UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL

INSTITUTO DE MATEMÁTICA

PROGRAMA DE PÓS-GRADUAÇÃO EM MATEMÁTICA

O CONJUNTO EXCEPCIONAL DO PROBLEMA DE GOLDBACH

DISSERTAÇÃO DE MESTRADO

LUIZ GUSTAVO DALPIZOL

PORTO ALEGRE, JULHO DE 2018

Resumo

Seja $E(X)$ a cardinalidade dos números pares menores ou iguais a X que não podem ser escritos como soma de dois primos. O objetivo central desta dissertação é apresentar uma demonstração de uma estimativa para $E(X)$ dada por Hugh L. Montgomery e Robert C. Vaughan em [22]. Mais precisamente, estabeleceremos a existência de uma constante positiva δ (efetivamente computável) tal que $E(X) \leq X^{1-\delta}$, para todo X suficientemente grande.

Palavras-chave: Conjectura de Goldbach; método circular; caracteres de Dirichlet, função Zeta de Riemann, L-funções de Dirichlet.

Abstract

Let $E(X)$ the cardinality of even numbers not exceeding X which cannot be written as a sum of two primes. The main goal of this dissertation is to present a proof of an estimate for $E(X)$ given by Hugh L. Montgomery e Robert C. Vaughan in [22]. More precisely, we will establish the existence of a positive constant δ (effectively computable) such that $E(X) \leq X^{1-\delta}$ for all sufficiently large X.

Keywords: Goldbach Conjecture; circular method; Dirichlet character; Zeta Riemann function; Dirichlet L-function.

Sumário

Notação

No que se segue, t, u, v, x, y, α, η, θ e σ denotam variáveis reais, enquanto N, P, Q, T e X denotam números reais positivos arbitrariamente grandes. O parâmetro δ é uma variável real positiva pequena, a qual eventualmente assume o valor de uma constante absoluta positiva. Assumimos que X é maior que alguma constante $X_0(\delta) > 0$. Ainda, a, b, d, h, j, k, q e r são números naturais, enquanto m e n são inteiros arbitrários, p é um número primo e s e z são variáveis complexas, sendo $s = \sigma + it$. As constantes C, c, c_1, $c_2, \ldots$ são absolutas e efetivamente computáveis. Aderimos a convenção usual de que a soma vazia é igual a zero e o produto vazio é igual a um.

Seja f uma função real ou complexa e g uma função positiva, por $\overline{f}$ entendemos como sendo a função conjugada de f, ou seja, $\overline{f}(y) = \overline{f(y)}$ para todo y no domínio de f. Quando f e g são funções de uma variável real x ou definidas apenas sobre os inteiros positivos (o que chamamos de uma função aritmética), escrevemos

$$f = O(g)$$

ou

$$f \ll g$$

ou

$$g \gg f,$$

se existe uma constante c positiva, absoluta e efetivamente computável, tal que $|f(x)| \leq cg(x)$ para todo x no domínio de f. A constante c é chamada constante implícita. Escrevemos

$$f = O_\lambda(g)$$

ou

$$f \ll_\lambda g,$$

se existe uma constante c positiva que depende de λ, tal que $|f(x)| \leq cg(x)$ para todo x no domínio de f.

Por

$$f = o(g),$$

entende-se que

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

A função f é assintótica a g, o qual denotamos por $f \sim g$, se

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1.$$

Ainda, $e(x) := exp(2\pi ix)$. Usamos $\binom{n}{k} := \dfrac{n!}{k!(n-k)!}$, para representar o número de subconjuntos com k elementos de um conjunto com n elementos.

A seguinte notação é padrão:

$\mathbb{N}$	o conjunto dos inteiros positivos
$\mathbb{Z}$	o conjunto dos inteiros
$\mathbb{C}^*$	o grupo multiplicativo dos complexos diferentes de zero

$[x]$	o maior inteiro que não excede x
$\{x\}$	a parte fracionária de x, isto é, $\{x\} = x - [x]$
$\|x\|$	a distância do número real x ao inteiro mais próximo, isto é, $\|x\| = \min\{\lvert x-m\rvert;\ m \in \mathbb{Z}\}$
(a,b)	o maior divisor comum de a e b
$[a,b]$	o menor múltiplo comum de a e b
$\mathbb{Z}/n\mathbb{Z}$	o anel dos resíduos módulo n
$\mathbb{Z}/n\mathbb{Z}^*$	o grupo dos resíduos reduzidos módulo n
$d \mid n$	d é um divisor de n
$p^\alpha \Vert n$	p^α é a maior potência de p que divide n
$\lvert z\rvert$	a norma do número complexo z
$\Re z$	parte real do número complexo z
$\Im z$	parte imaginária do número complexo z
$\lvert A\rvert$	a cardinalidade do conjunto A

Introdução

Christian Goldbach (1690 - 1764), membro da Academia de Petersburgo, em uma carta de 1742 endereçada a Leonard Euler levantou a hipótese de que todo número ímpar $n > 5$ pode ser representado como uma soma de três primos. Euler respondeu propondo que todo número par $n \geq 4$ é soma de dois primos. O primeiro problema é conhecido hoje como (ex-)conjectura de Goldbach fraca e o segundo como conjectura de Goldbach forte. Claramente a forte implica a fraca.

G. H. Hardy e J. E. Littlewood [12] usando o método circular atacaram as conjecturas de Goldbach, resolvendo, sob a Hipótese de Riemann Generalizada (HRG), a conjectura de Goldbach fraca para todo ímpar suficientemente grande (o enunciado preciso da HRG pode ser visto na primeira seção do Capítulo 3). Em 1937, Ivan M. Vinogradov provou o mesmo resultado seguindo a linha de métodos usada por Hardy e Littlewood, no entanto ele removeu o uso da HRG, tornando o resultado incondicional. Por fim, em 2013, o matemático peruano Harald A. Helfgott demonstrou a conjectura fraca de Goldbach, a prova dada por ele pode ser vista em [14] e [15].

Nenhum dos métodos desenvolvidos até o momento foi capaz de resolver a conjectura forte, porém alguns resultados no sentido de estimar o tamanho do conjunto dos números pares que podem ser escritos como soma de dois primos foram obtidos. Se denotarmos por $E(X)$ a função que conta os números pares não excedendo X que não podem ser escritos como soma de dois primos, o conjunto de tais números é comumente conhecido como conjunto excepcional do problema de Goldbach, a conjectura de Goldbach torna-se equivalente a afirmar que $E(X) = 1$, para todo $X \geq 2$. Inspirados no trabalho de Vinogradov sobre soma de três primos, N. G. Cudakov [7], T. Estermann [9] e van der Corput [25] provaram independentemente que $E(X) = o(X)$, de onde segue que quase todo número par pode ser expresso como soma de dois primos. Em 1973, R. C. Vaughan [26] melhorou os resultados anteriores provando que

$$E(X) < X \exp(-c \log^{\frac{1}{2}} X),$$

para todo $X \geq 2$, sendo c uma constante positiva efetivamente computável.

O principal objetivo desta dissertação é discutir o trabalho de Hugh L. Montgomery e Robert C. Vaughan [22], o qual apresenta uma melhora à estimativa anterior dada por Vaughan. Mais precisamente, demonstraremos o seguinte teorema:

Teorema (Montgomery-Vaughan). *Existe uma constante positiva δ (efetivamente computável) tal que para todo X suficientemente grande, temos*

$$E(X) < X^{1-\delta}.$$

A princípio, Montgomery e Vaughan não deram um valor numérico para a constante δ, embora os métodos usados por eles fossem efetivos. No entanto, valores admissíveis para esta constante foram obtidos posteriormente, por exemplo:

$\delta = 0.01$	Jingrun Chen e Chengdong Pan [5] - 1980;
$\delta = 0.086$	Hongze Li [17] - 2000;
$\delta = 0.121$	Wen C. Lu [20] - 2010.

