Università degli studi di Padova

Dipartimento di Matematica "Tullio Levi-Civita"

Laurea Magistrale in Matematica

Su recenti risultati relativi a piccole distanze tra primi consecutivi

Relatore:
Chiar.mo
Alessandro Languasco

Candidato:
Daniele Mastrostefano
matricola 1130713

Sessione del 21/04/2017
Anno Accademico 2016-2017

Indice

Introduzione **2**

1 Notazioni e prerequisiti **4**
1.1 Definizioni fondamentali 4
1.2 Risultati fondamentali 10

2 Nozioni preliminari **16**
2.1 Primi in progressioni aritmetiche 16
2.2 Stime asintotiche per medie di funzioni aritmetiche 23
2.3 Note sulla teoria dei crivelli 25

3 Il teorema di Maynard **28**
3.1 Insiemi ammissibili e teoria dei crivelli 28
3.2 Il crivello di Goldston-Pintz-Yildirim 31
3.3 Manipolazioni in stile Selberg 33
3.3.1 Stima di S_1 33
3.3.2 Stima di S_2 42
3.4 Relazione tra $y_{r_1,\dots,r_k}$ e $y^{(m)}_{r_1,\dots,r_k}$ 48
3.5 Scelta di una funzione liscia per y 51
3.5.1 Nuova forma per S_1 52
3.5.2 Nuova forma per S_2 56
3.6 1° applicazione alle distanze tra numeri primi 60
3.7 Scelta dei pesi per grandi k 62
3.8 2° applicazione alle distanze tra numeri primi 69
3.9 Scelta dei pesi per piccoli k 71
3.10 3° applicazione alle distanze tra numeri primi 75

Bibliografia **78**

Introduzione

Un problema molto studiato in teoria analitica dei numeri riguarda l'analisi delle distanze tra numeri primi. Uno degli esempi maggiori è dato dalla seguente

Congettura (Congettura dei primi gemelli)**.** Esistono infinite coppie di primi consecutivi, cioè con differenza pari a 2.

Ci sono molte generalizzazioni di questo concetto. Ad esempio:

Congettura (Congettura dei primi gemelli generalizzata)**.** Esistono infinite coppie di primi con distanza $2r$, con r un intero pari.

Nel caso in cui ci siano infinite coppie p, $p+h$ di numeri primi, tale h viene chiamato un numero di de Polignac. Una naturale generalizzazione di quest'ultimo problema riguarda la ricerca di triple o di quadruple composte da numeri primi, invece che di coppie, chiedendo ad esempio di trovare infiniti n tali che $n, n+3, n+5$ siano numeri primi o $10n+1, 10n+3, 10n+5, 10n+7$ siano tutti numeri primi. Bisogna però prestare attenzione ad alcuni casi specifici in cui sono presenti solo un numero finito di n che soddisfano tale condizione. Ad esempio, se si considera $n, n+2, n+4$, troviamo un'unica tripla di primi $3, 5, 7$; se si considera invece $n, n+6, n+12, n+18, n+24$, allora uno tra questi sarà sempre divisibile per 5 e quindi l'unico esempio si ottiene per $n = 5$, per il quale abbiamo $5, 11, 17, 23, 29$. Quindi, ci si potrebbe chiedere:

Congettura (Congettura delle k-uple di primi)**.** Dato un insieme di interi distinti $h_1 < h_2 < ... < h_k$, tali che per ogni primo p esiste almeno un intero n per cui p non divide $n + h_1, ..., n + h_k$, allora esistono infiniti n tali che $n + h_1, ..., n + h_k$ sono tutti primi.

Il matematico Yitang Zhang, lavorando su tale problema, dimostrò per primo l'esistenza di un numero reale positivo B per cui ci sono infinite coppie p_n, p_{n+1} di numeri primi consecutivi per i quali $p_{n+1} - p_n \leq B$ (peraltro dimostrò tale risultato con $B = 70{\cdot}000{\cdot}000$). Lo scopo di questa tesi è quello di affrontare il problema delle piccole distanze tra numeri primi, analizzando l'articolo di Maynard [5], nel quale viene migliorata la stima di Zhang, portando la costante B a 600. A differenza dell'approccio di Zhang, che si basa sull'inserire un forte risultato analitico all'interno del crivello di Goldston-Pintz-Yildirim, Maynard imposta il problema in maniera più elementare, anche se in vari punti della dimostrazione è necessario ricorrere a strumenti tipici del calcolo delle variazioni. L'unica eccezione è data dal teorema di Bombieri-Vinogradov, che viene usato da Maynard in un passaggio cruciale, il

quale è stato dimostrato attraverso l'uso dell'identità di Vaughan [10],[11] e usando il teorema di Siegel-Walfisz, la cui dimostrazione fa uso dell'analisi complessa. Il teorema di Bombieri-Vinogradov riveste un ruolo importante nella dimostazione di Maynard ed un ruolo centrale in gran parte della teoria analitica dei numeri; per questo motivo nel capitolo 2 cercheremo di capire la sua importanza, confrontandolo con i risultati principali nella teoria delle progressioni aritmetiche. Nel capitolo 1 verranno enunciate le definizioni di tutte le funzioni aritmetiche che saranno usate nel seguito ed i risultati di base che verranno richiamati all'occorrenza. Infine, nel capitolo 3 descriveremo in modo dettagliato la dimostrazione di Maynard, presente nell'articolo [5]. Ricordiamo che, basandosi sul risultato di Maynard, un gruppo di matematici, identificatosi con il nome di Polymath, è riuscito ad ottenere il record attuale di $B = 246$ [7]. Riguardo il problema opposto, sullo studio delle grandi distanze tra numeri primi consecutivi, è stato dimostrato da Kevin Ford, Ben Green, Sergei Konyagin, James Maynard e Terence Tao [1] il seguente risultato[1]:

Teorema. Se X è sufficientemente grande, allora:

$$\max_{p_{n+1}\leq X}(p_{n+1}-p_n) \gg \frac{(\log X)(\log\log X)(\log\log\log\log X)}{\log\log\log X}.$$

[1]Nella tesi non verranno trattati né il lavoro del gruppo Polymath né quello sulle grandi distanze tra numeri primi consecutivi.

Capitolo 1

Notazioni e prerequisiti

In questo primo capitolo daremo le definizioni di tutte le funzioni aritmetiche che useremo nel seguito, senza doverle introdurre o richiamare cammin facendo. Inoltre, enunceremo i risultati fondamentali che verranno usati nel capitolo 3, presenti con la loro relativa dimostrazione in qualsiasi libro introduttivo di teoria analitica dei numeri, anche se consigliamo come prima referenza il libro di Montgomery-Vaughan [M-V] [6].

1.1 Definizioni fondamentali

In tutto il successivo trattamento denoteremo sempre con p un numero primo; l, m, n, k verranno usati per denotare numeri naturali e x, y, w, z denoteranno usualmente numeri reali. Con il simbolo $\lfloor x \rfloor$ indicheremo la parte intera di x, il più grande intero minore di x, e con $\{x\}$ la sua parte frazionaria, ovvero $x - \lfloor x \rfloor$. Se $s \in \mathbb{C}$, allora $Re(s)$ indicherà la sua parte reale e $Im(s)$ la sua parte immaginaria. Scrivendo $f(x) \ll g(x)$, per due funzioni reali $f(x), g(x)$ di variabile reale, con $g(x) \geq 0$, intendiamo che esiste $C > 0$ tale che $|f(x)| \leq Cg(x)$. Al posto di $f(x) \ll g(x)$ si può scrivere analogamente $f(x) = O(g(x))$. La relazione $f(x) \gg g(x)$, con $f(x) \geq 0$, indicherà che $|g(x)| \leq Cf(x)$, per un'opportuna costante $C > 0$. Le notazioni $\ll_A$ o $\gg_A$, stanno ad indicare che l'eventuale costante C può dipendere solamente dal parametro A, se $A > 0$ reale. La notazione $f(x) = o(g(x)), x \to x_0$, con f, g come sopra, indica che $\lim_{x \to x_0} \frac{f(x)}{g(x)} = 0$, con $x_0 \in \mathbb{R} \cup \{\pm\infty\}$ da specificare. Similmente, $f(x) \sim g(x), x \to x_0$ indicherà che $\lim_{x \to x_0} \frac{f(x)}{g(x)} = 1$, con x_0 come sopra. La notazione $x \approx y$, per due numeri reali x, y, indicherà che il $|x-y|$ è piccolo rispetto ad altre quantità a cui è rapportato. Se $m, n \in \mathbb{Z}$, denotiamo con (n, m) il loro massimo comun divisore e con $[n, m]$ il loro minimo comune multiplo. Una funzione $f : \mathbb{Z} \to \mathbb{C}$, si dirà una funzione aritmetica. Inoltre, diciamo che $f(n)$ è moltiplicativa se $f(nm) = f(n)f(m)$, quando $(n, m) = 1$; diciamo che è completamente o totalmente moltiplicativa se $f(nm) = f(n)f(m)$ vale per ogni n, m. Con il simbolo $|\mathcal{A}|$ intendiamo la cardinalità dell'insieme $\mathcal{A}$, mentre con $|z|$ il valore assoluto di $z \in \mathbb{C}$. Se $n, m \in \mathbb{Z}$, scriveremo $n|m$, se n divide m, altrimenti scriveremo $n \nmid m$. Una funzione reale $f(x)$ si dirà non negativa se $f(x) \geq 0$ in ogni punto x del suo dominio; se $f(x)$ è > 0, in ogni punto x del suo dominio, si dirà

positiva. Indichiamo con $\mathbb{N}^+, \mathbb{R}^+$ l'insieme dei numeri naturali e reali strettamente maggiori di zero.

Definizione 1.1 (Funzione φ di Eulero)**.** Sia $q \in \mathbb{N}^+$. Definiamo,

$$\varphi(q) = \sum_{\substack{1 \le n \le q \\ (n,q)=1}} 1. \tag{1.1.1}$$

Definizione 1.2 (Funzione enumerativa fattori primi)**.** Definiamo la funzione che conta il numero dei fattori primi presenti in un intero $n \notin \{-1, 0, 1\}$, come:

$$\omega(n) = \sum_{p|n} 1, \tag{1.1.2}$$

altrimenti $\omega(\pm 1) = 0$ e $\omega(0)$ non è ben definito.

Osserviamo che se $n \in \mathbb{N}^+$ allora,

$$2^{\omega(n)} \le \prod_{p|n} p \le n.$$

Definizione 1.3 (Funzione di Möbius)**.**

$$\mu(n) = \begin{cases} (-1)^{\omega(n)} & \text{se } n \ge 1 \text{ non è diviso da alcun quadrato perfetto;} \\ 0 & \text{altrimenti.} \end{cases}$$

Definizione 1.4 (Carattere di Dirichlet)**.** Diciamo che χ è un carattere del gruppo $(\mathbb{Z}/q\mathbb{Z})^*$ se esso è un morfismo di gruppi moltiplicativi tra:

$$\chi : (\mathbb{Z}/q\mathbb{Z})^* \to \mathbb{C}^*, \tag{1.1.3}$$

con q numero naturale non nullo. Dato un $n \in \mathbb{Z}$ con $(n, q) = 1$, definiamo $\chi(n) = \chi(\bar{n})$, ove $\bar{n} \in (\mathbb{Z}/q\mathbb{Z})^*$. Tale definizione si estende in modo naturale a tutti i numeri interi, ponendo χ periodica di periodo q, con $\chi(n) = 0$, se $(n, q) > 1$. L'estensione così ottenuta viene denominata carattere di Dirichlet.

Tra i caratteri di Dirichlet è importante mettere in luce due casi particolari:

Definizione 1.5 (Carattere principale)**.** Un carattere di Dirichlet χ modulo $q \in \mathbb{N}^+$ si dice principale se per ogni n con $(n, q) = 1$ vale $\chi(n) = 1$. Esso viene indicato con χ_0.

Definizione 1.6 (Carattere quadratico)**.** Un carattere di Dirichlet χ modulo $q \in \mathbb{N}^+$ si dice carattere quadratico se $\chi^2(n) = 1$, per ogni n con $(n, q) = 1$.

Definizione 1.7 (Quasiperiodo di un carattere)**.** Sia χ un carattere di Dirichlet modulo $q \in \mathbb{N}^+$. Diciamo che $d \in \mathbb{N}^+$ è un quasiperiodo di χ se per ogni m, n con $(nm, q) = 1$ e $m \equiv n (\mathrm{mod}\ d)$, abbiamo $\chi(m) = \chi(n)$.

Enunciamo qualche proprietà dei quasiperiodi di un carattere:

Teorema 1.1.1. *Sia χ un carattere di Dirichlet modulo $q \in \mathbb{N}^+$. Allora q è un quasiperiodo di χ. 1 è un quasiperiodo di χ se e solo se $\chi = \chi_0$. Il più piccolo quasiperiodo di χ divide q.*

Dimostrazione. Le prime due affermazioni seguono facilmente; per l'ultima, vedi [M-V] [6], Teorema 9.2. □

Ora siamo pronti per enunciare la seguente

Definizione 1.8 (Carattere primitivo)**.** Sia $q \in \mathbb{N}^+$. Un carattere di Dirichlet χ modulo q si dice primitivo se il suo più piccolo quasiperiodo è q stesso.

Dal Teorema 1.1.1, segue che se $q > 1$, il carattere principale χ_0 modulo q non è primitivo. Quando $q = 1$, esiste un solo carattere, ovvero quello principale, automaticamente primitivo. Supponiamo ora $d|q$ e sia χ^* un carattere di Dirichlet modulo d; poniamo:

$$\chi(n) = \begin{cases} \chi^*(n) & \text{se } (n,q) = 1; \\ 0 & \text{altrimenti.} \end{cases}$$

Visto che $\chi(n)$ è una funzione completamente moltiplicativa, ha periodo q e $\chi(n) = 0$ se $(n,q) > 1$, abbiamo che $\chi(n)$ è un carattere di Dirichlet modulo q, che diremo carattere indotto da χ^*. Si può mostrare che vale anche il viceversa, ovvero:

Teorema 1.1.2. *Sia χ un carattere di Dirichlet modulo $q \in \mathbb{N}^+$ e d il più piccolo quasiperiodo di χ. Allora esiste un unico carattere primitivo χ^* modulo d che induce χ.*

Dimostrazione. Vedi [M-V] [6], Teorema 9.2. □

Associato ad ogni carattere di Dirichlet χ viene definita una serie di Dirichlet, ovvero una serie formale del tipo:

$$\sum_{n \geq 1} \frac{a(n)}{n^s},$$

con $a(n) : \mathbb{N}^+ \to \mathbb{C}$ e s variabile complessa. Casi particolari molto interessanti sono i seguenti:

Definizione 1.9 (Funzioni L di Dirichlet e funzione ζ di Riemann)**.** Sia $q \in \mathbb{N}^+$ e χ un carattere di Dirichlet modulo q. Diciamo funzione L di Dirichlet la funzione $L(s,\chi) : \mathbb{C} \to \mathbb{C}$, definita, per $Re(s) > 1$, dalla seguente serie:

$$L(s,\chi) := \sum_{n=1}^{+\infty} \frac{\chi(n)}{n^s}. \tag{1.1.4}$$

Nel caso del carattere principale modulo $q = 1$, la serie L si riduce a:

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

Definizione 1.10 (Funzione caratteristica dei numeri primi)**.** Sia $n \in \mathbb{N}$. Diciamo:

$$\chi_{\mathbb{P}}(n) = \begin{cases} 1 & \text{se } n \text{ è primo;} \\ 0 & \text{altrimenti.} \end{cases} \tag{1.1.5}$$

Definizione 1.11 (Funzione θ di Chebyshev)**.** Sia $x > 0$. Diciamo:

$$\theta(x) = \sum_{p \leq x} \log p. \tag{1.1.6}$$

Definizione 1.12 (Funzione Λ di Von Mangoldt)**.** Sia $n \in \mathbb{N}$. Diciamo:

$$\Lambda(n) = \begin{cases} \log n & \text{se } n = p^k, k \geq 1; \\ 0 & \text{altrimenti.} \end{cases}$$

Definizione 1.13 (Funzione ψ di Chebyshev)**.** Sia $x > 0$. Diciamo:

$$\psi(x) = \sum_{n \leq x} \Lambda(n). \tag{1.1.7}$$

Definizione 1.14 (Funzione enumerativa dei numeri primi)**.** Sia $x > 0$. Diciamo:

$$\pi(x) = \sum_{p \leq x} 1. \tag{1.1.8}$$

Analogamente si definiscono:

Definizione 1.15 (Funzione θ di Chebyshev per progressioni aritmetiche)**.** Sia $x > 0$, $q \in \mathbb{N}^+$, $0 \leq a \leq q$. Diciamo:

$$\theta(x, q, a) = \sum_{\substack{p \leq x \\ p \equiv a (\bmod q)}} \log p. \tag{1.1.9}$$

Definizione 1.16 (Funzione ψ di Chebyshev per progressioni aritmetiche)**.** Sia $x > 0$, $q \in \mathbb{N}^+$, $0 \leq a \leq q$. Diciamo:

$$\psi(x, q, a) = \sum_{\substack{n \leq x \\ n \equiv a (\bmod q)}} \Lambda(n). \tag{1.1.10}$$

Definizione 1.17 (Funzione enumerativa dei numeri primi per progressioni aritmetiche)**.** Sia $x > 0$, $q \in \mathbb{N}^+$, $0 \leq a \leq q$. Diciamo:

$$\pi(x, q, a) = \sum_{\substack{p \leq x \\ p \equiv a (\bmod q)}} 1. \tag{1.1.11}$$

Generalizzando le definizioni date nelle equazioni (1.1.9), (1.1.10), (1.1.11), si possono ottenere facilmente le loro controparti relative a singoli caratteri di Dirichlet:

Definizione 1.18. Sia $q \in \mathbb{N}^+$, χ un carattere di Dirichlet modulo q e $x > 0$. Poniamo,

$$\theta(x,\chi) = \sum_{p \leq x} \chi(p) \log p, \tag{1.1.12}$$

$$\psi(x,\chi) = \sum_{n \leq x} \chi(n)\Lambda(n), \tag{1.1.13}$$

$$\pi(x,\chi) = \sum_{p \leq x} \chi(p). \tag{1.1.14}$$

Infatti, consideriamo ad esempio $\psi(x,q,a)$ (per le altre due funzioni i ragionamenti sono analoghi) e ricordiamo il seguente

Teorema 1.1.3 (Ortogonalità tra caratteri di Dirichlet)**.** *Sia χ un carattere di Dirichlet modulo $q \in \mathbb{N}^+$, allora abbiamo,*

$$\sum_{\substack{1 \leq n \leq q \\ (n,q)=1}} \chi(n) = \begin{cases} \varphi(q) & \text{se } \chi = \chi_0; \\ 0 & \text{altrimenti.} \end{cases} \tag{1.1.15}$$

Se $(n,q) = 1$ allora,

$$\sum_{\chi} \chi(n) = \begin{cases} \varphi(q) & \text{se } n \equiv 1 (\text{mod } q), \\ 0 & \text{altrimenti,} \end{cases} \tag{1.1.16}$$

dove la somma è estesa a tutti i caratteri di Dirichlet modulo $q \in \mathbb{N}^+$.

Dimostrazione. Vedi [M-V] [6], Corollario 4.5. □

È dunque chiaro che se $(a,q) = 1$, con $0 \leq a \leq q$ e $q \in \mathbb{N}^+$ allora,

$$\frac{1}{\varphi(q)} \sum_{\chi} \chi(a)^{-1}\chi(n) = \begin{cases} 1 & \text{se } n \equiv a (\text{mod } q), \\ 0 & \text{altrimenti,} \end{cases} \tag{1.1.17}$$

dove la somma è estesa a tutti i caratteri di Dirichlet modulo $q \in \mathbb{N}^+$. Notiamo che $\chi(a)^{-1} = \chi(a^{-1}) = \overline{\chi(a)}$, per ogni $a \in \mathbb{Z}$, ove $\overline{\chi(a)}$ è il coniugato complesso di $\chi(a)$, visto che χ è un carattere di $(\mathbb{Z}/q\mathbb{Z})^*$. Moltiplicando (1.1.17) per $\Lambda(n)$ e sommando sugli $n \leq x$ si ottiene subito che:

$$\psi(x,q,a) = \frac{1}{\varphi(q)} \sum_{\chi} \chi(a)^{-1}\psi(x,\chi). \tag{1.1.18}$$

Definizione 1.19. Definiamo $\tau_k(n)$ come il numero di modi di scrivere $n \in \mathbb{N}$ come prodotto di $k \in \mathbb{N}$ fattori interi. Osserviamo che $\tau_k(n)$ è una funzione moltiplicativa, tale che nei primi p vale $\tau_k(p) = k$.

Introduciamo ora la costante di Eulero-Mascheroni, che sarà sempre denotata nel seguito con la lettera γ:

Definizione 1.20 (Costante Eulero-Mascheroni)**.**

$$\gamma = \lim_{N\to+\infty} \left(\sum_{n=1}^{N} \frac{1}{n} - \log N \right). \tag{1.1.19}$$

Definizione 1.21 (Funzione Γ)**.** Definiamo la funzione Γ di Eulero attraverso la sua forma integrale:

$$\Gamma(s) = \int_0^{+\infty} e^{-t} t^{s-1} dt, \tag{1.1.20}$$

per ogni s con $Re(s) > 0$. Siccome l'integrale converge normalmente per $Re(s) > 0$, la funzione $\Gamma(s)$ è olomorfa in tale regione.

Ricordiamo inoltre una delle proprietà fondamentali della funzione Γ:

$$\Gamma(k) = (k-1)!, \tag{1.1.21}$$

per ogni $k \in \mathbb{N}^+$. Essa è un caso particolare di:

$$\Gamma(z+1) = z\Gamma(z),$$

valida per ogni $z \in \mathbb{C}$ con $Re(z) > 0$, usando che $\Gamma(1) = 1$. È utile enunciare il seguente

Teorema 1.1.4. *La funzione Γ ammette un'estensione meromorfa in $\mathbb{C}$ con i poli che costituiscono esattamente l'insieme $\{-n : n \in \mathbb{N}\}$.*

Dimostrazione. Infatti, è sufficiente definire per $z \in \mathbb{C} \setminus \{-n : n \in \mathbb{N}\}$:

$$\Gamma(z) = \begin{cases} \displaystyle\int_0^{+\infty} e^{-t} t^{z-1} & \text{se } Re(z) > 0\ ; \\ \\ \displaystyle\frac{\Gamma(z+n+1)}{(z+n)\cdots(z+1)z} & \text{se } Re(z) > -n-1, \text{ con } z \notin \{-n : n \in \mathbb{N}\}, \end{cases} \tag{1.1.22}$$

e utilizzare il principio di identità analitica per dimostrare che $\Gamma(z)$ è ben definita ed olomorfa in $\mathbb{C}\setminus\{-n : n \in \mathbb{N}\}$. Infine, è chiaro che i suoi poli costituiscono esattamente l'insieme $\{-n : n \in \mathbb{N}\}$. □

Si può dimostrare che tale estensione coincide con il seguente prodotto infinito:

Teorema 1.1.5. *Per ogni $s \in \mathbb{C} \setminus \{-n : n \in \mathbb{N}\}$,*

$$\Gamma(s) = \frac{e^{-\gamma s}}{s} \prod_{n=1}^{+\infty} \frac{e^{\frac{s}{n}}}{1+\frac{s}{n}}, \tag{1.1.23}$$

ove γ è la costante di Eulero-Mascheroni (1.1.19).

Dimostrazione. Vedi [M-V] [6], Teorema C.2 . □

Usando (1.1.23) è chiaro che $\frac{1}{\Gamma(s)}$ ammette un'estensione intera, data appunto dall'inverso del prodotto infinito in (1.1.23), con zeri semplici che costituiscono l'insieme $\{-n : n \in \mathbb{N}\}$; ciò è equivalente a dire che $\Gamma(s)$ è una funzione mai nulla e meromorfa su $\mathbb{C}$, con poli semplici che formano l'insieme $\{-n : n \in \mathbb{N}\}$. Similmente introduciamo la funzione β:

Definizione 1.22 (Funzione β)**.**

$$\beta(s,t) = \int_0^1 v^{t-1}(1-v)^{s-1}dv, \tag{1.1.24}$$

per $Re(s), Re(t) > 0$.

Per essa vale:

$$\beta(a,b) = \frac{a!b!}{(a+b+1)!}, \tag{1.1.25}$$

per ogni coppia di interi positivi a, b.

Definizione 1.23 (Logaritmo integrale)**.** Per ogni $x \geq 2$,

$$\mathrm{li}(x) = \int_2^x \frac{dt}{\log t}. \tag{1.1.26}$$

Lo sviluppo asintotico di $\mathrm{li}(x)$ è dato da:

$$\mathrm{li}(x) = x\sum_{k=1}^{K}\frac{(k-1)!}{\log^k x} + O\left(\frac{x}{\log^{K+1} x}\right), x \to +\infty, \tag{1.1.27}$$

per ogni $K \in \mathbb{N}^+$.

1.2 Risultati fondamentali

È immediato verificare la seguente identità:

Teorema 1.2.1.

$$\sum_{d|n}\mu(d) = \begin{cases} 0 & se\ n > 1\ ; \\ 1 & se\ n = 1. \end{cases} \tag{1.2.1}$$

Dimostrazione. Supponiamo $n > 1$. Se n ha k fattori primi, allora è chiaro che:

$$\sum_{d|n}\mu(d) = 1 + (-1)\binom{k}{1} + (-1)^2\binom{k}{2} + ... + (-1)^k\binom{k}{k} = (1-1)^k = 0. \qquad \square$$

Attraverso di essa si può dimostrare la formula di inversione di Möbius:

Teorema 1.2.2. *Siano $f, g : \mathbb{N} \to \mathbb{C}$, tali che per ogni $n \in \mathbb{N}^+$ vale,*

$$g(n) = \sum_{d|n} f(d). \tag{1.2.2}$$

Allora,

$$f(n) = \sum_{d|n} g(d)\mu\left(\frac{n}{d}\right). \tag{1.2.3}$$

Dimostrazione. Infatti, sostituendo (1.2.2) in (1.2.3) e invertendo l'ordine delle somme:

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) g(d) = \sum_{d|n} \mu\left(\frac{n}{d}\right) \sum_{k|d} f(k) = \sum_{k|n} f(k) \sum_{j|\frac{n}{k}} \mu\left(\frac{n}{jk}\right) = f(n). \tag{1.2.4}$$ □

Un'importante applicazione di tale principio di inversione è il seguente

Teorema 1.2.3. *Per ogni $n \geq 1$ abbiamo,*

$$\varphi(n) = n \sum_{d|n} \frac{\mu(d)}{d}, \tag{1.2.5}$$

$$\sum_{d|n} \varphi(d) = n. \tag{1.2.6}$$

Dimostrazione. La prima identità segue immediatamente osservando che:

$$\sum_{d|n} \frac{\mu(d)}{d} = \prod_{p|n} \left(1 - \frac{1}{p}\right) = \frac{\varphi(n)}{n}. \tag{1.2.7}$$

Qui la prima uguaglianza è immediata e la seconda segue usando che $\frac{\varphi(n)}{n}$ è chiaramente una funzione moltiplicativa che nelle potenze dei primi vale:

$$\frac{\varphi(p^a)}{p^a} = \frac{p^{a-1}(p-1)}{p^a} = \frac{p-1}{p} = 1 - \frac{1}{p},$$

per ogni p primo e ogni $a \in \mathbb{N}^+$. La seconda identità segue subito dalla prima applicando il Teorema 1.2.2. □

Un ulteriore identità, che useremo nel seguito, è data da:

Teorema 1.2.4. *Per ogni $n \geq 1$,*

$$\frac{n}{\varphi(n)} = \sum_{d|n} \frac{\mu^2(d)}{\varphi(d)}. \tag{1.2.8}$$

Dimostrazione. Infatti,

$$\sum_{d|n} \frac{\mu^2(d)}{\varphi(d)} = \prod_{p|n} \left(1 + \frac{1}{p-1}\right) = \prod_{p|n} \left(\frac{p}{p-1}\right) = \prod_{p|n} \left(1 - \frac{1}{p}\right)^{-1} = \frac{n}{\varphi(n)}. \tag{1.2.9}$$ □

Riguardo la funzione $\varphi(n)$ riportiamo anche un importante risultato relativo al suo ordine minimale, nel particolare una minorazione asintotica:

Teorema 1.2.5.

$$\varphi(n) \gg \frac{n}{\log\log n}, n \to +\infty. \tag{1.2.10}$$

Dimostrazione. Vedi [M-V] [6], Teorema 2.9 oppure [Tenenbaum] [9], Teorema 4 in 5.3. □

Un'identità fondamentale legata alla funzione Λ è la seguente:

Teorema 1.2.6. *Per ogni $n \geq 1$,*

$$\log n = \sum_{d|n} \Lambda(d). \tag{1.2.11}$$

Dimostrazione. Per $n = 1$ il teorema è vero, visto che entrambi i membri di (1.2.11) sono nulli. Se $n > 1$, scriviamo:

$$n = \prod_{k=1}^{r} p_k^{a_k},$$

per opportuni numeri naturali $r, a_1, ..., a_r$ e primi $p_1, ..., p_r$. Allora abbiamo:

$$\sum_{d|n} \Lambda(d) = \sum_{k=1}^{r} \sum_{m=1}^{a_k} \Lambda(p_k^m) = \sum_{k=1}^{r} \sum_{m=1}^{a_k} \log p_k = \sum_{k=1}^{r} a_k \log p_k = \log n.$$ □

Molto utili sono i seguenti risultati di Mertens:

Teorema 1.2.7. *Per $x \geq 2$ abbiamo,*

$$\sum_{n \leq x} \frac{\Lambda(n)}{n} = \log x + O(1), \tag{1.2.12}$$

$$\sum_{p \leq x} \frac{\log p}{p} = \log x + O(1), \tag{1.2.13}$$

$$\sum_{p \leq x} \frac{1}{p} = \log\log x + b + O\left(\frac{1}{\log x}\right), \tag{1.2.14}$$

$$\prod_{p\leq x}\left(1-\frac{1}{p}\right)^{-1}=e^{\gamma}\log x+O(1), \tag{1.2.15}$$

ove γ è la costante di Eulero-Mascheroni, si veda (1.1.19), e la costante b è definita da:

$$b=\gamma-\sum_{p}\sum_{k=2}^{+\infty}\frac{1}{kp^{k}}.$$

Dimostrazione. Vedi [M-V] [6], Teorema 2.7. □

Teorema 1.2.8 (Teorema dei numeri primi)**.** *Esiste $c>0$ tale che,*

$$\psi(x)=x+O\left(x\exp(-c\sqrt{\log x})\right), \tag{1.2.16}$$

$$\theta(x)=x+O\left(x\exp(-c\sqrt{\log x})\right), \tag{1.2.17}$$

$$\pi(x)=\mathrm{li}(x)+O\left(x\exp(-c\sqrt{\log x})\right), \tag{1.2.18}$$

uniformemente per $x\geq 2$.

