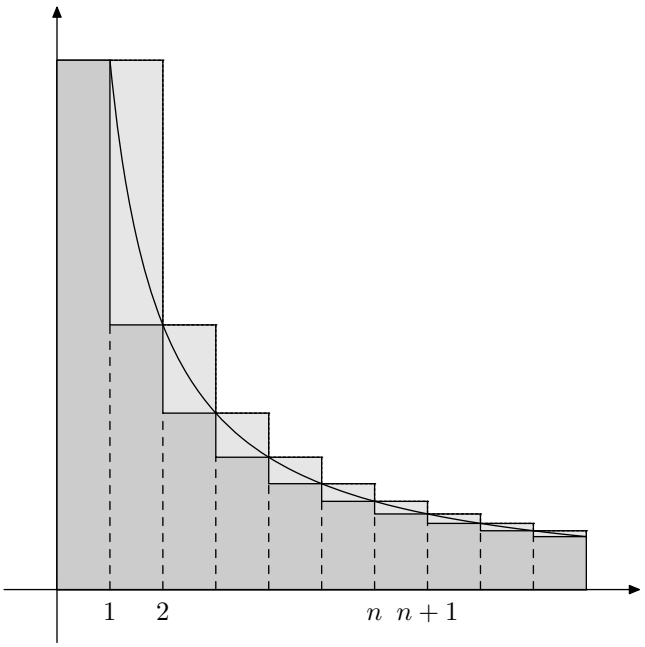


Figura A.1: Dimostrazione del Lemma A.1.3: l'area in grigio chiaro non supera $f(1)$. L'area in grigio scuro fra $x=0$ ed $x=n$ è piú grande di $f(1)+\cdots+f(n)$.

A.2 Le funzioni Gamma e Beta

Definizione A.2.1 (Funzione Gamma di Eulero) *Per $z=x+\mathrm{i}y\in\mathbb{C}$ con parte reale $x=\Re(z)>0$ definiamo*

$$\Gamma(z)\stackrel{\text{def}}{=}\int_0^{+\infty}t^{z-1}\mathrm{e}^{-t}\,\mathrm{d}t.$$

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 $\Gamma(1)=1$, $\Gamma\left(\frac12\right)=\pi^{1/2}$, 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

$$\frac{1}{z\Gamma(z)}=\mathrm{e}^{\gamma z}\prod_{n\geq1}\left(1+\frac{z}{n}\right)\mathrm{e}^{-z/n},\tag{A.2.1}$$

dove γ è la costante di Eulero definita dalla (A.4.1). Si osservi infine che vale la formula di Stirling generalizzata (cfr Appendice A.3): per ogni $\delta>0$ fissato si ha

$$\log\Gamma(z)=\left(z-\frac12\right)\log z-z+\frac12\log(2\pi)+O_\delta\left(|z|^{-1}\right),\tag{A.2.2}$$

quando $|z| \to +\infty$ nell'angolo $|\arg(z)| \leq \pi - \delta$. Questa formula è un ingrediente essenziale della dimostrazione del Teorema 6.4.5.

Altre due proprietà importanti sono la "formula di duplicazione" ed una relazione funzionale che lega Γ con la funzione seno:

$$\Gamma(2s) = \pi^{-1/2} 2^{2s-1} \Gamma(s) \Gamma\Big(s + \frac{1}{2}\Big) \tag{A.2.3}$$

$$\Gamma(s)\Gamma(1-s)\sin(\pi s) = \pi. \tag{A.2.4}$$

Sostituendo $s/2$ al posto di s nella (A.2.3), e $(s+1)/2$ al posto di s nella (A.2.4), e confrontando poi i due valori di $\Gamma\big((s+1)/2\big)$ cosí determinati, si trova la relazione

$$\frac{\Gamma(s/2)}{\Gamma((1-s)/2)} = \pi^{1/2} 2^{1-s} \cos\Big(\frac{\pi}{2} s\Big) \Gamma(s). \tag{A.2.5}$$

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

$$\mathrm{B}(x,y) = 2 \int_0^{\pi/2} (\cos u)^{2x-1} (\sin u)^{2y-1} \, \mathrm{d}u. \tag{A.2.6}$$

Riferimenti. Funzioni Gamma e Beta: Titchmarsh [138], §§1.86–1.87, Davenport [22], §10. Formula di Stirling in generale: Titchmarsh [138], §4.42.

A.3 La formula di Wallis e la formula di Stirling

Teorema A.3.1 (Formula di Wallis per π) *Si ha*

$$\lim_{N\to+\infty} \Big\{ \frac{2}{1} \cdot \frac{2}{3} \cdot \frac{4}{3} \cdot \frac{4}{5} \cdots \frac{2N}{2N-1} \cdot \frac{2N}{2N+1} \Big\} = \lim_{N\to+\infty} \prod_{m=1}^{N} \frac{4m^2}{4m^2-1} = \frac{\pi}{2}.$$

Dim. Per $m \in \mathbb{N}$ definiamo $0!! := (-1)!! := 1$ e $(m+2)!! := m!!(m+2)$, 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

$$\frac{I_{2m}}{I_{2m+1}} = \frac{\pi}{2}(2m+1)\cdot\frac{(2m-1)!!^2}{(2m)!!^2} = \frac{\pi}{2}\frac{(2m)!^2(2m+1)}{2^{4m}(m!^4)} = \binom{2m}{m}^2\frac{(2m+1)\pi}{2^{4m+1}}, \tag{A.3.3}$$

che insieme alla (A.3.2) implica la tesi ed anche la relazione asintotica $\binom{2m}{m} \sim 2^{2m}/\sqrt{\pi m}$. □