Hardy e Littlewood [13] provaram que, se a HRG é verdadeira, podemos tomar $\delta = \frac{1}{2} - \epsilon$, para todo ϵ positivo no teorema acima, tendo em mente que agora o teorema é válido para X maior que uma constante que depende de ϵ. Para evitar a HRG, Montgomery e Vaughan apelaram para um resultado de Patrick X. Gallagher [10], o qual reflete considerável conhecimento da distribuição dos zeros de L-funções. Para indicar a profundidade do resultado de Gallagher (Proposição 3.8), observamos no final da Seção 3.1 que tal resultado está relacionado com o celebrado teorema de Yu V. Linnik sobre o primeiro primo em progressões aritméticas. O método do grande crivo, o método de Turán e o fenômeno de Deuring-Heilbronn desempenham papéis importantes na prova de Gallagher.

O corpo principal deste trabalho é dividido em 4 capítulos. O Capítulo 1 inicia-se com alguns resultados em teoria elementar dos números que serão sistematicamente usados no decorrer da dissertação. Um roteiro da prova do Teorema (Montgomery-Vaughan) será apresentado, o qual servirá também para introduzir o método circular de Hardy-Littlewood-Vinogradov, bem como as noções de arcos maiores e arcos menores. Finalizamos o capítulo com estimativas relacionadas aos arcos menores.

No Capítulo 2, falaremos sobre caracteres de Dirichlet. O Capítulo 3 será inteiramente dedicado em demonstrar o já citado resultado de Patrick Gallagher [10], importante no tratamento do termo de erro dos arcos maiores. No Capítulo 4, usaremos os resultados contidos nos Capítulos 2 e 3 para estabelecer estimativas aos arcos maiores, as quais acompanhadas com os resultados relacionados aos arcos menores contidos no Capítulo 1 nos permitirão provar o Teorema (Montgomery-Vaughan).

Com os objetivos de tornar a dissertação mais completa e não interromper o fluxo do texto, colocamos na parte final deste trabalho três apêndices. O primeiro deles é uma coleção de resultados em Análise que serão utilizados no decorrer da dissertação. No segundo, apresentamos uma desigualdade do grande crivo devida a Gallagher, juntamente com um resultado de Bombieri. O último apêndice é dedicado as desigualdades de Turán para somas de potências.

Capítulo 1

Considerações Iniciais

Neste capítulo damos um roteiro da prova do Teorema (Montgomery-Vaughan), bem como iniciamos a aplicação do método de Hardy-Littlewood-Vinogradov, tratando inicialmente dos assim chamados arcos menores. Também discutimos alguns resultados clássicos em Teoria dos Números que serão utilizados ao longo deste trabalho.

1.1 Resultados elementares

Para a prova dos resultados apresentados sem demonstração ou referência específica nesta seção recomendamos [2]. Uma função real ou complexa definida sobre $\mathbb{N}$ é chamada uma função aritmética. Dois exemplos importantes, que aparecem inúmeras vezes neste trabalho, são a função μ de Möbius e a função φ de Euler.

Definição 1.1. *A função μ de Möbius é definida como segue: $\mu(1) = 1$ e se $n = p_1^{a_1} \dots p_k^{a_k}$, então*

$$\mu(n) = \begin{cases} (-1)^k, & \text{se } a_1 = \ldots = a_k = 1; \\ 0\,, & \text{em caso contrário.} \end{cases}$$

É fácil ver que μ^2 é a função característica do subconjunto dos números naturais livres de quadrados. A função de Möbius aparece em diversos lugares diferentes em teoria dos números e uma de suas propriedades fundamentais é a fórmula simples para a soma dos divisores

$$\sum_{d|n} \mu(d) = \left[\frac{1}{n}\right] = \begin{cases} 1, & \text{se } n = 1; \\ 0, & \text{se } n > 1, \end{cases} \tag{1.1}$$

para referência futura, definimos $I(n) := \left[\frac{1}{n}\right]$.

Definição 1.2. *A função φ de Euler é definida por $\varphi(n) = \left|\mathbb{Z}/n\mathbb{Z}^*\right|$, para todo $n > 0$.*

A função de Euler pode ser expressa através de um produto dos divisores primos de n, de fato

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right), \tag{1.2}$$

além disso

$$\liminf_{n\to\infty} \frac{\varphi(n)\log\log n}{n} = e^{-\gamma}, \tag{1.3}$$

onde γ é a constante de Euler-Mascheroni, definida por $\gamma = \lim_{n\to\infty} \left(1 + \frac{1}{2} + \ldots + \frac{1}{n} - \log n\right)$.

Definição 1.3. *Para $n \geq 1$, definimos $d(n) = \sum_{d|n} 1$, o número de divisores de n.*

Com relação a função divisor, sabemos que

$$d(n) \ll_\varepsilon n^\varepsilon, \tag{1.4}$$

para todo $\varepsilon > 0$, além disso as somas parciais desta função aritmética são dadas por

$$\sum_{n \leq x} d(n) = x \log x \; + \; (2\gamma - 1)x \; + \; O(x^{\frac{1}{2}}). \tag{1.5}$$

A próxima proposição, descoberta por Euler em 1737, é as vezes chamada de versão analítica do Teorema Fundamental da Aritmética. Antes de enunciarmos a proposição precisaremos de algumas simples e intuitivas definições.

Definição 1.4. *Seja f uma função aritmética não identicamente nula, dizemos que f é multiplicativa se $f(mn) = f(m)f(n)$, sempre que $(m,n) = 1$ e completamente multiplicativa se $f(mn) = f(m)f(n)$, para todo m e n.*

As funções $\mu(n), \varphi(n)$ e $d(n)$ são todas multiplicativas, enquanto $n \longmapsto n^s$, $I(n)$ são exemplos de funções completamente multiplicativas (outro exemplo importante de funções completamente multiplicativas são os caracteres de Dirichlet, ver Capítulo 2).

Proposição 1.5 (Produto de Euler)**.** *Seja f uma função aritmética multiplicativa, tal que a série $\sum_{n=1}^{\infty} f(n)$ é absolutamente convergente. Então a última soma pode ser expressa como um produto infinito*

$$\sum_{n=1}^{\infty} f(n) = \prod_p \left(1 + f(p) + f(p^2) + \ldots\right).$$

Se f é completamente multiplicativa, temos

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

Prova: Considere o produto finito

$$P(x) := \prod_{p \leq x} \left(1 + f(p) + f(p^2) + \ldots\right),$$

desde que este é o produto de um número finito de séries absolutamente convergentes, podemos multiplicar as séries e rearranjar os termos sem alterar o resultado da soma. Um termo típico desta soma é da forma

$$f(p_1^{a_1}) f(p_2^{a_2}) \ldots f(p_r^{a_r}) = f(p_1^{a_1} p_2^{a_2} \ldots p_r^{a_r}),$$

visto que f é multiplicativa. Pelo Teorema Fundamental da Aritmética podemos escrever

$$P(x) = \sum_{n \in A} f(n),$$

onde A consiste de todos os números n com fatores primos menores ou iguais a x. Então

$$\sum_{n=1}^{\infty} f(n) - P(x) = \sum_{n \in B} f(n),$$

onde B é o conjunto de todos os números n com pelo menos um fator primo maior que x, assim

$$\left| \sum_{n=1}^{\infty} f(n) - P(x) \right| \leq \sum_{n \in B} |f(n)| \leq \sum_{n > x} |f(n)|.$$

Fazendo $x \longrightarrow \infty$, a última soma à direita converge a 0, pois $\sum_{n=1}^{\infty} |f(n)|$ é convergente e assim $P(x) \longrightarrow \sum_{n=1}^{\infty} f(n)$, quando $x \longrightarrow \infty$. Se f é completamente multiplicativa, temos $f\left(p^m\right) = f(p)^m$ e daí

$$\sum_{m=1}^{\infty} f\left(p^m\right) = \sum_{m=1}^{\infty} f(p)^m = \left(1 - f(p)\right)^{-1},$$

de onde concluímos a prova.

No decorrer deste trabalho precisaremos de algumas estimativas para somas envolvendo a função $\varphi(n)$, as quais estão contidas no próximo resultado.

Lema 1.6. *Para todo $m \geq 1$ e $x > 1$, temos:*

(i) $\sum_{d|m} d\varphi(d)^{-1} \leq m\varphi(m)^{-1}d(m)$;

(ii) $\sum_{n \leq x} n\varphi(n)^{-2} \ll \log^2 x$;

(iii) $\sum_{n > x} \varphi(n)^{-2} \ll \dfrac{\log x}{x}$.