Dimostrazione. Vedi [M-V] [6], Teorema 6.9. □

L'equazione (1.2.18), usando (1.1.27), implica che:

$$\pi(x)=\frac{x}{\log x}+O\left(\frac{x}{\log^{2}x}\right), x\to+\infty. \tag{1.2.19}$$

Corollario 1.2.9 (Formula asintotica numeri primi)**.** *Sia $2=p_1<p_2<p_3<...$ la sequenza dei numeri primi. Allora,*

$$p_n\sim n\log n, n\to+\infty. \tag{1.2.20}$$

Dimostrazione. Sappiamo da (1.2.19) che:

$$\lim_{x\to+\infty}\frac{\pi(x)\log x}{x}=1. \tag{1.2.21}$$

Visto che:

$$\log\pi(x)=(1+o(1))\log x, x\to+\infty,$$

da (1.2.21), otteniamo che (1.2.21) stessa si può riscrivere come:

$$\lim_{x\to+\infty}\frac{\pi(x)\log\pi(x)}{x}=1. \tag{1.2.22}$$

Sostituendo $x=p_n$ in (1.2.22) abbiamo,

$$\lim_{n\to+\infty}\frac{n\log n}{p_n}=1, \tag{1.2.23}$$

da cui (1.2.20). □

Notiamo che (1.2.17) e (1.2.18) si ottengono da (1.2.16) per via del seguente

Lemma 1.2.10. *Per ogni $x \geq 2$,*

$$\theta(x) = \psi(x) + O(\sqrt{x}), \tag{1.2.24}$$

$$\pi(x) = \mathrm{li}(x) + \frac{\theta(x) - x}{\log x} + \frac{2}{\log 2} + \int_2^x \frac{\theta(u) - u}{u \log^2 u} du. \tag{1.2.25}$$

Dimostrazione. È chiaro che:

$$\psi(x) = \sum_{p^k \leq x} \log p = \sum_{k=1}^{+\infty} \theta(x^{\frac{1}{k}}).$$

Notiamo che la serie $\sum_{k=1}^{+\infty} \theta(x^{\frac{1}{k}})$ converge, poiché concide con:

$$\sum_{k=1}^{\lfloor \frac{\log x}{\log 2} \rfloor} \theta(x^{\frac{1}{k}}),$$

dal fatto che $\theta(y) = 0$, se $y < 2$. Siccome da (1.2.16) abbiamo $\theta(y) \leq \psi(y) \ll y$, per ogni $y \geq 2$, si ha:

$$\psi(x) - \theta(x) = \sum_{k=2}^{+\infty} \theta(x^{\frac{1}{k}}) \ll \sqrt{x} + \sqrt[3]{x} \log x \ll \sqrt{x}.$$

Così otteniamo (1.2.24) e (1.2.17) si ottiene immediatamente inserendo (1.2.16) in (1.2.24). Per (1.2.25) osserviamo che:

$$\begin{aligned}
\pi(x) &= \int_2^x \frac{d(\theta(u))}{\log u} = \int_2^x \frac{du}{\log u} + \int_2^x \frac{d(\theta(u) - u)}{\log u} \\
&= \mathrm{li}(x) + \frac{\theta(u) - u}{\log u}\Big|_{2^-}^{x} + \int_2^x \frac{\theta(u) - u}{u \log^2 u} du \\
&= \mathrm{li}(x) + \frac{\theta(x) - x}{\log x} + \frac{2}{\log 2} + \int_2^x \frac{\theta(u) - u}{u \log^2 u} du.
\end{aligned}$$

Partendo da (1.2.25) e inserendo (1.2.16) si ottiene subito (1.2.18), osservando che:

$$\begin{aligned}
\frac{\theta(x) - x}{\log x} + \int_2^x \frac{\theta(u) - u}{u \log^2 u} du &= O\left(x \exp(-c\sqrt{\log x}) + \int_2^x \frac{u \exp(-c\sqrt{\log u})}{u \log^2 u} du \right) \\
&= O\left(x \exp(-c\sqrt{\log x}) \right).
\end{aligned}$$

□

Riguardo alle serie di Dirichlet, un risultato di grande importanza è il teorema di Eulero che collega tali serie al loro prodotto infinito su tutti i numeri primi; nel particolare abbiamo:

Teorema 1.2.11 (Prodotto di Eulero)**.** *Per* $Re(s) > \sigma$*,*

$$\sum_{n=1}^{+\infty} \frac{f(n)}{n^s} = \prod_p \left(1 + \frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} + ...\right), \tag{1.2.26}$$

ove supponiamo che $f(n)$ *sia moltiplicativa e che la sua serie di Dirichlet converga assolutamente per* $Re(s) > \sigma \in \mathbb{R}$*. Nel caso in cui* $f(n)$ *sia completamente moltiplicativa, la formula si riduce a:*

$$\sum_{n=1}^{+\infty} \frac{f(n)}{n^s} = \prod_p \left(1 - \frac{f(p)}{p^s}\right)^{-1}. \tag{1.2.27}$$

Dimostrazione. Vedi [M-V] [6], Teorema 1.9. □

Capitolo 2

Nozioni preliminari

2.1 Primi in progressioni aritmetiche

Durante la dimostrazione del teorema di Maynard nel capitolo 3 sarà essenziale l'uso del teorema di Bombieri-Vinogradov. Dato che è un risultato di grande rilievo nella teoria analitica dei numeri, in questo capitolo cercheremo di comprendere la sua importanza, passando attraverso i risultati fondamentali nella teoria dei primi in progressioni aritmetiche. Iniziamo occupandoci della funzione L. La serie (1.1.4) può essere estesa in quasi tutto il piano complesso. Infatti, dato $\chi \neq \chi_0$, carattere di Dirichlet modulo $q \in \mathbb{N}^+$, si può dimostrare che esiste una estensione olomorfa di (1.1.4), che continueremo a chiamare $L(s,\chi)$, su tutto $\mathbb{C}$. Per quanto riguarda $L(s,\chi_0)$ si può solo dimostrare l'esistenza di una estensione meromorfa su $\mathbb{C}$, con unico polo semplice in $s=1$, con residuo $\frac{\varphi(q)}{q}$. Più precisamente, per ogni carattere di Dirichlet χ, definiamo la costante:

$$\kappa = \kappa(\chi) = \begin{cases} 0 & \text{se } \chi(-1) = 1 \ ; \\ 1 & \text{se } \chi(-1) = -1. \end{cases}$$

È possibile dimostrare il seguente risultato:

Teorema 2.1.1. *Sia χ un carattere di Dirichlet primitivo modulo $q > 1$. La funzione:*

$$\xi(s,\chi) = L(s,\chi)\Gamma\left(\frac{s+\kappa}{2}\right)\left(\frac{q}{\pi}\right)^{\frac{s+\kappa}{2}}, \tag{2.1.1}$$

è intera e verifica l'equazione funzionale:

$$\xi(s,\chi) = \varepsilon(\chi)\xi(1-s,\chi^{-1}), \tag{2.1.2}$$

per ogni $s \in \mathbb{C}$, con la costante $\varepsilon(\chi)$ di modulo 1.

Dimostrazione. Vedi [M-V] [6], Corollario 10.8. □

In particolare, visto che $\frac{1}{\Gamma\left(\frac{s+\kappa}{2}\right)}$ e $\left(\frac{\pi}{q}\right)^{\frac{s+\kappa}{2}}$ sono funzioni intere, per via di (1.1.23), dal Teorema 2.1.1 deduciamo che per le funzioni $L(s,\chi)$, con χ carattere primitivo

modulo $q > 1$, esiste un'estensione olomorfa su tutto $\mathbb{C}$. Notiamo che, se un carattere χ^* modulo $d|q$ induce un carattere χ modulo q, è chiaro che:

$$L(s,\chi) = L(s,\chi^*)\prod_{p|q}\left(1-\frac{\chi^*(p)}{p^s}\right), \tag{2.1.3}$$

usando (1.2.26), inizialmente per $Re(s) > 1$. Per ogni carattere χ non principale modulo $q > 1$ sappiamo, dal Teorema 1.1.1 e dal Teorema 1.1.2, che esiste un unico carattere primitivo χ^* non principale modulo $d > 1$, con $d|q$, che induce χ. Data (2.1.3) e visto che $\prod_{p|q}\left(1-\frac{\chi^*(p)}{p^s}\right)$ è una funzione intera, dal Teorema 2.1.1, concludiamo che, per ogni carattere χ non principale modulo $q > 1$, $L(s,\chi)$ ammette un'estensione olomorfa su $\mathbb{C}$. Inoltre, da (2.1.3), gli zeri di $L(s,\chi)$ e $L(s,\chi^*)$ sono gli stessi, eccetto per quelli situati sulla retta $Re(s) = 0$ provenienti da:

$$\prod_{p|q}\left(1-\frac{\chi^*(p)}{p^s}\right) = 0.$$

Quindi, per studiare il luogo degli zeri di $L(s,\chi)$, con $\chi \neq \chi_0$, basta concentrarsi su caratteri primitivi χ modulo $q > 1$. Sia dunque χ carattere primitivo modulo $q > 1$. Sappiamo che esso è una funzione completamente moltiplicativa e che la serie (1.1.4) converge assolutamente per $Re(s) > 1$; usando (1.2.26) si ha che per $Re(s) > 1$,

$$L(s,\chi) = \prod_{p}\left(1-\frac{\chi(p)}{p^s}\right)^{-1},$$

da cui si deduce immediatamente che $L(s,\chi) \neq 0$ per $Re(s) > 1$. Visto che la funzione Γ non ha zeri, per via di (1.1.23), segue da (2.1.1) che $\xi(s,\chi) \neq 0$ per $Re(s) > 1$ e lo stesso vale per $\xi(s,\chi^{-1})$. Da (2.1.2), $\xi(s,\chi) \neq 0$ anche per $Re(s) < 0$ e quindi anche $L(s,\chi) \neq 0$ per $Re(s) < 0$, eccetto nei punti $-\kappa, -\kappa-2, -\kappa-4, ...$, in cui deve avere zeri semplici (i così detti zeri banali) per compensare i poli semplici della funzione $\Gamma\left(\frac{s+\kappa}{2}\right)$. Inoltre, notiamo che se ρ è uno zero non banale di $L(s,\chi)$, da (2.1.2), si ottiene subito che $1-\rho$ è uno zero non banale di $L(s,\chi^{-1})$ e quindi $1-\bar{\rho}$ è uno zero non banale di $L(s,\chi)$, visto che $\bar{\chi} = \chi^{-1}$ e $L(\bar{s},\bar{\chi}) = \overline{L(s,\chi)}$. Qui $\bar{\chi}$ è il coniugato complesso di χ. Le coppie di zeri $\rho, 1-\bar{\rho}$ sono posizionate simmetricamente rispetto alla retta $Re(s) = \frac{1}{2}$. Per tali motivi, si congettura che gli zeri non banali di $L(s,\chi)$ siano tutti piazzati su tale retta. Più in generale è stata enunciata la seguente

Congettura 2.1 (Ipotesi di Riemann Generalizzata (GRH))**.** *Per ogni carattere di Dirichlet χ modulo $q \in \mathbb{N}^+$ tutti gli zeri della funzione $L(s,\chi)$ nel semipiano $Re(s) > 0$ sono disposti sulla retta $Re(s) = \frac{1}{2}$.*

Riemann studiò per primo il luogo degli zeri di $L(s,\chi)$, nel caso speciale dell'unico carattere χ modulo $q = 1$. In tal caso, la funzione in questione si semplifica alla serie $\zeta(s)$ e per essa Riemann dimostrò il seguente

Teorema 2.1.2. *La funzione:*

$$\xi(s) = \frac{1}{2}s(s-1)\zeta(s)\Gamma\left(\frac{s}{2}\right)\left(\frac{1}{\pi}\right)^{\frac{s}{2}}, \tag{2.1.4}$$

è intera e verifica l'equazione funzionale:

$$\xi(s) = \xi(1-s). \tag{2.1.5}$$

Dimostrazione. Vedi [M-V] [6], Corollario 10.3. □

In particolare, con ragionamenti analoghi a quelli svolti per $L(s,\chi)$, deduciamo che per la funzione $\zeta(s)$, esiste un'estensione meromorfa su $\mathbb{C}$, con unico polo semplice in $s = 1$ con residuo 1. Inoltre, a parte gli zeri banali $-2, -4, -6, ...$, situati in $Re(s) < 0$, tutti i suoi zeri si trovano nella striscia $0 < Re(s) < 1$ e sono posizionati simmetricamente rispetto alla retta $Re(s) = \frac{1}{2}$. Da queste considerazioni, Riemann suppose che fossero tutti posti su tale retta. Analizziamo ora il caso di caratteri χ_0 principali di modulo $q > 1$. Dal Teorema 1.1.1, sappiamo che χ_0 ha come più piccolo quasiperiodo $d = 1$. Usando (1.2.26) otteniamo:

$$L(s,\chi_0) = \zeta(s)\prod_{p|q}\left(1 - \frac{1}{p^s}\right), \tag{2.1.6}$$

per $Re(s) > 1$. Visto che $\prod_{p|q}\left(1 - \frac{1}{p^s}\right)$ è una funzione intera, grazie al Teorema 2.1.2 otteniamo che $L(s,\chi_0)$ estende ad una funzione meromorfa su $\mathbb{C}$ con unico polo semplice in $s = 1$ con residuo $\frac{\varphi(q)}{q}$. Inoltre, il luogo degli zeri di $L(s,\chi_0)$ è lo stesso di $\zeta(s)$, ad eccezione degli zeri su $Re(s) = 0$ della forma $\frac{2k\pi i}{\log p}$, con $k \in \mathbb{Z}$ e $p|q$. Dunque, per ogni carattere di Dirichlet χ conosciamo un'estensione di $L(s,\chi)$ su $\mathbb{C}$ e per ognuno di essi possiamo congetturare che gli zeri di $L(s,\chi)$ in $0 < Re(s) < 1$ si trovino in realtà su $Re(s) = \frac{1}{2}$. In tale direzione, abbiamo il seguente

Teorema 2.1.3. *Esiste $c > 0$ tale che, se χ è un carattere di Dirichlet modulo $q \in \mathbb{N}^+$, abbiamo che la regione,*

$$R_q = \left\{s : Re(s) > 1 - \frac{c}{\log(q(|Im(s)| + 4))}\right\}, \tag{2.1.7}$$

non contiene zeri di $L(s,\chi)$, a meno che χ sia un carattere quadratico. In tal caso, $L(s,\chi)$ possiede al più uno zero, necessariamente reale, $\beta < 1$ dentro R_q. Tale zero β si dice eccezionale e il carattere a lui associato χ si dice carattere eccezionale.

Dimostrazione. Vedi [M-V] [6], Teorema 11.3. □

Riguardo alla localizzazione degli zeri eccezionali vale il seguente

Teorema 2.1.4 (Siegel)**.** *Per ogni $\varepsilon > 0$ esiste una costante $C(\varepsilon) > 0$ tale che se χ è un carattere quadratico modulo $q \in \mathbb{N}^+$ e β uno zero reale di $L(s,\chi)$, allora:*

$$\beta < 1 - C(\varepsilon)q^{-\varepsilon}. \tag{2.1.8}$$

Dimostrazione. Vedi [M-V] [6], Corollario 11.15. □

Il prossimo passo consiste nell'enunciare il teorema dei numeri primi per progressioni aritmetiche; a tal fine riportiamo un risultato tecnico sulle serie di Dirichlet:

Teorema 2.1.5 (Formula di Perron con resto)**.** *Sia $a(n) : \mathbb{N} \to \mathbb{C}$ e sia*

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

la sua serie di Dirichlet; sia $\sigma_a \in \mathbb{R}$ l'estremo di convergenza assoluta di $\alpha(s)$, ovvero per ogni $s \in \mathbb{C}$ con $Re(s) > \sigma_a$ la serie $\alpha(s)$ converge assolutamente. Infine, siano $\sigma_0 > \max(0, \sigma_a)$ e $x > 0$. Allora vale,

$$\sum_{n \leq x}{}' a_n = \frac{1}{2\pi i} \int_{\sigma_0 - iT}^{\sigma_0 + iT} \alpha(s) \frac{x^s}{s} ds + R, \tag{2.1.9}$$

con $T > 0$ reale e R un opportuno resto, dipendente da $\alpha(s), T, x$ e σ_0. Qui Σ' indica che se x è intero, allora l'ultimo termine nella somma va contato con peso $1/2$.

Dimostrazione. Vedi [M-V] [6], Teorema 5.2. □

Il prossimo teorema fa da trampolino per il teorema dei numeri primi:

Teorema 2.1.6. *Esiste $c_1 > 0$ tale che, se $q \leq \exp(2c_1\sqrt{\log x})$, allora abbiamo,*

$$\psi(x, \chi) = E_0(\chi)x + O(x \exp(-c_1\sqrt{\log x})), \tag{2.1.10}$$

quando $L(s, \chi)$ non ha zeri eccezionali, e

$$\psi(x, \chi) = -\frac{x^{\beta_1}}{\beta_1} + O(x \exp(-c_1\sqrt{\log x})), \tag{2.1.11}$$

quando $L(s, \chi)$ ha uno zero eccezionale β_1. Qui abbiamo posto:

$$E_0(\chi) = \begin{cases} 1 & \text{se } \chi = \chi_0 \text{ ;} \\ 0 & \text{altrimenti.} \end{cases}$$

Dimostrazione. Descriveremo qui di seguito solo un accenno di dimostrazione, per capire le idee fondamentali usate. Per una dimostrazione completa vedere [M-V] [6], Teorema 11.16. Usando (1.2.26), è facile mostrare che:

$$-\frac{L'(s, \chi)}{L(s, \chi)} = \sum_{n=1}^{+\infty} \frac{\Lambda(n)\chi(n)}{n^s},$$

per $Re(s) > 1$, che inserito nel Teorema 2.1.5, da:

$$\psi(x, \chi) = -\frac{1}{2\pi i} \int_{\sigma_0 - iT}^{\sigma_0 + iT} \frac{L'(s, \chi)}{L(s, \chi)} \frac{x^s}{s} ds + R, \tag{2.1.12}$$

dove scegliamo $2 \leq T \leq x$ e $\sigma_0 = 1 + \frac{1}{\log x}$, per cui si dimostra che $R \ll \frac{x}{T} \log^2 x$. Ora sia $\mathcal{C}$ il contorno integrale chiuso definito da segmenti che uniscono i punti $\sigma_0 - iT$, $\sigma_0 + iT$, $\sigma_1 + iT$, $\sigma_1 - iT$, con σ_1 da scegliere in modo opportuno all'interno di R_q (2.1.7). In particolare, si sceglierà σ_1 dipendente da T in modo che il contorno e l'interno di $\mathcal{C}$ siano contenuti in R_q. Se non ci sono zeri eccezionali, abbiamo che l'integranda è analitica dentro $\mathcal{C}$, se $\chi \neq \chi_0$, altrimenti se $\chi = \chi_0$ ha un polo in $s = 1$ con residuo $-x$. Quindi dal teorema dei residui otteniamo:

$$-\frac{1}{2\pi i} \int_{\mathcal{C}} \frac{L'(s,\chi)}{L(s,\chi)} \frac{x^s}{s} = E_0(\chi) x. \tag{2.1.13}$$

Se esiste uno zero eccezionale β_1, allora l'integranda possiede un polo dentro $\mathcal{C}$ in corrispondenza di β_1 con residuo $\frac{x^{\beta_1}}{\beta_1}$, da cui:

$$-\frac{1}{2\pi i} \int_{\mathcal{C}} \frac{L'(s,\chi)}{L(s,\chi)} \frac{x^s}{s} = -\frac{x^{\beta_1}}{\beta_1}. \tag{2.1.14}$$

In entrambi i casi, scegliendo opportunamente σ_1, si riesce a stimare l'integrale da $\sigma_0 + iT$ a $\sigma_1 + iT$, da $\sigma_1 + iT$ a $\sigma_1 - iT$ e da $\sigma_1 - iT$ a $\sigma_0 - iT$, ottenendo (2.1.10) e (2.1.11). □

Il teorema dei numeri primi per progressioni aritmetiche afferma che:

Teorema 2.1.7 (Page)**.** *Esiste $c > 0$ tale che, dati due numeri interi positivi fissati a, q con $(a, q) = 1$ e $0 \leq a \leq q$, si ha:*

$$\psi(x, q, a) = \frac{x}{\varphi(q)} + O(x \exp(-c\sqrt{\log x})), \tag{2.1.15}$$

quando non ci sono caratteri eccezionali modulo q, altrimenti se χ_1 è un carattere eccezionale modulo q con zero eccezionale associato β_1 allora vale,

$$\psi(x, q, a) = \frac{x}{\varphi(q)} - \frac{\chi_1(a) x^{\beta_1}}{\varphi(q)\beta_1} + O(x \exp(-c\sqrt{\log x})). \tag{2.1.16}$$

Qui tutte le stime sono intese per $x \to +\infty$. Infine, notiamo che è possibile trovare relazioni tra $\psi(x, q, a), \theta(x, q, a), \pi(x, q, a)$ analoghe a quelle descritte nel Lemma 1.2.10, con le quali è immediato enunciare l'equivalente di (2.1.15) e (2.1.16) per $\theta(x, q, a)$ e $\pi(x, q, a)$.

Dimostrazione. Se $q \leq \exp(2c_1\sqrt{\log x})$, allora dobbiamo solo inserire le stime del Teorema 2.1.6 in (1.1.18). Se invece $q \geq \exp(2c_1\sqrt{\log x})$, allora osserviamo che la stima banale $\psi(x, q, a) \leq \left(\frac{x}{q} + 1\right) \log x$, porta immediatamente a:

$$\psi(x, q, a) \ll x \exp(-c_1\sqrt{\log x}). \tag{2.1.17}$$

Ora, visto che $\varphi(q) \gg \sqrt{q}$, si ha che i termini principali in (2.1.15) e (2.1.16) sono chiaramente

$$\ll x \exp(-c_1\sqrt{\log x}).$$

Unendo quest'ultima osservazione con (2.1.17), si ottiene che anche nel caso $q \geq \exp(2c_1\sqrt{\log x})$ le stime (2.1.15) e (2.1.16) continuano a valere, anche se banalmente. Otteniamo così il teorema. □

I precedenti risultati, come il teorema dei numeri primi, valgono per valori di q fissati. Aggiungendo un'ipotesi più restrittiva su q, possiamo eliminare la presenza dei termini dipendenti dai caratteri eccezionali, ottenendo un risultato uniforme in q.

Teorema 2.1.8. *Sia c_1 come nel Teorema 2.1.6. Per ogni $A > 0$ esiste $x_0(A)$ tale che, se $0 < q \leq (\log x)^A$ reale, allora per ogni carattere χ modulo $q \in \mathbb{N}^+$ abbiamo,*

$$\psi(x, \chi) = E_0(\chi)x + O(x \exp(-c_1\sqrt{\log x}), \tag{2.1.18}$$

per $x \geq x_0(A)$.

Dimostrazione. Dal Teorema 2.1.6, abbiamo che se non ci sono zeri eccezionali, vale:

$$\psi(x, \chi) = E_0(\chi)x + O(x \exp(-c_1\sqrt{\log x}),$$

se $q \leq \exp(2c_1\sqrt{\log x})$. Quindi, tale stima vale a maggior ragione per ogni $q \leq (\log x)^A$, per ogni $A > 0$, se $x \geq x_0(A)$ con $x_0(A)$ un opportuno numero reale. Supponiamo ora che χ sia quadratico e che $L(s, \chi)$ abbia uno zero eccezionale β_1. Allora,

$$x^{\beta_1} = x \exp(-(1 - \beta_1) \log x) \leq x \exp(-C(\varepsilon)q^{-\varepsilon} \log x), \tag{2.1.19}$$

per il Teorema 2.1.4. Visto che $q \leq \log^A x$, (2.1.19) diventa:

$$\leq x \exp(-C(\varepsilon)(\log x)^{1-A\varepsilon}). \tag{2.1.20}$$

Se scegliamo $\varepsilon = \frac{1}{3A}$, abbiamo che (2.1.20) diventa:

$$\leq x \exp(-c_1\sqrt{\log x}), \tag{2.1.21}$$

se $x \geq x_0 := \exp\big(\big(\frac{c_1}{C(\varepsilon)}\big)^6\big)$. Quindi otteniamo (2.1.18) per ogni carattere χ e con essa il teorema. □

Combinando il Teorema 2.1.8 con (1.1.18) otteniamo il seguente

Teorema 2.1.9 (Siegel-Walfisz)**.** *Sia c_1 come nel Teorema 2.1.6. Per ogni $A > 0$ esiste $x_0(A) \in \mathbb{R}$ tale che, se $0 < q \leq (\log x)^A$ reale e $(a, q) = 1$ con $0 \leq a \leq q$, per ogni $x \geq x_0(A)$ abbiamo,*

$$\psi(x, q, a) = \frac{x}{\varphi(q)} + O_A(x \exp(-c_1\sqrt{\log x})). \tag{2.1.22}$$

Usando l'analogo di (1.2.24) e di (1.2.25) per $\theta(x, q, a)$ e $\pi(x, q, a)$ si ottengono facilmente le rispettive versioni di (2.1.22) per queste due funzioni.

Dimostrazione. L'equazione (2.1.22) segue subito combinando (2.1.18) con (1.1.18). Per maggiori dettagli, vedere [M-V] [6], Corollario 11.19 e Corollario 11.21. □

Si può mettere in luce un'esplicita relazione tra il teorema dei numeri primi per progressioni aritmetiche e l'Ipotesi di Riemann Generalizzata, sintetizzata nel seguente

Teorema 2.1.10 (Formula esplicita)**.** *Sia $c > 1$ e χ un carattere modulo q. Per $x \geq c$ e $T \geq 2$, esiste un'opportuna funzione $E(x, T, \chi)$ tale che:*

$$\psi(x, \chi) = E_0(\chi)x - \sum_{\substack{\rho: \\ |\gamma| \leq T}} \frac{x^\rho}{\rho} + E(x, T, \chi), \tag{2.1.23}$$

ove la somma è estesa agli zeri ρ di $L(s, \chi)$ con $\rho = \beta + i\gamma$, con $0 < \beta < 1$ e $|\gamma| \leq T$.