𝔈 1 **Teorema A.3.2 (Formula di Stirling)** *Per $N \to +\infty$ ed $N \in \mathbb{N}$ si ha*

$$\log N! = N\log N - N + \frac{1}{2}\log(2\pi N) + O(N^{-1}).$$

Dim. Per la formula di sommazione parziale (A.1.3) con $a_n = 1$ e $\phi(t) = \log t$, se $N \in \mathbb{N}$ si ha

$$\begin{aligned}\log N! = \sum_{n=1}^{N}\log n &= N\log N - \int_1^N \frac{[t]}{t}\,\mathrm{d}t \\ &= N\log N - (N-1) + \int_1^N \frac{\{t\}}{t}\,\mathrm{d}t.\end{aligned} \tag{A.3.4}$$

Posto $g(t) := \frac{1}{2}\big(\{t\}^2 - \{t\}\big)$, per il Lemma A.4.6 si ha che g è continua, derivabile per $t \notin \mathbb{Z}$ e che $g'(t) = \{t\} - \frac{1}{2}$. Quindi, integrando per parti,

$$\int_1^N \frac{\{t\}}{t}\,\mathrm{d}t = \left[\frac{g(t)}{t} + \frac{1}{2}\log t\right]_1^N + \int_1^N \frac{g(t)}{t^2}\,\mathrm{d}t = \frac{1}{2}\log N + \frac{1}{2}\int_1^N \frac{\{t\}^2 - \{t\}}{t^2}\,\mathrm{d}t.$$

L'ultimo integrale esteso a tutto l'intervallo $[1,+\infty)$ è chiaramente convergente poiché il numeratore è limitato, e si ha

$$\int_1^N \frac{\{t\}^2 - \{t\}}{t^2}\,\mathrm{d}t = \int_1^{+\infty} \frac{\{t\}^2 - \{t\}}{t^2}\,\mathrm{d}t + O(N^{-1}).$$

Sostituendo in (A.3.4) otteniamo immediatamente, per qualche $C \in \mathbb{R}$,

$$\log N! = N\log N - N + \frac{1}{2}\log N + C + O\big(N^{-1}\big). \tag{A.3.5}$$

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.2.6) $I_m = \mathrm{B}\big(\frac{1}{2}, \frac{1}{2}(m+1)\big)$ 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

$$\log N! = N\log N - N + \frac{1}{2}\log(2\pi N) + \frac{1}{12N} + O\big(N^{-2}\big),$$

cioè che

$$N! = \sqrt{2\pi N}\left(\frac{N}{\mathrm{e}}\right)^N \left(1 + \frac{1}{12N} + O\big(N^{-2}\big)\right).$$

Da questa segue che, detta a_N la successione nell'enunciato della formula di Wallis, si ha $\pi = 2a_N + O\big(N^{-1}\big)$. La convergenza non è molto veloce perché, dopo una riduzione ai minimi termini, si scopre che il numeratore di a_N è una potenza di 2 e non c'è motivo particolare per pensare che frazioni di questo tipo debbano essere buone approssimazioni di π.

Esercizi.

𝔈 1. Usare la formula di Euler-McLaurin A.1.2 per ridimostrare la formula di Stirling A.3.2.

Riferimenti. Formula di Stirling A.3.2: per una dimostrazione simile, ma con una conclusione leggermente piú debole, si veda Apostol [5], Teorema 3.15, oppure Titchmarsh [138], §1.87. Una dimostrazione della formula di Stirling completamente diversa si trova in Marsaglia & Marsaglia [99].

A.4 Lemmi

𝔈 1 **Teorema A.4.1** *Per ogni $k \in \mathbb{R}$ fissato si ha, quando $N \to +\infty$ ed $N \in \mathbb{N}$,*

$$\sum_{n\le N} n^k = \begin{cases} \frac{1}{k+1}N^{k+1} + \frac{1}{2}N^k + O_k\big(N^{k-1}\big) & \text{se } k > 0, \\ N & \text{se } k = 0, \\ \frac{1}{k+1}N^{k+1} + c_k + O_k\big(N^k\big) & \text{se } k \in (-1,0), \\ \log N + c_{-1} + O\big(N^{-1}\big) & \text{se } k = -1, \\ \zeta(-k) + O_k\big(N^{k+1}\big) & \text{se } k < -1, \end{cases}$$

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 $k > -1$

$$\begin{aligned}\sum_{n=1}^{N} n^k &= N^{k+1} - k\int_1^N [t]t^{k-1}\,\mathrm{d}t = \frac{N^{k+1}+k}{k+1} + k\int_1^N \{t\}t^{k-1}\,\mathrm{d}t \\ &= \frac{N^{k+1}+k}{k+1} + \frac{k}{2}\int_1^N t^{k-1}\,\mathrm{d}t + k\int_1^N \left(\{t\}-\frac{1}{2}\right)t^{k-1}\,\mathrm{d}t \\ &= \frac{N^{k+1}+k}{k+1} + \frac{N^k-1}{2} + k\big[g(t)t^{k-1}\big]_1^N - k(k-1)\int_1^N g(t)t^{k-2}\,\mathrm{d}t\end{aligned}$$

dove $g(t) := \frac{1}{2}\big(\{t\}^2 - \{t\}\big)$ è una primitiva continua di $\{t\} - \frac{1}{2}$. Se $k \geq 0$ 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 $c_k' + O\big(N^{k-1}\big)$.