Prova: (i) Seja $S_1 := \sum_{d|m} d\varphi(d)^{-1}$, claramente $S_1 = m\varphi(m)^{-1} \sum_{d|m} \dfrac{d}{m} \dfrac{\varphi(m)}{\varphi(d)}$, mas por (1.2) temos $\dfrac{\varphi(m)}{\varphi(d)} = \dfrac{m}{d} \prod_{\substack{p|m \\ p\nmid d}} \left(1 - \dfrac{1}{p}\right)$ $\leq \dfrac{m}{d}$, logo $S_1 \leq m\varphi(m)^{-1} \sum_{d|m} 1 = m\varphi(m)^{-1}d(m)$.

Para a prova dos dois últimos itens, observe que

$$\varphi(n)^{-2} = n^{-2} \prod_{p|n} \left(1 - \frac{1}{p}\right)^{-2} = n^{-2} \prod_{p|n} \left(\frac{1 - \frac{1}{p^2}}{1 + \frac{1}{p}}\right)^{-2} \leq \prod_{p} \left(1 - \frac{1}{p^2}\right)^{-2} n^{-2} \prod_{p|n} \left(1 + \frac{1}{p}\right)^2,$$

da Proposição 1.5 concluímos que $\prod_{p} \left(1 - \dfrac{1}{p^2}\right)$ converge, portanto

$$\varphi(n)^{-2} \ll n^{-2} \prod_{p|n} \left(1 + \frac{3}{p}\right) \ll n^{-2}d(n).$$

(ii) Seja $S_2 := \sum_{n \leq x} n\varphi(n)^{-2}$. Então $S_2 \ll \sum_{n \leq x} \dfrac{d(n)}{n} = \displaystyle\int_{1^-}^{x} t^{-1} d\left(\sum_{n \leq t} d(n)\right) = x^{-1} \sum_{n \leq x} d(n) + \int_{1}^{x} t^{-2} \sum_{n \leq t} d(n) dt.$

Por (1.5), segue que

$$S_2 \ll \log x + \int_{1}^{x} t^{-1}(\log t)dt \ll \log^2 x.$$

(iii) Análogo ao item *(ii)*.

Para $x > 0$, seja $\pi(x)$ a função que expressa a quantidade de números primos $p \leq x$. Então $\pi(x) \longrightarrow \infty$ quando $x \longrightarrow \infty$, visto que há infinitos números primos. O comportamento de $\pi(x)$ como função de x tem sido objeto de intenso estudo por muitos matemáticos célebres desde o século XIX. Inspecionando tabelas de primos, Gauss (1792) e Legendre (1798) conjecturaram que $\pi(x)$ é assintótico a $\frac{x}{\log x}$. Esta conjectura foi provada independentemente em 1896 por Hadamard e de la Vallée Poussin e hoje é conhecida como o Teorema dos Números Primos.

A primeira tentativa significante na direção da prova do Teorema dos Números Primos foi dada por Chebyshev em 1848-1852, o qual estabeleceu que $\frac{x}{\log x}$ é a ordem de grandeza correta para a função $\pi(x)$. Este resultado será usado por nós para obter estimativas de somas envolvendo números primos e por essa razão vamos discutí-lo nesta seção.

Iniciamos definindo a função Λ de von Mangoldt, importante na teoria da distribuição de primos.

Definição 1.7. *Para $n \geq 1$, definimos*

$$\Lambda(n) = \begin{cases} \log p\,, & \textit{se } n = p^m \textit{ para algum primo } p \textit{ e } m \geq 1; \\ 0\,, & \textit{em caso contrário.} \end{cases}$$

Chebyshev percebeu que é mais simples contar primos p com peso $\log p$, assim ele investigou a soma

$$\theta(x) := \sum_{p \leq x} \log p,$$

ao invés de $\pi(x)$. No entanto, é ainda mais conveniente trabalhar com as somas parciais da função de von Mangoldt

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

Observe que $\psi(x) = \sum_{m\leq \frac{\log x}{\log 2}} \theta\left(x^{\frac{1}{m}}\right)$, assim $0 \leq \psi(x) - \theta(x) \leq \sum_{2\leq m\leq \frac{\log x}{\log 2}} \theta\left(x^{\frac{1}{m}}\right)$, usando a estimativa trivial $\theta(x) \leq x\log x$, chegamos a

$$0 \leq \psi(x) - \theta(x) \leq \sum_{2\leq m\leq \frac{\log x}{\log 2}} x^{\frac{1}{m}} \log(x^{\frac{1}{m}}) \leq \frac{\log x}{\log 2}\left(x^{\frac{1}{2}} \log\left(x^{\frac{1}{2}}\right)\right) = \frac{x^{\frac{1}{2}}\log^2 x}{2\log 2}. \tag{1.6}$$

Em particular, se uma das funções $\frac{\psi(x)}{x}$ e $\frac{\theta(x)}{x}$ possui um limite quando $x \longrightarrow \infty$, a outra também possui e ambos os limites são iguais.

Usando somas parciais podemos relacionar $\pi(x)$ com $\theta(x)$. De fato,

$$\theta(x) = \int_{2^-}^{x} (\log t) d\pi(t) = \pi(x)\log x - \int_{2}^{x} t^{-1}\pi(t)dt \tag{1.7}$$

e

$$\pi(x) = \int_{2^-}^{x} (\log^{-1} t) d\theta(t) = \frac{\theta(x)}{\log x} + \int_{2}^{x} \frac{\theta(t)}{t\log^2 t}dt. \tag{1.8}$$

A partir de (1.6), (1.7) e (1.8), vemos que qualquer estimativa feita a uma das três funções acima se estende às outras, nesta direção temos a

Proposição 1.8. *As seguintes relações são equivalentes:*

(i) $\pi(x) \sim \frac{x}{\log x}$;

(ii) $\theta(x) \sim x$;

(iii) $\psi(x) \sim x$.

Ou seja, θ e ψ nos dão versões equivalentes para o Teorema dos Números Primos.

Proposição 1.9 (Chebyshev, Capítulo 2 de [16])**.** *Seja* $\alpha = \frac{1}{2}\log 2 + \frac{1}{3}\log 3 + \frac{1}{5}\log 5 - \frac{1}{30}\log 30 = 0.9212\ldots$, *então*

$$\alpha x + O(\log x) \leq \psi(x) \leq \frac{6}{5}\alpha x + O(\log x),$$

para todo $x > 1$.

Da proposição acima e da relação (1.6), segue

$$\alpha x + O\left(x^{\frac{1}{2}}\log^2 x\right) \leq \theta(x) \leq \frac{6}{5}\alpha x + O(\log x). \tag{1.9}$$

Agora, usando (1.9) e (1.8), chegamos a

$$\alpha\frac{x}{\log x} + O\left(x^{\frac{1}{2}}\log x\right) \leq \pi(x) \leq \frac{6}{5}\alpha\frac{x}{\log x} + O\left(\frac{x}{\log^2 x}\right). \tag{1.10}$$

Fechamos esta discussão sobre distribuição de primos com a estimativa

$$\sum_{n\leq x}\frac{\Lambda(n)}{n} \ll \log x, \tag{1.11}$$

a qual pode ser provada usando a Proposição 1.9 e somas parciais.

Finalizamos esta seção enunciando o Teorema de Dirichlet em aproximações diofantinas. Este será usado na última seção deste capítulo.

Proposição 1.10 (Dirichlet, Capítulo 7 de [1])**.** *Dados* α *um número real e* N *um inteiro positivo, existem inteiros* a *e* q, *com* $1 \leq q \leq N$, *tais que*

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

1.2 Um roteiro da prova

Em vez de considerarmos o número de representações de n como soma de dois primos, trabalhamos com a quantidade relacionada

$$R(n) := \sum \log p_1 \log p_2,$$

onde a soma é estendida sobre todas as duplas p_1 e p_2 de primos, para os quais vale $n = p_1 + p_2$. Isto é, $R(n)$ conta o número de representações de n como soma de dois primos atribuindo-lhes um peso. Repare que, $R(n) > 0$ implica que n é soma de dois primos.