Dimostrazione. Vedi [M-V] [6], Teorema 12.12. □

In questa direzione concludiamo osservando che:

Teorema 2.1.11. *Per ogni $x \geq 2$, fissato $q \in \mathbb{N}^+$ e preso $0 \leq a \leq q$ con $(a, q) = 1$, supponendo vera la Congettura 2.1 per ogni funzione $L(s, \chi)$, con χ modulo q, abbiamo:*

$$\psi(x, q, a) = \frac{x}{\varphi(q)} + O(\sqrt{x} \log^2 x). \tag{2.1.24}$$

Dimostrazione. Basta inserire (2.1.23) in (1.1.18), stimando opportunamente il contributo degli zeri di $L(s, \chi)$ alla somma in (2.1.23), usando la Congettura 2.1. Per maggiori dettagli vedere [M-V] [6], Corollario 13.8. □

Notiamo che banalmente:

$$0 \leq \psi(x, q, a) \leq (\log x) \sum_{\substack{0 \leq n \leq x \\ n \equiv a (\bmod q)}} 1 \leq (\log x)\left(1 + \frac{x}{q}\right). \tag{2.1.25}$$

Quindi la stima (2.1.24) è peggiore di (2.1.25), se $q > \sqrt{x}$. Se invece $q \leq x^\theta$, con $\theta < \frac{1}{2}$, (2.1.24) fornisce un termine d'errore migliore di quello presente nel Teorema 2.1.7. Nonostante ciò si può dimostrare che (2.1.24) vale in media su $q \leq x^\theta$, con $\theta < \frac{1}{2}$, e senza l'uso di GRH. Infatti, è stato dimostrato il seguente

Teorema 2.1.12 (Bombieri-Vinogradov)**.** *Per ogni costante $A > 0$, uniformemente in $Q \geq 1$ e in $x \geq 1$, abbiamo,*

$$\sum_{q \leq Q} \max_{\substack{(a,q)=1 \\ y \leq x}} \left| \psi(y, q, a) - \frac{y}{\varphi(q)} \right| \ll_A \frac{x}{\log^A x} + \sqrt{x} Q (\log xQ)^4. \tag{2.1.26}$$

Dimostrazione. Vedi [Vaughan] [10] e [11]. □

Un risultato analogo vale anche per le funzioni $\theta(x, q, a)$ e $\pi(x, q, a)$. Osserviamo che (2.1.26), in media su q, è forte quanto avere GRH per tutti i caratteri χ di tutti i moduli $q \leq \frac{\sqrt{x}}{\log^{A+4} x}$. Inoltre, usando per ogni termine nella sommatoria di (2.1.26) la stima banale $\left(\frac{x}{q} + 1\right) \log x$, otteniamo la maggiorazione banale:

$$\ll x \log x \log Q + Q \log x. \tag{2.1.27}$$

Si vede facilmente che (2.1.27) è una stima migliore di quella del Teorema 2.1.12, se $Q > \sqrt{x}$. Quindi in realtà il teorema è valido, con tutta la sua forza, in media per $Q \leq \sqrt{x}$. Nel capitolo 3 useremo una formulazione più debole del Teorema 2.1.12, o meglio, della sua versione con $\pi(x, q, a)$ al posto di $\psi(x, q, a)$. Più precisamente,

Definizione 2.1 (Livello di distribuzione numeri primi)**.** Diciamo che i primi hanno livello di distribuzione $\theta > 0$, se per ogni $A > 0$, $q \in \mathbb{N}^+$, $0 \leq a \leq q$ e per ogni $x > 1$, vale:

$$\sum_{q \leq x^\theta} \max_{(a,q)=1} \left| \pi(x,q,a) - \frac{\pi(x)}{\varphi(q)} \right| \ll_A \frac{x}{\log^A x}. \tag{2.1.28}$$

Il teorema che useremo nel capitolo 3 è il seguente:

Teorema 2.1.13 (Bombieri-Vinogradov)**.** *I primi hanno livello di distribuzione θ per ogni $\theta < 1/2$.*

La più importante congettura legata a tale teorema afferma che:

Congettura 2.2 (Elliott-Halberstam)**.** *I primi hanno livello di distribuzione θ per ogni $\theta < 1$.*

2.2 Stime asintotiche per medie di funzioni aritmetiche

Nel capitolo 3 incontreremo molti esempi del tipo: data una funzione aritmetica $f(n)$, stimare dall'alto $\sum_{n \leq x} f(n)$, per $x \to +\infty$. Nel caso in cui la funzione in questione $f(n)$ sia non negativa e moltiplicativa, ci possiamo appellare ad un risultato sorprendentemente facile e di grande applicazione:

Proposizione 2.2.1 (Rankin)**.** *Sia $f(n) \geq 0$ e moltiplicativa. Allora per ogni $x \geq 1$ si ha che,*

$$\sum_{n \leq x} f(n) \leq \prod_{p \leq x} \sum_{l \geq 0} f(p^l). \tag{2.2.1}$$

Dimostrazione. Possiamo supporre che tutte le somme $\sum_{l \geq 0} f(p^l)$ convergano, altrimenti il risultato è banale. In tal caso, se sviluppiamo il prodotto a destra di (2.2.1) troviamo immediatamente:

$$\prod_{p \leq x} \sum_{l \geq 0} f(p^l) = \sum_{\substack{n \geq 1 \\ p|n \Rightarrow p \leq x}} f(n),$$

usando la moltiplicatività di f. Infine, dalla non negatività di f otteniamo:

$$\sum_{\substack{n \geq 1 \\ p|n \Rightarrow p \leq x}} f(n) \geq \sum_{n \leq x} f(n). \qquad \square$$

Ora passiamo ad un'utile risultato che ricalca quello di Rankin:

Teorema 2.2.2. *Sia f una funzione non negativa e moltiplicativa tale che per ogni $x \geq 1$,*

$$\sum_{p \leq x} f(p) \log p \ll x, \tag{2.2.2}$$

$$\sum_{p^k, k \geq 2} \frac{f(p^k) k \log p}{p^k} \ll 1. \tag{2.2.3}$$

Allora per ogni $x > 1$,

$$\sum_{n \leq x} f(n) \ll \frac{x}{\log x} \prod_{p \leq x} \sum_{l \geq 0} \frac{f(p^l)}{p^l}. \tag{2.2.4}$$

Dimostrazione. La stima (2.2.4) si ottiene sommando le seguenti due stime:

$$\sum_{n \leq x} f(n) \log\left(\frac{x}{n}\right) \ll x \sum_{n \leq x} \frac{f(n)}{n}, \tag{2.2.5}$$

$$\sum_{n \leq x} f(n) \log n \ll x \sum_{n \leq x} \frac{f(n)}{n}. \tag{2.2.6}$$

La (2.2.5) è immediata, siccome $f \geq 0$ e

$$\log\left(\frac{x}{n}\right) \ll \frac{x}{n},$$

uniformemente per $1 \leq n \leq x$. Per via di (1.2.11), la (2.2.6) diventa:

$$\sum_{d \leq x} \Lambda(d) \sum_{m \leq x/d} f(md). \tag{2.2.7}$$

Scrivendo $d = p^i, m = p^j r$, con $p \nmid r$, osserviamo che (2.2.7) corrisponde a:

$$\sum_{\substack{p, i \geq 1, j \geq 0 \\ p^{i+j} \leq x}} f(p^{i+j}) \log p \sum_{\substack{r \leq x/p^{i+j} \\ p \nmid r}} f(r) = \sum_{\substack{p,k \\ p^k \leq x}} k \log p f(p^k) \sum_{\substack{r \leq x/p^k \\ p \nmid r}} f(r), \tag{2.2.8}$$

in cui abbiamo posto $i + j = k$. Omettiamo ora la condizione $p \nmid r$ e consideriamo il contributo delle potenze proprie di primi. Stimando:

$$\sum_{r \leq x/p^k} f(r) \leq \sum_{r \leq x/p^k} \frac{x}{r p^k} f(r),$$

osserviamo che i termini in (2.2.8), per i quali $k \geq 2$, contribuiscono con un:

$$\ll x \sum_{\substack{p^k \leq x \\ k \geq 2}} \frac{\log(p^k) f(p^k)}{p^k} \sum_{r \leq x/p^k} \frac{f(r)}{r} \ll x \sum_{n \leq x} \frac{f(n)}{n}, \tag{2.2.9}$$

usando l'ipotesi (2.2.3). Rimane da stimare:

$$\sum_{p\le x} f(p)\log p \sum_{r\le x/p} f(r) = \sum_{r\le x} f(r) \sum_{p\le x/r} f(p)\log p \ll x\sum_{r\le x}\frac{f(r)}{r}, \tag{2.2.10}$$

per l'ipotesi (2.2.2). Infine, applicando (2.2.1) alla funzione non negativa e moltiplicativa $\frac{f(n)}{n}$ si ottiene che:

$$\sum_{n\le x}\frac{f(n)}{n} \le \prod_{p\le x}\sum_{l\ge 0}\frac{f(p^l)}{p^l},$$

che unito a (2.2.5) e (2.2.6) da (2.2.4). □

2.3 Note sulla teoria dei crivelli

Lo scopo della teoria dei crivelli è quello di stimare il numero di interi rimasti in un insieme dopo che i suoi membri appartenenti a certe progressioni aritmetiche siano stati tolti. Se P è un numero naturale non nullo fissato, definiamo:

$$S(x,y,P) = |\{n : x < n \le x+y, (n,P)=1\}|,$$

per $y>0$ e $x\in\mathbb{R}$. Il primo risultato in questa direzione è il seguente

Teorema 2.3.1 (Eratostene-Legendre)**.** *Sia $P\in\mathbb{N}^+$. Per ogni reale x e ogni $y\ge 0$ vale,*

$$S(x,y,P) = \frac{\varphi(P)}{P}y + O(2^{\omega(P)}). \tag{2.3.1}$$

Dimostrazione. Se $\chi_P(n)$ è la funzione caratteristica degli interi n coprimi con P, è chiaro che:

$$S(x,y,P) = \sum_{x<n\le x+y}\chi_P(n) = \sum_{x<n\le x+y}\sum_{\substack{d|n\\ d|P}}\mu(d) = \sum_{d|P}\mu(d)\sum_{\substack{x<n\le x+y\\ d|n}} 1 \tag{2.3.2}$$

$$= \sum_{d|P}\mu(d)\left(\left\lfloor\frac{x+y}{d}\right\rfloor - \left\lfloor\frac{x}{d}\right\rfloor\right) = y\sum_{d|P}\frac{\mu(d)}{d} + O\left(\sum_{d|P}|\mu(d)|\right),$$

dove abbiamo usato in successione (1.2.1), ovvero che $\chi_P(n) = \sum_{d|(n,P)}\mu(d)$, e (1.2.5), ottenendo (2.3.1). □

Riassumiamo qui di seguito alcuni risultati sul crivello di Selberg che useremo nel capitolo 3. Ci ispireremo a quanto presentato in [M-V] [6] e per una lettura più approfondita rimandiamo ad [Selberg] [8].

Teorema 2.3.2. *Siano x,y,z numeri reali tali che $y>0$ e $z\ge 1$. Per ogni intero positivo P abbiamo,*

$$S(x,y,P) \le \frac{y}{L_P(z)} + O\left(\frac{z^2}{L_P(z)^2}\right), \tag{2.3.3}$$

dove

$$L_P(z) = \sum_{\substack{n\le z\\ n|P}} \frac{\mu(n)^2}{\varphi(n)}. \tag{2.3.4}$$

Dimostrazione. Sia Λ_n una funzione aritmetica reale con $\Lambda_1 = 1$. Allora,

$$\left(\sum_{d|n}\Lambda_d\right)^2 \ge \begin{cases} 1 & \text{se } n = 1;\\ 0 & \text{se } n > 1.\end{cases}$$

Usando tale disuguaglianza con (n, P) al posto di n, otteniamo:

$$S(x,y,P) = \sum_{\substack{x<n\le x+y\\ (n,P)=1}} 1 \le \sum_{x<n\le x+y}\left(\sum_{\substack{d|n\\ d|P}}\Lambda_d\right)^2 = \sum_{\substack{d|P\\ e|P}}\Lambda_d\Lambda_e \sum_{\substack{x<n\le x+y\\ d|n\\ e|n}} 1 \tag{2.3.5}$$

$$= \sum_{\substack{d|P\\ e|P}}\Lambda_d\Lambda_e\left(\left\lfloor\frac{x+y}{[d,e]}\right\rfloor - \left\lfloor\frac{x}{[d,e]}\right\rfloor\right) = y\sum_{\substack{d|P\\ e|P}}\frac{\Lambda_d\Lambda_e}{[d,e]} + O\left(\left(\sum_{d|P}|\Lambda_d|\right)^2\right).$$

Vista la definizione di $L_P(z)$ possiamo assumere che P sia libero da quadrati. Visto che $[d,e](d,e) = de$, usando (1.2.6), osserviamo che:

$$\frac{1}{[d,e]} = \frac{(d,e)}{de} = \frac{1}{de}\sum_{f|d,f|e}\varphi(f). \tag{2.3.6}$$

Quindi,

$$\sum_{d|P,e|P}\frac{\Lambda_d\Lambda_e}{[d,e]} = \sum_{f|P}\varphi(f)\sum_{\substack{d:\\ f|d|P}}\frac{\Lambda_d}{d}\sum_{\substack{e:\\ f|e|P}}\frac{\Lambda_e}{e} = \sum_{f|P}\varphi(f)y_f^2, \tag{2.3.7}$$

dove

$$y_f = \sum_{\substack{d:\\ f|d|P}}\frac{\Lambda_d}{d}. \tag{2.3.8}$$

Il cambiamento di variabili (2.3.8) è lineare e non singolare, cioè dati i vari y_f, esiste un'unica funzione Λ_d tale che (2.3.8) sia soddisfatta. Infatti, usando il Teorema 1.2.2, troviamo che:

$$\Lambda_d = d\sum_{\substack{f:\\ d|f|P}} y_f\mu\left(\frac{f}{d}\right). \tag{2.3.9}$$

In più da (2.3.8) e (2.3.9) osserviamo che $\Lambda_d = 0$ per $d > z$ se e solo se $y_f = 0$ per $f > z$. Quindi abbiamo diagonalizzato la forma quadratica in (2.3.5) e da (2.3.9) osserviamo che la restrizione $\Lambda_1 = 1$ è equivalente alla condizione lineare:

$$\sum_{f|P} y_f\mu(f) = 1. \tag{2.3.10}$$

Ora cerchiamo il valore di y_f che rende minimo (2.3.7) usando la tecnica del completamento del quadrato:

$$\sum_{f|P} \varphi(f) y_f^2 = \sum_{\substack{f|P \\ f\leq z}} \varphi(f)\left(y_f - \frac{\mu(f)}{\varphi(f)L_P(z)}\right)^2 + \frac{1}{L_P(z)}. \tag{2.3.11}$$

Chiaramente la parte destra di (2.3.11) è minimizzata per:

$$y_f = \frac{\mu(f)}{\varphi(f)L_P(z)}, \tag{2.3.12}$$

per $f \leq z$ e notiamo che tale scelta di y_f soddisfa (2.3.10). Dunque il minimo della forma quadratica in (2.3.5) soggetta a $\Lambda_1 = 1$ è esattamente $\frac{1}{L_P(z)}$. Unendo questo con (2.3.5) otteniamo il termine principale in (2.3.3). Trattiamo ora il termine d'errore in (2.3.5). Siccome P è libero da quadrati, da (2.3.9) e da (2.3.12) osserviamo che:

$$\Lambda_d = \frac{d}{L_P(z)} \sum_{\substack{f: \\ d|f|P \\ f\leq z}} \frac{\mu(f)\mu(f/d)}{\varphi(f)} = \frac{d\mu(d)}{L_P(z)\varphi(d)} \sum_{\substack{m|P \\ (m,d)=1 \\ m\leq z/d}} \frac{\mu(m)^2}{\varphi(m)}, \tag{2.3.13}$$

in cui abbiamo posto $m = \frac{f}{d}$. Quindi,

$$\sum_{d\leq z} |\Lambda_d| \leq \frac{1}{L_P(z)} \sum_{d\leq z} \frac{d}{\varphi(d)} \sum_{m\leq z/d} \frac{1}{\varphi(m)} = \frac{1}{L_P(z)} \sum_{m\leq z} \frac{1}{\varphi(m)} \sum_{d\leq z/m} \frac{d}{\varphi(d)}. \tag{2.3.14}$$

Usando (1.2.8), otteniamo che:

$$\sum_{d\leq w} \frac{d}{\varphi(d)} = \sum_{r\leq w} \frac{\mu^2(r)}{\varphi(r)} \left\lfloor \frac{w}{r} \right\rfloor \leq w \sum_r \frac{\mu^2(r)}{r\varphi(r)} \ll w, \tag{2.3.15}$$

per ogni $w \in \mathbb{N}^+$, in cui abbiamo usato che:

$$\sum_r \frac{\mu^2(r)}{r\varphi(r)} \ll 1, \tag{2.3.16}$$

visto il risultato (1.2.10) sull'ordine minimale di $\varphi(n)$. Inserendo (2.3.15) in (2.3.14) otteniamo:

$$\sum_{d\leq z} |\Lambda_d| \ll \frac{z}{L_P(z)} \sum_{m\leq z} \frac{1}{m\varphi(m)} \ll \frac{z}{L_P(z)}. \tag{2.3.17}$$

Qui abbiamo usato:

$$\sum_m \frac{1}{m\varphi(m)} \ll 1, \tag{2.3.18}$$

che deriva immediatamente dalla stima su $\varphi(m)$ data da (1.2.10). Inserendo anche (2.3.17) in (2.3.5) otteniamo (2.3.3) e quindi il risultato. □

Capitolo 3

Il teorema di Maynard

In questo capitolo cercheremo di analizzare in modo dettagliato la dimostrazione di Maynard [5] sull'esistenza di infinite coppie di primi con distanza limitata.

3.1 Insiemi ammissibili e teoria dei crivelli

Iniziamo subito con la definizione più importante in questo ambito:

Definizione 3.1 (Insieme ammissibile)**.** Un insieme $\mathcal{H} = \{h_1, ..., h_k\}$ di interi non negativi distinti si dice ammissibile se per ogni primo p, esiste un intero a_p tale che $a_p \not\equiv h (\text{mod } p)$ per ogni $h \in \mathcal{H}$.

Si può vedere facilmente che tale condizione è equivalente a: per ogni p primo esiste n tale che $n + h_1, ..., n + h_k$ non sono divisibili per p (consideriamo ad esempio $a_p = -n$). Un modo semplice di produrre insiemi ammissibili di k elementi è quello di prendere $\mathcal{H} = \{p_{\pi(k)+1}, ..., p_{\pi(k)+k}\}$, ove con p_n indichiamo l'ennesimo numero primo. Infatti, per ogni primo $p < p_{\pi(k)+1}$ possiamo prendere $a_p = 0$, visto che $p \nmid p_{\pi(k)+j}$ per tutti gli $j = 1, ..., k$ ed i k elementi in $\mathcal{H}$ non ricoprono tutte le classi residuali per ogni $p \geq p_{\pi(k)+1}$, visto che, per definizione, $p_{\pi(k)}$ è il più grande primo più piccolo di k e dunque $p_{\pi(k)+1}$ è il più piccolo primo più grande di k. In generale se $p > k$ possiamo trovare sempre un intero a_p tale che $a_p \not\equiv h (\text{mod } p)$, per ogni $h \in \mathcal{H}$. Ora siamo pronti ad enunciare la principale congettura:

Congettura 3.1 (Congettura delle k-uple di primi)**.** *Sia $\mathcal{H} = \{h_1, ..., h_k\}$ ammissibile. Allora ci sono infiniti interi n tali che tutti i numeri $n + h_1, ..., n + h_k$ sono primi.*

Quando $k > 1$ (il caso $k = 1$ è un caso speciale trattato dal teorema di Dirichlet, vedere ad esempio [M-V] [6], Corollario 4.10) nessun caso di tale congettura è ancora noto. Ci si può chiedere se le richieste nella Definizione 3.1 siano veramente necessarie per assicurarsi che tutti i k elementi $n+h_1, ..., n+h_k$ siano primi. Infatti, se esistesse p primo tale che per ogni n esiste $i = i(n)$ con $n+h_i \equiv 0 (\text{ mod } p)$, allora solo un numero finito di interi m potrebbe far sì che tutti i numeri $m + h_1, ..., m + h_k$ siano primi: se esistesse un numero infinito di tali interi m, possiamo sceglierne uno m_1, ed un indice

associato $i(m_1)$, tali che $m_1+h_{i(m_1)} \equiv 0(\text{ mod } p)$, da cui $m_1+h_{i(m_1)} = p$. Supponiamo che $h_1 < ... < h_k$. Consideriamo un altro intero m_2 con $m_2 + h_1 > m_1 + h_k$; allora esisterebbe $i(m_2)$ tale che $m_2 + h_{i(m_2)} \equiv 0(\text{mod } p)$. Quindi $m_2 + h_{i(m_2)} = p$, da cui otteniamo un assurdo $(p > p)$.

Osservazione 3.1. È facile verificare il viceversa della Congettura 3.1: se esistono infiniti interi n per i quali $n + h_j$ è primo per ogni $j = 1, ..., k$, allora per ogni primo p esiste $x(\text{mod } p)$ tale che $x + h_j \not\equiv 0(\text{mod } p)$, per ogni $1 \leq j \leq k$.

Dimostrazione. Infatti, supponiamo per assurdo che esista p primo tale che per ogni x esiste $j = 1, ..., k$ con $x + h_j \equiv 0(\text{mod } p)$. Allora per ipotesi esisterà un x con $x + h_i$ primo per ogni $i = 1, ..., k$, dunque necessariamente $x + h_j = p$. Ma ora basta scegliere, grazie all'ipotesi, un x più grande di quello precedente e ripetere il ragionamento appena esposto per trovare una contraddizione. □

Usando i risultati della teoria dei crivelli esposti in [Greaves] [4], nel particolare il Teorema 2 nella sezione 2.2.2 e il Teorema 3 nella sezione 2.2.3, si può maggiorare il numero degli $n \leq x$ per cui la Congettura 3.1 è vera. Dato $\mathcal{H} = \{h_1, ..., h_k\}$ insieme ammissibile, definiamo:

$$f(X) = \prod_{i=1}^{k}(X + h_i),$$

$$\rho(d) = |\{n : 0 \leq n \leq d, f(n) \equiv 0(\text{mod } d)\}|,$$

per ogni $d \in \mathbb{N}$ e infine

$$C = \prod_p \left(1 - \frac{1}{p}\right)^k \left(1 - \frac{\rho(p)}{p}\right)^{-1}.$$

Allora possiamo provare che:

Teorema 3.1.1.

$$|\{n : 1 \leq n \leq x \text{ } e \text{ } n + h_i \text{ } primo \text{ } \forall i = 1, ..., k\}|$$

$$\leq 2^k k! C \frac{x}{\log^k x}\left(1 + O\left(\frac{\log\log x}{\log x}\right)\right),$$

per $x \to +\infty$.

Dimostrazione. Poniamo:

$$\mathcal{B} = \{n \mid 1 \leq n \leq x, n + h_i \text{ } primo \text{ } \forall i = 1, ..., k\},$$

$$\mathcal{A} = \{f(n) \mid 1 \leq n \leq x\}$$

e infine

$$P = P(z) = \prod_{p \leq z} p,$$

con $z \in \mathbb{R}$. Poniamo:

$$\mathcal{A}_d = \{n \in \mathcal{A} : n \equiv 0(\text{mod } d)\},$$

$$r(d) = |\mathcal{A}_d| - \frac{\rho(d)}{d}x,$$

per ogni $d \in \mathbb{N}$. Allora otteniamo,

$$|\mathcal{A}_d| = \frac{\rho(d)}{d}x + r(d).$$

Dalla teoria generale sugli zeri di un polinomio su un campo finito è chiaro che $\rho(p) \leq k$ e $\rho(p) = k$ se gli $h_i(\bmod p)$ sono tutti distinti; in questo modo solo un numero finito di p verificano $\rho(p) < k$. Definiamo:

$$S(\mathcal{A}, P) = |\{n \in \mathcal{A} : (n, P) = 1\}|,$$

$$\mathcal{C} = \{n \mid 1 \leq n \leq x, n + h_i \; primo \; > z, \forall i\},$$

ove poniamo $z = \sqrt{D}$, con $D \geq 2$. Allora $|\mathcal{C}| \leq S(\mathcal{A}, P)$, poiché per ogni $n \in \mathcal{C}$ l'elemento $f(n)$ di $\mathcal{A}$ è chiaramente coprimo con P. Inoltre, $|\mathcal{B}| = |\mathcal{C}| + |\mathcal{B} \setminus \mathcal{C}| \leq S(\mathcal{A}, P) + |\mathcal{B} \setminus \mathcal{C}|$. Osserviamo che se $n \in \mathcal{B} \setminus \mathcal{C}$ si ha che esiste $j \in \{1, ..., k\}$ tale che $n + h_j$ è primo minore di z e dunque l'elemento $f(n)$ non viene contato in $S(\mathcal{A}, P)$, dato che $(f(n), P) \neq 1$. In particolare $|\mathcal{B} \setminus \mathcal{C}| \leq z$. Usando i risultati in [Greaves] [4], nel particolare il Teorema 2 in 2.2.2 e il Teorema 3 in 2.2.3, e seguendo le notazioni ivi introdotte osserviamo che:

$$S(\mathcal{A}, P) \leq \frac{x}{G(\sqrt{D})} + E(D, P), \tag{3.1.1}$$

con

$$G(\sqrt{D}) \geq \frac{e^{-\gamma k}}{\Gamma(k+1)V(P(\sqrt{D}))}\left(1 + O\left(\frac{1}{\log D}\right)\right), D \to +\infty, \tag{3.1.2}$$

in cui γ è la costante di Eulero-Mascheroni definita nella (1.1.19) e $E(D, P)$ un opportuno resto che grazie al Teorema 3 nella sezione 2.2.3 in [Greaves] [4], verifica:

$$E(D, P) < \frac{D}{\log^2 D}. \tag{3.1.3}$$

Qui abbiamo posto, per $x \in \mathbb{R}$ e $n \in \mathbb{N}$,

$$G(x) = \sum_{\substack{n<x \\ n|P}} g(n),$$

con

$$g(n) = \begin{cases} \frac{\rho(n)}{\rho^*(n)} & \text{se } n \text{ è libero da quadrati;} \\ 0 & \text{altrimenti,} \end{cases}$$

ove $\rho^*(n)$ è la funzione moltiplicativa definita sui primi da: $\rho^*(p) = p - \rho(p)$. Inoltre, abbiamo anche posto:

$$V(P(z)) = \prod_{p|P(z)}\left(1 - \frac{\rho(p)}{p}\right),$$

per $z \in \mathbb{R}$. Da (1.2.15) deduciamo che:
(3.1.4)
$$G(\sqrt{D}) \geq \frac{\log^k(\sqrt{D})}{k!}\left(1+O\left(\frac{1}{\log D}\right)\right)\prod_{p\leq\sqrt{D}}\left(1-\frac{1}{p}\right)^k\left(1-\frac{\rho(p)}{p}\right)^{-1}, D\to+\infty.$$

Possiamo stimare facilmente:

$$\prod_{p>\sqrt{D}}\left(1-\frac{1}{p}\right)^k\left(1-\frac{\rho(p)}{p}\right)^{-1} = \exp\left(\sum_{p>\sqrt{D}} k\log\left(1-\frac{1}{p}\right)-\log\left(1-\frac{\rho(p)}{p}\right)\right) \tag{3.1.5}$$

$$= \exp\left(\sum_{p>\sqrt{D}}\frac{-k}{p}+O\left(\frac{1}{p^2}\right)-\left(\frac{-k}{p}+O\left(\frac{1}{p^2}\right)\right)\right) = \exp\left(\sum_{p>\sqrt{D}} O\left(\frac{1}{p^2}\right)\right)$$

$$= \exp\left(O\left(\frac{1}{\sqrt{D}}\right)\right) = 1+O\left(\frac{1}{\sqrt{D}}\right), D\to+\infty.$$

Quindi combinando (3.1.1), (3.1.3), (3.1.4), (3.1.5) e il fatto che $|\mathcal{B}| \leq S(\mathcal{A},P)+\pi(\sqrt{D})$ otteniamo che:

$$|\mathcal{B}| \leq \pi(\sqrt{D})+\frac{x2^k k!}{\log^k D}C\left(1+O\left(\frac{1}{\log D}\right)\right)+\frac{D}{\log^2 D}+\sqrt{D}, D\to+\infty. \tag{3.1.6}$$

Ora possiamo prendere $D=\frac{x}{\log^k x}$, così il termine principale in (3.1.6) diventa:
(3.1.7)
$$\frac{x2^k k!C}{\log^k\left(\frac{x}{\log^k(x)}\right)} = \frac{x2^k k!C}{\log^k x}\frac{1}{(1-\frac{\log(\log^k x)}{\log x})^k} = \frac{x2^k k!C}{\log^k x}\left(1+O\left(\frac{\log\log x}{\log x}\right)\right), x\to+\infty,$$

visto che $(1-\frac{\log(\log^k x)}{\log x})^{-k} = 1+O_k(\frac{\log^k(\log^k x)}{\log^k x}) = 1+O_k(\frac{\log\log x}{\log x})$. Il termine d'errore in (3.1.6) diventa:

$$\frac{x}{\log^k x}\frac{1}{\log^2\left(\frac{x}{\log^k x}\right)} \sim \frac{x}{\log^{k+2} x}, x\to+\infty \tag{3.1.8}$$

e visto che gli ultimi due termini $\pi(\sqrt{D})$ e $\sqrt{D}$ sono $\leq\sqrt{x}$, otteniamo che:

$$|\mathcal{B}| \leq 2^k k!C\frac{x}{\log^k x}\left(1+O\left(\frac{\log\log x}{\log x}\right)\right). \tag{3.1.9}$$

□

3.2 Il crivello di Goldston-Pintz-Yildirim

La Congettura 3.1 è tutt'oggi aperta, ma il lavoro svolto nel tentativo di dimostrarla ha condotto a risultati importanti sullo studio delle piccole distanze tra numeri primi, come emergerà dal lavoro di Maynard. Si può però dimostrare che tale congettura vale per una proporzione positiva di insiemi ammissibili di k elementi. Per provare tali fatti dobbiamo mostrare che se $\mathcal{H}=\{h_1,...,h_k\}$ è un insieme ammissibile

allora esiste $r = r(k) > 0$ per cui esistono infiniti interi n con almeno r numeri primi tra gli $n + h_i$, $i = 1, ..., k$. In particolare, si ottiene che:

$$\liminf_{n\to+\infty}(p_{n+r-1} - p_n) \leq \max_{1\leq i,j\leq k}(h_i - h_j).$$

Vediamo ora le fondamenta del crivello GPY; per una lettura più approfondita rimandiamo a [Goldston-Pintz-Yildirim] [2] e [3]. L'idea di base è quella di considerare la seguente somma:

$$S(N,\rho) = \sum_{N\leq n<2N}\left(\sum_{i=1}^{k}\chi_{\mathbb{P}}(n+h_i) - \rho\right)w_n, \tag{3.2.1}$$

ove $\chi_{\mathbb{P}}$ è la funzione (1.1.5), $\rho > 0$ e w_n sono pesi non negativi. Se mostriamo che $S(N,\rho) > 0$ allora almeno un termine nella somma rispetto ad n deve essere positivo e quindi dalla non negatività degli w_n si ha che deve esistere un intero $n \in [N, 2N]$ tale che almeno $\lfloor\rho+1\rfloor$ degli $n+h_i$ sono primi. In particolare, ci sono infiniti intervalli di lunghezza limitata che contengono $\lfloor\rho+1\rfloor$ primi: si consideri ad esempio $[n, n+B]$, con $B = \max_{i=1,...,k} h_i$. Goldston, Pintz and Yildirim usarono:

$$w_n = \left(\sum_{\substack{d|\prod_{i=1}^{k}(n+h_i)\\ d<R}}\lambda_d\right)^2, \tag{3.2.2}$$

con

$$\lambda_d = \mu(d)F\left(\log\left(\frac{R}{d}\right)\right)^{k+l}, R \in \mathbb{R}^+, l \in \mathbb{N}, \tag{3.2.3}$$

usando un'opportuna funzione liscia F. Ma in questo modo ottennero solo risultati condizionali (ovvero sotto l'uso di una forte congettura enunciata da Elliott e Halberstam, che vedremo successivamente) relativamente allo studio del $\liminf_{n\to+\infty}(p_{n+h} - p_n)$, con $h \in \mathbb{N}$, e risultati incondizionali mostrando ad esempio che:

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

L'importanza del risultato di Maynard sta nell'aver superato le limitazioni presenti in questo metodo ottenendo risultati non condizionali sulla distanza tra primi consecutivi e migliorando al contempo i risultati ottenuti in questa direzione, come il risultato di Zhang [12]. Maynard riuscì in questo considerando la somma (3.2.1) e utilizzando come pesi:

$$w_n = \begin{cases} \left(\sum_{d_i|(n+h_i),\forall i}\lambda_{d_1,...,d_k}\right)^2 & \text{se } n \equiv v_0 (\text{mod } W);\\ 0 & \text{altrimenti,}\end{cases} \tag{3.2.4}$$

con v_0, W opportuni interi che descriveremo dopo, considerando un'opportuna funzione $\lambda_{d_1,...,d_k}$ che espliciteremo nel seguito. Sostituendo (3.2.4) in (3.2.1) risulta evidente

che per stimare $S = S(N, \rho)$ è sufficiente stimare le due somme:

$$S_1 = \sum_{\substack{N \leq n < 2N \\ n \equiv v_0 (\bmod W)}} \left(\sum_{d_i | (n+h_i), \forall i} \lambda_{d_1,\dots,d_k} \right)^2 \tag{3.2.5}$$

e

$$S_2 = \sum_{\substack{N \leq n < 2N \\ n \equiv v_0 (\bmod W)}} \left(\sum_{i=1}^{k} \chi_{\mathbb{P}}(n + h_i) \right) \left(\sum_{d_i | (n+h_i), \forall i} \lambda_{d_1,\dots,d_k} \right)^2. \tag{3.2.6}$$

3.3 Manipolazioni in stile Selberg

Usando ragionamenti analoghi a quelli già visti nel capitolo 2 o a quelli presenti in [Selberg] [8], riusciamo a riscrivere tali somme in una forma più maneggevole. Scegliamo $w_n = 0$ a meno che $n \equiv v_0 (\bmod W)$, dove poniamo:

$$W = \prod_{p \leq D_0} p \tag{3.3.1}$$

e

$$D_0 = \log\log\log N. \tag{3.3.2}$$

Osserviamo che dal teorema cinese dei resti possiamo scegliere v_0 con $v_0 + h_i$ coprimo con W, per ogni $i = 1, ..., k$, visto che abbiamo fissato $\mathcal{H} = \{h_1, ..., h_k\}$ ammissibile. D'ora in poi assumiamo che i primi abbiano livello di distribuzione θ e poniamo:

$$R = N^{\theta/2-\delta}, \delta > 0. \tag{3.3.3}$$

Restringiamo il supporto di $\lambda_{d_1,\dots,d_k}$ alle k-uple per le quali il prodotto $d = \prod_{i=1}^{k} d_i$ verifichi $d < R$, $(d, W) = 1$, $\mu^2(d) = 1$, cosicché in particolare $(d_i, d_j) = 1$, per tutti gli $i \neq j$. Infine, notiamo che avendo fissato k e un insieme ammissibile $\mathcal{H} = \{h_1, ..., h_k\}$, ogni costante implicita nelle notazioni asintotiche o, O, oppure $\ll$ potrebbe dipendere da k o da $\mathcal{H}$; inoltre, tutte le notazioni asintotiche si intenderanno rispetto al limite $N \to +\infty$.