Per la penultima relazione la formula di sommazione parziale dà

$$\begin{aligned}\sum_{n\leq N}\frac{1}{n} &= 1 + \int_1^N \frac{[t]}{t^2}\,\mathrm{d}t = 1 + \log N - \int_1^N \frac{\{t\}}{t^2}\,\mathrm{d}t \\ &= \log N + 1 - \int_1^{+\infty}\frac{\{t\}}{t^2}\,\mathrm{d}t + O\left(\int_N^{+\infty}\frac{\mathrm{d}t}{t^2}\right),\end{aligned}$$

e dunque il risultato segue, con

$$c_{-1} = \gamma \overset{\text{def}}{=} 1 - \int_1^{+\infty}\frac{\{t\}}{t^2}\,\mathrm{d}t. \tag{A.4.1}$$

Per l'ultima relazione basta osservare che per $k < -1$

$$\sum_{n\leq N} n^k = \sum_{n\geq 1} n^k + O\left(\int_N^{+\infty} t^k\,\mathrm{d}t\right) = \zeta(-k) + O_k\big(N^{k+1}\big).$$

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 $[N]^{-1} \sim N^{-1}$, l'errore *non può* essere $o\big(N^{-1}\big)$. □

Definizione A.4.2 (Numeri di Bernoulli) *I numeri di Bernoulli B_n sono i coefficienti dello sviluppo*

$$\frac{z}{\mathrm{e}^z - 1} = 1 - \frac{1}{2}z + \frac{B_1}{2!}z^2 - \frac{B_2}{4!}z^4 + \frac{B_3}{6!}z^6 + \cdots$$

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* $\beta_0 := 1$, $\beta_1 := -\frac{1}{2}$, $\beta_{2k} := (-1)^{k-1}B_k$, $\beta_{2k+1} := 0$ *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

$$k!x\big(1+\mathrm{e}^x+\cdots+\mathrm{e}^{(n-1)x}\big) = k!\left(\beta_0+\frac{\beta_1}{1!}x+\frac{\beta_2}{2!}x^2+\cdots\right)\left(nx+\frac{n^2x^2}{2!}+\cdots\right),$$

che sono uguali entrambe a $k!x\big(\mathrm{e}^{nx}-1\big)\big(\mathrm{e}^x-1\big)^{-1}$. □

Lemma A.4.4 *Per ogni* $k \in \mathbb{R}^{0+}$ *si ha*

$$\sum_{d\le x}\left(\log\frac{x}{d}\right)^k \le x\Gamma(k+1).$$

Dim. Per $d \in \mathbb{N}^*$ si ha

$$\left(\log\frac{x}{d}\right)^k \le \int_{d-1}^{d}\left(\log\frac{x}{t}\right)^k \mathrm{d}t,$$

mentre se $d = 1$ l'integrale è improprio nell'estremo sinistro, ma convergente. Dunque

$$\sum_{d=1}^{[x]}\left(\log\frac{x}{d}\right)^k \le \int_0^x\left(\log\frac{x}{t}\right)^k \mathrm{d}t = x\int_0^{+\infty} u^k\mathrm{e}^{-u}\,\mathrm{d}u = x\Gamma(k+1),$$

mediante il cambiamento di variabile $t = x\mathrm{e}^{-u}$. □

Per $k = 1$ questa relazione implica la formula di Stirling nella forma piú debole $\log N! = N\log N + O(N)$, che è comunque sufficiente per ottenere i risultati del Capitolo 3.

Lemma A.4.5 *Sia* $f\colon \mathbb{R}\to\mathbb{R}$ *una funzione convessa. Per ogni* $\delta > 0$ *si ha*

$$f(x) \le \frac{1}{\delta}\int_{x-\frac{1}{2}\delta}^{x+\frac{1}{2}\delta} f(t)\,\mathrm{d}t.$$

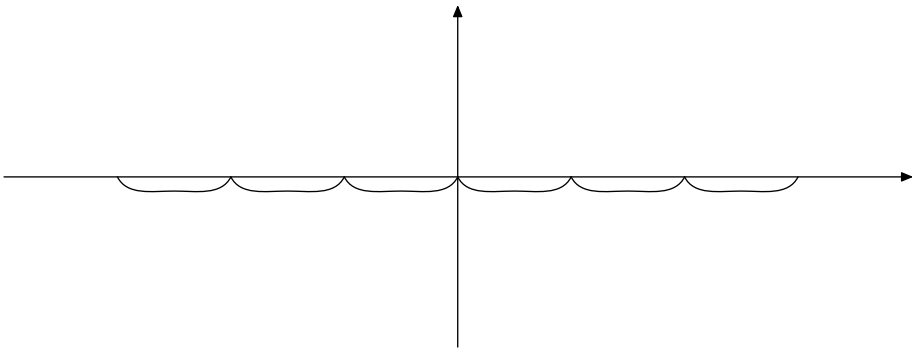


Figura A.2: Il grafico della funzione $g(t) := \frac{1}{2}\big(\{t\}^2 - \{t\}\big)$

Dim. Per ogni $\alpha \in \big[-\frac{1}{2}\delta, \frac{1}{2}\delta\big]$ si ha

$$f(x) = f\left(\frac{1}{2}(x-\alpha) + \frac{1}{2}(x+\alpha)\right) \le \frac{1}{2}\big(f(x-\alpha) + f(x+\alpha)\big).$$

Integrando rispetto ad α questa disuguaglianza su tutto l'intervallo $\big[0, \frac{1}{2}\delta\big]$ si ottiene la tesi. □

Lemma A.4.6 *Sia $g\colon \mathbb{R} \to \mathbb{R}$ la funzione definita da $g(t) := \frac{1}{2}\big(\{t\}^2 - \{t\}\big)$. Allora $g \in \mathcal{C}^0(\mathbb{R}) \cap \mathcal{C}^1(\mathbb{R} \setminus \mathbb{Z})$, e $g'(t) = \{t\} - \frac{1}{2}$ per $t \in \mathbb{R} \setminus \mathbb{Z}$. Inoltre, per qualunque funzione $f \in \mathcal{C}^1(\mathbb{R})$ e per $a, b \in \mathbb{R}$ si ha*

$$\int_a^b f(t)\left(\{t\} - \frac{1}{2}\right) \mathrm{d}t = \big[f(t)g(t)\big]_a^b - \int_a^b f'(t)g(t)\,\mathrm{d}t. \tag{A.4.2}$$