Definindo

$$S(\alpha) = \sum_{p \leq X} (\log p) e(p\alpha),$$

vemos que

$$S(\alpha)^2 = \sum_n R'(n) e(n\alpha),$$

com $R'(n)$ definido da mesma forma que $R(n)$ mas com a restrição que os primos p_1 e p_2 não excedam X. Assim, $R'(n) = R(n)$, para $n \leq X$. Como $S(\alpha)^2$ é um polinômio trigonométrico, podemos calcular $R(n)$, com $n \leq X$, através da fórmula do coeficiente de Fourier

$$R(n) = \int_0^1 S(\alpha)^2 e(-n\alpha) d\alpha. \tag{1.12}$$

Para estimar (1.12), dissecamos o intervalo unitário da seguinte maneira: defina $P = X^{6\delta}$ e $Q = X^{1-6\delta}$ (em particular $PQ = X$). Para $1 \leq a \leq q \leq P$, com $(a,q) = 1$, seja $\mathfrak{M}(q,a)$ o intervalo $\left[\frac{a}{q} - \frac{1}{qQ}, \frac{a}{q} + \frac{1}{qQ}\right] \bmod 1 \subset [0,1]$, o qual chamamos de um arco maior. Estes arcos não se sobrepõem. De fato, se $\frac{a}{q}$ e $\frac{a'}{q'}$ são frações distintas satisfazendo as condições acima, temos

$$\left|\frac{a}{q} - \frac{a'}{q'}\right| \geq \frac{1}{qq'} > \frac{2P}{qq'Q} \geq \frac{q+q'}{qq'Q} = \frac{1}{qQ} + \frac{1}{q'Q}.$$

Denote por $\mathfrak{M}$ a união de todos os arcos maiores, ou seja, $\mathfrak{M} = \bigcup_{q \leq P} \bigcup_{\substack{a=1 \\ (a,q)=1}}^{q} \mathfrak{M}(q,a)$ e por $\mathfrak{m}$ o conjunto de todos os $\alpha \in [0,1]$ que não estão em $\mathfrak{M}$, chamamos $\mathfrak{m}$ de arco menor. Claramente,

$$R(n) = R_1(n) + R_2(n), \tag{1.13}$$

onde

$$R_1(n) := \int_{\mathfrak{M}} S(\alpha)^2 e(-n\alpha) d\alpha;$$

e

$$R_2(n) := \int_{\mathfrak{m}} S(\alpha)^2 e(-n\alpha) d\alpha.$$

Os conjuntos $\mathfrak{M}$ e $\mathfrak{m}$ satisfazem $\mathfrak{M} = 1 - \mathfrak{M}$ e $\mathfrak{m} = 1 - \mathfrak{m}$, logo $R_1(n)$ e $R_2(n)$ são reais. Aqui, encaramos $R_1(n)$ como sendo o termo principal de $R(n)$ e $R_2(n)$ o termo de erro. O método descrito acima para estimar $R(n)$ é conhecido comumente como método circular de Hardy-Littlewood-Vinogradov.

Observe que $R(n) \geq R_1(n) - |R_2(n)|$ e assim n é representado como soma de dois primos se

$$R_1(n) > |R_2(n)|.$$

Provaremos então que o conjunto dos n no intervalo $\frac{1}{2}X < n \leq X$ que não satisfazem a desigualdade acima é pequeno, nos permitindo assim provar o Teorema (Montgomery-Vaughan). No restante da dissertação, $S(\alpha)$ passa a representar a soma $\sum_{P < p \leq X} (\log p) e(p\alpha)$. Fazendo os devidos ajustes nas definições de $R(n)$ e $R'(n)$, vemos que tudo o que foi discutido acima permanece válido se tomamos $S(\alpha)$ esta nova soma. A razão para esta mudança ficará clara no início do Capítulo 4.

À guisa de curiosidade, enunciamos uma versão quantitativa da Conjectura de Goldbach (a qual implica que todo n par suficientemente grande é soma de dois primos).

Conjectura 1.11. *Para todo $n \geq 4$ e $A > 0$, temos*

$$R(n) = \mathfrak{S}(n)n + O_A\left(n \log^{-A} n\right), \tag{1.14}$$

onde

$$\mathfrak{S}(n) := \prod_{p \nmid n}\left(1 - \frac{1}{(p-1)^2}\right)\prod_{p \mid n}\left(1 + \frac{1}{p-1}\right).$$

No Capítulo 4, encontraremos estimativas para $R_1(n)$ condizentes com (1.14). Na verdade, em determinada situação, o termo principal de $R_1(n)$ é precisamente $\mathfrak{S}(n)n$.

1.3 Os arcos menores

Esta seção é baseada em [22]. Para estimar as integrais sobre os arcos menores vamos mostrar que

$$\sum_{n \leq X} R_2(n)^2 \ll X^3 P^{-1} \log^9 X. \tag{1.15}$$

Esta estimativa nos permite obter o seguinte resultado.

Proposição 1.12. *A quantidade dos números $n \leq X$ para os quais $|R_2(n)| > XP^{-\frac{1}{3}}$ é no máximo $\ll XP^{-\frac{1}{3}} \log^9 X$.*

Prova: Seja $A(X) := \{n \leq X;\ |R_2(n)| > XP^{-\frac{1}{3}}\}$. Por (1.15), temos

$$X^2 P^{-\frac{2}{3}} |A(X)| < \sum_{n \leq X} R_2(n)^2 \ll X^3 P^{-1} \log^9 X,$$

de onde segue

$$|A(X)| \ll XP^{-\frac{1}{3}} \log^9 X,$$

o que conclui a demonstração da proposição.

Iniciamos a prova de (1.15) definindo $S_{\mathfrak{m}}(\alpha) = S(\alpha) I_{\mathfrak{m}}(\alpha)$, onde $I_{\mathfrak{m}}$ é a função característica do conjunto $\mathfrak{m}$. Assim, $R_2(n) = \widehat{S_{\mathfrak{m}}^2}(n)$, na qual $\widehat{S_{\mathfrak{m}}^2}(n)$ é o n-ésimo coeficiente de Fourier de $S_{\mathfrak{m}}^2$ (ver Apêndice A). Agora, usando a Identidade de Parseval (ver Teorema A.1), concluímos que

$$\sum_{n \leq X} R_2(n)^2 = \sum_{n \leq X} \left(\widehat{S_{\mathfrak{m}}^2}(n)\right)^2 \leq \sum_{n \in \mathbb{Z}} \left|\widehat{S_{\mathfrak{m}}^2}(n)\right|^2 = \int_0^1 |S_{\mathfrak{m}}(\alpha)|^4 d\alpha,$$

mas a última integral é igual a

$$\int_{\mathfrak{m}} |S(\alpha)|^4 d\alpha$$

e, portanto,

$$\sum_{n \leq X} R_2(n)^2 \leq \left(\max_{\alpha \in \mathfrak{m}} |S(\alpha)|\right)^2 \int_{\mathfrak{m}} |S(\alpha)|^2 d\alpha. \tag{1.16}$$

Estendendo o domínio de integração da integral em (1.16) para o intervalo $[0, 1]$, aplicando Parseval novamente e usando a estimativa de Chebyshev (1.9), encontramos

$$\int_{\mathfrak{m}} |S(\alpha)|^2 d\alpha \leq \int_0^1 |S(\alpha)|^2 d\alpha = \sum_{P < p \leq X} \log^2 p \overset{(1.9)}{\ll} X \log X.$$

Assim, para chegarmos a (1.15) é suficiente estabelecer que

$$\max_{\alpha \in \mathfrak{m}} |S(\alpha)| \ll XP^{-\frac{1}{2}} \log^4 X, \tag{1.17}$$

para isso apelamos a um resultado de Vinogradov, o qual enunciamos da seguinte forma.