3.3.1 Stima di S_1

Iniziamo con lo stimare la somma S_1 usando il seguente

Lemma 3.3.1. *Siano $r_1, ..., r_k \in \mathbb{N}$ e $\lambda_{d_1,\dots,d_k}$ funzioni reali di $d_1, ..., d_k \in \mathbb{N}$, con il supporto ristretto alle k-uple per cui il prodotto $d = \prod_{i=1}^{k} d_i$ verifichi $d < R$, $(d, W) = 1$, $\mu^2(d) = 1$. Siano anche:*

$$y_{r_1,\dots,r_k} = \left(\prod_{i=1}^{k} \mu(r_i)\varphi(r_i) \right) \sum_{\substack{d_1,\dots,d_k \\ r_i | d_i, \forall i}} \frac{\lambda_{d_1,\dots,d_k}}{\prod_{i=1}^{k} d_i}, \tag{3.3.4}$$

(3.3.5) $$y_{max} = \sup_{r_1,...,r_k} |y_{r_1,...,r_k}|.$$

Allora,

(3.3.6) $$S_1 = \frac{N}{W} \sum_{r_1,...,r_k} \frac{y^2_{r_1,...,r_k}}{\prod_{i=1}^k \varphi(r_i)} + O\bigg(\frac{y^2_{max}\varphi(W)^k N \log^k R}{W^{k+1} D_0}\bigg),$$

dove S_1 è definito nella (3.2.5).

Dimostrazione. Per ottenere il risultato desiderato usiamo tecniche analoghe a quelle già usate nel capitolo 2 per stimare (2.3.3): ovvero espandiamo il quadrato e scambiamo l'ordine delle somme per poi usare un opportuno cambio di variabili. Così facendo otteniamo:

(3.3.7)
$$S_1 = \sum_{\substack{N\le n<2N \\ n\equiv v_0(\bmod W)}} \bigg(\sum_{d_i|(n+h_i),\forall i} \lambda_{d_1,...,d_k} \bigg)^2 = \sum_{\substack{d_1,...,d_k \\ e_1,...,e_k}} \lambda_{d_1,...,d_k}\lambda_{e_1,...,e_k} \sum_{\substack{N\le n<2N \\ n\equiv v_0(\bmod W) \\ [d_i,e_i]|n+h_i,\forall i=1,...,k}} 1.$$

Dal teorema cinese dei resti, la somma interna può essere riscritta come una somma su una singola classe residuale a modulo $q = W\prod_{i=1}^k [d_i, e_i]$, a patto che gli interi $W, [d_1, e_1], ..., [d_k, e_k]$ siano coprimi a due a due. Infatti, dal supporto di $\lambda_{d_1,...,d_k}$ è chiaro che $(W, [d_i, e_i]) = 1$, per ogni $i = 1, ..., k$ e quindi le congruenze della forma:

$$\begin{cases} n \equiv v_0 (\bmod\ W); \\ n \equiv -h_i (\bmod\ [d_i, e_i]), \end{cases}$$

sono soddisfatte se e solo se $(W, [d_i, e_i]) = 1$. Per quanto riguarda le congruenze della forma:

$$\begin{cases} n \equiv -h_j (\bmod\ [d_j, e_j]); \\ n \equiv -h_i (\bmod\ [d_i, e_i]), \end{cases}$$

esse sono soddisfatte se e solo se $(d_ie_i, d_je_j)|(h_j - h_i)$. Dal supporto di $\lambda_{d_1,...,d_k}$ è chiaro che, se esiste un primo $p|(d_ie_i, d_je_j)$, vale $p > D_0$ e siccome D_0 può essere scelto arbitrariamente grande usando un opportuno N, possiamo supporre che $p > h_k > ... > h_1$; da qui è chiaro che la congruenza $h_j \equiv h_i (\bmod\ p)$ non ha soluzione e dunque troviamo che $([d_i, e_i], [d_j, e_j]) = 1$. Quindi, se gli interi $W, [d_1, e_1], ..., [d_k, e_k]$ non sono a due a due coprimi la somma interna in (3.3.7) è nulla. In caso contrario essa diventa:

(3.3.8) $$\sum_{\substack{N\le n<2N \\ n\equiv a(\bmod q)}} 1 = \bigg\lfloor \frac{2N-a}{q} \bigg\rfloor - \bigg\lfloor \frac{N-a}{q} \bigg\rfloor = \frac{N}{q} + O(1).$$

Quindi otteniamo:

(3.3.9) $$S_1 = \frac{N}{W} \sum_{\substack{d_1,...,d_k \\ e_1,...,e_k}}{}' \frac{\lambda_{d_1,...,d_k}\lambda_{e_1,...,e_k}}{\prod_{i=1}^k [d_i, e_i]} + O\bigg(\sum_{\substack{d_1,...,d_k \\ e_1,...,e_k}}{}' |\lambda_{d_1,...,d_k}\lambda_{e_1,...,e_k}| \bigg),$$

dove Σ' denota la restrizione per cui $W, [d_1, e_1], ..., [d_k, e_k]$ siano coprimi a coppie. Poniamo $\lambda_{max} = \sup_{d_1,...,d_k} |\lambda_{d_1,...,d_k}|$. Ricordiamo che $\lambda_{d_1,...,d_k}$ è diverso da zero solo quando $d = \prod_{i=1}^{k} d_i < R$ e d è libero da quadrati. Il termine d'errore in (3.3.9) contribuisce dunque per un

$$\ll \lambda_{max}^2 R^2 \log^{2k} R, \tag{3.3.10}$$

perché:

$$\Bigg(\sum_{\substack{d_1,...,d_k \\ e_1,...,e_k}}{}' |\lambda_{d_1,...,d_k} \lambda_{e_1,...,e_k}| \Bigg) \leq \Bigg(\sum_{d_1,...,d_k} |\lambda_{d_1,...,d_k}| \Bigg)^2 \leq \lambda_{max}^2 \Bigg(\sum_{\substack{d_1,...,d_k \\ d=\prod_{i=1}^{k} d_i < R}} \mu^2(d) \Bigg)^2$$

$$= \lambda_{max}^2 \Bigg(\sum_{d<R} \mu^2(d) \tau_k(d) \Bigg)^2 \ll \lambda_{max}^2 R^2 \log^{2k} R.$$

Infatti, resta da dimostrare che:

$$\sum_{d<R} \mu^2(d) \tau_k(d) \ll R \log^k R. \tag{3.3.11}$$

A tal fine ci appelliamo alla Proposizione 2.2.1:

$$\sum_{d<R} \mu^2(d) \tau_k(d) \leq \sum_{d<R} \frac{R}{d} \mu^2(d) \tau_k(d) \leq R \prod_{p \leq R} \left(1 + \frac{k}{p} \right) \leq R \exp \left(\sum_{p \leq R} \frac{k}{p} \right) \ll R \log^k R,$$

per il risultato di Mertens (1.2.14). Attraverso le identità:

$$\frac{1}{[d_i, e_i]} = \frac{(d_i, e_i)}{d_i e_i} = \frac{1}{d_i e_i} \sum_{u_i | (d_i, e_i)} \varphi(u_i), \tag{3.3.12}$$

ove usiamo (1.2.6), possiamo riscrivere il termine principale in (3.3.9) come:

$$\frac{N}{W} \sum_{u_1,...,u_k} \left(\prod_{i=1}^{k} \varphi(u_i) \right) \sum_{\substack{d_1,...,d_k \\ e_1,...,e_k \\ u_i | (d_i, e_i), \forall i}}{}' \frac{\lambda_{d_1,...,d_k} \lambda_{e_1,...,e_k}}{\left(\prod_{i=1}^{k} d_i \right) \left(\prod_{i=1}^{k} e_i \right)}. \tag{3.3.13}$$

Ricordiamo che $\lambda_{d_1,...,d_k}$ è supportata sugli interi $d_1, ..., d_k$ con $(d_i, W) = 1$ per ogni i e $(d_i, d_j) = 1$, per ogni $i \neq j$. In questo modo possiamo omettere nella sommatoria la richiesta che W sia coprimo con ognuno dei $[d_i, e_i]$; similmente possiamo omettere la richiesta che i numeri d_i siano tutti coprimi tra loro. L'unica restrizione rimanente e proveniente dalla coprimalità di $W, [d_1, e_1], ..., [d_k, e_k]$ è che $(d_i, e_j) = 1$, per ogni $i \neq j$. Quindi, usando (1.2.1), per rimuovere questa richiesta moltiplichiamo per:

$$\sum_{s_{i,j} | (d_i, e_j)} \mu(s_{i,j}),$$

per ogni $i \neq j$. Quindi (3.3.13) diventa:
(3.3.14)

$$\frac{N}{W}\sum_{u_1,\dots,u_k}\Big(\prod_{i=1}^{k}\varphi(u_i)\Big)\sum_{s_{i,j},i\neq j}\Big(\prod_{\substack{1\leq i,j\leq k\\ i\neq j}}\mu(s_{i,j})\Big)\sum_{\substack{d_1,\dots,d_k\\ e_1,\dots,e_k\\ u_i|(d_i,e_i),\forall i\\ s_{i,j}|(d_i,e_j),\forall i\neq j}}\frac{\lambda_{d_1,\dots,d_k}\lambda_{e_1,\dots,e_k}}{(\prod_{i=1}^{k}d_i)(\prod_{i=1}^{k}e_i)}.$$

Ma ora possiamo restringere gli $s_{i,j}$ ad essere coprimi con u_i, u_j, perché i termini con $s_{i,j}$ non coprimo con u_i o u_j non danno contributo nella somma. Infatti, se ad esempio $(s_{i,j}, u_i) > 1$ allora esisterebbe $p|s_{i,j}, u_i$, da cui $p|e_i, e_j$ e quindi $\lambda_{e_1,\dots,e_k} = 0$. Similmente possiamo restringere la nostra somma agli $s_{i,j}$ coprimi con $s_{i,a}, s_{b,j}$, per ogni $a \neq j$ e $b \neq i$, perché se ad esempio $(s_{i,j}, s_{i,a}) > 1$ allora esisterebbe $p|s_{i,j}, s_{i,a}$, da cui $p|d_i, e_j$ e $p|d_i, e_a$ e quindi $p|(e_j, e_a)$, con $j \neq a$, e dunque $\lambda_{e_1,\dots,e_k} = 0$. Lo stesso vale per il caso $(s_{i,j}, s_{b,j}) > 1$. Introduciamo ora il cambio di variabili (3.3.4); questo cambio di variabili è invertibile. Infatti, per $d_1, ..., d_k$ con $\prod_{i=1}^{k} d_i$ libero da quadrati, calcoliamo:
(3.3.15)

$$\sum_{\substack{r_1,\dots,r_k\\ d_i|r_i,\forall i}}\frac{y_{r_1,\dots,r_k}}{\prod_{i=1}^{k}\varphi(r_i)}=\sum_{\substack{r_1,\dots,r_k\\ d_i|r_i,\forall i}}\prod_{i=1}^{k}\mu(r_i)\sum_{\substack{e_1,\dots,e_k\\ r_i|e_i,\forall i}}\frac{\lambda_{e_1,\dots,e_k}}{\prod_{i=1}^{k}e_i}=\sum_{e_1,\dots,e_k}\frac{\lambda_{e_1,\dots,e_k}}{\prod_{i=1}^{k}e_i}\sum_{\substack{r_1,\dots,r_k\\ d_i|r_i|e_i,\forall i}}\prod_{i=1}^{k}\mu(r_i).$$

Ora scriviamo $r_i = d_i f_i$, con $f_i|\frac{e_i}{d_i}$, e usiamo che tutte le variabili coinvolte sono supposte essere libere da quadrati; quindi tutte le funzioni moltiplicative in gioco si possono considerare in questo caso completamente moltiplicative. Questa osservazione verrà riutilizzata parecchie volte nel seguito ma senza indicazione esplicita. Fissati $d_1, ..., d_k, e_1, ..., e_k$, abbiamo:

$$\sum_{\substack{r_1,\dots,r_k\\ d_i|r_i|e_i,\forall i}}\prod_{i=1}^{k}\mu(r_i)=\prod_{i=1}^{k}\sum_{\substack{r_i:\\ d_i|r_i|e_i,\forall i}}\mu(r_i)=\prod_{i=1}^{k}\mu(d_i)\sum_{f_i|\frac{e_i}{d_i}}\mu(f_i). \tag{3.3.16}$$

Grazie a (1.2.1), l'espressione (3.3.16) è uguale a:

$$\begin{cases}\prod_{i=1}^{k}\mu(d_i) & \text{se e soltanto se } e_i = d_i, \forall i;\\ 0 & \text{altrimenti.}\end{cases}$$

Otteniamo che (3.3.15) diventa:

$$\frac{\lambda_{d_1,\dots,d_k}}{\prod_{i=1}^{k}\mu(d_i)d_i}. \tag{3.3.17}$$

Quindi ogni scelta di $y_{r_1,\dots,r_k}$, supportata sugli $r_1, .., r_k$ con il prodotto $r = \prod_{i=1}^{k} r_i$ libero da quadrati che soddisfa $r < R$ e $(r, W) = 1$, ci darà una opportuna scelta di $\lambda_{d_1,\dots,d_k}$ e viceversa. Poniamo $y_{max} = \sup_{r_1,\dots,r_k} |y_{r_1,\dots,r_k}|$. Usando (1.2.8), ovvero nel nostro caso:

$$\frac{d}{\varphi(d)} = \sum_{e|d}\frac{1}{\varphi(e)}, \tag{3.3.18}$$

per valori d liberi da quadrati, da (3.3.15) e (3.3.17) troviamo che:

$$\lambda_{max} \leq \sup_{\substack{d_1,\dots,d_k \\ \mu^2(\prod_{i=1}^k d_i)=1}} y_{max}\left(\prod_{i=1}^k d_i\right) \sum_{\substack{d_1,\dots,d_k \\ d_i|r_i,\forall i \\ \prod_{i=1}^k r_i<R \\ \mu^2(\prod_{i=1}^k r_i)=1}} \left(\frac{\prod_{i=1}^k \mu(r_i)^2}{\varphi(r_i)}\right). \tag{3.3.19}$$

Usando $r_i = d_i f_i$, con $r' = \prod_{i=1}^k f_i$, otteniamo:

$$\lambda_{max} \leq \sup_{\substack{d_1,\dots,d_k \\ \mu^2(\prod_{i=1}^k d_i)=1}} y_{max}\left(\prod_{i=1}^k \frac{d_i}{\varphi(d_i)}\right) \sum_{\substack{r'<\frac{R}{\prod_{i=1}^k d_i} \\ (r',\prod_{i=1}^k d_i)=1}} \frac{\mu(r')^2\tau_k(r')}{\varphi(r')} \tag{3.3.20}$$

e grazie all'equazione (3.3.18) otteniamo:

$$\lambda_{max} \leq \sup_{d_1,\dots,d_k} y_{max} \sum_{d|\prod_{i=1}^k d_i} \frac{\mu(d)^2}{\varphi(d)} \sum_{\substack{r'<\frac{R}{\prod_{i=1}^k d_i} \\ (r',\prod_{i=1}^k d_i)=1}} \frac{\mu(r')^2\tau_k(r')}{\varphi(r')} \tag{3.3.21}$$

$$\leq y_{max} \sum_{u<R} \frac{\mu(u)^2\tau_k(u)}{\varphi(u)} \ll y_{max} \log^k R,$$

dove abbiamo usato $u = dr'$ e il fatto che chiaramente $\tau_k(dr') \geq \tau_k(r')$. Infine, per stimare la parte finale di (3.3.21), abbiamo usato che, dall'equazione (2.2.1) e da (1.2.14), si ha:

$$\sum_{u<R} \frac{\mu(u)^2\tau_k(u)}{\varphi(u)} \leq \prod_{p\leq R}\left(1+\frac{k}{p-1}\right) \leq \exp\left(\sum_{p\leq R}\frac{k}{p-1}\right) \ll_k \log^k R. \tag{3.3.22}$$

Quindi il termine d'errore in (3.3.9) che sappiamo essere $O(\lambda_{max}^2 R^2 \log^{2k} R)$ è dell'ordine di $O(y_{max}^2 R^2 \log^{4k} R)$. Ora sostituendo l'equazione (3.3.4) nel termine principale di (3.3.9) e usando la stima appena trovata per il termine d'errore, abbiamo

$$S_1 = \frac{N}{W} \sum_{u_1,\dots,u_k} \left(\prod_{i=1}^k \varphi(u_i)\right) \sideset{}{^*}\sum_{s_{i,j},i\neq j} \prod_{\substack{1\leq i,j\leq k \\ i\neq j}} \mu(s_{i,j}) \left(\prod_{i=1}^k \frac{\mu(a_i)\mu(b_i)}{\varphi(a_i)\varphi(b_i)}\right) y_{a_1,\dots,a_k} y_{b_1,\dots,b_k} \tag{3.3.23}$$

$$+O(y_{max}^2 R^2 \log^{4k} R),$$

dove $a_j = u_j \prod_{i\neq j} s_{j,i}$ e $b_j = u_j \prod_{i\neq j} s_{i,j}$, denotando con Σ^* la somma sugli $s_{i,j}$ coprimi con u_i, u_j e con $s_{i,a}, s_{b,j}$, per ogni $a \neq j$ e $b \neq i$. Infatti,

$$\sum_{\substack{d_1,\dots,d_k \\ e_1,\dots,e_k \\ u_i|(d_i,e_i),\forall i \\ s_{i,j}|(d_i,e_j),\forall i\neq j}} \frac{\lambda_{d_1,\dots,d_k}\lambda_{e_1,\dots,e_k}}{(\prod_{i=1}^k d_i)(\prod_{i=1}^k e_i)} \tag{3.3.24}$$

$$= \sum_{\substack{d_1,\dots,d_k\\ e_1,\dots,e_k\\ u_i|(d_i,e_i),\forall i\\ s_{i,j}|(d_i,e_j),\forall i\neq j}} \frac{\lambda_{d_1,\dots,d_k}\lambda_{e_1,\dots,e_k}}{\big(\prod_{i=1}^k d_i\big)\big(\prod_{i=1}^k e_i\big)} \prod_{i=1}^k \frac{\mu(a_i)\mu(b_i)}{\varphi(a_i)\varphi(b_i)} \prod_{i=1}^k \frac{\varphi(a_i)\varphi(b_i)}{\mu(a_i)\mu(b_i)}$$

e ora usando la (3.3.17) con $a_1,...,a_k$ e $b_1,...,b_k$ al posto di $r_1,...,r_k$ e raccogliendo in modo ovvio i termini si ottiene (3.3.23). Notare che possiamo scrivere $\mu(a_j) = \mu(u_j)\prod_{i\neq j}\mu(s_{j,i})$ e $\mu(b_j) = \mu(u_j)\prod_{i\neq j}\mu(s_{i,j})$, perché abbiamo ristretto gli $s_{i,j}$ ad essere coprimi con gli altri termini nell'espressione per a_i, b_j; lo stesso vale per $\varphi(a_j), \varphi(b_j)$. Quindi da (3.3.23) abbiamo:

(3.3.25)

$$S_1 = \frac{N}{W}\sum_{u_1,\dots,u_k}\Big(\prod_{i=1}^k \frac{\mu(u_i)^2}{\varphi(u_i)}\Big)\sideset{}{^*}\sum_{s_{i,j},i\neq j}\prod_{\substack{1\leq i,j\leq k\\ i\neq j}}\frac{\mu(s_{i,j})}{\varphi(s_{i,j})^2} y_{a_1,\dots,a_k}y_{b_1,\dots,b_k} + O(y_{max}^2 R^2\log^{4k} R).$$

Ma ora osserviamo che non c'è contributo dagli $s_{i,j}$ con $(s_{i,j}, W) \neq 1$ a causa del supporto di y. Quindi dobbiamo solo considerare $s_{i,j} = 1$ o $s_{i,j} > D_0$. Nell'ultimo caso il contributo è:

$$\ll y_{max}^2 \frac{N}{W}\Big(\sum_{\substack{u<R\\ (u,W)=1}}\frac{\mu(u)^2}{\varphi(u)}\Big)^k\Big(\sum_{s_{i,j}>D_0}\frac{\mu(s_{i,j})^2}{\varphi(s_{i,j})^2}\Big)\Big(\sum_{s\geq 1}\frac{\mu(s)^2}{\varphi(s)^2}\Big)^{k^2-k-1}, \tag{3.3.26}$$

semplicemente perché cambiando l'ordine di somma e prodotto abbiamo:

$$\sum_{u_1,\dots,u_k}\prod_{i=1}^k\frac{\mu(u_i)^2}{\varphi(u_i)} = \Big(\sum_{\substack{u<R\\ (u,W)=1}}\frac{\mu(u)^2}{\varphi(u)}\Big)^k \tag{3.3.27}$$

e possiamo scrivere

$$\sideset{}{^*}\sum_{s_{i,j},i\neq j}\prod_{\substack{1\leq i,j\leq k\\ i\neq j}}\frac{\mu(s_{i,j})}{\varphi(s_{i,j})^2} \ll \sum_{s_{i,j}>D_0}\frac{\mu(s_{i,j})^2}{\varphi(s_{i,j})^2}\Big(\sum_{s\geq 1}\frac{\mu(s)^2}{\varphi(s)^2}\Big)^{k^2-k-1}, \tag{3.3.28}$$

scambiando prodotto e somma, mettendo in evidenza la somma rispetto agli $s_{i,j} > D_0$ e stimando il resto con la serie convergente per $s \geq 1$, elevata alla $k^2 - k - 1$, visto che abbiamo $k^2 - k$ coppie (i, j) con $i \neq j$. Osserviamo che la serie converge per via di (1.2.7). Ora resta da stimare la sommatoria:

$$\sum_{\substack{n<R\\ (n,W)=1}}\frac{\mu(n)^2}{\varphi(n)}. \tag{3.3.29}$$

A tal proposito iniziamo col notare che usando $m = dn$, con $d|W, (n, W) = 1$, otteniamo:

$$\sum_{m<R}\frac{\mu(m)^2}{\varphi(m)} = \sum_{d|W}\sum_{\substack{n<R/d\\ (n,W)=1}}\frac{\mu(n)^2}{\varphi(n)}\frac{\mu(d)^2}{\varphi(d)} \leq \sum_{d|W}\frac{\mu(d)^2}{\varphi(d)}\sum_{\substack{n<R\\ (n,W)=1}}\frac{\mu(n)^2}{\varphi(n)}$$

$$= \frac{W}{\varphi(W)} \sum_{\substack{n<R \\ (n,W)=1}} \frac{\mu(n)^2}{\varphi(n)},$$

per via di (1.2.8), da cui:

$$\sum_{\substack{n<R \\ (n,W)=1}} \frac{\mu(n)^2}{\varphi(n)} \geq \frac{\varphi(W)}{W} \sum_{m<R} \frac{\mu(m)^2}{\varphi(m)}. \tag{3.3.30}$$

Per ottenere una maggiorazione di (3.3.29) la questione si fa più delicata: vogliamo infatti trovare una convoluzione per la funzione:

$$\frac{\mu(n)^2}{\varphi(n)} \chi_W(n), \tag{3.3.31}$$

dove abbiamo posto:

$$\chi_W(n) = \begin{cases} 1 & \text{se } (n,W)=1; \\ 0 & \text{altrimenti.} \end{cases}$$

A tale scopo consideriamo la serie di Dirichlet associata, che da (1.2.26) è:

$$\sum_{n=1}^{+\infty} \frac{\mu(n)^2}{\varphi(n) n^s} \chi_W(n) = \prod_{p \nmid W} \left(1 + \frac{1}{(p-1)p^s}\right) \tag{3.3.32}$$

$$= \sum_{n=1}^{+\infty} \frac{\mu(n)^2}{\varphi(n) n^s} \prod_{p|W} \left(1 + \frac{1}{(p-1)p^s}\right)^{-1} = \sum_{n=1}^{+\infty} \frac{\mu(n)^2}{\varphi(n) n^s} \sum_{n=1}^{+\infty} \frac{a(n)}{n^s}.$$

Osserviamo che la serie $\sum_{n\geq 1} \frac{\mu(n)^2}{\varphi(n)n^s} \chi_W(n)$ è assolutamente convergente per $Re(s) > 0$, a causa di (1.2.10), ed è la serie di Dirichlet di una funzione moltiplicativa, quindi ammette un prodotto di Eulero in tale regione. Notiamo anche che abbiamo definito $a(n)$ implicitamente attraverso:

$$\sum_{n=1}^{+\infty} \frac{a(n)}{n^s} = \prod_{p|W} \left(1 + \frac{1}{(p-1)p^s}\right)^{-1} = \prod_{p|W} \left(1 - \frac{\mu(p)}{(p-1)p^s}\right)^{-1} = \prod_{p|W} \sum_{k=0}^{+\infty} \frac{\mu(p)^k}{(p-1)^k p^{ks}}.$$

Sviluppando il prodotto otteniamo facilmente che:

$$a(n) = \begin{cases} \frac{(-1)^{a_1+\ldots+a_k}}{(p_1-1)^{a_1}\cdots(p_k-1)^{a_k}} & \text{se } \forall p|n \Rightarrow p|W \text{ con } n = p_1^{a_1}\cdots p_k^{a_k}; \\ 0 & \text{altrimenti.} \end{cases}$$

Osserviamo che dati due numeri interi n, m, se esiste $p|nm$ con $p \nmid W$, allora $a(nm) = 0 = a(n)a(m)$. Se invece ciò non accade allora $a(nm) = a(n)a(m)$, che si deduce immediatamente dalla definizione esplicita di $a(n)$ e dal fatto che $a(p^k) = \frac{\mu(p)^k}{(p-1)^k} = \left(\frac{\mu(p)}{p-1}\right)^k = a(p)^k$, per ogni primo p e intero positivo k. Quindi $a(n)$ è completamente moltiplicativa. È chiaro che la serie $\sum_{n=1}^{+\infty} \frac{a(n)}{n^s}$ converge per $s = 0$. Quindi otteniamo:

$$\sum_{n<R} \frac{\mu(n)^2}{\varphi(n)} \chi_W(n) = \sum_{n<R} \sum_{d|n} \frac{\mu(d)^2}{\varphi(d)} a\left(\frac{n}{d}\right) = \sum_{d<R} \frac{\mu(d)^2}{\varphi(d)} \sum_{k<\frac{R}{d}} a(k).$$

Usando il prodotto di Eulero si ottiene:

$$\sum_{k<\frac{R}{d}} a(k) = \sum_{k=1}^{+\infty} a(k) + o(1) = \prod_{p|W}\left(1+\frac{1}{(p-1)}\right)^{-1} + o(1) = \frac{\varphi(W)}{W} + o(1), \tag{3.3.33}$$

visto che W è libero da quadrati. In totale abbiamo:

$$\sum_{\substack{n<R\\(n,W)=1}} \frac{\mu(n)^2}{\varphi(n)} = \sum_{d<R} \frac{\mu(d)^2}{\varphi(d)}\left(\frac{\varphi(W)}{W} + o(1)\right). \tag{3.3.34}$$

Ora è sufficiente mostrare che:

$$\sum_{d<R} \frac{\mu(d)^2}{\varphi(d)} \ll \log R. \tag{3.3.35}$$

Usando la Proposizione 2.2.1 si ottiene:

$$\sum_{d<R} \frac{\mu(d)^2}{\varphi(d)} \leq \prod_{p\leq R}\left(1+\frac{1}{(p-1)}\right) \leq \exp\left(\sum_{p\leq R}\frac{1}{(p-1)}\right) \ll \log R, \tag{3.3.36}$$

per l'equazione (1.2.14). Quindi otteniamo:

$$\sum_{\substack{n<R\\(n,W)=1}} \frac{\mu(n)^2}{\varphi(n)} \ll \frac{\varphi(W)}{W}\log R. \tag{3.3.37}$$

Da (1.2.10) abbiamo:

$$\sum_{s\geq 1} \frac{\mu(s)^2}{\varphi(s)^2} \ll 1 \tag{3.3.38}$$

e infine ci resta da stimare:

$$\sum_{s\geq D_0} \frac{\mu(s)^2}{\varphi(s)^2}. \tag{3.3.39}$$

A tal proposito notiamo innanzitutto che:

$$S(t) = \sum_{n\leq t}\left(\frac{\mu(n)n}{\varphi(n)}\right)^2 \ll t. \tag{3.3.40}$$