Dim. La funzione g ha periodo 1; per la continuità in 0 è sufficiente verificare che

$$\lim_{t \to 0-} g(t) = g(0) = 0.$$

Per $n \in \mathbb{Z}$ e $t \in (n, n+1)$ si ha $\{t\} = t - n$ e quindi $g(t) = \frac{1}{2}(t^2 - (2n+1)t + n^2 + n)$ da cui $g'(t) = \{t\} - \frac{1}{2}$. Infine, per l'ultima parte è sufficiente scrivere l'intervallo $[a,b]$ come unione di intervalli i cui estremi (a parte eventualmente l'estremo sinistro del primo e quello destro dell'ultimo) sono interi consecutivi, sui quali la (A.4.2) non presenta problemi. □

Si noti che la funzione $\{t\} - \frac{1}{2}$ ha media nulla sul suo periodo.

Esercizi.

℄ 1. Ridimostrare il Teorema A.4.1 per mezzo della formula di Euler-McLaurin A.1.2.

Riferimenti. Teoremi A.4.1 e A.4.4: Apostol [5] Teorema 3.2; Hardy & Wright [57] Teoremi 422 (per il caso $k = -1$) e 423. Per il caso di $k \in \mathbb{N}$ si veda anche Levy [94], [95]. Numeri di Bernoulli: Hardy & Wright [57] §7.9 o Apostol [5] §12.12.

Appendice B

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 $N/(\log N - 1)$, Gauss $\mathrm{li}(N)$, mentre Riemann dette l'approssimazione piú complicata

$$R(N) \stackrel{\text{def}}{=} \sum_{n\ge 1} \frac{\mu(n)}{n} \mathrm{li}\big(N^{1/n}\big),$$

dove la funzione logaritmo integrale li è definita dalla (3.1.1).

Si calcola $\pi(x)$ in modo efficiente per mezzo di una variante della formula di Legendre 5.1.1. Indichiamo con p_1, p_2, ..., i numeri primi in ordine crescente. Fissati a e $k \in \mathbb{N}$ poniamo

$$\phi(x;a) \stackrel{\text{def}}{=} \big|\{n \le x\colon\ p \mid n \Rightarrow p > p_a\}\big|$$
$$P_k(x;a) \stackrel{\text{def}}{=} \big|\{n \le x\colon\ \Omega(n) = k \text{ e } p \mid n \Rightarrow p > p_a\}\big|$$

Per convenzione poniamo $P_0(x;a) := 1$. Raggruppando gli interi con $\Omega(n) = k$ si ha

$$\phi(x;a) = \sum_{k=0}^{\infty} P_k(x;a),$$

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 [23] sono fatti scegliendo $y \in \big[x^{1/3}, x^{1/2}\big]$, $a := \pi(y)$, da cui si ottiene $P_1(x;a) = \pi(x) - a$, $P_k(x;a) = 0$ per $k \ge 3$ e quindi

$$\pi(x) = \phi(x;a) + a - 1 - P_2(x;a).$$

Il calcolo di ϕ e di P_2 è relativamente meno oneroso del Crivello di Eratostene o della formula di Legendre. 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.

N	$\pi(N)$	$\Delta_L(N)$	$\Delta_G(N)$	$\Delta_R(N)$
10	4	4	2	
10^2	25	3	5	1
10^3	168	-1	10	0
10^4	1229	-11	17	-2
10^5	9592	-80	38	-5
10^6	78498	-468	130	29
10^7	664579	-3120	339	88
10^8	5761455	-21151	754	97
10^9	50847534	-145992	1701	-79
10^{10}	455052511	-1040540	3104	-1828
10^{11}	4118054813	-7638512	11588	-2318
10^{12}	37607912018	-57718368	38263	-1476
10^{13}	346065536839	-446676618	108971	-5773
10^{14}	3204941750802	-3527115021	314890	-19200
10^{15}	29844570422669	-28336573668	1052619	73218
10^{16}	279238341033925	-231082803105	3214632	327052
10^{17}	2623557157654233	-1909190842202	7956589	-598255
10^{18}	24739954287740860	-15955501820884	21949555	-3501366

Tabella B.1: Le funzioni Δ_L, Δ_G e Δ_R sono definite rispettivamente da $\Delta_L(N) := N/(\log N - 1) - \pi(N)$, $\Delta_G(N) := \mathrm{li}(N) - \pi(N)$ e $\Delta_R(N) := R(N) - \pi(N)$. I valori sono approssimati all'intero piú vicino. Questi dati sono tratti dalla Tavola 5.2 di Conway & Guy [18], e dalle Tavole 26 e 27 di Ribenboim [128].

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

Tabella B.2: Questi dati sono tratti da Deléglise & Rivat [23], [24].

Appendice C

Funzioni Aritmetiche Elementari

Queste Tavole contengono i valori delle funzioni aritmetiche elementari per $1 \leq n \leq 100$.

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

n	ϕ	d	μ	ω	Ω	Λ
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
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

n	ϕ	d	μ	ω	Ω	Λ
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
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

n	ϕ	d	μ	ω	Ω	Λ
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
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

Appendice D

Generatori e Ordini modulo p

Gli ordini degli interi $n = 2, \ldots, 13$ modulo i primi $p = 2, \ldots, 59$. Le colonne corrispondenti ai generatori sono indicate da un $\star$.