Proposição 1.13 (Vinogradov). *Se* $\left|\alpha - \frac{a}{q}\right| \leq \frac{1}{q^2}$, *com* $(a,q) = 1$, *então*

$$\sum_{n\leq X} \Lambda(n)e(n\alpha) \ll (Xq^{-\frac{1}{2}} + X^{\frac{4}{5}} + X^{\frac{1}{2}}q^{\frac{1}{2}})\log^4 X. \tag{1.18}$$

Vinogradov em 1937 introduziu um método para estimar $\sum\limits_{p\leq X} e(f(p))$ para uma classe de funções f, em particular obteve estimativas para a soma $\sum\limits_{n\leq X} \Lambda(n)e(n\alpha)$. Como consequência, ele provou que todo número ímpar suficientemente grande pode ser escrito como soma de três primos (os trabalhos de Vinogradov podem ser vistos em [27]). Em 1977, Vaughan encontrou uma nova versão do método de Vinogradov, onde os detalhes são mais simples. Uma prova da Proposição 1.13 dada por Vaughan e o resultado de Vinogradov sobre somas de três primos podem ser encontrados em [8].

Observe que usando as estimativas de Chebyshev, obtemos

$$\begin{aligned}
\sum_{n\leq X} \Lambda(n)e(n\alpha) = \sum_{p^n\leq X} (\log p)e(p^n\alpha) \quad &= \quad \sum_{p\leq X}(\log p)e(p\alpha) + \sum_{p\leq X^{\frac{1}{2}}} \sum_{n=2}^{\left[\frac{\log X}{\log p}\right]} (\log p)e(p^n\alpha) \\
&= \quad S(\alpha) + \sum_{p\leq P}(\log p)e(p\alpha) + O\left(\sum_{p\leq X^{\frac{1}{2}}} \sum_{n=2}^{\left[\frac{\log X}{\log p}\right]} \log p\right) \\
&= \quad S(\alpha) + O\left(\sum_{p\leq P}\log p + \sum_{p\leq X^{\frac{1}{2}}} \log X\right) \\
&\overset{(1.9)\,(1.10)}{=} \quad S(\alpha) + O\left(X^{\frac{1}{2}}\right). \qquad (1.19)
\end{aligned}$$

Portanto, a Proposição 1.13 continua válida se substituirmos a soma em (1.18) por $S(\alpha)$.

Suponhamos que $\alpha \in \mathfrak{m}$. Pela Proposição 1.10 de Dirichlet existem $q \leq Q$ e $1 \leq a \leq q$, com $(a,q) = 1$, tais que $\left|\alpha - \frac{a}{q}\right| \leq \frac{1}{qQ}$, isto implicaria que $\alpha \in \mathfrak{M}(q,a) \subseteq \mathfrak{M}$ se $q \leq P$. Portanto $P < q \leq Q$. Isto é, para cada $\alpha \in \mathfrak{m}$ existe $\frac{a}{q}$ com $\left|\alpha - \frac{a}{q}\right| \leq \frac{1}{qQ} \leq \frac{1}{q^2}$, $(a,q) = 1$ e $P < q \leq Q$. Assim, pela Proposição 1.13 conclui-se que

$$S(\alpha) \ll (XP^{-\frac{1}{2}} + X^{\frac{4}{5}} + X^{\frac{1}{2}}Q^{\frac{1}{2}})\log^4 X,$$

mas $X^{\frac{1}{2}}Q^{\frac{1}{2}} = XP^{-\frac{1}{2}}$, logo

$$S(\alpha) \ll (XP^{-\frac{1}{2}} + X^{\frac{4}{5}})\log^4 X.$$

Agora, tomando $\delta \leq \frac{1}{15}$ chegamos a (1.17), como desejado.

Capítulo 2

Caracteres de Dirichlet

Neste capítulo trabalhamos com caracteres de Dirichlet, objetos importantes em teoria analítica dos números. Estes foram introduzidos por Dirichlet por volta de 1837 em seus trabalhos sobre a existência de primos em progressões aritméticas da forma $a, a+q, a+2q, \ldots$, com a e q coprimos.

Definição 2.1. *Seja G um grupo abeliano finito arbitrário. Um caráter de G é um homomorfismo de grupos $f : G \longrightarrow \mathbb{C}^*$. Escrevemos f_0 para indicar o caráter principal $f(g) = 1$, $\forall\, g \in G$.*

Se a multiplicação entre dois caracteres f e g é definida pela relação $(fg)(a) = f(a)g(a)$, para todo a em G, então o conjunto de todos os caracteres de G forma um grupo abeliano, o qual denotamos por $\widehat{G}$. A identidade de $\widehat{G}$ é o caráter principal f_0 e o inverso de um elemento $f \in \widehat{G}$ é dado por $1/f$. Se e é a identidade do grupo G, o Teorema de Lagrange nos diz que $g^{|G|} = e$, para todo g elemento do grupo. Portanto, $f(g)^{|G|} = f(g^{|G|}) = f(e) = 1$, de onde segue que $f(g)$ é uma $|G|$-ésima raiz da unidade para todo $g \in G$. Assim temos $f^{-1} = \overline{f}$.

Proposição 2.2. *G e $\widehat{G}$ são isomorfos. Em particular, G e $\widehat{G}$ possuem a mesma cardinalidade.*

Prova: Se G é um grupo cíclico de ordem n gerado por um elemento g, pela discussão feita acima, vemos que todos os caracteres de G são definidos por $f_j\left(g^k\right) = e\left(\frac{kj}{n}\right)$, onde $j \in \{0,\ 1, \ldots, n-1\}$ e $k \in \mathbb{N}$. Logo $\widehat{G} = \langle f_1 \rangle$, mas f_1 tem ordem n, assim $G \simeq \widehat{G}$. Se G não é cíclico, o Teorema de Estrutura para Grupos Abelianos Finitos diz que $G \simeq G_1 \oplus \ldots \oplus G_k$, com G_j cíclicos. Assim para finalizar a prova usando o caso cíclico acima basta provar que $\widehat{G} \simeq \widehat{G_1} \oplus \ldots \oplus \widehat{G_k}$.

Para isso é suficiente provar que $\widehat{G_1 \oplus G_2} \simeq \widehat{G_1} \oplus \widehat{G_2}$, com G_1 e G_2 grupos abelianos finitos arbitrários. Seja e_i a unidade de G_i e f_i um caráter de $\widehat{G_i}$, para $i = 1, 2$. Defina a aplicação Ψ que leva $(f_1, f_2) \in \widehat{G_1} \oplus \widehat{G_2}$ em $(g_1, g_2) \longmapsto f_1(g_1)f_2(g_2) \in \widehat{G_1 \oplus G_2}$, onde $g_i \in G_i$, para $i = 1, 2$. Por outro lado, se $f \in \widehat{G_1 \oplus G_2}$, defina Φ que leva f em $(f_1, f_2) \in \widehat{G_1} \oplus \widehat{G_2}$, onde $f_1(g_1) = f(g_1, e_2)$ e $f_2(g_2) = f(e_1, g_2)$. Como as funções Ψ e Φ são homomorfismos e inversas uma da outra, segue o resultado.

Seja G um grupo abeliano de ordem n com elementos $g_1, \ldots, g_n$ e $f_0, \ldots, f_{n-1}$ os caracteres de G. Com estas notações podemos enunciar o próximo resultado.

Lema 2.3. *Temos*

$$\sum_{r=1}^{n} f_i(g_r) = \begin{cases} n, & \textit{se } f_i \textit{ é o caráter principal } (i = 0); \\ 0, & \textit{em caso contrário.} \end{cases}$$

Prova: Chamamos de S a soma em questão. Se $f_i = f_0$, cada termo da soma é igual a 1 e $S = n$. Se $f_i \neq f_0$, existe um elemento $h \in G$, tal que $f_i(h) \neq 1$. Como $\{hg_r;\ 1 \leq r \leq n\} = G$, temos

$$S = \sum_{r=1}^{n} f_i(hg_r) = f_i(h) \sum_{r=1}^{n} f_i(g_r) = f_i(h)S,$$

de onde segue $S(1 - f_i(h)) = 0$, desde que $f_i(h) \neq 1$ concluímos que $S = 0$.

Denotamos por $A = A(G)$ a matriz $n \times n$ dada por $[f_{i-1}(g_j)]_{1 \leq i,j \leq n}$. Usando o Lema 2.3 vamos provar que a matriz A é invertível e então usar esta propriedade para deduzir a assim chamada relação de ortogonalidade para caracteres.

Lema 2.4. *Seja A^* a matriz transposta conjugada de A. Então*

$$AA^* = nI,$$

onde I é a matriz identidade $n \times n$. Em particular, $n^{-1}A^*$ é a inversa de A.