Commentiamo che in generale si ottiene lo stesso risultato se sostituiamo un qualsiasi numero reale r al posto di 2, usando una facile applicazione del Teorema 2.2.2, vedere ad esempio [M-V] [6] equazione (2.32). Nel nostro caso, verifichiamo innanzitutto che le ipotesi del Teorema 2.2.2 sono verificate:

$$\sum_{p\leq x} \frac{p^2\log p}{(p-1)^2} \ll \sum_{p\leq x} \log p \ll x,$$

usando il teorema dei numeri primi nella forma $\theta(x) \backsim x$ e il fatto che $\frac{p}{(p-1)} = 1+\frac{1}{p-1} \leq 2$. Infine,

$$\sum_{p^k, k\geq 2} \frac{p^{2k}\mu^2(p^k)k\log p}{p^{3k-2}(p-1)^2} = 0.$$

Quindi otteniamo da (2.2.4) che:

$$\sum_{n\leq x}\left(\frac{\mu(n)n}{\varphi(n)}\right)^2 \ll \frac{x}{\log x}\prod_{p\leq x}\left(1+\frac{p^2}{p(p-1)^2}\right) = \frac{x}{\log x}\prod_{p\leq x}\left(1+\frac{p}{(p-1)^2}\right)$$

$$= \frac{x}{\log x}\prod_{p\leq x}\left(1+\frac{p}{(p-1)^2}\right)\prod_{p\leq x}\left(1-\frac{1}{p}\right)\prod_{p\leq x}\left(1-\frac{1}{p}\right)^{-1} \ll x,$$

visto che da (1.2.15) sappiamo che:

$$\prod_{p\leq x}\left(1-\frac{1}{p}\right)^{-1} \ll \log x.$$

Inoltre,

$$\prod_{p\leq x}\left(1+\frac{p}{(p-1)^2}\right)\prod_{p\leq x}\left(1-\frac{1}{p}\right) = \prod_{p\leq x}\left(\frac{p^2-p+1}{p^2-p}\right) = \prod_{p\leq x}\left(1+\frac{1}{p^2-p}\right) \ll 1.$$

Ora usando la tecnica di sommazione parziale attraverso l'integrazione di Riemann-Stieltjes otteniamo:

$$\sum_{n>x}\frac{\mu^2(n)}{\varphi(n)^2} = \int_x^{+\infty}\frac{d(S(t))}{t^2} = \frac{S(t)}{t^2}\Big|_x^{+\infty} + 2\int_x^{+\infty}\frac{S(t)}{t^3} \ll \frac{1}{x}, \tag{3.3.41}$$

da cui deduciamo che:

$$\sum_{s\geq D_0}\frac{\mu(s)^2}{\varphi(s)^2} \ll \frac{1}{D_0}. \tag{3.3.42}$$

Utilizzando (3.3.37), (3.3.38), (3.3.42) otteniamo che (3.3.26) diventa:

$$\ll \frac{y_{max}^2\varphi(W)^k N\log^k R}{W^{k+1}D_0}. \tag{3.3.43}$$

Inoltre, se restringiamo la nostra attenzione al caso $s_{i,j} = 1$, per ogni $i \neq j$, allora il termine principale di S_1 in (3.3.25) diventa chiaramente:

$$\frac{N}{W}\sum_{u_1,\dots,u_k}\frac{y_{u_1,\dots,u_k}^2}{\prod_{i=1}^k\varphi(u_i)}, \tag{3.3.44}$$

da cui otteniamo:

$$S_1 = \frac{N}{W}\sum_{u_1,\dots,u_k}\frac{y_{u_1,\dots,u_k}^2}{\prod_{i=1}^k\varphi(u_i)} + O\left(\frac{y_{max}^2\varphi(W)^k N\log^k R}{W^{k+1}D_0} + y_{max}^2R^2\log^{4k}R\right). \tag{3.3.45}$$

Ricordando che $R^2 = N^{\theta-2\delta} \leq N^{1-2\delta}$ e

$$W = \prod_{p \leq D_0} p = \exp(\theta(D_0)) \ll \exp(D_0) = \log\log N \ll N^{\frac{\delta}{k+1}},$$

da (1.2.17), si ha che:

$$R^2 \log^{3k} R \ll N^{1-2\delta}\Big((1-\delta)\log N\Big)^{3k} \ll N^{1-2\delta}\log^{3k} N,$$

$$\frac{N}{D_0 W^{k+1}} \gg \frac{N}{N^{\delta}\log\log\log N} \gg \frac{N^{1-\delta}}{\log\log\log N}.$$

Quindi il primo termine d'errore in (3.3.45) domina e il Lemma segue. □

3.3.2 Stima di S_2

Consideriamo ora la somma S_2. Possiamo riscriverla come $S_2 = \sum_{m=1}^{k} S_2^{(m)}$, dove:

$$S_2^{(m)} = \sum_{\substack{N \leq n < 2N \\ n \equiv v_0 (\bmod W)}} \chi_{\mathbb{P}}(n+h_m)\Bigg(\sum_{\substack{d_1,\dots,d_k \\ d_i \mid n+h_i, \forall i}} \lambda_{d_1,\dots,d_k}\Bigg)^2. \tag{3.3.46}$$

Il procedimento per stimare $S_2^{(m)}$ e i conti coinvolti sono molto simili a quelli svolti per S_1. Il nostro obiettivo è dimostrare il seguente

Lemma 3.3.2. *Sia $m \in \{1,\dots,k\}$, $r_1,\dots,r_k \in \mathbb{N}$ e*

$$y^{(m)}_{r_1,\dots,r_k} = \Bigg(\prod_{i=1}^{k} \mu(r_i) g(r_i)\Bigg) \sum_{\substack{d_1,\dots,d_k \\ r_i \mid d_i, \forall i \\ d_m = 1}} \frac{\lambda_{d_1,\dots,d_k}}{\prod_{i=1}^{k} \varphi(d_i)}, \tag{3.3.47}$$

dove g è la funzione completamente moltiplicativa definita sui primi da $g(p) = p-2$. Sia $y_{max} = \sup_{r_1,\dots,r_k} |y^{(m)}_{r_1,\dots,r_k}|$. Allora per ogni fissato $A > 0$ abbiamo,

$$S_2^{(m)} = \frac{N}{\log N \varphi(W)} \sum_{r_1,\dots,r_k} \frac{(y^{(m)}_{r_1,\dots,r_k})^2}{\prod_{i=1}^{k} g(r_i)} \tag{3.3.48}$$

$$+O\Bigg(\frac{(y^{(m)}_{max})^2 \varphi(W)^{k-2} N \log^{k-2} N}{W^{k-1} D_0}\Bigg) + O\Bigg(\frac{y^2_{max} N}{\log^A N}\Bigg).$$

Dimostrazione. Come per S_1 espandiamo il quadrato:

$$S_2^{(m)} = \sum_{\substack{d_1,\dots,d_k \\ e_1,\dots,e_k}} \lambda_{d_1,\dots,d_k}\lambda_{e_1,\dots,e_k} \sum_{\substack{N \leq n < 2N \\ n \equiv v_0 (\bmod W) \\ [d_i,e_i] \mid n+h_i, \forall i}} \chi_{\mathbb{P}}(n+h_m). \tag{3.3.49}$$

Sempre come in S_1 la somma interna può essere riscritta come somma su una singola classe residuale a modulo $q = W\prod_{i=1}^{k}[d_i, e_i]$, a patto che gli interi $W, [d_1, e_1], ..., [d_k, e_k]$ siano coprimi a coppie. Osserviamo che $n + h_m$ appartiene ad una classe residuale coprima con il modulo q se e solo se $d_m = e_m = 1$, visto che $[d_m, e_m]|(q, n + h_m)$. In tal caso, la somma interna in (3.3.49) equivale ad:

$$\sum_{\substack{N\leq n<2N\\ n\equiv v_0(\bmod W)\\ [d_i,e_i]|n+h_i,\forall i\\ (n+h_m,q)=1}} \chi_{\mathbb{P}}(n+h_m) = \sum_{\substack{N\leq n<2N\\ n\equiv a(\bmod q)}} \chi_{\mathbb{P}}(n), \tag{3.3.50}$$

in cui abbiamo riscritto la somma rispetto ad $n \equiv b(\bmod\ q)$, per un opportuno intero b, e poi abbiamo rimpiazzato n stesso con $n + h_m$, riscrivendo la somma rispetto ad $n \equiv a(\bmod\ q)$, per un opportuno intero a. Ora (3.3.50) è uguale a:

$$\begin{aligned}&\frac{1}{\varphi(q)}\sum_{N\leq n<2N}\chi_{\mathbb{P}}(n) + \Bigg(\sum_{\substack{N\leq n<2N\\ n\equiv a(\bmod q)}}\chi_{\mathbb{P}}(n) - \frac{1}{\varphi(q)}\sum_{N\leq n<2N}\chi_{\mathbb{P}}(n)\Bigg)\\ &= \frac{X_N}{\varphi(q)} + O\Bigg(\sup_{(a,q)=1}\Bigg|\sum_{\substack{N\leq n<2N\\ n\equiv a(\bmod q)}}\chi_{\mathbb{P}}(n) - \frac{X_N}{\varphi(q)}\Bigg|\Bigg),\end{aligned} \tag{3.3.51}$$

dove abbiamo posto:

$$X_N = \sum_{N\leq n<2N}\chi_{\mathbb{P}}(n). \tag{3.3.52}$$

Quindi riscriviamo (3.3.50) come:

$$\frac{X_N}{\varphi(q)} + O(E'(N, q)). \tag{3.3.53}$$

Se d_m oppure e_m non sono 1, il contributo alla somma interna in (3.3.49) è pari ad:

$$\ll \sum_{\substack{d_1,\dots,d_k\\ e_1,\dots,e_k}} |\lambda_{d_1,\dots,d_k}\lambda_{e_1,\dots,e_k}|, \tag{3.3.54}$$

visto che esiste al più un n che soddisfa $n+h_m$ primo e $[d_m, e_m]|(n+h_m)$, con $d_m > 1$ o $e_m > 1$. Otteniamo che:

$$S_2^{(m)} = \frac{X_N}{\varphi(W)}\sum_{\substack{d_1,\dots,d_k\\ e_1,\dots,e_k\\ d_m=1=e_m}}\frac{\lambda_{d_1,\dots,d_k}\lambda_{e_1,\dots,e_k}}{\prod_{i=1}^{k}\varphi([d_i,e_i])} + O\Bigg(\sum_{\substack{d_1,\dots,d_k\\ e_1,\dots,e_k}}|\lambda_{d_1,\dots,d_k}\lambda_{e_1,\dots,e_k}|E(N,q)\Bigg), \tag{3.3.55}$$

a patto di sostituire $E'(N, q)$ con:

$$E(N, q) = 1 + E'(N, q), \tag{3.3.56}$$

dove $E'(N,q)$ è definito in (3.3.53). Iniziamo con l'analizzare il contributo del termine d'errore. Dal supporto di $\lambda_{d_1,\dots,d_k}$ si evince che dobbiamo solo considerare il caso in cui q è libero da quadrati con $q < R^2W$. Dato un intero libero da quadrati r, ci sono al più $\tau_{3k}(r)$ scelte per $d_1,\dots,d_k,e_1,\dots,e_k$ per le quali $W\prod_{i=1}^{k}[d_i,e_i]=r$. Quindi il termine d'errore in (3.3.55) contribuisce:

$$\ll y_{max}^2 \log^{2k} R \sum_{r<R^2W} \mu(r)^2\tau_{3k}(r)E(N,r), \tag{3.3.57}$$

dove abbiamo usato (3.3.21). Dalla disuguaglianza di Cauchy-Schwarz, (3.3.57) è

$$\ll y_{max}^2 \log^{2k} R \sqrt{\sum_{r<R^2W} \mu(r)^2\tau_{3k}^2(r)E(N,r)}\sqrt{\sum_{r<R^2W} \mu(r)^2E(N,r)} \tag{3.3.58}$$

$$\leq y_{max}^2 \log^{2k} R \sqrt{\sum_{r<R^2W} \mu(r)^2\tau_{3k}^2(r)\frac{N}{\varphi(r)}}\sqrt{\sum_{r<R^2W} \mu(r)^2E(N,r)},$$

usando la stima banale $E(N,r) \ll \frac{N}{\varphi(r)}$. Ora da (3.3.56) abbiamo,

$$\sum_{r<R^2W} \mu(r)^2E(N,r) \leq \sum_{r<R^2W} E(N,r)$$

$$\ll \sum_{r<R^2W} \max_{(a,r)=1}\Big|\sum_{\substack{N\leq n<2N\\ n\equiv a(\bmod q)}} \chi_{\mathbb{P}}(n) - \frac{X_N}{\varphi(q)}\Big| \ll \frac{N}{\log^{A'}(N)},$$

per ogni $A'>0$, dalla Definizione 2.1 ed il Teorema 2.1.13, usando che:

$$R^2W \ll N^{\theta-2\delta}\log\log N \ll N^{\theta-2\delta}N^{2\delta} = N^{\theta}$$

e che $\theta < \frac{1}{2}$. Quindi il termine d'errore in (3.3.55) contribuisce per:

$$\ll y_{max}^2\sqrt{N}\log^{2k}(R)\log^{3k}(R^2W)\frac{\sqrt{N}}{\log^{A'/2}N},$$

visto che possiamo stimare la somma nella prima radice in (3.3.58) come in (3.3.22). Ora dato che:

$$\log^{2k}(R)\log^{3k}(R^2W) \ll \log^{5k}N$$

e ponendo $A' = 2A+10k$, otteniamo che per ogni $A>0$ il termine d'errore diventa

$$\ll y_{max}^2\frac{N}{\log^{A}N}. \tag{3.3.59}$$

Passiamo ora al termine principale. Come per S_1 riscriviamo le condizioni $(d_i,e_j)=1$ moltiplicando la nostra espressione per $\sum_{s_{i,j}|(d_i,e_j)}\mu(s_{i,j})$ e restringiamo ancora una volta gli $s_{i,j}$ ad essere coprimi con $u_i,u_j,s_{i,a},s_{b,j}$, per ogni $a\neq j$ e $b\neq i$. Infine, osserviamo che $\varphi([d_i,e_i]) = \varphi\big(\frac{d_i}{(d_i,e_i)}\big)\varphi(e_i)$, visto che $\big(\frac{d_i}{(d_i,e_i)},e_i\big)=1$ e d_i,e_i sono liberi

da quadrati. Inoltre, per le stesse ragioni abbiamo $\varphi\big(\frac{d_i}{(d_i,e_i)}\big) = \frac{\varphi(d_i)}{\varphi((d_i,e_i))}$, quindi in conclusione:

$$\varphi([d_i,e_i]) = \frac{\varphi(d_i)\varphi(e_i)}{\varphi((d_i,e_i))}.$$

Ma ora se definiamo $g(p) = p-2$ sui primi, estendendola ad una funzione completamente moltiplicativa, otteniamo che:

$$\sum_{d|p} g(d) = 1 + (p-2) = p-1 = \varphi(p)$$

e siccome la convoluzione di due funzioni moltiplicative è ancora moltiplicativa otteniamo che sugli interi n liberi da quadrati vale,

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

e quindi in definitiva:

$$\frac{1}{\varphi([d_i,e_i])} = \frac{1}{\varphi(d_i)\varphi(e_i)} \sum_{u_i|(d_i,e_i)} g(u_i).$$

Osserviamo che c'erano molti altri modi di scrivere $\varphi(n)$ tramite una convoluzione di una funzione $g(d)$ ma abbiamo scelto tale funzione proprio perché sugli interi liberi da quadrati d abbiamo $g(d) \approx \varphi(d)$, ovvero $g(d)$ e $\varphi(d)$ sono due numeri interi molto vicini, visto che $|\varphi(p) - g(p)| = 1$, per ogni primo p. Questo ci permetterà nei prossimi conti di semplificare le espressioni e di trovarci a valutare somme praticamente identiche a quelle già incontrate nella stima di S_1, in cui al posto di $g(n)$ c'era $\varphi(n)$. Il termine principale in (3.3.55) viene riscritto come:

$$\frac{X_N}{\varphi(W)} \sum_{u_1,\dots,u_k} \Big(\prod_{i=1}^{k} g(u_i)\Big) \sum_{s_{i,j},i\neq j}^{*} \Big(\prod_{\substack{1\le i,j\le k\\ i\neq j}} \mu(s_{i,j})\Big) \sum_{\substack{d_1,\dots,d_k\\ e_1,\dots,e_k\\ u_i|(d_i,e_i),\forall i\\ s_{i,j}|(d_i,e_j),\forall i\neq j\\ d_m=1=e_m}} \frac{\lambda_{d_1,\dots,d_k}\lambda_{e_1,\dots,e_k}}{\prod_{i=1}^{k}\varphi(d_i)\varphi(e_i)}, \tag{3.3.60}$$

dove denotiamo con Σ^* la somma sugli $s_{i,j}$ coprimi con u_i, u_j e con $s_{i,a}, s_{b,j}$, per ogni $a \neq j$ e $b \neq i$. Ora sostituiamo (3.3.47) in (3.3.60) notando che $y^{(m)}_{r_1,\dots,r_k} = 0$, a meno che $r_m = 1$. Quindi otteniamo,

$$\frac{X_N}{\varphi(W)} \sum_{u_1,\dots,u_k} \Big(\prod_{i=1}^{k} \frac{\mu(u_i)^2}{g(u_i)}\Big) \sum_{s_{i,j},i\neq j}^{*} \Big(\prod_{\substack{1\le i,j\le k\\ i\neq j}} \frac{\mu(s_{i,j})}{g(s_{i,j})^2}\Big) y^{(m)}_{a_1,\dots,a_k} y^{(m)}_{b_1,\dots,b_k}, \tag{3.3.61}$$

dove, come per S_1, raggruppiamo i termini e sostituiamo (3.3.47) usando le identità $a_j = u_j \prod_{i\neq j} s_{j,i}$ e $b_j = u_j \prod_{i\neq j} s_{i,j}$, per ogni $1 \le i \le k$, e il fatto che i termini con a_j, b_j non liberi da quadrati non danno contributo. Notiamo che $g(n) = 0$ se n è pari, quindi a priori non possiamo dividere per lui stesso. Visto che $\lambda_{d_1,\dots,d_k} = 0$

se $(d = \prod_{i=1}^{k} d_i, W) > 1$, abbiamo necessariamente che tutti i d_i sono dispari e nell'operare il cambio di variabili (3.3.47), con $a_1, ...a_k$ e $b_1, ...b_k$ al posto di $r_1, ...r_k$, i valori $g(a_j), g(b_j)$ sono diversi da zero, per ogni $j = 1, ..., k$. Dunque è sottinteso che le due somme in (3.3.61) siano calcolate solo su numeri dispari. Osserviamo che il contributo dagli $s_{i,j} \neq 1$ è dell'ordine di:

$$\ll \frac{(y_{max}^{(m)})^2 N}{\varphi(W)\log N}\Big(\sum_{\substack{u<R\\(u,W)=1}}\frac{\mu(u)^2}{g(u)}\Big)^{k-1}\Big(\sum_{s}\frac{\mu(s)^2}{g(s)^2}\Big)^{k^2-k-1}\sum_{s_{i,j}>D_0}\frac{\mu(s_{i,j})^2}{g(s_{i,j})^2}, \tag{3.3.62}$$

dove abbiamo usato la forma debole del teorema dei numeri primi, dicendo che $X_N \ll \frac{N}{\log N}$, dove X_N è definito nella (3.3.52), e il resto delle maggiorazioni segue la stessa logica di quanto già fatto nella stima di S_1. Per concludere bisogna stimare le tre somme in (3.3.62), ove la variabile di sommatoria varia, in aggiunta, nell'insieme dei numeri naturali dispari. Da (2.2.1) segue:

$$\sum_{u\leq R}\frac{\mu(u)^2}{g(u)} \leq \prod_{2<p\leq R}\Big(1+\frac{1}{p-2}\Big) \leq \exp\Big(\sum_{2<p\leq R}\frac{1}{p-2}\Big) \ll \log R, \tag{3.3.63}$$

dove nella somma iniziale la variabile u varia sui numeri dispari. Muovendoci come per la stima di (3.3.29) otteniamo immediatamente:

$$\sum_{\substack{u<R\\(u,W)=1}}\frac{\mu(u)^2}{g(u)} \ll \prod_{2<p|W}\Big(1+\frac{1}{p-2}\Big)^{-1}\log R = \prod_{2<p|W}\Big(\frac{p-2}{p-1}\Big)\log R \tag{3.3.64}$$

$$= \prod_{2<p|W}\Big(1-\frac{1}{p-1}\Big)\log R \leq \prod_{p|W}\Big(1-\frac{1}{p}\Big)\log R = \frac{\varphi(W)}{W}\log R.$$

Ancora utilizzando la Proposizione 2.2.1 e considerando sempre la variabile s tra i numeri dispari abbiamo,

$$\sum_{s\leq R}\frac{\mu(s)^2}{g(s)^2} \leq \prod_{2<p\leq R}\Big(1+\frac{1}{(p-2)^2}\Big) \leq \exp\Big(\sum_{2<p\leq R}\frac{1}{(p-2)^2}\Big) \ll 1. \tag{3.3.65}$$

Infine, calcoliamo la somma $\sum_{s_{i,j}>D_0}\frac{\mu(s_{i,j})^2}{g(s_{i,j})^2}$, per $s_{i,j}$ dispari: calcoliamo in primis la somma:

$$\sum_{\substack{s\leq x\\ s\equiv 1(\bmod 2)}}\frac{s^2\mu^2(s)}{g(s)^2}.$$

Per fare ciò ci appelliamo al Teorema 2.2.2 . Nel nostro caso usiamo $f(n) = \big(\frac{n\mu(n)}{g(n)}\big)^2$, dove n varia tra gli interi dispari maggiori di 2, quindi osserviamo che:

$$\sum_{p\leq x} f(p)\log p = \sum_{2<p\leq x}\Big(\frac{p}{p-2}\Big)^2\log p \ll \sum_{2<p\leq x}\log p \ll x, \tag{3.3.66}$$

visto che $\left(\frac{p}{p-2}\right) = \left(1+\frac{2}{p-2}\right) \leq 3$. Inoltre,

$$\sum_{p^k,k\geq 2} \frac{f(p^k)k\log p}{p^k} = \sum_{\substack{p^k \\ k\geq 2 \\ p>2}} \frac{p^{2k}k(\log p)\mu^2(p^k)}{p^k(p-2)^{2k}} = 0. \tag{3.3.67}$$

Pertanto il Teorema 2.2.2 implica:

(3.3.68)

$$\sum_{\substack{n\leq x \\ n\equiv 1(\bmod 2)}} \left(\frac{n\mu(n)}{g(n)}\right)^2 \ll \frac{x}{\log x}\prod_{2<p\leq x}\left(1+\frac{p^2}{p(p-2)^2}\right) = \frac{x}{\log x}\prod_{2<p\leq x}\left(1+\frac{p}{(p-2)^2}\right)$$

$$\ll \frac{x}{\log x}\prod_{2<p\leq x}\left(1+\frac{p}{(p-2)^2}\right)\prod_{2<p\leq x}\left(1-\frac{1}{p}\right)\prod_{2<p\leq x}\left(1-\frac{1}{p}\right)^{-1} \ll x,$$

visto che da (1.2.15) sappiamo che:

$$\prod_{2<p\leq x}\left(1-\frac{1}{p}\right)^{-1} \ll \log x$$

e che:

$$\prod_{2<p\leq x}\left(1+\frac{p}{(p-2)^2}\right)\prod_{2<p\leq x}\left(1-\frac{1}{p}\right) = \prod_{2<p\leq x}\left(\frac{(p^2-3p+4)(p-1)}{p(p-2)^2}\right)$$

$$= \prod_{2<p\leq x}\left(1+\frac{3p-4}{p^3-4p^2+4p}\right) \ll 1.$$

Quindi,

$$\sum_{\substack{n\leq x \\ n\equiv 1(\bmod 2)}} \left(\frac{n\mu(n)}{g(n)}\right)^2 \ll x$$

e usando la tecnica di sommazione parziale come in (3.3.41) otteniamo immediatamente:

$$\sum_{\substack{s_{i,j}>D_0 \\ s_{i,j}\equiv 1(\bmod 2)}} \frac{\mu(s_{i,j})^2}{g(s_{i,j})^2} \ll \frac{1}{D_0}. \tag{3.3.69}$$

Unendo insieme le stime (3.3.64), (3.3.65), (3.3.69) abbiamo che il contributo al termine principale di $S_2^{(m)}$ in (3.3.61) proveniente dagli $s_{i,j} \neq 1$ è:

$$\ll \frac{(y_{max}^{(m)})^2\varphi(W)^{k-2}N\log^{k-1}R}{W^{k-1}D_0\log N}. \tag{3.3.70}$$

Dunque abbiamo trovato che:

$$S_2^{(m)} = \frac{X_N}{\varphi(W)} \sum_{u_1,\dots,u_k} \frac{(y^{(m)}_{u_1,\dots,u_k})^2}{\prod_{i=1}^k g(u_i)} + O\bigg(\frac{(y^{(m)}_{max})^2 \varphi(W)^{k-2} N \log^{k-1} R}{W^{k-1} D_0 \log N} + \frac{y^2_{max} N}{\log^A N} \bigg) \tag{3.3.71}$$

e visto che dal teorema dei numeri primi (1.2.19) vale:

$$X_N = \frac{N}{\log N} + O\bigg(\frac{N}{\log^2 N} \bigg), N \to +\infty,$$

abbiamo,

(3.3.72)

$$S_2^{(m)} = \frac{N}{\varphi(W) \log N} \sum_{u_1,\dots,u_k} \frac{(y^{(m)}_{u_1,\dots,u_k})^2}{\prod_{i=1}^k g(u_i)} + O\left(\frac{N}{\varphi(W) \log^2 N} \sum_{u_1,\dots,u_k} \frac{(y^{(m)}_{u_1,\dots,u_k})^2}{\prod_{i=1}^k g(u_i)} \right)$$

$$+ O\bigg(\frac{(y^{(m)}_{max})^2 \varphi(W)^{k-2} N \log^{k-1} R}{W^{k-1} D_0 \log N} + \frac{y^2_{max} N}{\log^A N} \bigg).$$

Siccome:

$$\frac{N}{\varphi(W) \log^2 N} \sum_{u_1,\dots,u_k} \frac{(y^{(m)}_{u_1,\dots,u_k})^2}{\prod_{i=1}^k g(u_i)} \ll \frac{(y^{(m)}_{max})^2 N}{\varphi(W) \log^2 N} \bigg(\sum_{\substack{u<R \\ (u,W)=1}} \frac{\mu(u)^2}{g(u)} \bigg)^{k-1} \tag{3.3.73}$$

$$\ll \frac{(y^{(m)}_{max})^2 \varphi(W)^{k-2} N \log^{k-3} R}{W^{k-1}},$$

perché $\log N \gg \log R$, il termine d'errore (3.3.73) può essere assorbito nel secondo termine d'errore in (3.3.72), visto che $D_0 \ll \log R$. Inserendo (3.3.73) in (3.3.72) otteniamo (3.3.48). □

3.4 Relazione tra $y_{r_1,\dots,r_k}$ e $y^{(m)}_{r_1,\dots,r_k}$

Cerchiamo di trovare ora una relazione tra $y_{r_1,\dots,r_k}$ e $y^{(m)}_{r_1,\dots,r_k}$, definiti nelle (3.3.4) e (3.3.47), attraverso il seguente

Lemma 3.4.1. *Fissiamo $m \in \{1,\dots,k\}$ e $r_m = 1$. Sia $a_m \in \mathbb{N}$, $(a_m, W) = 1$, $a_m < R$ e libero da quadrati. Allora vale,*

$$y^{(m)}_{r_1,\dots,r_k} = \sum_{a_m} \frac{y_{r_1,\dots,r_{m-1},a_m,r_{m+1},\dots,r_k}}{\varphi(a_m)} + O\bigg(\frac{y_{max} \varphi(W) \log R}{W D_0} \bigg). \tag{3.4.1}$$

Dimostrazione. Assumiamo attraverso tutta la dimostrazione che $r_m = 1$. Da (3.3.17) e (3.3.47) abbiamo,

$$y^{(m)}_{r_1,\dots,r_k} = \bigg(\prod_{i=1}^k \mu(r_i) g(r_i) \bigg) \sum_{\substack{d_1,\dots,d_k \\ r_i | d_i, \forall i \\ d_m = 1}} \frac{\lambda_{d_1,\dots,d_k}}{\prod_{i=1}^k \mu(d_i) d_i} \prod_{i=1}^k \frac{\mu(d_i) d_i}{\varphi(d_i)} \tag{3.4.2}$$

$$= \Big(\prod_{i=1}^{k} \mu(r_i)g(r_i)\Big) \sum_{\substack{d_1,\dots,d_k \\ r_i|d_i,\forall i \\ d_m=1}} \prod_{i=1}^{k} \frac{\mu(d_i)d_i}{\varphi(d_i)} \sum_{\substack{a_1,\dots,a_k \\ d_i|a_i,\forall i}} \frac{y_{a_1,\dots,a_k}}{\prod_{i=1}^{k}\varphi(a_i)}.$$

Scambiando le somme sulle variabili d ed a otteniamo:

$$y^{(m)}_{r_1,\dots,r_k} = \Big(\prod_{i=1}^{k} \mu(r_i)g(r_i)\Big) \sum_{\substack{a_1,\dots,a_k \\ r_i|a_i,\forall i}} \frac{y_{a_1,\dots,a_k}}{\prod_{i=1}^{k}\varphi(a_i)} \sum_{\substack{d_1,\dots,d_k \\ r_i|d_i|a_i,\forall i \\ d_m=1}} \prod_{i=1}^{k} \frac{\mu(d_i)d_i}{\varphi(d_i)}. \tag{3.4.3}$$

Osserviamo che:

$$\sum_{\substack{d_1,\dots,d_k \\ r_i|d_i|a_i,\forall i \\ d_m=1}} \prod_{i=1}^{k} \frac{\mu(d_i)d_i}{\varphi(d_i)} = \prod_{i\neq m} \sum_{\substack{d_i: \\ r_i|d_i|a_i}} \frac{\mu(d_i)d_i}{\varphi(d_i)}$$

$$= \prod_{i\neq m} \sum_{\substack{f_i: \\ f_i|\frac{a_i}{r_i}}} \frac{\mu(r_i)r_i}{\varphi(r_i)} \frac{\mu(f_i)f_i}{\varphi(f_i)} = \prod_{i\neq m} \frac{\mu(r_i)r_i}{\varphi(r_i)} \sum_{\substack{f_i: \\ f_i|\frac{a_i}{r_i}}} \frac{\mu(f_i)f_i}{\varphi(f_i)},$$

dove abbiamo posto $d_i = r_i f_i$, per ogni $i = 1, ..., k$. Siccome per valori di n liberi da quadrati vale,

$$\sum_{d|n} \frac{\mu(d)d}{\varphi(d)} = \prod_{p|n}\Big(1 - \frac{p}{p-1}\Big) = \prod_{p|n}\Big(\frac{-1}{p-1}\Big) = \frac{(-1)^{\omega(n)}}{\varphi(n)} = \frac{\mu(n)}{\varphi(n)},$$

otteniamo:

$$\sum_{\substack{d_1,\dots,d_k \\ r_i|d_i|a_i,\forall i \\ d_m=1}} \prod_{i=1}^{k} \frac{\mu(d_i)d_i}{\varphi(d_i)} = \prod_{i\neq m} \frac{\mu(r_i)r_i}{\varphi(r_i)} \frac{\mu\big(\frac{a_i}{r_i}\big)}{\varphi\big(\frac{a_i}{r_i}\big)} = \prod_{i\neq m} \frac{\mu(a_i)r_i}{\varphi(a_i)}.$$