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	$58^\star$

$341 = 11 \cdot 31$	$2^{10} \equiv 1 (341)$	$10 \mid 340$	$561 = 3 \cdot 11 \cdot 17$	$5^{80} \equiv 1 (561)$	$80 \mid 560$
$561 = 3 \cdot 11 \cdot 17$	$2^{40} \equiv 1 (561)$	$40 \mid 560$	$35 = 5 \cdot 7$	$6^2 \equiv 1 (35)$	$2 \mid 34$
$645 = 3 \cdot 5 \cdot 43$	$2^{28} \equiv 1 (645)$	$28 \mid 644$	$217 = 7 \cdot 31$	$6^6 \equiv 1 (217)$	$6 \mid 216$
$91 = 7 \cdot 13$	$3^6 \equiv 1 (91)$	$6 \mid 90$	$25 = 5^2$	$7^4 \equiv 1 (25)$	$4 \mid 24$
$703 = 19 \cdot 37$	$3^{18} \equiv 1 (703)$	$18 \mid 702$	$561 = 3 \cdot 11 \cdot 17$	$7^{80} \equiv 1 (561)$	$80 \mid 560$
$15 = 3 \cdot 5$	$4^2 \equiv 1 (15)$	$2 \mid 14$	$9 = 3^2$	$8^2 \equiv 1 (9)$	$2 \mid 8$
$85 = 5 \cdot 17$	$4^8 \equiv 1 (85)$	$8 \mid 84$	$21 = 3 \cdot 7$	$8^2 \equiv 1 (21)$	$2 \mid 20$
$561 = 3 \cdot 11 \cdot 17$	$4^{20} \equiv 1 (561)$	$20 \mid 560$	$45 = 3^2 \cdot 5$	$8^4 \equiv 1 (45)$	$4 \mid 44$
$217 = 7 \cdot 31$	$5^6 \equiv 1 (217)$	$6 \mid 216$	$65 = 5 \cdot 13$	$8^4 \equiv 1 (65)$	$4 \mid 64$

Alcuni pseudoprimi nelle basi $2, \dots, 8$. 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

$$a^{n-1} \equiv 1 \mod n \iff \begin{cases} a^{pq-1} \equiv 1 \mod p \\ a^{pq-1} \equiv 1 \mod q \end{cases} \iff \begin{cases} r_p \mid pq-1 \\ r_q \mid pq-1. \end{cases}$$

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

$$\begin{cases} p \equiv 1 \mod r_q, \\ q \equiv 1 \mod r_p. \end{cases}$$

Bibliografia

[1] L. M. Adleman, C. Pomerance, and R. S. Rumely, *On distinguishing prime numbers from composite numbers*, Ann. Math. **117** (1983), 173–206.

[2] L. V. Ahlfors, *Complex Analysis*, third ed., Mc Graw-Hill, 1979.

[3] W. R. Alford, A. Granville, and C. Pomerance, *There are infinitely many Carmichael numbers*, Ann. Math. **140** (1994), 703–722.

[4] T. M. Apostol, *Some properties of completely multiplicative arithmetical functions*, Amer. Math. Monthly **78** (1971), 266–271.

[5] ———, *Introduction to Analytic Number Theory*, Springer, 1976.

[6] R. C. Baker, G. Harman, and J. Pintz, *The difference between consecutive primes, II*, Proc. London Math. Soc. (3) **83** (2001), 532–562.

[7] P. T. Bateman and H. G. Diamond, *A hundred years of prime numbers*, Amer. Math. Monthly **103** (1996), 729–741.

[8] A. H. Beiler, *Recreations in the Theory of Numbers*, Dover, New York, 1964.

[9] 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.

[10] ———, *Le Grand Crible dans la Théorie Analytique des Nombres*, Societé Mathématique de France, Paris, 1974, Astérisque n. 18.

[11] ———, *Problems of the Millennium: the Riemann Hypothesis*, 2000, See `http://www.claymath.org/prize_problems/index.html`.

[12] 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.

[13] K. Chandrasekharan, *Introduction to Analytic Number Theory*, Grundlehren math. Wiss., vol. 148, Springer, 1968.

[14] ———, *Arithmetical Functions*, Springer, 1970.

[15] L. Childs, *A Concrete Introduction to Higher Algebra*, Springer, 1979.

[16] H. Cohen, *A Course in Computational Algebraic Number Theory*, third ed., Graduate Texts in Mathematics, vol. 138, Springer, 1996.

[17] J. B. Conrey, *The Riemann Hypothesis*, Notices of the American Mathematical Society **50** (2003), 341–353.

[18] J. H. Conway and R. K. Guy, *Il libro dei numeri*, Hoepli, Milano, 1999.

[19] H. Cramér, *On the order of magnitude of the difference between consecutive prime numbers*, Acta Arith. **2** (1937), 23–46.

[20] R. Crandall and C. Pomerance, *Prime numbers. A computational perspective*, Springer, New York, 2001.

[21] H. Daboussi, *Sur le Théorème des Nombres Premiers*, C. R. Acad. Sc. Paris Série I **298** (1984), 161–164.

[22] H. Davenport, *Multiplicative Number Theory*, third ed., Graduate Texts in Mathematics, vol. 74, Springer, 2000.

[23] M. Deléglise and J. Rivat, *Computing $\pi(x)$: The Meissel, Lehmer, Lagarias, Miller, Odlyzko method*, Math. Comp. **65** (1996), 235–245.

[24] ———, *Computing $\psi(x)$*, Math. Comp. **67** (1998), 1691–1696.

[25] J.-M. Deshouillers, G. Effinger, H. te Riele, and D. Zinoviev, *A complete Vinogradov 3-primes Theorem under the Riemann Hypothesis*, Electr. Res. Announcements American Mathematical Society **3** (1997), 99–104.

[26] H. G. Diamond, *Elementary methods in the study of the distribution of prime numbers*, Bull. Amer. Math. Soc. **3** (1982), 553–589.

[27] L. E. Dickson, *History of the Theory of Numbers (3 volumes)*, Carnegie, 1919–1923, Reprint Chelsea–AMS, 1999.