Prova: Seja $B := AA^*$. A entrada b_{ij} da matriz B é dada por

$$\sum_{r=1}^{n} f_{i-1}(g_r)\overline{f}_{j-1}(g_r) = \sum_{r=1}^{n} (f_{i-1}\overline{f}_{j-1})(g_r) = \sum_{r=1}^{n} f_k(g_r),$$

onde $f_k = f_{i-1}\overline{f}_{j-1} = f_{i-1}/f_{j-1}$, mas $f_{i-1}/f_{j-1} = f_0 \iff i = j$, então pelo Lema 2.3 segue que $b_{ij} = \begin{cases} n, & \text{se } i = j; \\ 0, & \text{se } i \neq j, \end{cases}$ em outras palavras $B = nI$. Como uma matriz quadrada comuta com sua inversa à direita (ou à esquerda), conclui-se que $n^{-1}A^*$ é a inversa de A.

Pelo lema anterior temos $A^*A = nI$, mas o elemento da i-ésima linha e j-ésima coluna de A^*A é precisamente $\sum\limits_{r=1}^{n} \overline{f}_{r-1}(g_i)f_{r-1}(g_j)$. Obtemos assim a

Proposição 2.5 (Ortogonalidade dos caracteres)**.** *Temos*

$$\sum_{r=1}^{n} \overline{f}_{r-1}(g_i)f_{r-1}(g_j) = \begin{cases} n, & se\ g_i = g_j; \\ 0, & se\ g_i \neq g_j. \end{cases}$$

Até este momento discutimos caracteres de um grupo abeliano finito arbitrário. A partir de agora tomamos G como sendo o grupo multiplicativo dos resíduos reduzidos módulo um inteiro positivo q, isto é, $G = \mathbb{Z}/q\mathbb{Z}^*$. Por $\overline{n}$ entendemos a classe de equivalência módulo q do inteiro n. Partindo dos caracteres de G, construímos funções sobre os inteiros da seguinte maneira:

Definição 2.6. *Para cada f em $\widehat{G}$, definimos a função $\chi = \chi_f : \mathbb{Z} \longrightarrow \mathbb{C}$ como segue:*

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

As funções χ são chamadas de caracteres de Dirichlet módulo q. O caráter principal $\chi_0 = \chi_{f_0}$ caracteriza-se por

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

Usando os resultados obtidos para grupos arbitrários, concluímos que há $\varphi(q)$ caracteres de Dirichlet módulo q e cada um deles é completamente multiplicativo e periódico com período q, ou seja, $\chi(nm) = \chi(n)\chi(m)$ e $\chi(n+q) = \chi(n)$, para todos m e n inteiros. Reciprocamente, se χ é uma função aritmética completamente multiplicativa, periódica de período q e $\chi(n) = 0$, sempre que $(n,q) > 1$, então χ é um caráter de Dirichlet módulo q.

Ainda, pela Proposição 2.5, temos

Proposição 2.7 (Ortogonalidade para caracteres de Dirichlet)**.** *Sejam m e n dois inteiros, com $(n,q) = 1$. Então*

$$\sum_{\chi\ (mod\ q)} \overline{\chi}(m)\chi(n) = \begin{cases} \varphi(q), & se\ m \equiv n\ (mod\ q); \\ 0, & se\ m \not\equiv n\ (mod\ q), \end{cases}$$

onde $\sum\limits_{\chi\ (mod\ q)}$ denota a soma sobre todos os caracteres módulo q.

2.1 Caracteres primitivos e somas de Gauss

É possível que para valores de n restritos pela condição $(n, q) = 1$, a função $n \longmapsto \chi(n)$ tenha períodos menores que q. Nesta direção, dizemos que $d \leq q$ é um quase-período de um caráter χ módulo q, se para todos m e n satisfazendo $(m, q) = (n, q) = 1$ e $m \equiv n \,(mod\, d)$, vale $\chi(m) = \chi(n)$.

Definição 2.8. *Dizemos que χ módulo q é primitivo, se q for o único quase-período de χ.*

Observe que 1 é um quase-período para todo caráter principal mod q. Assim, se $q > 1$, tais caracteres não são primitivos.

Proposição 2.9. *Se d_1 e d_2 são quase-períodos de χ, então (d_1, d_2) também é um quase-período.*

Prova: Defina $g = (d_1, d_2)$. Sejam m e n tais que $m \equiv n \,(mod\, g)$ e $(mn, q) = 1$. Então podemos escrever $m - n = rg$, para algum $r \in \mathbb{Z}$. Mas como g é o maior divisor comum de d_1 e d_2, existem j e k satisfazendo $g = jd_1 + kd_2$. Portanto, $m = n + (rj)d_1 + (rk)d_2$, ou seja, existem a' e b' inteiros tais que $m = n + a'd_1 + b'd_2$. Tome $\widetilde{q} = \prod_{\substack{p|q \\ p\nmid d_2}} p$. É fácil ver que $\widetilde{q}$ e d_2 são coprimos. Pelo Teorema Chinês dos Restos existe a satisfazendo

$$\begin{aligned} a &\equiv a' \,(mod\, d_2); \\ a &\equiv 0 \,\,(mod\, \widetilde{q})\,, \end{aligned}$$

assim podemos escrever $m = n + ad_1 + bd_2$, onde $b = \frac{a'-a}{d_2}d_1 + b' \in \mathbb{Z}$. Repare que $n + ad_1 \equiv n \,(mod\, \widetilde{q})$, mas $(n, q) = 1$, logo $(n + ad_1, \widetilde{q}) = 1$. Agora, se p é um fator primo de q com $p|d_2$, segue da igualdade $m = n + ad_1 + bd_2$ e do fato de $(m, q) = 1$ que $p \nmid n + ad_1$. Portanto $(n + ad_1, q) = 1$ e como d_1 e d_2 são quase-períodos de χ, chegamos a

$$\chi(n) = \chi(n + ad_1) = \chi(n + ad_1 + bd_2) = \chi(m),$$

provando que g é também um quase-período.

Seja r o menor quase-período de χ. Então, pela Proposição 2.9, r divide todos os quase-períodos, em particular divide q. Daí segue que todo caráter de Dirichlet não principal módulo um primo é primitivo. Chamamos r o condutor de χ.

Proposição 2.10. *Sejam χ um caráter módulo q e d um quase-período de χ, com $d|q$. Então existe um único caráter χ^* módulo d tal que*

$$\chi = \chi_0\chi^*,$$

onde χ_0 é o caráter principal módulo q. Neste caso, dizemos que χ^* induz χ.

Prova: Dado n, com $(n, d) = 1$, existe k inteiro tal que $(n + kd, q) = 1$. De fato, tome $k = \prod_{\substack{p|q \\ p\nmid n}} p$. Então, se $p|q$ e $p|n$ temos que $p \nmid kd$, logo $(n + kd, p) = 1$. Agora, $p|q$ e $p \nmid n$ implicam em $p|kd$, logo $(n + kd, p) = 1$. Portanto $(n + kd, q) = 1$.

Com base na existência de k, definimos

$$\chi^*(n) = \begin{cases} \chi(n + kd), & \text{se } (n, d) = 1; \\ 0, & \text{em caso contrário.} \end{cases}$$

Repare que a definição acima não depende da escolha de k, pois d é um quase-período de χ. Logo, χ^* é periódica de período d, completamente multiplicativa e $\chi^*(n) = 0$ sempre que $(n, d) > 1$. Isto é, χ^* é um caráter módulo d. Quando $(n, q) = 1$, podemos tomar $k = 0$ na definição de χ^*. Assim $\chi = \chi_0\chi^*$, onde χ_0 é o caráter principal módulo q.

Provaremos agora a unicidade. Seja χ_1 um caráter módulo d tal que $\chi = \chi_0\chi_1$. Dado n, com $(n, d) = 1$, existe k satisfazendo $(n + kd, q) = 1$, logo $\chi^*(n) = \chi^*(n + kd) = \chi_1(n + kd) = \chi_1(n)$. Daí segue que $\chi^* = \chi_1$.

A próxima proposição destaca a importância dos caracteres primitivos.