Quindi, possiamo riscrivere (3.4.3) come:

$$y^{(m)}_{r_1,\dots,r_k} = \Big(\prod_{i=1}^{k} \mu(r_i)g(r_i)\Big) \sum_{\substack{a_1,\dots,a_k \\ r_i|a_i,\forall i}} \frac{y_{a_1,\dots,a_k}}{\prod_{i=1}^{k}\varphi(a_i)} \prod_{i\neq m} \frac{\mu(a_i)r_i}{\varphi(a_i)}. \tag{3.4.4}$$

Osserviamo che, dal supporto di $y_{a_1,\dots,a_k}$, definito sotto (3.3.17), possiamo restringere la somma sugli a_j, chiedendo $(a_j, W) = 1$. Quindi, anche $\big(\frac{a_j}{r_j}, W\big) = 1$, e deve valere $a_j = r_j$ o $a_j > D_0 r_j$. Per $j \neq m$, il contributo totale da $a_j \neq r_j$ è:

$$y_{max}\Big(\prod_{i=1}^{k} g(r_i)r_i\Big)\Big(\sum_{\substack{a_j > D_0 r_j \\ r_j|a_j}} \frac{\mu(a_j)^2}{\varphi(a_j)^2}\Big)\Big(\sum_{\substack{a_m<R \\ (a_m,W)=1}} \frac{\mu(a_m)^2}{\varphi(a_m)}\Big) \prod_{\substack{1\leq i\leq k \\ i\neq j,m}} \Big(\sum_{r_i|a_i} \frac{\mu(a_i)^2}{\varphi(a_i)^2}\Big), \tag{3.4.5}$$

semplicemente separando in tre parti la somma in (3.4.4) rispetto a $i = m$, $i = j$ o $i \neq j, m$. Sostituendo $a_i = r_i f_i$, per ogni $i \neq m$, e stimando le tre somme:

$$\sum_{f_j > D_0} \frac{\mu(f_j)^2}{\varphi(f_j)^2} \ll \frac{1}{D_0},$$

$$\sum_{\substack{a_m<R\\(a_m,W)=1}}\frac{\mu(a_m)^2}{\varphi(a_m)}\ll\frac{\varphi(W)\log R}{W},$$

$$\sum_{f_i}\frac{\mu(f_i)^2}{\varphi(f_i)^2}\ll 1,$$

come già fatto in (3.3.37), (3.3.38), (3.3.42), otteniamo che l'espressione (3.4.5) è:

$$\ll\left(\prod_{i=1}^{k}\frac{g(r_i)r_i}{\varphi(r_i)^2}\right)\frac{y_{max}\varphi(W)\log R}{WD_0}\ll\frac{y_{max}\varphi(W)\log R}{WD_0}, \tag{3.4.6}$$

perché:

$$\frac{g(p)p}{\varphi(p)^2}=\frac{(p-2)p}{(p-1)^2}\leq 1,$$

per ogni primo p, e quindi a maggior ragione $\prod_{i=1}^{k}\frac{g(r_i)r_i}{\varphi(r_i)^2}\leq 1$, visto che r_i è libero da quadrati e $\frac{g(n)n}{\varphi(n)}$ è una funzione moltiplicativa. Troviamo che il contributo principale in (3.4.4) proviene dagli $a_j=r_j$, per tutti gli $j\neq m$. Abbiamo,

$$y^{(m)}_{r_1,\dots,r_k}=\left(\prod_{i=1}^{k}\frac{r_ig(r_i)}{\varphi(r_i)^2}\right)\sum_{a_m}\frac{y_{r_1,\dots,r_{m-1},a_m,r_{m+1},\dots,r_k}}{\varphi(a_m)}+O\left(\frac{y_{max}\varphi(W)\log R}{WD_0}\right). \tag{3.4.7}$$

Infine, notiamo che:

(3.4.8)

$$\prod_{i=1}^{k}\frac{r_ig(r_i)}{\varphi(r_i)^2}=\prod_{i=1}^{k}\prod_{p|r_i}\frac{p(p-2)}{(p-1)^2}=\prod_{i=1}^{k}\prod_{p|r_i}\left(1-\frac{1}{(p-1)^2}\right)\leq\prod_{i=1}^{k}\prod_{p|r_i}\left(1+\frac{1}{(p-1)^2}\right)$$

$$\leq\prod_{i=1}^{k}\prod_{p|r_i}\left(1+\frac{4}{p^2}\right)\leq\prod_{i=1}^{k}\exp\left(\sum_{p|r_i}\frac{4}{p^2}\right)\leq\prod_{i=1}^{k}\exp\left(\sum_{p>D_0}\frac{4}{p^2}\right)\leq\prod_{i=1}^{k}\exp\left(\frac{C}{D_0}\right),$$

per una certa costante $C>0$, usando che se $p|r_i$, allora $p>D_0$, visto che $(r_i,W)=1$. Siccome:

$$\prod_{i=1}^{k}\exp\left(\frac{C}{D_0}\right)\ll 1+\frac{1}{D_0},$$

inserendo (3.4.8) in (3.4.7) otteniamo che:

(3.4.9)

$$y^{(m)}_{r_1,\dots,r_k}=\sum_{a_m}\frac{y_{r_1,\dots,r_{m-1},a_m,r_{m+1},\dots,r_k}}{\varphi(a_m)}+O\left(\frac{y_{max}\varphi(W)\log R}{WD_0}\right)+O\left(\frac{y_{max}}{D_0}\sum_{\substack{a\leq R\\(a,W)=1}}\frac{\mu^2(a)}{\varphi(a)}\right)$$

$$=\sum_{a_m}\frac{y_{r_1,\dots,r_{m-1},a_m,r_{m+1},\dots,r_k}}{\varphi(a_m)}+O\left(\frac{y_{max}\varphi(W)\log R}{WD_0}\right)+O\left(\frac{y_{max}}{D_0}\frac{\varphi(W)}{W}\log R\right)$$

$$=\sum_{a_m}\frac{y_{r_1,\dots,r_{m-1},a_m,r_{m+1},\dots,r_k}}{\varphi(a_m)}+O\left(\frac{y_{max}\varphi(W)\log R}{WD_0}\right),$$

da (3.3.37). Questo conclude la dimostrazione. □

3.5 Scelta di una funzione liscia per y

Scegliamo ora opportuni valori per le nostre variabili y, in modo da massimizzare S_2/S_1, ovvero cerchiamo di massimizzare:

$$\lambda = \frac{\frac{N}{\log N\varphi(W)} \sum_{m=1}^{k} \sum_{r_1,\dots,r_k} \frac{(y^{(m)}_{r_1,\dots,r_k})^2}{\prod_{i=1}^{k} g(r_i)}}{\frac{N}{W} \sum_{r_1,\dots,r_k} \frac{y^2_{r_1,\dots,r_k}}{\prod_{i=1}^{k} \varphi(r_i)}}, \tag{3.5.1}$$

supponendo infatti nei nostri ragionamenti che i termini d'errore siano trascurabili. Consideriamo:

$$S_2\varphi(W)\log N - W\lambda S_1,$$

che da (3.5.1) possiamo supporre essere circa:

$$\sum_{m=1}^{k} \sum_{r_1,\dots,r_k} \frac{(y^{(m)}_{r_1,\dots,r_k})^2}{\prod_{i=1}^{k} g(r_i)} - \lambda \sum_{r_1,\dots,r_k} \frac{y^2_{r_1,\dots,r_k}}{\prod_{i=1}^{k} \varphi(r_i)}. \tag{3.5.2}$$

A questo punto cerchiamo i punti critici di (3.5.2) come funzione delle variabili $y_{b_1,\dots,b_k}$, con $b = b_1 \cdots b_k \leq R$ e $(b, W) = 1$, derivando e imponendo:

$$\sum_{m=1}^{k} \left(\frac{2y^{(m)}_{b_1,\dots,1,\dots,b_k}}{\prod_{i=1}^{k} g(b_i)} \right) - 2\lambda \frac{y_{b_1,\dots,b_k}}{\prod_{i=1}^{k} \varphi(b_i)} = 0, \tag{3.5.3}$$

ove in $y^{(m)}_{b_1,\dots,b_k}$ compare un 1 nella posizione $m-$esima, visto che $y^{(m)}_{b_1,\dots,b_k} = 0$ se $b_m \neq 1$. Quindi, per ogni tale scelta di $(b_1, \dots, b_k)$ arriviamo alla condizione:

$$\lambda y_{b_1,\dots,b_k} = \sum_{m=1}^{k} \prod_{i=1}^{k} \frac{\varphi(b_i)}{g(b_i)} y^{(m)}_{b_1,\dots,1,\dots,b_k}. \tag{3.5.4}$$

Ora visto che i termini y sono supportati sugli interi privi di piccoli fattori primi e che per gli interi r privi di piccoli fattori primi abbiamo $g(r) \approx \varphi(r) \approx r$, ovvero che questi tre numeri interi sono abbastanza vicini, la condizione (3.5.4) diventa:

$$\lambda y_{b_1,\dots,b_k} \approx \sum_{m=1}^{k} y^{(m)}_{b_1,\dots,1,\dots,b_k}, \tag{3.5.5}$$

ovvero possiamo trascurare il $\prod_{i=1}^{k} \frac{\varphi(b_i)}{g(b_i)}$ al fine di trovare una buona approssimazione per la funzione $y_{b_1,\dots,b_k}$ che soddisfi (3.5.4) e che massimizzi (3.5.1). Tale condizione sembra "liscia", nel senso che non dipende dalla fattorizzazione in primi degli b_i e quindi potrebbe essere soddisfatta scegliendo $y_{b_1,\dots,b_k}$ come un'opportuna funzione liscia degli $b_1, \dots, b_k$. Motivati da quanto detto, usando un'opportuna funzione liscia $F : \mathbb{R}^k \to \mathbb{R}$, supportata su:

$$\mathcal{R}_k := \{(x_1, \dots, x_k) \in [0,1]^k : \sum_{i=1}^{k} x_i \leq 1\},$$

scegliamo:

$$y_{b_1,\dots,b_k} = \begin{cases} F\left(\frac{\log b_1}{\log R}, \dots, \frac{\log b_k}{\log R}\right) & \text{se } (b = \prod_{i=1}^{k} b_i, W) = 1, \mu^2(b) = 1; \\ 0 & \text{altrimenti.} \end{cases} \tag{3.5.6}$$

3.5.1 Nuova forma per S_1

Usando (3.5.6) possiamo dedurre una nuova forma per S_1. Prima enunciamo un Lemma fondamentale nella teoria dei crivelli, il Lemma e la sua dimostrazione si possono trovare in [Greaves] [4], Teorema 2 in 2.2.2.

Lemma 3.5.1. *Sia γ una funzione moltiplicativa e $A_1, A_2, L > 0$ tali che:*

$$0 \leq \frac{\gamma(p)}{p} \leq 1 - \frac{1}{A_1}, \tag{3.5.7}$$

per ogni p primo, e per ogni $w, z \geq 2$ reali vale,

$$-L \leq \sum_{w \leq p < z} \frac{\gamma(p)\log p}{p} - k\log\left(\frac{z}{w}\right) \leq A_2, \tag{3.5.8}$$

per qualche $k \in \mathbb{R}$. Sia $g(d)$ la funzione completamente moltiplicativa definita sui primi da:

$$g(p) = \frac{\gamma(p)}{p - \gamma(p)}. \tag{3.5.9}$$

Allora,

$$\sum_{d<z} \mu(d)^2 g(d) = c_\gamma \frac{\log^k z}{\Gamma(k+1)}\left(1 + O\left(\frac{L}{\log z}\right)\right), \tag{3.5.10}$$

dove

$$c_\gamma = \prod_p \left(1 - \frac{\gamma(p)}{p}\right)^{-1}\left(1 - \frac{1}{p}\right)^k. \tag{3.5.11}$$

Ora enunciamo e dimostriamo un'importante risultato che segue dal Lemma 3.5.1.

Lemma 3.5.2. *Supponiamo verificate tutte le ipotesi del Lemma 3.5.1 e prendiamo $F : [0,1] \to \mathbb{R}$ differenziabile a tratti. Allora,*

(3.5.12)

$$\sum_{d<z} \mu(d)^2 g(d) F\left(\frac{\log\left(\frac{z}{d}\right)}{\log z}\right) = c_\gamma \frac{\log^k z}{\Gamma(k)} \int_0^1 F(1-x)x^{k-1}dx + O\big(c_\gamma L M(F)\log^{k-1} z\big),$$

dove

$$M(F) = \sup_{t\in[0,1]} \{|F(x)| + |F'(x)|\}. \tag{3.5.13}$$

Dimostrazione. Se poniamo:

$$H(u) = \sum_{d<u} \mu(d)^2 g(d), \tag{3.5.14}$$

usando la tecnica di sommazione parziale, otteniamo che:

$$\sum_{d<z}\mu(d)^2 g(d)F\left(\frac{\log\left(\frac{z}{d}\right)}{\log z}\right)=\int_1^z F\left(\frac{\log\left(\frac{z}{u}\right)}{\log z}\right)dH(u) \tag{3.5.15}$$

e dal Lemma 3.5.1 deduciamo che:

$$H(u)=c_\gamma\frac{\log^k u}{\Gamma(k+1)}+E(u), \tag{3.5.16}$$

con

$$E(u)\ll c_\gamma L\log^{k-1}(u). \tag{3.5.17}$$

Sostituendo (3.5.16) e (3.5.17) in (3.5.15) otteniamo,

$$\sum_{d<z}\mu(d)^2 g(d)F\left(\frac{\log\left(\frac{z}{d}\right)}{\log z}\right)=\int_1^z F\left(\frac{\log\left(\frac{z}{u}\right)}{\log z}\right)d\left(c_\gamma\frac{\log^k u}{\Gamma(k+1)}\right)+\int_1^z F\left(\frac{\log\left(\frac{z}{u}\right)}{\log z}\right)dE(u). \tag{3.5.18}$$

Nel primo integrale usiamo la sostituzione $u=z^x$ e visto che:

$$\frac{\log\left(\frac{z}{u}\right)}{\log z}=1-\frac{\log u}{\log z}=1-x,$$

$$d\left(c_\gamma\frac{\log^k u}{\Gamma(k+1)}\right)=c_\gamma\frac{\log^{k-1}u}{\Gamma(k)u}du=c_\gamma\frac{x^{k-1}\log^{k-1}z}{\Gamma(k)z^x}du=c_\gamma\frac{x^{k-1}\log^k z}{\Gamma(k)}dz,$$

poiché $du=z^x\log z dz$, otteniamo:

$$\int_1^z F\left(\frac{\log\left(\frac{z}{u}\right)}{\log z}\right)d\left(c_\gamma\frac{\log^k u}{\Gamma(k+1)}\right)=c_\gamma\frac{\log^k z}{\Gamma(k)}\int_0^1 F(1-x)x^{k-1}dx. \tag{3.5.19}$$

Nel secondo integrale integriamo per parti:

$$\int_1^z F\left(\frac{\log\left(\frac{z}{u}\right)}{\log z}\right)dE(u)=\int_1^z F\left(\frac{\log\left(\frac{z}{u}\right)}{\log z}\right)E(u)\Big|_1^z+\int_1^z E(u)F'\left(\frac{\log\left(\frac{z}{u}\right)}{\log z}\right)\frac{du}{u\log z} \tag{3.5.20}$$

$$\ll c_\gamma L\log^{k-1}(z)M(F)+\frac{c_\gamma LM(F)}{\log(z)}\int_1^z\frac{\log^{k-1}u}{u}du\ll c_\gamma L\log^{k-1}(z)M(F),$$

visto che l'ultimo integrale è uguale a $\frac{\log^k(z)}{k}$. Unendo (3.5.18), (3.5.19), (3.5.20) otteniamo (3.5.12). □

Notiamo che se $k=1$ e se poniamo:

$$G\left(\frac{\log d}{\log z}\right)=F\left(\frac{\log\left(\frac{z}{d}\right)}{\log z}\right), \tag{3.5.21}$$

ovvero $G(t) = F(1-t)$, allora (3.5.12) si semplifica ad:

$$\sum_{d<z} \mu(d)^2 g(d) G\left(\frac{\log d}{\log z}\right) = \prod_p \left(1 - \frac{\gamma(p)}{p}\right)^{-1} \left(1 - \frac{1}{p}\right) \log z \int_0^1 G(x)dx \tag{3.5.22}$$

$$+O(c_\gamma L G_{max} \log^{k-1} z),$$

ove:

$$G_{max} = \sup_{t\in[0,1]} (|G(t)| + |G'(t)|).$$

Nel prossimo Lemma deriviamo una nuova applicabile forma per S_1.

Lemma 3.5.3. *Per valori $r_1, ..., r_k$ naturali liberi da quadrati con $r = \prod_{i=1}^k r_i < R$ e coprimo con W, poniamo:*

$$y_{r_1,...,r_k} = F\left(\frac{\log r_1}{\log R}, \cdots, \frac{\log r_k}{\log R}\right), \tag{3.5.23}$$

con F come in (3.5.6); sia

$$F_{max} = \sup_{(t_1,...,t_k)\in[0,1]^k} \left(|F(t_1, ..., t_k)| + \sum_{i=1}^k \left|\frac{\partial F}{\partial t_i}(t_1, ..., t_k)\right|\right). \tag{3.5.24}$$

Allora abbiamo,

$$S_1 = \frac{\varphi(W)^k N(\log^k R) I_k(F)}{W^{k+1}} + O\left(\frac{F_{max}^2 \varphi(W)^k N \log^k R}{W^{k+1} D_0}\right), \tag{3.5.25}$$

dove

$$I_k(F) = \int_0^1 \cdots \int_0^1 F(t_1, ..., t_k)^2 dt_1 \cdots dt_k. \tag{3.5.26}$$

Dimostrazione. Inserendo (3.5.23) in (3.3.6), osserviamo che:

$$S_1 = \frac{N}{W} \sum_{\substack{u_1,...,u_k \\ (u_i,u_j)=1,\forall i\neq j \\ (u_i,W)=1,\forall i}} \left(\prod_{i=1}^k \frac{\mu(u_i)^2}{\varphi(u_i)}\right) F\left(\frac{\log u_1}{\log R}, \cdots, \frac{\log u_k}{\log R}\right)^2 \tag{3.5.27}$$

$$+O\left(\frac{F_{max}^2 \varphi(W)^k N \log^k R}{W^{k+1} D_0}\right).$$

Notiamo che due interi a, b con $(a, W) = (b, W) = 1$, ma con $(a, b) \neq 1$, devono avere un fattore primo in comune maggiore di D_0. Quindi possiamo omettere la richiesta $(u_i, u_j) = 1$, al costo di un errore pari a:

(3.5.28)

$$\ll \frac{F_{max}^2 N}{W} \sum_{p>D_0} \sum_{\substack{u_1,...,u_k<R \\ p|(u_i,u_j) \\ (u_i,W)=1,\forall i}} \left(\prod_{i=1}^k \frac{\mu(u_i)^2}{\varphi(u_i)}\right) \ll \frac{F_{max}^2 N}{W} \sum_{p>D_0} \frac{1}{(p-1)^2} \left(\sum_{\substack{u<R \\ (u,W)=1}} \frac{\mu(u)^2}{\varphi(u)}\right)^k$$

$$\ll \frac{F_{max}^2 \varphi(W)^k N \log^k R}{W^{k+1} D_0},$$

visto che:

$$\sum_{p>D_0} \frac{1}{(p-1)^2} \leq \sum_{n>D_0} \frac{1}{(n-1)^2} \ll \frac{1}{D_0}.$$

Quindi non ci resta che stimare la somma:

$$\sum_{\substack{u_1,\dots,u_k \\ (u_i,W)=1,\forall i}} \left(\prod_{i=1}^{k} \frac{\mu(u_i)^2}{\varphi(u_i)}\right) F\left(\frac{\log u_1}{\log R}, \cdots, \frac{\log u_k}{\log R}\right)^2. \tag{3.5.29}$$

A tal proposito applichiamo $k-$ volte il Lemma 3.5.2, lavorando ad ogni passo con la somma su ognuno degli u_i. In ogni passo usiamo:

$$\gamma(p) = \begin{cases} 1 & \text{se } p \nmid W; \\ 0 & \text{altrimenti.} \end{cases}$$

La scelta di $\gamma(p)$ è dettata dal fatto che, la funzione $g(d)$ del Lemma 3.5.2, in questo caso corrisponde a:

$$g(d) = \begin{cases} \frac{1}{\varphi(d)} & \text{se } (d,W)=1; \\ 0 & \text{altrimenti.} \end{cases}$$

Dunque, se $p \nmid W$ allora $\frac{\gamma(p)}{p-\gamma(p)} = \frac{1}{p-1}$ e così $\gamma(p) = 1$; altrimenti $g(p) = 0$ e anche $\gamma(p) = 0$. Con tale scelta di $\gamma(p)$ abbiamo,

$$0 \leq \frac{\gamma(p)}{p} \leq \frac{1}{p'} \leq 1 - A_1,$$

dove p' è il più piccolo primo maggiore di D_0. Visto che:

$$\sum_{w\leq p<z} \frac{\gamma(p)\log p}{p} = \sum_{w\leq p<z} \frac{\log p}{p} - \sum_{\substack{w\leq p<z \\ p|W}} \frac{\log p}{p} = \log\left(\frac{z}{w}\right) + O(1) - \sum_{\substack{w\leq p<z \\ p|W}} \frac{\log p}{p}$$

$$= \log\left(\frac{z}{w}\right) + O(1) + O(\log D_0),$$

troviamo che:

$$L \ll 1 + \log D_0 \ll \log D_0, N \to +\infty.$$

Infine, osserviamo che in ognuno dei k passi ci ritroviamo a stimare una somma simile a:

$$\sum_{u<R} \mu(u)^2 g(u) G\left(\cdots, \frac{\log u}{\log R}, \cdots\right) := \sum_{\substack{u<R \\ (u,W)=1}} \frac{\mu(u)^2}{\varphi(u)} F\left(\cdots, \frac{\log u}{\log R}, \cdots\right)^2, \tag{3.5.30}$$

che dal Lemma 3.5.2 è uguale a:

$$c_\gamma \log R \int_0^1 F\big(\cdots, t, \cdots\big)^2 dt \tag{3.5.31}$$

$$+O\Big(c_\gamma L(\log^{k-1} R)\sup_{t\in[0,1]}\Big\{\big|F\big(\cdots,t,\cdots\big)^2\big|+\big|2F\big(\cdots,t,\cdots\big)\frac{\partial F}{\partial t}\big(\cdots,t,\cdots\big)\big|\Big\}\Big),$$

dove ora:

$$c_\gamma=\prod_p\Big(1-\frac{\gamma(p)}{p}\Big)^{-1}\Big(1-\frac{1}{p}\Big)=\prod_{p\nmid W}\Big(1-\frac{1}{p}\Big)^{-1}\Big(1-\frac{1}{p}\Big)\prod_{p|W}\Big(1-\frac{1}{p}\Big)$$

$$=\prod_{p|W}\Big(1-\frac{1}{p}\Big)=\frac{\varphi(W)}{W}. \tag{3.5.32}$$

Iterando questo procedimento $k-$volte si ottiene immediatamente che (3.5.29) è uguale a:

$$\frac{\varphi(W)^k\log^k R}{W^k}I_k(F)+O\Big(\frac{F_{max}^2\varphi(W)^k(\log D_0)\log^{k-1}R}{W^k}\Big). \tag{3.5.33}$$

Unendo (3.5.27), (3.5.28) e (3.5.33) si ottiene la tesi. □

3.5.2 Nuova forma per S_2

Ora enunciamo e proviamo la controparte per S_2.

Lemma 3.5.4. *Fissato $m\in\{1,...,k\}$ abbiamo,*

$$S_2^{(m)}=\frac{\varphi(W)^kN\log^{k+1}R}{W^{k+1}\log N}J_k^{(m)}(F)+O\Big(\frac{F_{max}^2\varphi(W)^kN\log^kR}{W^{k+1}D_0}\Big), \tag{3.5.34}$$

dove

$$J_k^{(m)}(F)=\int_0^1\cdots\int_0^1\Big(\int_0^1F(t_1,...,t_k)dt_m\Big)^2dt_1\cdots dt_{m-1}dt_{m+1}\cdots dt_k. \tag{3.5.35}$$

Dimostrazione. La stima di $S_2^{(m)}$ è di nuovo simile a quella di S_1. Osserviamo che $y_{r_1,...,r_k}^{(m)}=0$ a meno che $r_m=1$ e $(r,W)=1$, con $r=\prod_{i=1}^k r_i$ libero da quadrati, nel qual caso $y_{r_1,...,r_k}^{(m)}$ è scritto in termini di $y_{r_1,...,r_k}$, grazie a (3.4.1). Ci concentriamo dunque sul caso in cui $y_{r_1,...,r_k}^{(m)}\neq 0$. Sostituiamo (3.5.23) in (3.4.1) e otteniamo:

$$y_{r_1,...,r_k}^{(m)}=\sum_{(u,Wr)=1}\frac{\mu(u)^2}{\varphi(u)}F\Big(\frac{\log r_1}{\log R},\cdots,\frac{\log r_{m-1}}{\log R},\frac{\log u}{\log R},\frac{\log r_{m+1}}{\log R},\cdots,\frac{\log r_k}{\log R}\Big)$$

$$+O\Big(\frac{F_{max}\varphi(W)\log R}{WD_0}\Big). \tag{3.5.36}$$

Ora stimiamo la somma in (3.5.36). Qui usiamo solo una volta il Lemma 3.5.2, con:

$$\gamma(p)=\begin{cases}1 & \text{se } p\nmid W;\\ 0 & \text{altrimenti.}\end{cases}$$

Scegliamo tale γ seguendo le stesse motivazioni già espresse nel Lemma 3.5.3. Inoltre, come nel Lemma 3.5.3, troviamo:

$$L \ll 1 + \sum_{p|Wr} \frac{\log p}{p} \ll \sum_{p \le \log R} \frac{\log p}{p} + \sum_{\substack{p|Wr \\ p > \log R}} \frac{\log p}{p}. \tag{3.5.37}$$

La prima somma è chiaramente $\ll \log\log R \ll \log\log N$ per (1.2.13) e (3.3.3). Siccome $W \ll \log\log N$ e $r < R$, se $p|Wr$ è chiaro che $p \le WR \ll (\log N)\log\log N$. Quindi $\log p \ll \log\log N$ e abbiamo,

$$\sum_{\substack{p|Wr \\ p > \log R}} \frac{\log p}{p} \ll \sum_{\substack{p|Wr \\ p > \log R}} \frac{\log\log N}{\log N} \le \frac{\log\log N}{\log N}\omega(Wr) \tag{3.5.38}$$

$$\ll \frac{\log\log N}{\log N}\log(WR) \ll \frac{(\log\log N)^2}{\log N},$$

poiché sappiamo che:

$$\omega(Wr) \le \frac{\log(Wr)}{\log 2} \le \frac{\log(WR)}{\log 2}.$$

Così otteniamo $L \ll \log\log N$. Questo ci fornisce:

$$y^{(m)}_{r_1,\dots,r_k} = (\log R)\frac{\varphi(W)}{W}\prod_{i=1}^{k}\frac{\varphi(r_i)}{r_i}F^{(m)}_{r_1,\dots,r_k} + O\left(\frac{F_{max}\varphi(W)\log R}{WD_0}\right), \tag{3.5.39}$$

lavorando come nella stima di (3.5.29), ponendo:

$$F^{(m)}_{r_1,\dots,r_k} := \int_0^1 F\left(\frac{\log r_1}{\log R},\cdots,\frac{\log r_{m-1}}{\log R},t_m,\frac{\log r_{m+1}}{\log R},\cdots,\frac{\log r_k}{\log R}\right)dt_m, \tag{3.5.40}$$

$$c_\gamma = \prod_{p|Wr}\left(1-\frac{1}{p}\right) = \frac{\varphi(W)}{W}\prod_{i=1}^{k}\frac{\varphi(r_i)}{r_i}. \tag{3.5.41}$$

Sostituendo l'equazione (3.5.39) nella (3.3.48) otteniamo:

$$S_2^{(m)} = \frac{N}{\log N\varphi(W)} \sum_{\substack{r_1,\dots,r_k \\ (r_i,W)=1,\forall i \\ (r_i,r_j)=1,\forall i\neq j \\ r_m=1}} \frac{(y^{(m)}_{r_1,\dots,r_k})^2}{\prod_{i=1}^k g(r_i)} \tag{3.5.42}$$

$$+O\left(\frac{(y^{(m)}_{max})^2\varphi(W)^{k-2}N\log^{k-2}N}{W^{k-1}D_0}\right) + O\left(\frac{y^2_{max}N}{\log^A N}\right)$$

$$= \frac{N\varphi(W)\log^2 R}{W^2\log N} \sum_{\substack{r_1,\dots,r_k \\ (r_i,W)=1,\forall i \\ (r_i,r_j)=1,\forall i\neq j \\ r_m=1}} \left(\prod_{i=1}^{k}\frac{\mu(r_i)^2\varphi(r_i)^2}{g(r_i)r_i^2}\right)(F^{(m)}_{r_1,\dots,r_k})^2$$

$$+O\bigg(\frac{(y_{max}^{(m)})^2\varphi(W)^{k-2}N\log^{k-2}N}{W^{k-1}D_0}\bigg)+O\bigg(\frac{y_{max}^2N}{\log^A N}\bigg)$$

$$+O\bigg(\frac{(F_{max})^2\varphi^2(W)\log^2 R}{W^2D_0^2}\frac{N}{\varphi(W)\log N}\sum_{\substack{r_1,\dots,r_k\\(r_i,W)=1,\forall i\\(r_i,r_j)=1,\forall i\neq j\\r_m=1}}\frac{1}{\prod_{i=1}^k g(r_i)}\bigg)$$

$$+O\bigg(\frac{(F_{max})^2\varphi^2(W)\log^2 R}{W^2D_0}\frac{N}{\varphi(W)\log N}\sum_{\substack{r_1,\dots,r_k\\(r_i,W)=1,\forall i\\(r_i,r_j)=1,\forall i\neq j\\r_m=1}}\prod_{i=1}^k\frac{\varphi(r_i)}{r_ig(r_i)}\bigg).$$