[28] P. G. L. Dirichlet, *Lectures on Number Theory (with supplements by R. Dedekind)*, American Mathematical Society, Providence, RI, 1999.

[29] J. D. Dixon, *Factorization and primality tests*, Amer. Math. Monthly **91** (1984), 333–352.

[30] U. Dudley, *History of a formula for primes*, Amer. Math. Monthly **76** (1969), 23–28.

[31] H. M. Edwards, *Riemann's Zeta Function*, Academic Press, 1974, Dover Reprint 2001.

[32] ———, *Fermat's Last Theorem*, Springer, 1977.

[33] W. J. Ellison, *Waring's problem*, Amer. Math. Monthly **78** (1971), 10–36.

[34] J. Elstrodt, *A quick proof of the Prime Number Theorem for arithmetic progressions*, Charlemagne and his heritage. 1200 years of civilization and science in Europe, vol. 2 (Aachen 1995) (Turnhout), Brepols, 1998, pp. 521–530.

[35] P. Erdős, *On a new method in elementary number theory which leads to an elementary proof of the Prime Number Theorem*, Proc. Nat. Acad. Sci. U.S.A. **35** (1949), 374–384.

[36] J. S. Frame, *A short proof of quadratic reciprocity*, Amer. Math. Monthly **85** (1978), 818–819.

[37] J. Friedlander, A. Granville, A. Hildebrand, and H. Maier, *Oscillation theorems for primes in arithmetic progressions and for sifting functions*, Journal of the American Mathematical Society **4** (1991), 25–86.

[38] J. Friedlander and H. Iwaniec, *The polynomial $x^2 + y^4$ captures its primes*, Ann. Math. **148** (1998), 945–1040.

[39] J. M. Gandhi, *Review n. 7003*, Mathematical Reviews **50** (1975), 963.

[40] K. F. Gauss, *Disquisitiones Arithmeticae*, G. Fleischer, Leipzig, 1801, English translation by W. C. Waterhouse. Springer, New York, 1986.

[41] S. Gerig, *A Simple Proof of the Prime Number Theorem*, J. Number Theory **8** (1976), 131–136.

[42] L. J. Goldstein, *A History of the Prime Number Theorem*, Amer. Math. Monthly **80** (1973), 599–615.

[43] D. A. Goldston, Y. Motohashi, J. Pintz, and C. Y. Yıldırım, *Small gaps between primes exist*, Proc. Japan Acad. Ser. A Math. Sci. **82** (2006), 61–65, disponibile all'indirizzo `http://xxx.sissa.it/pdf/math.NT/0505300`.

[44] S. W. Golomb, *A direct interpretation of Gandhi's formula*, Amer. Math. Monthly **81** (1974), 752–754.

[45] A. Granville, *On elementary proofs of the Prime Number Theorem for arithmetic progressions, without characters*, Proceedings of the Amalfi Conference on Analytic Number Theory, held at Maiori, Amalfi, Italy, from 25 to 29 September, 1989 (E. Bombieri, A. Perelli, S. Salerno, and U. Zannier, eds.), Università di Salerno, 1992, pp. 157–194.

[46] ———, *Harald Cramér and the distribution of prime numbers*, Scand. Actuarial J. **1** (1995), 12–28.

[47] ———, *Unexpected irregularities in the distribution of prime numbers*, Proceedings of the International Congress of Mathematicians, Zürich, Switzerland, 1994 (Basel), Birkhäuser, 1995, pp. 388–399.

[48] G. Greaves, *Sieves in Number Theory*, Springer, Berlin, 2001.

[49] R. K. Guy, *Unsolved Problems in Number Theory*, second ed., Springer, 1994.

[50] H. Halberstam and H.-E. Richert, *Sieve Methods*, Academic Press, London, 1974.

[51] H. Halberstam and K. F. Roth, *Sequences*, Oxford University Press, Oxford, 1966.

[52] G. H. Hardy, *Divergent Series*, second ed., Chelsea, New York, 1991.

[53] ———, *Ramanujan. Twelve lectures on subjects suggested by his life and works*, third ed., Chelsea, New York, 1999.

[54] G. H. Hardy and 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.

[55] ———, *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.

[56] G. H. Hardy and 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 and B. M. Wilson, Third ed., AMS–Chelsea, 1999; n. 36, 276–309.

[57] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, fifth ed., Oxford Science Publications, Oxford, 1979.

[58] G. Harman, *On the number of Carmichael numbers up to x*, Bull. London Math. Soc. **37** (2005), 641–650.

[59] _____, *Prime-Detecting Sieves*, London Mathematical Society Monographs, vol. 33, Princeton University Press, Princeton, 2007.

[60] D. R. Heath-Brown, *Artin's conjecture for primitive roots*, Quart. J. Math. Oxford (2) **37** (1986), 27–38.

[61] _____, *The number of primes in a short interval*, J. Reine Angew. Math. **389** (1988), 22–63.

[62] _____, *Zero-free regions for Dirichlet L-functions and the least prime in an arithmetic progression*, Proc. London Math. Soc. (3) **64** (1992), 265–338.

[63] _____, *Primes represented by* $x^3 + 2y^3$, Acta Math. **186** (2001), 1–84.

[64] A. Hildebrand, *The Prime Number Theorem via the large sieve*, Mathematika **33** (1986), 23–30.

[65] _____, *Large values of character sums*, J. Number Theory **29** (1988), 271–296.

[66] _____, *On the constant in the Pólya–Vinogradov inequality*, Canad. Bull. Math. **31** (1988), 347–352.

[67] A. Hildebrand and H. Maier, *Irregularities in the distribution of primes in short intervals*, J. Reine Angew. Math. **397** (1989), 162–193.

[68] A. Hildebrand and G. Tenenbaum, *Integers without large prime factors*, J. Théorie des Nombres Bordeaux **5** (1993), 411–484.