Proposição 2.11. *Existe um único caráter primitivo χ^* que induz χ. Além disso, χ^* é um caráter módulo r.*

Prova: Pela Proposição 2.10 existe um caráter χ^* módulo r que induz χ. Tal caráter é necessariamente primitivo, pois a existência de um quase-período menor que r para χ^* implicaria na existência de um quase-período de χ menor que r. Uma contradição. Para finalizar, provaremos a unicidade. Seja χ_1 caráter primitivo módulo q_1 que induz χ, então q_1 é um quase-período de χ, logo $r|q_1$. Dados m e n, com $m \equiv n \ (mod\, r)$ e $(mn, q_1) = 1$, existem t_1 e t_2 inteiros, tais que $(m+t_1q_1, q) = (n+t_2q_1, q) = 1$ (ver a demonstração da Proposição 2.10). Portanto $\chi_1(m) = \chi_1(m+t_1q_1) = \chi(m+t_1q_1)$, mas como r é quase-período de χ, segue $\chi_1(m) = \chi(n+t_2q_1)$. Portanto $\chi_1(m) = \chi_1(n)$, ou seja, r é um quase-período de χ_1. Sendo este último primitivo, concluímos que $r = q_1$. Assim, pela unicidade na Proposição 2.10, obtemos $\chi_1 = \chi^*$.

Exemplo: A seguinte tabela descreve um caráter χ módulo 10.

n	1	2	3	4	5	6	7	8	9	10
$\chi(n)$	1	0	i	0	0	0	$-i$	0	-1	0

O caráter χ^* módulo 5 que induz χ é dado por:

n	1	2	3	4	5
$\chi^*(n)$	1	$-i$	i	-1	0

Definição 2.12. *Para cada caráter de Dirichlet $\chi \ (mod\, q)$ e $n \in \mathbb{Z}$, a soma $c_\chi(n) := \sum_{m=1}^{q} \chi(m)e\left(\frac{mn}{q}\right)$ é chamada soma de Gauss associada a χ. Quando $n = 1$, denotamos tal soma por $\tau(\chi)$.*

Se $\chi = \chi_0$, o caráter principal mod q, temos $\chi_0(n) = 1$, se $(n, q) = 1$ e $\chi_0(n) = 0$, em caso contrário. Neste caso, a soma de Gauss se reduz ao que chamamos de soma de Ramanujan:

$$c_{\chi_0}(n) = \sum_{\substack{m=1 \\ (m,q)=1}}^{q} e\left(\frac{mn}{q}\right)$$

e é comum denotar tal soma por $c_q(n)$.

Repare que se $(n, q) = 1$, então $\{mn;\ 1 \le m \le q\}$ é um sistema completo de resíduos módulo q e, portanto,

$$c_\chi(n) = \overline{\chi}(n) \sum_{m=1}^{q} \chi(mn)e\left(\frac{mn}{q}\right) = \overline{\chi}(n) \sum_{h=1}^{q} \chi(h)e\left(\frac{h}{q}\right) = \overline{\chi}(n)\tau(\chi). \tag{2.1}$$

Tendo em vista a igualdade acima, definimos:

Definição 2.13. *A soma de Gauss $c_\chi(n)$ é dita separável em n se $c_\chi(n) = \overline{\chi}(n)\tau(\chi)$.*

Assim, (2.1) nos diz que $c_\chi(n)$ é separável sempre que $(n, q) = 1$. A separabilidade das somas de Gauss está relacionada com caracteres primitivos, como mostra o seguinte resultado cuja prova pode ser encontrada em ([2], Capítulo 8).

Proposição 2.14. *A soma $c_\chi(n)$ é separável para todo $n \in \mathbb{Z}$ se, e somente se, χ é primitivo.*

Um caráter χ é dito real (ou quadrático) se χ é uma função real. Como $\chi(n)$ é uma raiz da unidade se $(n, q) = 1$, vemos que χ é real se, e somente se, $\chi^2 = \chi_0$. Caracteres reais são de interesse particular em teoria dos números, por exemplo, no estudo de corpos quadráticos as funções de Dedekind associadas a esses corpos podem ser expressas em termos de L-funções com caracteres reais. Assim, questões relativas ao número de classe de corpos quadráticos estão intimamente relacionadas com esta classe de caracteres. Além disso, no estudo de regiões livres de zeros para L-funções de Dirichlet, os caracteres reais demonstram um comportamento diferenciado dos demais caracteres (ver Seção 3.1, Proposições 3.6 e 3.7).

Lema 2.15. *Se χ é um caráter primitivo módulo q, então $|\tau(\chi)| = q^{\frac{1}{2}}$. Se χ é um caráter real primitivo módulo q, então*

$$\tau(\chi)^2 = \chi(-1)q \tag{2.2}$$

e $q/(4, q)$ é um inteiro livre de quadrados.

Prova: Observe que

$$|\tau(\chi)|^2 = \tau(\chi)\overline{\tau(\chi)} = \tau(\chi)\sum_{m=1}^{q}\overline{\chi}(m)e\left(-\frac{m}{q}\right) = \sum_{m=1}^{q}\overline{\chi}(m)\tau(\chi)e\left(-\frac{m}{q}\right),$$

deste modo, usando a Proposição 2.14 na última soma, obtemos

$$|\tau(\chi)|^2 = \sum_{m=1}^{q} c_\chi(m)e\left(-\frac{m}{q}\right) = \sum_{m=1}^{q}\sum_{r=1}^{q}\chi(r)e\left(\frac{mr}{q}\right)e\left(-\frac{m}{q}\right) = \sum_{r=1}^{q}\chi(r)\sum_{m=1}^{q}e\left(\frac{m(r-1)}{q}\right) = q\chi(1) = q.$$

Quando χ é quadrático, temos

$$\overline{\tau(\chi)} = \sum_{m=1}^{q}\chi(m)e\left(-\frac{m}{q}\right) = \chi(-1)\sum_{m=1}^{q}\chi(-m)e\left(-\frac{m}{q}\right) = \chi(-1)\tau(\chi).$$

Em particular, $\tau(\chi) = \chi(-1)\overline{\tau(\chi)}$. Portanto, $\tau(\chi)^2 = \chi(-1)|\tau(\chi)|^2 = \chi(-1)q$. A prova da afirmação: $q/(4,q)$ é um inteiro livre de quadrados, necessita de uma discussão construtiva dos caracteres de Dirichlet. Uma prova deste fato pode ser encontrada em ([8], Capítulo 5).

Nosso objetivo nos próximos três resultados é estabelecer uma fórmula para $c_\chi(n)$ em termos de $\tau(\chi^*)$, onde χ^* é o caráter primitivo que induz χ.

Lema 2.16. *Seja χ um caráter módulo q, induzido pelo caráter primitivo χ^* módulo r, então*

$$\tau(\chi) = \mu\left(\frac{q}{r}\right)\chi^*\left(\frac{q}{r}\right)\tau(\chi^*).$$

Este último é um resultado bem conhecido, uma prova pode ser vista em ([8], Capítulo 9).

Corolário 2.17. *Mantendo as hipóteses do Lema 2.16 e adicionando a condição $(n,q) = 1$, temos*

$$c_\chi(n) = \overline{\chi^*}(n)\mu\left(\frac{q}{r}\right)\chi^*\left(\frac{q}{r}\right)\tau(\chi^*).$$

Prova: Como $(n,q) = 1$, (2.1) implica na separabilidade de $c_\chi(n)$ e, portanto, $c_\chi(n) = \overline{\chi}(n)\tau(\chi) = \overline{\chi^*}(n)\tau(\chi)$.

Usamos os dois últimos resultados para provar uma proposição que inclui o Lema 2.16 e o Corolário 2.17 como casos particulares.