Ora osserviamo che:

$$\sum_{\substack{r_1,\dots,r_k\\(r_i,W)=1,\forall i\\(r_i,r_j)=1,\forall i\neq j\\r_m=1}}\frac{1}{\prod_{i=1}^k g(r_i)}\ll\bigg(\sum_{\substack{u\leq R\\(u,W)=1}}\frac{\mu(u)^2}{g(u)}\bigg)^{k-1}, \tag{3.5.43}$$

$$\sum_{\substack{r_1,\dots,r_k\\(r_i,W)=1,\forall i\\(r_i,r_j)=1,\forall i\neq j\\r_m=1}}\prod_{i=1}^k\frac{\varphi(r_i)}{r_ig(r_i)}\ll\bigg(\sum_{\substack{u\leq R\\(u,W)=1}}\frac{\varphi(u)\mu(u)^2}{ug(u)}\bigg)^{k-1}. \tag{3.5.44}$$

La somma in (3.5.43), dalla stima (3.3.64), sappiamo essere:

$$\ll\bigg(\frac{\varphi(W)\log R}{W}\bigg)^{k-1}$$

e siccome la somma in (3.5.44) è più piccola di quella in (3.5.43), otteniamo che il termine d'errore in (3.5.42) proveniente dagli ultimi due termini O-grande è:

$$O\bigg(\frac{F_{max}^2\varphi(W)^kN\log^k R}{W^{k+1}D_0}\bigg). \tag{3.5.45}$$

Ricordiamo che da (3.5.36) si deduce immediatamente che:

$$y_{max}^{(m)}\ll\frac{\varphi(W)F_{max}\log R}{W}. \tag{3.5.46}$$

Dunque, il termine d'errore (3.5.45) domina sui primi due in (3.5.42), visto che il secondo è chiaramente più piccolo di (3.5.45) e il primo è:

$$O\bigg(\frac{F_{max}^2\varphi(W)^kN\log^k N}{W^{k+1}D_0}\bigg). \tag{3.5.47}$$

Quindi abbiamo provato che:

$$S_2^{(m)} = \frac{N\varphi(W)\log^2 R}{W^2 \log N} \sum_{\substack{r_1,\dots,r_k \\ (r_i,W)=1,\forall i \\ (r_i,r_j)=1,\forall i\neq j \\ r_m=1}} \left(\prod_{i=1}^{k} \frac{\mu(r_i)^2\varphi(r_i)^2}{g(r_i)r_i^2}\right)(F^{(m)}_{r_1,\dots,r_k})^2 \tag{3.5.48}$$

$$+O\left(\frac{F_{max}^2\varphi(W)^k N\log^k R}{W^{k+1}D_0}\right).$$

Come per la stima di S_1 possiamo rimuovere la condizione $(r_i, r_j) = 1$ (vedi ad esempio (3.5.28)), introducendo un termine d'errore dell'ordine di:

$$\frac{F_{max}^2 N\varphi(W)\log^2 R}{W^2\log N}\left(\sum_{p>D_0}\frac{\varphi(p)^4}{p^4 g(p)^2}\right)\left(\sum_{\substack{r<R \\ (r,W)=1}}\frac{\mu(r)^2\varphi(r)^2}{g(r)r^2}\right)^{k-1}. \tag{3.5.49}$$

Siccome:

$$\sum_{\substack{r<R \\ (r,W)=1}}\frac{\mu(r)^2\varphi(r)^2}{g(r)r^2} \leq \sum_{\substack{r<R \\ (r,W)=1}}\frac{\mu(r)^2}{g(r)} \ll \frac{\varphi(W)\log R}{W}, \tag{3.5.50}$$

$$\sum_{p>D_0}\frac{\varphi(p)^4}{p^4 g(p)^2} = \sum_{p>D_0}\frac{(p-1)^4}{p^4(p-2)^2} \ll \sum_{p>D_0}\frac{1}{p^2} \ll \frac{1}{D_0}, \tag{3.5.51}$$

otteniamo che (3.5.49) è:

$$\ll \frac{F_{max}^2\varphi(W)^k N\log^k R}{W^{k+1}D_0}. \tag{3.5.52}$$

Dunque rimane solo da stimare la somma:

$$\sum_{\substack{r_1,\dots,r_{m-1},r_{m+1},\dots,r_k \\ (r_i,W)=1,\forall i}}\left(\prod_{\substack{i=1,\dots,k \\ i\neq m}}\frac{\mu(r_i)^2\varphi(r_i)^2}{g(r_i)r_i^2}\right)(F^{(m)}_{r_1,\dots,r_k})^2. \tag{3.5.53}$$

A tal proposito basta applicare ad ogni sommatoria coinvolta, rispetto alle variabili r_i, il Lemma 3.5.2. Infatti, in ogni passo basta prendere, per le stesse considerazioni già fatte nel Lemma 3.5.3 e nel Lemma 3.5.4, la funzione:

$$\gamma(p) = \begin{cases} 1 - \frac{p^2-3p+1}{p^3-p^2-2p+1} & \text{se } p \nmid W; \\ 0 & \text{altrimenti.} \end{cases}$$

In questo caso vale ancora che $L \ll 1 + \sum_{p|W}\frac{\log p}{p} \ll \log D_0$. Questo ci da (3.5.34) e con esso il Lemma. Infatti, il resto della stima di (3.5.53) segue in modo analogo

a quanto già fatto per stimare (3.5.29), con l'unica eccezione che ora la costante c_γ equivale a:

(3.5.54)

$$\prod_p\left(1-\frac{\gamma(p)}{p}\right)^{-1}\left(1-\frac{1}{p}\right)=\prod_{p\nmid W}\left(1-\frac{1}{p}+\frac{p^2-3p+1}{p^4-p^3-2p^2+p}\right)^{-1}\left(1-\frac{1}{p}\right)\prod_{p|W}\left(1-\frac{1}{p}\right)$$

$$\leq\prod_{p\nmid W}\left(1-\frac{1}{p}\right)^{-1}\left(1-\frac{1}{p}\right)\prod_{p|W}\left(1-\frac{1}{p}\right)=\prod_{p|W}\left(1-\frac{1}{p}\right)=\frac{\varphi(W)}{W},$$

dove abbiamo usato che:

$$1-\frac{1}{p}+\frac{p^2-3p+1}{p^4-p^3-2p^2+p}\geq 1-\frac{1}{p},$$

il che è coerente con il fatto che:

$$p\nmid W\Rightarrow p>D_0=\log\log\log N, N\to+\infty.$$ □

3.6 1° applicazione alle distanze tra numeri primi

Vediamo ora come applicare le stime di S_1 e S_2 per dimostrare che $S>0$, trovando risultati per distanze tra numeri primi.

Teorema 3.6.1. *Supponiamo che i primi abbiano livello di distribuzione $\theta>0$ e che $\mathcal{H}=\{h_1,...,h_k\}$ sia un insieme ammissibile. Sia S_k l'insieme di tutte le funzioni Riemann-integrabili della forma $F:[0,1]^k\to\mathbb{R}$ supportate su $\mathcal{R}_k$, con $I_k(F)\neq 0$ e $J_k^{(m)}(F)\neq 0$, per ogni $m=1,...,k$. Siano:*

(3.6.1)
$$M_k=\sup_{F\in S_k}\frac{\sum_{m=1}^k J_k^{(m)}(F)}{I_k(F)},$$

(3.6.2)
$$r_k=\left\lfloor\frac{\theta M_k}{2}\right\rfloor+1.$$

Allora ci sono infiniti interi n tali che almeno r_k tra gli $n+h_i$ $(1\leq i\leq k)$ sono primi. In particolare,

$$\liminf_{n\to+\infty}(p_{n+r_k-1}-p_n)\leq\max_{1\leq i,j\leq k}(h_i-h_j).$$

Dimostrazione. Sappiamo che $S=S_2-\rho S_1$ e ricordiamo che per dimostrare l'esistenza di infiniti interi n tali che almeno $\lfloor\rho+1\rfloor$ degli $n+h_i$ sono primi è sufficiente provare che $S>0$, se N è sufficientemente grande. Per definizione di M_k, possiamo scegliere $F_0\in S_k$ tale che:

(3.6.3)
$$\sum_{m=1}^k J_k^{(m)}(F_0)>(M_k-\delta)I_k(F_0),$$

se poniamo come sempre $R = N^{\theta/2-\delta}$. Siccome F_0 è Riemann-integrabile, esiste una funzione liscia F_1 tale che:

$$\sum_{m=1}^{k} J_k^{(m)}(F_1) > (M_k - 2\delta) I_k(F_1) > 0. \tag{3.6.4}$$

Ma ora sappiamo da (3.5.25) e da (3.5.34) che possiamo scegliere $\lambda_{d_1,\dots,d_k}$ tale che:

$$S = \frac{\varphi(W)^k N \log^k R}{W^{k+1}} \left(\frac{\log R}{\log N} \sum_{j=1}^{k} J_k^{(m)}(F_1) - \rho I_k(F_1) + o(1) \right) \tag{3.6.5}$$

$$\geq \frac{I_k(F_1)\varphi(W)^k N \log^k R}{W^{k+1}} \left(\left(\frac{\theta}{2} - \delta \right)(M_k - 2\delta) - \rho + o(1) \right), N \to +\infty.$$

Infine, scegliamo $\rho = \frac{\theta M_k}{2} - \varepsilon$, in modo tale che, scegliendo δ opportunamente piccolo, cioè che soddisfi:

$$\left(\left(\frac{\theta}{2} - \delta \right)(M_k - 2\delta) - \rho + o(1) \right) = \theta M_k/2 - \delta(M_k + \theta) + 2\delta^2 - \theta M_k/2 + \varepsilon + o(1) \tag{3.6.6}$$

$$= -\delta(M_k + \theta) + 2\delta^2 + \varepsilon + o(1) > 0,$$

otteniamo che $S > 0$, se N è sufficientemente grande. Infatti, è sufficiente mostrare che:

$$-\delta(M_k + \theta) + 2\delta^2 + \varepsilon > 0. \tag{3.6.7}$$

A tal fine possiamo prendere $\delta = \frac{\varepsilon}{(M_k+\theta)}$, ottenendo che (3.6.7) si riduce a:

$$-\frac{\varepsilon}{(M_k + \theta)}(M_k + \theta) + 2\left(\frac{\varepsilon}{(M_k + \theta)} \right)^2 + \varepsilon = 2\left(\frac{\varepsilon}{(M_k + \theta)} \right)^2 > 0. \tag{3.6.8}$$

Quindi, ci sono infiniti interi n tali che almeno $\lfloor \rho + 1 \rfloor$ degli $n + h_i$ sono primi. Per concludere basta mostrare che:

$$\lfloor \rho + 1 \rfloor = \left\lfloor \frac{\theta M_k}{2} \right\rfloor + 1,$$

se ε è sufficientemente piccolo. Per far questo notiamo che le seguenti disuguaglianze:

$$0 < \varepsilon < \frac{\theta M_k}{2} + 1 - \left\lfloor \frac{\theta M_k}{2} + 1 \right\rfloor = \left\{ \frac{\theta M_k}{2} \right\} < 1, \tag{3.6.9}$$

sono certamente verificate per ε sufficientemente piccolo. □

3.7 Scelta dei pesi per grandi k

Cercheremo ora di trovare dei pesi opportuni per costruire una buona minorazione di M_k, se k è grande. Otterremo tale minorazione costruendo un'opportuna funzione $F = F_k$ che renda il quoziente $\frac{\sum_{m=1}^{k} J_k^{(m)}(F)}{I_k(F)}$ grande, se k è grande. L'idea è quella di separare le variabili per facilitare i conti negli integrali e rendere F simmetrica in modo da togliere la dipendenza da m in tale quoziente. Quindi scegliamo F della forma:

$$F(t_1, ..., t_k) = \begin{cases} \prod_{i=1}^{k} g(kt_i) & \text{se } \sum_{i=1}^{k} t_i \leq 1; \\ 0 & \text{altrimenti.} \end{cases}$$

Qui usiamo una funzione $g : [0, +\infty] \to \mathbb{R}$, supportata su $[0, T]$, con $T \in \mathbb{R}^+$, che definiremo successivamente. Osserviamo dunque che con tale scelta basta considerare $J_k = J_k^{(1)}(F)$ e similmente scriviamo $I_k = I_k(F)$. Al fine di facilitare le notazioni poniamo:

$$\gamma = \int_{u \geq 0} g(u)^2 du \tag{3.7.1}$$

e restringiamo la nostra attenzione alle funzioni g per cui $\gamma > 0$.

Teorema 3.7.1. *Se k è sufficientemente grande vale,*

$$M_k \geq \log k - 2 \log \log k,$$

dove M_k è definito nella (3.6.1).

Dimostrazione. Abbiamo,

$$I_k(F) = \int_{\mathcal{R}_k} \cdots \int F(t_1, ..., t_k)^2 dt_1 \cdots dt_k \leq \left(\int_0^{+\infty} g(kt)^2 dt \right)^k = k^{-k} \gamma^k, \tag{3.7.2}$$

che si ottiene immediatamente dalla definizione di F, scambiando prodotto e integrali. Consideriamo ora J_k. Visto che i quadrati sono non negativi, per ottenere una minorazione di J_k, basta restringere l'integrale esterno a:

$$\sum_{i=2}^{k} t_i < 1 - \frac{T}{k}.$$

In tal modo, dal supporto di g, non ci sono ulteriori restrizioni da prendere in considerazione sull'integrale interno. Dunque,

$$J_k \geq \int_{\substack{t_2, ..., t_k \\ \sum_{i=2}^{k} t_i < 1 - T/k}} \cdots \int \left(\int_0^{T/k} \left(\prod_{i=1}^{k} g(kt_i) \right) dt_1 \right)^2 dt_2 \cdots dt_k. \tag{3.7.3}$$

Scriviamo la parte destra di (3.7.3) come $J_k' - E_k$, dove:

$$J_k' = \int_{t_2, ..., t_k \geq 0} \cdots \int \left(\int_0^{T/k} \left(\prod_{i=1}^{k} g(kt_i) \right) dt_1 \right)^2 dt_2 \cdots dt_k \tag{3.7.4}$$

$$= \left(\int_0^{+\infty} g(kt_1)dt_1\right)^2 \left(\int_0^{+\infty} g(kt)^2 dt\right)^{k-1} = k^{-k-1}\gamma^{k-1}\left(\int_0^{+\infty} g(u)du\right)^2,$$

visto che $g(kt)$ è supportata su $[0, \frac{T}{k}]$, mentre invece:

$$E_k = \int\cdots\int_{\substack{t_2,\ldots,t_k\geq 0 \\ \sum_{i=2}^k t_i > 1-T/k}} \left(\int_0^{T/k}\left(\prod_{i=1}^k g(kt_i)\right)dt_1\right)^2 dt_2\cdots dt_k \tag{3.7.5}$$

$$= k^{-k-1}\left(\int_0^{+\infty} g(u)du\right)^2 \int\cdots\int_{\substack{u_2,\ldots,u_k\geq 0 \\ \sum_{i=2}^k u_i > k-T}} \left(\prod_{i=2}^k g(u_i)^2\right)du_2\cdots du_k.$$

Per prima cosa mostriamo che l'integrale E_k è piccolo. Introduciamo una restrizione su g chiedendo che:

$$\mu := \frac{\int_0^{+\infty} ug(u)^2 du}{\int_0^{+\infty} g(u)^2 du} < 1 - \frac{T}{k}. \tag{3.7.6}$$

Quindi l'unica richiesta su g è quella di soddisfare (3.7.6). Poniamo:

$$\eta = \frac{k-T}{k-1} - \mu > 0. \tag{3.7.7}$$

Quando:

$$\sum_{i=2}^k u_i > k - T,$$

abbiamo,

$$\sum_{i=2}^k u_i > (k-1)(\mu+\eta)$$

e quindi:

$$1 \leq \eta^{-2}\left(\frac{1}{k-1}\sum_{i=2}^k u_i - \mu\right)^2. \tag{3.7.8}$$

Dunque, per ottenere una maggiorazione di E_k basta moltiplicare l'integranda per:

$$\eta^{-2}\left(\frac{1}{k-1}\sum_{i=2}^k u_i - \mu\right)^2 \tag{3.7.9}$$

e cancellare la richiesta $\sum_{i=1}^k u_i > k - T$. Questo ci da:

(3.7.10)

$$E_k \leq \frac{1}{\eta^2 k^{k+1}}\left(\int_0^{+\infty} g(u)du\right)^2 \int_0^{+\infty}\cdots\int_0^{+\infty}\left(\frac{\sum_{i=2}^k u_i}{k-1} - \mu\right)^2\left(\prod_{i=2}^k g(u_i)^2\right)du_2\cdots du_k.$$

Espandiamo il quadrato interno in (3.7.10) e troviamo:

$$\left(\frac{\sum_{i=2}^{k} u_i}{k-1} - \mu\right)^2 = \left(\frac{\sum_{i=2}^{k} u_i^2}{(k-1)^2} + \mu^2 - \frac{2\mu \sum_{i=2}^{k} u_i}{k-1} + \frac{2\sum_{2\le i<j\le k} u_i u_j}{(k-1)^2}\right). \tag{3.7.11}$$

Sostituendo (3.7.11) in (3.7.10) riscriviamo la parte destra di (3.7.10) come:

$$I_1 + I_2 + I_3 + I_4,$$

omettendo per il momento il fattore:

$$\frac{1}{\eta^2 k^{k+1}} \left(\int_0^{+\infty} g(u)du\right)^2.$$

Analizziamo tutti i quattro termini separatamente. Iniziamo con:

$$I_1 = \int_0^{+\infty} \cdots \int_0^{+\infty} \left(\frac{1}{(k-1)^2} \sum_{i=2}^{k} u_i^2\right) \left(\prod_{i=2}^{k} g(u_i)^2\right) du_2 \cdots du_k \tag{3.7.12}$$

$$= \frac{1}{(k-1)^2} \sum_{i=2}^{k} \int_0^{+\infty} \cdots \int_0^{+\infty} u_i^2 \left(\prod_{i=2}^{k} g(u_i)^2\right) du_2 \cdots du_k$$

$$\le \frac{1}{(k-1)^2} \sum_{i=2}^{k} \int_0^{+\infty} \cdots \int_0^{+\infty} T u_i g(u_i)^2 \left(\prod_{\substack{j=2,\dots,k \\ j\neq i}} g(u_j)^2\right) du_2 \cdots du_k$$

$$\le \frac{1}{(k-1)^2} \sum_{i=2}^{k} T\gamma^{k-2} \int_0^{+\infty} u_i g(u_i)^2 du_i = \frac{1}{(k-1)^2} \sum_{i=2}^{k} \mu T \gamma^{k-1} = \frac{1}{k-1} \mu T \gamma^{k-1},$$

dove nel passaggio dalla seconda alla terza riga abbiamo usato che, dal supporto di g, abbiamo:

$$u_j^2 g(u_j)^2 \le T u_j g(u_j)^2,$$

poiché solo gli $u_j \le T$ danno un contributo non nullo. Il termine:

$$I_2 = \mu^2 \int_0^{+\infty} \cdots \int_0^{+\infty} \prod_{i=2}^{k} g(u_i)^2 du_2 \cdots du_k,$$

è uguale a:

$$\mu^2 \gamma^{k-1}. \tag{3.7.13}$$

Infatti, basta scambiare prodotto e integrali, utilizzando (3.7.1) $(k-1)$-volte. Consideriamo ora:

$$I_3 = \frac{-2\mu}{k-1} \int_0^{+\infty} \cdots \int_0^{+\infty} \sum_{i=2}^{k} u_i \prod_{i=2}^{k} g(u_i)^2 du_2 \cdots du_k \tag{3.7.14}$$

$$= \frac{-2\mu}{k-1} \int_0^{+\infty} g(u_k)^2 du_k \cdots \int_0^{+\infty} g(u_3)^2 du_3 \int_0^{+\infty} g(u_2)^2 \sum_{i=2}^{k} u_i du_2.$$

Per calcolarlo esplicitamente ci concentriamo sull'integrale interno:
(3.7.15)

$$\int_0^{+\infty} g(u_2)^2 \sum_{i=2}^{k} u_i du_2 = \int_0^{+\infty} g(u_2)^2 u_2 du_2 + \int_0^{+\infty} g(u_2)^2 \sum_{i=3}^{k} u_i du_2 = \mu\gamma + \gamma \sum_{i=3}^{k} u_i.$$

Quindi (3.7.14) diventa:

$$\frac{-2\mu}{k-1} \mu\gamma\gamma^{k-2} + \gamma \int_0^{+\infty} \cdots \int_0^{+\infty} \prod_{i=3}^{k} g(u_i)^2 \sum_{i=3}^{k} u_i du_3 \cdots du_k. \tag{3.7.16}$$

In tal modo abbiamo ottenuto una relazione per ricorrenza, da cui, iterando il calcolo svolto in (3.7.15), si ottiene immediatamente che (3.7.14) equivale a:

$$\frac{-2\mu}{k-1} \underbrace{\mu\gamma^{k-1} + ... + \mu\gamma^{k-1}}_{k-1} = \frac{-2\mu}{k-1}(k-1)\mu\gamma^{k-1} = -2\mu^2\gamma^{k-1}. \tag{3.7.17}$$

Infine, studiamo il termine:

$$I_4 = \int_0^{+\infty} \cdots \int_0^{+\infty} \frac{2}{(k-1)^2} \sum_{2 \le i < j \le k} u_i u_j \prod_{i=2}^{k} g(u_i)^2 du_2 \cdots du_k. \tag{3.7.18}$$

Consideriamo:

$$\int_0^{+\infty} g(u_k)^2 du_k \cdots \int_0^{+\infty} g(u_l)^2 du_l \sum_{l \le i < j \le k} u_i u_j \tag{3.7.19}$$

e studiamo in primis:

$$\int_0^{+\infty} g(u_l)^2 du_l \sum_{l \le i < j \le k} u_i u_j \tag{3.7.20}$$

$$= \int_0^{+\infty} g(u_l)^2 u_l \sum_{j=l+1}^{k} u_j du_l + \int_0^{+\infty} g(u_l)^2 \sum_{l+1 \le i < j \le k} u_i u_j du_l$$

$$= \gamma\mu \sum_{j=l+1}^{k} u_j + \gamma \sum_{l+1 \le i < j \le k} u_i u_j.$$

Quindi (3.7.19) diventa:

$$\int_0^{+\infty} g(u_k)^2 du_k \cdots \int_0^{+\infty} g(u_{l+1})^2 du_{l+1} \left(\gamma\mu \sum_{j=l+1}^{k} u_j + \gamma \sum_{l+1 \le i < j \le k} u_i u_j \right), \tag{3.7.21}$$

che da (3.7.14), (3.7.15) e (3.7.16) equivale a:
(3.7.22)

$$\gamma\mu(k-(l+1)+1)\mu\gamma^{k-(l+1)+1}+\gamma\int_0^{+\infty}g(u_k)^2du_k\cdots\int_0^{+\infty}g(u_{l+1})^2du_{l+1}\sum_{l+1\le i<j\le k}u_iu_j$$

$$=\mu^2(k-l)\gamma^{k-l}+\gamma\int_0^{+\infty}g(u_k)^2du_k\cdots\int_0^{+\infty}g(u_{l+1})^2du_{l+1}\sum_{l+1\le i<j\le k}u_iu_j.$$

Abbiamo trovato dunque una formula ricorsiva che ci dice che (3.7.18) è pari a:

$$\frac{2}{(k-1)^2}(\mu^2\gamma^{k-1}(k-2)+\mu^2\gamma^{k-1}(k-3)+...+\mu^2\gamma^{k-1}) \tag{3.7.23}$$

$$=\frac{2}{(k-1)^2}\mu^2\gamma^{k-1}\frac{(k-1)(k-2)}{2}=\frac{\mu^2\gamma^{k-1}(k-2)}{(k-1)}.$$

Unendo (3.7.12), (3.7.13), (3.7.17), (3.7.23) troviamo che:
(3.7.24)

$$E_k\le\eta^{-2}k^{-k-1}\left(\int_0^{+\infty}g(u)du\right)^2\left(\frac{\mu T\gamma^{k-1}}{k-1}+\mu^2\gamma^{k-1}-2\mu^2\gamma^{k-1}+\mu^2\gamma^{k-1}\frac{k-2}{k-1}\right)=$$

$$\frac{1}{\eta^2k^{k+1}}\left(\int_0^{+\infty}g(u)du\right)^2\left(\frac{\mu T\gamma^{k-1}}{k-1}-\frac{\mu^2\gamma^{k-1}}{k-1}\right)\le\left(\int_0^{+\infty}g(u)du\right)^2\eta^{-2}k^{-k-1}\frac{\mu T\gamma^{k-1}}{k-1}.$$

Ora passiamo alla minorazione di M_k. Unendo (3.7.2), (3.7.4) e (3.7.24), troviamo che:

$$\frac{kJ_k}{I_k}\ge\frac{k}{k^{-k}\gamma^k}\left(k^{-k-1}\gamma^{k-1}-\frac{\mu}{\eta^2}\frac{\gamma^{k-1}k^{-k-1}T}{k-1}\right)\left(\int_0^{+\infty}g(u)du\right)^2 \tag{3.7.25}$$

$$=\frac{1}{\gamma}\left(\int_0^{+\infty}g(u)du\right)^2\left(1-\frac{\mu}{\eta^2}\frac{T}{k-1}\right)=\frac{\left(\int_0^{+\infty}g(u)du\right)^2}{\int_0^{+\infty}g(u)^2du}\left(1-\frac{\mu}{\eta^2}\frac{T}{k-1}\right).$$

Infine, osservando che:

$$(k-1)\eta^2\ge k\left(1-\frac{T}{k}-\mu\right)^2,$$

con $\mu\le 1$, troviamo che:

$$\frac{kJ_k}{I_k}\ge\frac{\left(\int_0^{+\infty}g(u)du\right)^2}{\int_0^{+\infty}g(u)^2du}\left(1-\frac{T}{k(1-T/k-\mu)^2}\right). \tag{3.7.26}$$

Per massimizzare (3.7.26) dobbiamo massimizzare $\int_0^T g(u)du$ soggetto alle restrizioni (3.7.1) e (3.7.6). Quindi vorremmo massimizzare l'espressione:

$$\int_0^T g(u)du-\alpha\left(\int_0^T g(u)^2du-\gamma\right)-\beta\left(\int_0^T ug(u)^2du-\mu\gamma\right) \tag{3.7.27}$$

$$= \int_0^T (g(u) - \alpha g(u)^2 - \beta u g(u)^2 du + \gamma(\alpha + \mu\beta),$$

rispetto a g ed $\alpha, \beta \in \mathbb{R}$. A tal proposito definiamo la Lagrangiana:

$$\mathcal{L}(t, g(t), g'(t)) = g(t) - \alpha g(t)^2 - \beta t g(t)^2 \tag{3.7.28}$$

e cerchiamo un punto stazionario per il funzionale azione:

$$S(g) = \int_0^T \mathcal{L}(t, g(t), g'(t))dt, \tag{3.7.29}$$

che chiaramente sarà dato da:

$$\frac{\partial}{\partial g}\mathcal{L}(t, g(t), g'(t)) = 0 \Leftrightarrow 1 - 2\alpha g - 2\beta t g = 0 \Leftrightarrow g = \frac{1}{2\alpha + 2\beta t}, \tag{3.7.30}$$

per $0 \leq t \leq T$. Visto che il quoziente da massimizzare non varia se moltiplico g per una costante positiva, possiamo restringere la nostra attenzione sulle funzioni g della forma:

$$g(t) = \frac{1}{1 + At},$$

per $0 \leq t \leq T$ ed $A > 0$. Con tale scelta di g troviamo che:

$$\int_0^T g(u)du = \frac{\log(1 + At)}{A}, \tag{3.7.31}$$

$$\int_0^T g(u)^2 du = \frac{1}{A}\left(1 - \frac{1}{1 + At}\right), \tag{3.7.32}$$

$$\int_0^T u g(u)^2 du = \frac{1}{A^2}\left(\log(1 + AT) - 1 + \frac{1}{1 + AT}\right). \tag{3.7.33}$$

Ora dobbiamo scegliere T ed A in modo che la funzione g verifichi (3.7.6). In tal modo troveremmo una minorazione per M_k via (3.7.26). Scegliamo per comodità T tale che $1 + AT = e^A$. Con tale scelta troviamo subito che:

$$\mu = \frac{\frac{1}{A^2}(A - 1 + e^{-A})}{\frac{1}{A}(1 - e^{-A})} = \frac{1}{(1 - e^{-A})} - \frac{1}{A} \tag{3.7.34}$$

e $T \leq e^A/A$. Quindi,

$$1 - \frac{T}{k} - \mu \geq 1 - \frac{e^A}{Ak} + \frac{1}{A} - \frac{1}{1 - e^{-A}} = \frac{1}{A}\left(1 - \frac{e^A}{k} - \frac{Ae^A}{e^A - 1} + A\right) \tag{3.7.35}$$

$$= \frac{1}{A}\left(1 - \frac{e^A}{k} - \frac{A}{e^A - 1}\right).$$

Sostituendo in (3.7.26) le stime (3.7.31), (3.7.32) e (3.7.35) troviamo che:

$$\frac{kJ_k}{I_k} \geq \left(1 - \frac{T}{k(1-T/k-\mu)^2}\right) \frac{\frac{\log(1+AT)^2}{A^2}}{\frac{1}{A}\left(1 - \frac{1}{1+AT}\right)} \tag{3.7.36}$$

$$\geq \left(1 - \frac{T}{k(1-T/k-\mu)^2}\right) \frac{A}{1-e^{-A}} \geq \frac{A}{1-e^{-A}} \left(1 - \frac{e^A}{A}\frac{1}{k}\frac{A^2}{\left(1 - \frac{A}{e^A-1} - \frac{e^A}{k}\right)^2}\right)$$

$$\geq A\left(1 - \frac{Ae^A}{k\left(1 - \frac{A}{e^A-1} - \frac{e^A}{k}\right)^2}\right).$$