[69] L.-K. Hua, *Introduction to Number Theory*, Springer, 1982.

[70] D. Husemöller, *Elliptic Curves*, Graduate Texts in Mathematics, vol. 111, Springer, New York, 1987.

[71] M. Huxley, *The Distribution of Prime Numbers*, Clarendon Press, Oxford, 1972.

[72] A. E. Ingham, *Review*, Mathematical Reviews **10** (1949), 595–596.

[73] ———, *The Distribution of Prime Numbers*, Cambridge University Press, Cambridge, 1990.

[74] A. Ivić, *The Theory of the Riemann Zeta–Function*, J. Wiley, New York, 1985.

[75] R. D. James, *On the sieve method of Viggo Brun*, Bull. Amer. Math. Soc. **49** (1943), 422–432.

[76] ———, *Recent progress in the Goldbach problem*, Bull. Amer. Math. Soc. **55** (1949), 246–260.

[77] J. Knopfmacher, *Abstract Analytic Number Theory*, Dover, New York, 1989.

[78] D. E. Knuth, *The Art of Computer Programming. Vol. 2. Seminumerical Algorithms*, Second ed., Addison Wesley, Reading (Mass.), 1981.

[79] N. Koblitz, *A Course in Number Theory and Cryptography*, second ed., Graduate Texts in Mathematics, vol. 114, Springer, New York, 1994.

[80] A. V. Kumchev and D. I. Tolev, *An invitation to additive prime number theory*, 2004, Unpublished.

[81] J. Lagarias, *An elementary problem equivalent to the Riemann Hypothesis*, Amer. Math. Monthly **109** (2002), 534–543.

[82] 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.

[83] ———, *Handbuch der Lehre von der Verteilung der Primzahlen*, Teubner, Leipzig, 1909.

[84] ———, *Vorlesungen über Zahlentheorie*, Hirzel, Leipzig, 1927.

[85] ———, *Elementary Number Theory*, Chelsea, New York, 1960.

[86] S. Lang, *La bellezza della matematica*, Bollati Boringhieri, 1991.

[87] A. Languasco, *Some results on Goldbach's problem*, Rend. Sem. Mat. Univ. Pol. Torino **53 (4)** (1995), 325–337.

[88] A. Languasco and A. Zaccagnini, *Introduzione alla crittografia*, Ulrico Hoepli Editore, Milano, 2004.

[89] ———, *Alcune proprietà dei numeri primi, II*, Sito web Bocconi-Matematica Pristem (2005), `http://matematica.unibocconi.it/LangZac/LangZacc2.pdf`.

[90] ———, *Intervalli fra numeri primi consecutivi*, Sito web Bocconi-Matematica Pristem (2005), `http://matematica.unibocconi.it/LangZac/home3.htm`.

[91] D. H. Lehmer, *On the converse of Fermat's Theorem*, Amer. Math. Monthly **43** (1936), 347–350.

[92] ———, *On the exact number of primes less than a given limit*, Illinois J. Math. **3** (1959), 381–388.

[93] N. Levinson, *A motivated account of an elementary proof of the Prime Number Theorem*, Amer. Math. Monthly **76** (1969), 225–245.

[94] L. S. Levy, *Summation of the series* $1^n + 2^n + \cdots + x^n$ *using elementary calculus*, Amer. Math. Monthly **77** (1970), 840–847.

[95] ———, *Corrigendum*, Amer. Math. Monthly **78** (1971), 987.

[96] Yu. V. Linnik, *On the least prime in an arithmetic progression I. The basic theorem*, Mat. Sbornik **15 (57)** (1944), 139–178 (Russian).

[97] J. E. Littlewood, *Sur la distribution des nombres premiers*, C. R. Acad. Sc. Paris **158** (1914), 1869–1872.

[98] H. Maier, *Primes in short intervals*, Michigan Math. J. **32** (1985), 221–225.

[99] G. Marsaglia and J. C. W. Marsaglia, *A new derivation of Stirling's approximation to* $n!$, Amer. Math. Monthly **97** (1990), 826–829.

[100] H. L. Montgomery, *Topics in Multiplicative Number Theory*, Lecture Notes in Mathematics, vol. 227, Springer, New York, 1971.

[101] ———, *The analytic principle of the large sieve*, Bull. Amer. Math. Soc. **84** (1978), 547–567.

[102] _____, *Ten Lectures on the Interface Between Analytic Number Theory and Harmonic Analysis*, CBMS, vol. 84, American Mathematical Society, Providence, RI, 1994.

[103] H. L. Montgomery and R. C. Vaughan, *On the large sieve*, Mathematika **20** (1973), 119–134.

[104] _____, *The exceptional set in Goldbach's problem*, Acta Arith. **27** (1975), 353–370.

[105] _____, *Multiplicative Number Theory. I. Classical Theory*, Cambridge University Press, Cambridge, 2007.

[106] P. Morton, *Musings on the prime divisors of arithmetic sequences*, Amer. Math. Monthly **97** (1990), 323–328.

[107] T. Nagel, *Généralisation d'un théorème de Tchebycheff*, J. Math. Pures Appl. (8) **4** (1921), 343–356.

[108] M. Nair, *A new method in elementary prime number theory*, J. London Math. Soc. (2) **25** (1982), 385–391.

[109] _____, *On Chebyshev-type inequalities for primes*, Amer. Math. Monthly **89** (1982), 126–129.

[110] W. Narkiewicz, *The Development of Prime Number Theory*, Springer, 2000.

[111] M. B. Nathanson, *Additive Number Theory: the Classical Bases*, Graduate Texts in Mathematics, vol. 164, Springer, 1996.

[112] D. J. Newman, *Simple analytic proof of the Prime Number Theorem*, Amer. Math. Monthly **87** (1980), 693–696.

[113] O. Ore, *Number Theory and its History*, Dover, New York, 1976.