Infine, scegliamo:

$$A = \log k - 2\log\log k > 0. \tag{3.7.37}$$

Per k sufficientemente grande abbiamo,

$$1 - \frac{T}{k} - \mu \geq \frac{1}{A}\left(1 - \frac{A}{\left(\frac{k}{\log^2 k} - 1\right)} - \frac{k}{k\log^2 k}\right) \geq \frac{1}{A}\left(1 - \frac{A\log^2 k}{k - \log^2 k} - \frac{1}{\log^2 k}\right). \tag{3.7.38}$$

Osserviamo che:

$$\frac{A}{k - \log^2 k} \leq \frac{\log k}{k},$$

che è vero se e solo se:

(3.7.39)

$$Ak \leq k\log k - \log^3 k \Leftrightarrow k\log k - 2k\log\log k \leq k\log k - \log^3 k \Leftrightarrow 2k\log\log k \geq \log^3 k,$$

che è certamente vero se k è sufficientemente grande. Quindi,

$$1 - \frac{T}{k} - \mu \geq \frac{1}{A}\left(1 - \frac{\log^3 k}{k} - \frac{1}{\log^2 k}\right) > 0, \tag{3.7.40}$$

per k sufficientemente grande. Questo implica che $\mu < 1 - \frac{T}{k}$ e quindi i conti svolti, per cercare una minorazione di M_k, sono consistenti con la scelta di $g(t) = \frac{1}{1+At}$, con $A = \log k - 2\log\log k$. Otteniamo che:

$$M_k \geq \frac{kJ_k}{I_k} \geq (\log k - 2\log\log k)\left(1 - \frac{(\log k - 2\log\log k)\frac{k}{\log^2 k}}{k\left(1 - \frac{(\log k - 2\log\log k)}{\frac{k}{\log^2 k} - 1} - \frac{1}{\log^2 k}\right)^2}\right) \tag{3.7.41}$$

$$\geq (\log k - 2\log\log k)\left(1 - \frac{\log k}{(\log^2 k)\left(1 - \frac{\log^2 k(\log k - 2\log\log k)}{k - \log^2 k} - \frac{1}{\log^2 k}\right)^2}\right)$$

$$= (\log k - 2\log\log k)\left(1 - \frac{\log k}{(\log^2 k)\left(1 + O\left(\frac{1}{\log^2 k}\right)\right)}\right),$$

svolgendo il quadrato al denominatore e osservando che tutti i termini, a parte 1, sono un $O\left(\frac{1}{\log^2 k}\right)$. Quindi (3.7.41) diventa:

$$\geq (\log k - 2\log\log k)\left(1 - \frac{\log k}{\log^2 k + O(1)}\right) \geq \log k - 2\log\log k - 1,$$

se k è sufficientemente grande. Infatti,

$$\frac{(\log k - 2\log\log k)\log k}{\log^2 k + O(1)} \leq 1$$

$$\Leftrightarrow (\log k - 2\log\log k)\log k \leq \log k\left(\log k + O\left(\frac{1}{\log k}\right)\right),$$

che è vero se k è sufficientemente grande, dato che:

$$\log k + o(1) \geq \log k - 2\log\log k, \tag{3.7.42}$$

se k è sufficientemente grande. □

3.8 2° applicazione alle distanze tra numeri primi

Vedremo ora come tale minorazione per M_k conduce ad informazioni sulle distanze tra numeri primi:

Teorema 3.8.1. *Per ogni $m \in \mathbb{N}$ si ha,*

$$\liminf_{n\to+\infty}(p_{n+m} - p_n) \ll m^3 e^{4m}. \tag{3.8.1}$$

Dimostrazione. Dal Teorema 2.1.13 possiamo prendere $\theta = \frac{1}{2} - \varepsilon$, con $\frac{1}{2} > \varepsilon > 0$, e ottenere dal Teorema 3.7.1:

$$\frac{\theta M_k}{2} \geq \left(\frac{1}{4} - \frac{\varepsilon}{2}\right)(\log k - 2\log\log k - 1). \tag{3.8.2}$$

Ora vorremmo:

$$\frac{\theta M_k}{2} \geq m,$$

che è vero se:

$$(1-2\varepsilon)(\log k - 2\log\log k - 1) > 4m \Leftrightarrow \frac{k^{1-2\varepsilon}}{\log^{2-4\varepsilon} k} > e^{4m+1-2\varepsilon}. \tag{3.8.3}$$

Basta dimostrare che:

$$\frac{k^{1-2\varepsilon}}{\log^2 k} > e^{4m+1}, \tag{3.8.4}$$

per k sufficientemente grande. Scegliamo:

$$\varepsilon = \frac{1}{2\log k},$$

così che:

$$k^{1-2\varepsilon} = \frac{k}{e}.$$

Ci riduciamo a trovare un k per cui vale:

$$\frac{k}{\log^2 k} > e^2 e^{4m}. \tag{3.8.5}$$

Osserviamo che la funzione $h(t) = \frac{t}{\log^2 t}$ è crescente per $t \geq e^2$ e quindi basta mostrare l'esistenza di uno speciale valore $k_0 \in \mathbb{R}$, per cui (3.8.5) sia verificata, e poi lo sarà automaticamente per ogni $k \geq k_0$. Consideriamo ad esempio:

$$k_0 = 1065m^2e^{4m}. \tag{3.8.6}$$

Notiamo che vale:

$$1065m^2e^{4m} < e^{12m}, \tag{3.8.7}$$

per ogni $m \in \mathbb{N}$. Infatti, la disuguaglianza:

$$1065m^2 < e^{8m},$$

è verificata per ogni m, come si può vedere con un semplice ragionamento induttivo. Quindi, per tale k_0 abbiamo,

$$\frac{k_0}{\log^2 k_0} > \frac{1065m^2e^{4m}}{144m^2} > e^{4m+2}, \tag{3.8.8}$$

visto che:

$$1065 > 144e^2 = 1064,024078...$$

Quindi, per ogni insieme ammissibile $\mathcal{H} = \{h_1, ..., h_k\}$, con $k \geq 1065m^2e^{4m}$, intero positivo, esistono infiniti interi n tali che almeno $m+1$ degli $n + h_i$ devono essere primi. Visto che possiamo scegliere il nostro insieme come $\{p_{\pi(k)+1}, ..., p_{\pi(k)+k}\}$ (vedi quanto specificato sotto la Definizione 3.1) che ha diametro:

$$p_{\pi(k)+k} - p_{\pi(k)+1} \ll k\log k, \tag{3.8.9}$$

usando il Corollario 1.2.9, abbiamo che:

$$\liminf_{n\to+\infty}(p_{n+m} - p_n) \ll k\log k \ll m^3e^{4m}, \tag{3.8.10}$$

se prendiamo $k = \lfloor 1065m^2e^{4m} + 1 \rfloor$. Questo conclude il teorema. □

Ora proveremo che una proporzione positiva di $m-$uple ammissibili soddisfa la Congettura 3.1, per ogni m, in un senso appropriato.

Teorema 3.8.2. *Sia $m \in \mathbb{N}$ e $r \in \mathbb{N}$ sufficientemente grande e dipendente da m, e sia $\mathcal{A} = \{a_1, ..., a_r\}$ un insieme di r interi distinti. Definiamo:*

$$\mathcal{B}_1 = \{\{h_1, ..., h_m\} \subset \mathcal{A} : \textit{per infiniti } n, \textit{ tutti gli } n + h_1, ..., n + h_m \textit{ sono primi}\},$$

$$\mathcal{B}_2 = \{\{h_1, ..., h_m\} \subset \mathcal{A}\}.$$

Allora abbiamo,

$$\frac{|\mathcal{B}_1|}{|\mathcal{B}_2|} \gg_m 1. \tag{3.8.11}$$

Dimostrazione. Dato m, poniamo $k = \lfloor 1065m^2e^{4m} + 1 \rfloor$. Allora se $\{h_1, ..., h_k\}$ è ammissibile, esiste un sottoinsieme:

$$\{h_1', ..., h_m'\} \subset \{h_1, ..., h_k\}, \tag{3.8.12}$$

con la proprietà che esistono infiniti interi n per i quali tutti gli $n + h_i'$ sono primi $(1 \leq i \leq m)$. Denotiamo con $\mathcal{A}^*$ l'insieme formato partendo inizialmente da $\mathcal{A}$ e rimuovendo successivamente, per ogni primo $p \leq k$, tutti gli elementi delle classi residuali modulo p che contengono il più piccolo intero rimasto. Osserviamo che:

$$|\mathcal{A}^*| \geq r \prod_{p \leq k} \left(1 - \frac{1}{p}\right) \gg \frac{r}{\log k} \gg_m r. \tag{3.8.13}$$

Inoltre, ogni sottoinsieme di $\mathcal{A}^*$, composto da k elementi, deve essere ammissibile, dato che non può ricoprire tutte le classi residuali modulo p, per ogni primo $p \leq k$. Poniamo $s = |\mathcal{A}^*|$. Siccome r è preso sufficientemente grande in termini di m, possiamo assumere $s > k$. Osserviamo che ci sono $\binom{s}{k}$ insiemi $\mathcal{H} \subset \mathcal{A}^*$ composti da k elementi. Ognuno di questi è ammissibile e quindi contiene almeno un sottoinsieme $\{h_1', ..., h_m'\} \subset \mathcal{A}^*$ che soddisfa la Congettura 3.1, per (3.8.12). Ogni insieme ammissibile $\mathcal{B} \subset \mathcal{A}^*$, di m elementi, è contenuto in $\binom{s-m}{k-m}$ insiemi $\mathcal{H} \subset \mathcal{A}^*$ di k elementi. Quindi ci sono almeno:

(3.8.14)

$$\binom{s}{k}\binom{s-m}{k-m}^{-1} = \frac{s!(k-m)!(s-k)!}{k!(s-k)!(s-m)!} = \frac{s!(k-m)!}{k!(s-m)!} = \frac{s(s-1)\cdots(s-m+1)}{k(k-1)\cdots(k-m+1)}$$

$$\gg_m \frac{s^m}{k^m} \gg_m s^m \gg_m r^m$$

insiemi ammissibili $\mathcal{B} \subset \mathcal{A}^*$, composti da m elementi, che soddisfano la Congettura 3.1, dove abbiamo usato che $k \ll m^2e^{4m}$. Siccome ci sono $\binom{r}{m} \leq r^m$ insiemi $\{h_1, ..., h_m\} \subset \mathcal{A}$, il teorema segue. □

3.9 Scelta dei pesi per piccoli k

In questo capitolo cercheremo di trovare delle buone maggiorazioni per M_k, nel caso di piccoli k. A tal proposito, fissato P polinomio, introduciamo la funzione ottimale:

$$F(t_1, ..., t_k) = \begin{cases} P(t_1, ..., t_k) & \text{se } (t_1, ..., t_k) \in \mathcal{R}_k; \\ 0 & \text{altrimenti.} \end{cases}$$

Dalla simmetria di $\sum_{m=1}^{k} J_k^{(m)}(F)$ e $I_k(F)$, possiamo restringere la nostra attenzione ai polinomi che sono espressioni simmetriche di $t_1, ..., t_k$. Ogni tale polinomio può essere scritto come un'espressione polinomiale nei polinomi $P_j = \sum_{i=1}^{k} t_i^j$.

Lemma 3.9.1. *Siano $a, b, j \in \mathbb{N}$. Abbiamo,*

$$\int_{\mathcal{R}_k} \cdots \int (1 - P_1)^a P_j^b dt_1 \cdots dt_k = \frac{a!}{(k + jb + a)!} G_{b,j}(k), \tag{3.9.1}$$

dove

$$G_{b,j}(k) = b! \sum_{r=1}^{k} \binom{k}{r} \sum_{\substack{b_1,...,b_r \geq 1 \\ \sum_{i=1}^{r} b_i = b}} \prod_{i=1}^{r} \frac{(jb_i)!}{b_i!}. \tag{3.9.2}$$

Dimostrazione. Per prima cosa mostriamo per induzione su k che:

$$\int_{\mathcal{R}_k} \cdots \int \left(1 - \sum_{i=1}^{k} t_i\right)^a \prod_{i=1}^{k} t_i^{a_i} dt_1 \cdots dt_k = \frac{a! \prod_{i=1}^{k} a_i!}{(k + a + \sum_{i=1}^{k} a_i)!}, \tag{3.9.3}$$

per $a_1, ..., a_k \in \mathbb{N}$, considerando inizialmente l'integrale rispetto a t_1. I limiti di integrazione sono 0 e $1 - \sum_{i=2}^{k} t_i$, per $(t_2, ..., t_k) \in \mathcal{R}_{k-1}$. Sostituendo:

$$v = \frac{t_1}{\left(1 - \sum_{i=2}^{k} t_i\right)}, \tag{3.9.4}$$

troviamo:

$$\int_0^{1-\sum_{i=2}^{k} t_i} \left(1 - \sum_{i=1}^{k} t_i\right)^a \prod_{i=1}^{k} t_i^{a_i} dt_1 = \prod_{i=2}^{k} t_i^{a_i} \left(1 - \sum_{i=1}^{k} t_i\right)^{a+a_1+1} \int_0^1 (1-v)^a v^{a_1} dv. \tag{3.9.5}$$

Infatti, sostituiamo $t_1 = v\left(1 - \sum_{i=2}^{k} t_i\right)$ e osserviamo che:

(3.9.6)

$$1 - \sum_{i=1}^{k} t_i = \frac{t_1}{v} - t_1 = t_1\left(-1 + \frac{1}{v}\right) = \left(-1 + \frac{1}{v}\right) v \left(1 - \sum_{i=2}^{k} t_i\right) = (1 - v)\left(1 - \sum_{i=2}^{k} t_i\right).$$

Infine, sostituiamo:

$$dv = \frac{dt_1}{\left(1 - \sum_{i=2}^{k} t_i\right)}. \tag{3.9.7}$$

Ora si deduce immediatamente che (3.9.5) è uguale a:

$$\frac{a! a_1!}{(a + a_1 + 1)!} \left(\prod_{i=2}^{k} t_i^{a_i}\right) \left(1 - \sum_{i=2}^{k} t_i\right)^{a+a_1+1}, \tag{3.9.8}$$

dove abbiamo usato l'identità (1.1.25):

$$\int_0^1 (1-v)^a v^b dv = \frac{a!b!}{(a+b+1)!}. \tag{3.9.9}$$

Iterando tali ragionamenti k volte si ottiene subito (3.9.3). Ora dal teorema binomiale si evince che:

$$P_j^b = \sum_{\substack{b_1,\dots,b_k \\ \sum_{i=1}^k b_i = b}} \frac{b!}{\prod_{i=1}^k b_i!} \prod_{i=1}^k t_i^{jb_i}. \tag{3.9.10}$$

Combinando (3.9.3) e (3.9.10) è evidente che:

$$\int_{\mathcal{R}_k} \cdots \int (1-P_1)^a P_j^b dt_1 \cdots dt_k = \frac{a!b!}{(k+jb+a)!} \sum_{\substack{b_1,\dots,b_k \\ \sum_{i=1}^k b_i = b}} \prod_{i=1}^k \frac{(jb_i)!}{b_i!}. \tag{3.9.11}$$

In vista dei successivi calcoli, in cui b sarà piccolo, cerchiamo di isolare, nella somma in (3.9.11), la parte in cui i vari b_i sono non nulli. A tal proposito, notiamo che dato un intero r, ci sono $\binom{k}{r}$ modi di scegliere r elementi tra $b_1, ..., b_k$ non nulli. Quindi,

$$\sum_{\substack{b_1,\dots,b_k \\ \sum_{i=1}^k b_i = b}} \prod_{i=1}^k \frac{(jb_i)!}{b_i!} = \sum_{r=1}^k \binom{k}{r} \sum_{\substack{b_1,\dots,b_r \geq 1 \\ \sum_{i=1}^r b_i = b}} \prod_{i=1}^r \frac{(jb_i)!}{b_i!}. \tag{3.9.12}$$

Unendo (3.9.11) con (3.9.12) si ottiene la tesi. □

Utilizzeremo ora il Lemma 3.9.1 per ottenere espressioni più maneggevoli per $I_k(F)$ e $J_k^{(m)}(F)$, scegliendo P come espressione polinomiale dei soli P_1, P_2.

Lemma 3.9.2. *Siano F e P come sopra. Siano $a_i \in \mathbb{R}$, $b_i, c_i \in \mathbb{N}$, per ogni $i = 1, ..., d$ con $d \in \mathbb{N}$. In particolare, scegliamo:*

$$P = \sum_{i=1}^d a_i (1-P_1)^{b_i} P_2^{c_i}. \tag{3.9.13}$$

Allora per ogni $1 \leq m \leq k$ abbiamo,

$$I_k(F) = \sum_{1 \leq i,j \leq d} a_i a_j \frac{(b_i+b_j)! G_{c_i+c_j,2}(k)}{(k+b_i+b_j+2c_i+2c_j)!}, \tag{3.9.14}$$

$$J_k^{(m)}(F) = \sum_{1 \leq i,j \leq d} a_i a_j \sum_{c_1'=0}^{c_i} \sum_{c_2'=0}^{c_j} \binom{c_i}{c_1'} \binom{c_j}{c_2'} \frac{\gamma_{b_i,b_j,c_i,c_j,c_1',c_2'} G_{c_1'+c_2',2}(k-1)}{(k+b_i+b_j+2c_i+2c_j+1)!}, \tag{3.9.15}$$

dove

$$\gamma_{b_i,b_j,c_i,c_j,c_1',c_2'} = \frac{b_i! b_j! (2c_i-2c_1')! (2c_j-2c_2')! (b_i+b_j+2c_i+2c_j-2c_1'-2c_2'+2)!}{(b_i+2c_i-2c_1'+1)! (b_j+2c_j-2c_2'+1)!}. \tag{3.9.16}$$

Dimostrazione. Consideriamo per primo $I_k(F)$. Usando il Lemma 3.9.1 otteniamo:
(3.9.17)

$$I_k(F) = \int_{\mathcal{R}_k} \cdots \int P^2 dt_1 \cdots dt_k = \sum_{1\le i,j\le k} a_i a_j \int_{\mathcal{R}_k} \cdots \int (1-P_1)^{b_i+b_j} P_2^{c_i+c_j} dt_1 \cdots dt_k$$

$$= \sum_{1\le i,j\le k} a_i a_j \frac{(b_i+b_j)! G_{c_i+c_j,2}(k)}{(k+b_i+b_j+2c_i+2c_j)!}.$$

Ora consideriamo $J_k^{(m)}(F)$. Visto che F è simmetrico in $t_1,..,t_k$, osserviamo che $J_k^{(m)}(F)$ è indipendente da m, e quindi è sufficiente considerare $J_k^{(1)}(F)$. Abbiamo,
(3.9.18)

$$\int_0^{1-\sum_{i=2}^k t_i} (1-P_1)^b P_2^c dt_1 = \sum_{c'=0}^{c} \binom{c}{c'} \left(\sum_{i=2}^k t_i^2\right)^{c'} \int_0^{1-\sum_{i=2}^k t_i} \left(1-\sum_{i=1}^k t_i\right)^b t_1^{2c-2c'} dt_1$$

$$= \sum_{c'=0}^{c} \binom{c}{c'} (P_2')^{c'} (1-P_1')^{b+2c-2c'+1} \int_0^1 (1-u)^b u^{2c-2c'} du$$

$$= \sum_{c'=0}^{c} \binom{c}{c'} (P_2')^{c'} (1-P_1')^{b+2c-2c'+1} \frac{b!(2c-2c')!}{(b+2c-2c'+1)!},$$

dove $P_1' = \sum_{i=2}^k t_i$ e $P_2' = \sum_{i=2}^k t_i^2$, con $b, c \in \mathbb{N}$, usando (1.1.25) per calcolare l'ultimo integrale e un cambiamento di variabili analogo a (3.9.4) per calcolare il primo integrale a destra dell'uguaglianza in (3.9.18). Quindi,

$$\left(\int_0^1 F dt_1\right)^2 = \left(\sum_{i=1}^d a_i \int_0^{1-\sum_{j=2}^k t_j} (1-P_1)^{b_i} P_2^{c_i} dt_1\right)^2 \tag{3.9.19}$$

$$= \sum_{1\le i,j\le d} a_i a_j \sum_{c_1'=0}^{c_i} \sum_{c_2'=0}^{c_j} \binom{c_i}{c_1'} \binom{c_j}{c_2'} (P_2')^{c_1'+c_2'} (1-P_1')^{b_i+b_j+2c_i+2c_j-2c_1'-2c_2'+2}$$

$$\times \frac{b_i! b_j! (2c_i-2c_1')! (2c_j-2c_2')!}{(b_i+2c_i-2c_1'+1)!(b_j+2c_j-2c_2'+1)!}.$$

Infine, applichiamo ancora una volta il Lemma 3.9.1, ottenendo:

$$\int_{\mathcal{R}_{k-1}} \cdots \int (1-P_1')^b P_2'^c dt_2 \cdots dt_k = \frac{b!}{(k+b+c-1)!} G_{c,2}(k-1). \tag{3.9.20}$$

Unendo (3.9.19) e (3.9.20) otteniamo il risultato. □

Osserviamo che $I_k(F)$ e $J_k^{(m)}(F)$ possono essere espressi come forme quadratiche nei coefficienti $\mathbf{a} = (a_1, ..., a_d)$ di P. Inoltre, esse saranno forme quadratiche reali definite positive. Infatti, se scriviamo:

$$\frac{\sum_{m=1}^k J_k^{(m)}(F)}{I_k(F)} = \frac{\mathbf{a}^T A_2 \mathbf{a}}{\mathbf{a}^T A_1 \mathbf{a}}, \tag{3.9.21}$$

usando che le matrici hanno coefficienti reali positivi, che $I_k(F)$ e $\sum_{m=1}^{k} J_k^{(m)}(F)$ sono positivi e che vale la relazione (3.9.21), troviamo che A_1, A_2 sono definite positive. Notiamo che (3.9.21), come quoziente di due forme quadratiche definite positive simmetriche e reali, può essere calcolato esplicitamente attraverso il seguente

Lemma 3.9.3. *Siano A_1, A_2 matrici reali, simmetriche e definite positive. Allora,*

$$\frac{\boldsymbol{a}^T A_2 \boldsymbol{a}}{\boldsymbol{a}^T A_1 \boldsymbol{a}} \tag{3.9.22}$$

è massimizzato quando $\boldsymbol{a}$ è un autovettore di:

$$A_1^{-1} A_2, \tag{3.9.23}$$

corrispondente al più grande autovalore di (3.9.23). Il valore massimo di (3.9.22) è pari all'autovalore massimo di (3.9.23).

Dimostrazione. Osserviamo che moltiplicare $\mathbf{a}$ per uno scalare non nullo non cambia il valore di (3.9.22); quindi possiamo assumere senza perdita di generalità che $\mathbf{a}^T A_1 \mathbf{a} = 1$. Dalla teoria dei moltiplicatori di Lagrange, otteniamo che $\mathbf{a}^T A_2 \mathbf{a}$ è massimizzato, soggetto ad $\mathbf{a}^T A_1 \mathbf{a} = 1$, quando $\mathbf{a}$ è un punto stazionario per:

$$L(\mathbf{a},\lambda) = \mathbf{a}^T A_2 \mathbf{a} - \lambda(\mathbf{a}^T A_1 \mathbf{a} - 1). \tag{3.9.24}$$

Questo succede quando:

$$0 = \frac{\partial L}{\partial \mathbf{a}} \Leftrightarrow 2A_2\mathbf{a} - 2\lambda A_1 \mathbf{a} = 0 \Leftrightarrow A_2\mathbf{a} = \lambda A_1 \mathbf{a} \Leftrightarrow A_1^{-1} A_2 \mathbf{a} = \lambda \mathbf{a}. \tag{3.9.25}$$

È ora chiaro che:

$$\mathbf{a}^T A_1 \mathbf{a} = \lambda^{-1} \mathbf{a}^T A_2 \mathbf{a}. \tag{3.9.26}$$

□

Il lavoro svolto fino ad ora ci permette attraverso l'ausilio del calcolo computazionale di trovare ottime maggiorazioni per M_k, quando k è piccolo. In particolare, vedremo nella prossima sezione quali sono i risultati ottenuti scegliendo $k = 5$ e $k = 105$.

3.10 3° applicazione alle distanze tra numeri primi

Teorema 3.10.1. *Abbiamo,*

$$M_5 > 2, \tag{3.10.1}$$

$$M_{105} > 4. \tag{3.10.2}$$

Dimostrazione. Siano F e P come sopra. In particolare, prendiamo P come espressione polinomiale nei polinomi P_1 e P_2 e più nello specifico combinazione lineare di $(1-P_1)^b P_2^c$, con b, c interi non negativi tali che $b+2c \leq 11$. Ci sono 42 tali monomi usando $k = 105$. Attraverso l'uso di specifici programmi possiamo calcolare le 42×42 matrici simmetriche e razionali A_1, A_2 corrispondenti ai coefficienti delle forme quadratiche $I_k(F)$ e $\sum_{m=1}^{k} J_k^{(m)}(F)$. Troviamo che il più grande autovalore di $A_1^{-1}A_2$ è:

$$\lambda \approx 4.0020697... > 4. \tag{3.10.3}$$

Tali calcoli sono stati prodotti attraverso l'impiego di un programma, elaborato attraverso l'uso del software Mathematica; per una descrizione esplicita di tale programma rimandiamo a [Maynard] [5], in cui viene allegato un file contenente l'algoritmo in questione. Troviamo dunque $M_{105} > 4$. Se prendiamo invece $k = 5$ e:

$$P = (1-P_1)P_2 + \frac{7}{10}(1-P_1)^2 + \frac{1}{14}P_2 - \frac{3}{14}(1-P_1), \tag{3.10.4}$$

otteniamo che:

$$M_5 \geq \frac{\sum_{m=1}^{k} J_k^{(m)}(F)}{I_k(F)} = \frac{1417255}{708216} > 2. \tag{3.10.5}$$

Questo completa la dimostrazione. □

Vediamo ora quali sono le conseguenze del Teorema 3.10.1 sulle distanze tra numeri primi:

Teorema 3.10.2. *Abbiamo,*

$$\liminf_{n\to+\infty}(p_{n+1}-p_n) \leq 600. \tag{3.10.6}$$

Supponendo vera invece la Congettura 2.2 abbiamo,

$$\liminf_{n\to+\infty}(p_{n+1}-p_n) \leq 12, \tag{3.10.7}$$

$$\liminf_{n\to+\infty}(p_{n+2}-p_n) \leq 600. \tag{3.10.8}$$

Dimostrazione. Prendendo $k = 105$, sappiamo che $M_{105} > 4$. Dal Teorema 2.1.13 possiamo scrivere:

$$\theta = \frac{1}{2} - \varepsilon, \tag{3.10.9}$$

per ogni $\frac{1}{2} > \varepsilon > 0$. Dunque, se prendiamo $\varepsilon > 0$ sufficientemente piccolo, abbiamo:

$$\frac{\theta M_{105}}{2} > 1. \tag{3.10.10}$$

Di conseguenza:

$$\liminf_{n\to+\infty}(p_{n+1}-p_n)\leq \max_{1\leq i,j\leq 105}(h_i-h_j), \tag{3.10.11}$$

per ogni insieme ammissibile $\mathcal{H}=\{h_1,...,h_{105}\}$. Dai calcoli effettuati da Thomas Engelsma (non pubblicati), possiamo prendere $\mathcal{H}$ tale che:

$$0=h_1<h_2<...<h_{105}=600. \tag{3.10.12}$$

Per una descrizione esplicita di tale insieme ammissibile $\mathcal{H}$ rimandiamo a [Maynard] [5], pag. 390. Otteniamo quindi (3.10.6). Se assumiamo la Congettura 2.2, allora possiamo scrivere:

$$\theta=1-\varepsilon, \tag{3.10.13}$$

per ogni $1>\varepsilon>0$. Consideriamo per primo $k=105$ e vediamo che:

$$\frac{\theta M_{105}}{2}>2, \tag{3.10.14}$$

per ε sufficientemente piccolo. Quindi,

$$\liminf_{n\to+\infty}(p_{n+2}-p_n)\leq \max_{1\leq i,j\leq 105}(h_i-h_j)\leq 600, \tag{3.10.15}$$

procedendo come sopra. Infine, prendiamo $k=5$ e

$$\mathcal{H}=\{0,2,6,8,12\}, \tag{3.10.16}$$

usando ancora (3.10.13). Abbiamo $M_5>2$ e quindi:

$$\frac{\theta M_5}{2}>1, \tag{3.10.17}$$

per ε sufficientemente piccolo. Dunque,

$$\liminf_{n\to+\infty}(p_{n+1}-p_n)\leq 12. \tag{3.10.18}$$

Questo prova il teorema. □

Bibliografia

[1] K. Ford, B. Green, S. Konyagin, J. Maynard e T. Tao, Long gaps between primes, https://arxiv.org/pdf/1412.5029.pdf.

[2] D. A. Goldston, J. Pintz, and C. Y. Yildirim, Primes in tuples. I, Ann. of Math. 170 (2009), 819-862.

[3] D. A. Goldston, J. Pintz, and C. Y. Yildirim, Primes in tuples. III. On the difference $p_{n+\nu} - p_n$, Funct. Approx. Comment. Math. 35 (2006), 79-89.

[4] G. Greaves, Sieves in Number theory, Springer 2001.

[5] J. Maynard, Small gaps between primes, Annals of Mathematics 181 (2015), 383-413.

[6] H. Montgomery, R. Vaughan, Multiplicative Number theory I: Classical theory, Cambridge U. P., 2006.

[7] D.H.J. Polymath, Variants of the Selberg sieve, and bounded intervals containing many primes, Research in the Mathematical Sciences 1 (2014), 1-12, Corrigendum, ibid. 2 (2015), 1-15.

[8] A. Selberg, Collected Papers. Vol. II, Springer 1991.

[9] G. Tenenbaum, Introduction to Analytic and Probabilistic Number Theory, Cambridge U. P., 1995.

[10] R.C. Vaughan, The Bombieri Vinogradov Theorem, A.I.M. Discussion paper, November 2005, http://www.personal.psu.edu/rcv4/Bombieri.pdf.

[11] R.C. Vaughan, An elementary method in prime number theory, Acta Arithmetica 37 (1980), 111-115.

[12] Y. Zhang, Bounded gaps between primes, Ann. of Math. 179 (2014), 1121-1174.