[114] J. Pintz, *On Legendre's prime number formula*, Amer. Math. Monthly **87** (1980), 733–735.

[115] _____, *On the remainder term of the prime number formula and the zeros of the Riemann zeta-function*, Number Theory (Noordwijkerhout), Lecture Notes in Mathematics, vol. 1068, Springer, 1984, pp. 186–197.

[116] _____, *Very large gaps between consecutive primes*, J. Number Theory **63** (1997), 286–301.

[117] _____, *Recent results on the Goldbach conjecture*, Proceedings of the ELAZ Conference, May 24–28, 2004 (Stuttgart) (W. Schwarz and J. Stending, eds.), Franz Steiner Verlag, 2006, pp. 220–254.

[118] G. Pólya, *Heuristic reasoning in the theory of numbers*, Amer. Math. Monthly **66** (1959), 375–384.

[119] C. Pomerance, *A note on the least prime in an arithmetic progression*, J. Number Theory **12** (1980), 218–223.

[120] _____, *Recent developments in primality testing*, Math. Intellig. **3** (1981), 97–105.

[121] _____, *Alla ricerca dei numeri primi*, Le Scienze **174** (1983), 86–94.

[122] _____, *The quadratic sieve factoring algorithm*, Advances in Cryptology, Proceedings of EUROCRYPT 84, Lecture Notes in Computer Science, vol. 209, Springer, 1985, pp. 169–182.

[123] _____, *Factoring*, Cryptology and computational number theory, Lect. Notes American Mathematical Society Short Course, Boulder, CO (USA), 1989. Proc. Symp. Appl. Math., vol. 42, 1990, pp. 27–47.

[124] _____, *A tale of two sieves*, Notices American Mathematical Society **43** (1996), 1473–1485.

[125] C. Pomerance, J. L. Selfridge, and S. S. Wagstaff, *The pseudoprimes to* $25 \cdot 10^9$, Math. Comp. **35** (1980), 1003–1026.

[126] K. Prachar, *Primzahlverteilung*, Springer, 1957.

[127] O. Ramaré, *On Šnirel'man's constant*, Ann. Scuola Norm. Sup. IV **22** (1995), 645–706.

[128] P. Ribenboim, *The New Book of Prime Numbers Records*, Springer, New York, 1996.

[129] G. F. B. Riemann, *Über die Anzahl der Primzahlen unter einer gegebenen Grösse*, Monatsber. Königl. Preuss. Akad. Wiss. Berlin (1859), 671–680, in "Gesammelte Mathematische Werke" (ed H. Weber), Dover reprint 1953.

[130] H. Riesel, *Prime Numbers and Computer Methods for Factorization*, second ed., Birkhäuser, Boston, 1994.

[131] J. B. Rosser and L. Schoenfeld, *Approximate formulae for some functions of prime numbers*, Illinois J. Math. **6** (1962), 64–94.

[132] W. Rudin, *Functional Analysis*, Mc Graw-Hill, 1973, Reprint TMH, New Delhi (1985).

[133] I. Schur, *Über die Existenz unendlich vieler Primzahlen in einiger speziellen arithmetischen Progressionen*, Sitzungber. Berliner Math. Ges. **11** (1912), 40–50.

[134] A. Selberg, *An elementary proof of the Prime Number Theorem*, Ann. Math. **(2) 50** (1949), 305–313.

[135] D. Shanks, *Solved and Unsolved Problems in Number Theory*, fourth ed., Chelsea, New York, 1993.

[136] G. Tenenbaum and M. Mendès France, *The Prime Numbers and their Distribution*, American Mathematical Society, 2000.

[137] E. C. Titchmarsh, *The Theory of the Riemann Zeta–Function*, second ed., Oxford University Press, Oxford, 1986.

[138] ———, *The Theory of Functions*, second ed., Oxford University Press, Oxford, 1988.

[139] P. Turán, *On a new Method of Analysis and its Applications*, J. Wiley & Sons, New York, 1984.

[140] C. Vanden Eynden, *A proof of Gandhi's formula for the n-th prime*, Amer. Math. Monthly **79** (1982), 625.

[141] R. C. Vaughan, *The Hardy–Littlewood Method*, second ed., Cambridge University Press, Cambridge, 1997.

[142] I. M. Vinogradov, *Some theorems concerning the theory of primes*, Mat. Sb. **N. S. 2** (1937), 179–195 (Russian).

[143] S. Wagon, *Editor's corner: the euclidean algorithm strikes again*, Amer. Math. Monthly **97** (1990), 125–129.

[144] E. Waring, *Meditationes Algebraicæ*, Cambridge, 1770.

[145] A. Weil, *Teoria dei numeri*, Einaudi, Torino, 1993.

[146] E. T. Whittaker and G. N. Watson, *Modern Analysis*, fourth ed., Cambridge University Press, Cambridge, 1927.

[147] N. Wiener, *The Fourier Integral and Certain of its Applications*, Dover, New York, 1958.

[148] T. D. Wooley, *Large improvements in Waring's problem*, Ann. Math. **135** (1992), 131–164.

[149] A. Zaccagnini, *Additive problems with prime numbers*, Rend. Sem. Mat. Univ. Pol. Torino **53** (1995), 471–486, Atti del "Primo Incontro Italiano di Teoria dei Numeri," Roma, 3–5 gennaio 1995.

[150] ———, *Variazioni Goldbach: problemi con numeri primi*, L'Educazione Matematica, Anno XXI, Serie VI **2** (2000), 47–57, `http://people.math.unipr.it/alessandro.zaccagnini/psfiles/papers/Goldbach_I.pdf`.

[151] D. Zagier, *A one-sentence proof that every prime* $p \equiv 1 \mod 4$ *is a sum of two squares*, Amer. Math. Monthly **97** (1990), 144.