Proposição 2.18. *Seja χ um caráter módulo q, induzido pelo caráter primitivo χ^* módulo r. Para um inteiro arbitrário n, defina $q_1 = q/(q,|n|)$. Se $r \nmid q_1$, então $c_\chi(n) = 0$. Agora, se $r \mid q_1$, temos*

$$c_\chi(n) = \overline{\chi^*}\left(\frac{n}{(q,|n|)}\right)\frac{\varphi(q)}{\varphi(q_1)}\mu\left(\frac{q_1}{r}\right)\chi^*\left(\frac{q_1}{r}\right)\tau(\chi^*). \tag{2.3}$$

Para referência futura, note que quando tomamos $\chi = \chi_0$ na Proposição 2.18 chegamos na seguinte fórmula fechada para a soma de Ramanujan:

$$c_q(n) = \mu(q_1)\frac{\varphi(q)}{\varphi(q_1)}. \tag{2.4}$$

No que se segue, usamos a notação $\sum_{a=1}^{q}{}'$ para indicar a soma sobre todos os resíduos reduzidos $a\,(mod\,q)$.

Prova da Proposição 2.18: Como ambos os lados da igualdade (2.3) são periódicos com período q, podemos supor sem perda de generalidade que n é positivo. Escrevemos $q = q_1q_2$. Então $\frac{n}{q} = \frac{m_1}{q_1}$, com $(m_1,q_1) = 1$. Como $\{aq_1 + b;\ 1 \le a \le q_2,\ 1 \le b \le q_1\}$ é um sistema completo de resíduos módulo q, segue-se que

$$c_\chi(n) = \sum_{m=1}^{q}\chi(m)e\left(\frac{m_1 m}{q_1}\right) = \sum_{\substack{1\le a\le q_2\\ 1\le b\le q_1}} e\left(\frac{m_1(aq_1+b)}{q_1}\right)\chi(aq_1+b) = \sum_{b=1}^{q_1}e\left(\frac{m_1 b}{q_1}\right)\sum_{a=1}^{q_2}\chi(aq_1+b).$$

A soma em b pode ser restrita à classe dos resíduos reduzidos módulo q_1, desde que $\chi(aq_1+b)=0$ se $(b,q_1)>1$. Assim

$$c_\chi(n) = \sideset{}{'}\sum_{b=1}^{q_1} e\left(\frac{m_1 b}{q_1}\right) S(b), \tag{2.5}$$

onde $S(b) := \sum_{a=1}^{q_2} \chi(aq_1+b)$. Consideramos agora dois casos.

Caso 1. Suponha que $r \nmid q_1$. Vamos provar que $S(b)=0$ se $(b,q_1)=1$. Para qualquer d, temos

$$\chi(d)S(b) = \sum_{a=1}^{q_2} \chi(adq_1+bd).$$

Agora se $(d,q)=1$, a última soma é igual a $\sum_{a=1}^{q_2} \chi(aq_1+bd)$. Além disso, se d satisfaz a condição $d \equiv 1\,(mod\, q_1)$, a última soma é igual a

$$\sum_{a=1}^{q_2} \chi(aq_1+b)(=S(b)).$$

Portanto se adicionarmos a condição $\chi(d)\neq 1$, deduzimos que $S(b)=0$. Mostraremos agora que existe d satisfazendo as três condições acima. Desde que $r \nmid q_1$, q_1 não é um quase-período de χ. Então existem d_1 e d_2 tais que $(d_1,q)=(d_2,q)=1$ e $d_1 \equiv d_2\,(mod\, q_1)$, mas $\chi(d_1)\neq\chi(d_2)$. Portanto qualquer $d \equiv d_1 d_2^{-1} (mod\, q)$ tem as propriedades requeridas.

Caso 2. Suponha que $r|q_1$. Então $\chi(aq_1+b)=\chi^*(b)$, se $(aq_1+b,q)=1$, e 0 em caso contrário. Assim, se $(b,q_1)=1$, temos

$$S(b) = \chi^*(b) \sum_{\substack{a=1 \\ (aq_1+b,q)=1}}^{q_2} 1. \tag{2.6}$$

Usando a Identidade (1.1), podemos escrever (2.6) da forma

$$S(b) = \chi^*(b)\sum_{a=1}^{q_2} \sum_{d|(aq_1+b,q)} \mu(d) = \chi^*(b)\sum_{d|q}\mu(d) \sum_{\substack{a=1 \\ aq_1\equiv -b(mod\ d)}}^{q_2} 1.$$

A equação modular $aq_1 \equiv -b\,(mod\, d)$, com $(b,q_1)=1$, possui solução se, e somente se, $(d,q_1)=1$. Neste caso, se existir uma solução, então ela é única módulo d. Portanto,

$$S(b) = \chi^*(b)\sum_{\substack{d|q_2 \\ (q_1,d)=1}} \mu(d)\frac{q_2}{d} = \chi^*(b)q_2 \sum_{\substack{d|q_2 \\ (q_1,d)=1}} \frac{\mu(d)}{d} = \chi^*(b)q_2 \prod_{\substack{p|q_2 \\ p\nmid q_1}} \left(1-\frac{1}{p}\right) = \chi^*(b)\frac{\varphi(q)}{\varphi(q_1)}.$$

Assim, por (2.5), obtemos

$$c_\chi(n) = \sideset{}{'}\sum_{b=1}^{q_1} e\left(\frac{m_1 b}{q_1}\right)\chi^*(b)\frac{\varphi(q)}{\varphi(q_1)} = \frac{\varphi(q)}{\varphi(q_1)} c_{\chi_1}(m_1),$$

onde χ_1 é o caráter módulo q_1 induzido por χ^*. Como $(m_1,q_1)=1$, a Proposição 2.18 agora segue do Corolário 2.17.

Finalizamos este capítulo com uma estimativa para séries envolvendo somas de Gauss.

Proposição 2.19 (Montgomery-Vaughan, [22]). *Sejam χ_i caracteres primitivos módulo r_i, $i=1,2$. Então para $m\neq 0$, temos*

$$\sum_q \varphi(q)^{-2} |c_{\chi_1\chi_2\chi_0}(m)\tau(\overline{\chi_1}\chi_0)\tau(\overline{\chi_2}\chi_0)| \ll \frac{|m|}{\varphi(|m|)}, \tag{2.7}$$

onde a soma é sobre todos os q divisíveis por r_1 e r_2, e χ_0 é o caráter principal módulo q.

Prova: Podemos assumir sem perda de generalidade que $m>0$. Seja r_3 o condutor do caráter $\chi_1\chi_2\ (mod\, [r_1,r_2])$, $r_4=[r_1,r_2]$ e $r_5=(r_4,m)$. Definimos $a_i=a_i(p)$ como sendo $p^{a_i}\| r_i$, $1\le i\le 5$. Sendo r_3 um divisor de r_4, segue-se que $a_4=\max\{a_1,a_2,a_3\}$, para todo p. Como $r_4 \mid q$, escrevemos $q=r_4 k$, para algum k inteiro.

Se q está associado a um termo não nulo da soma em (2.7), então, pelo Lema 2.16, temos $\left(\frac{q}{r_i}, r_i\right) = 1$ e $\mu\left(\frac{q}{r_i}\right)^2 = 1$, $i = 1, 2$. Daí segue-se que $(k, r_4) = 1$ e $\mu(k)^2 = 1$. Assim

$$\varphi(q) = \varphi(r_4)\varphi(k) \qquad e \qquad \varphi\left(\frac{q}{(q,m)}\right) = \varphi\left(\frac{k}{(k,m)}\right)\varphi\left(\frac{r_4}{r_5}\right).$$

Podemos assumir que $r_3 | \frac{r_4}{r_5}$, pois em caso contrário $r_3 \nmid \frac{q}{(q,m)}$, o que implicaria em $c_{\chi_1\chi_2\chi_0}(m) = 0$, pela Proposição 2.18. Em particular $r_3 \leq \frac{r_4}{r_5}$. Da Proposição 2.18 e do Lema 2.15, as somas de Gauss correspondentes a q na soma em (2.7) obedecem as seguintes limitações:

$$|\tau(\overline{\chi}_i\chi_0)| \leq r_i^{\frac{1}{2}} \quad e \quad |c_{\chi_1\chi_2\chi_0}(m)| \leq r_3^{\frac{1}{2}} \frac{\varphi(q)}{\varphi\left(\frac{q}{(q,m)}\right)} \leq \left(\frac{r_4}{r_5}\right)^{\frac{1}{2}} \varphi(q)\varphi\left(\frac{k}{(k,m)}\right)^{-1}\varphi\left(\frac{r_4}{r_5}\right)^{-1},$$

para $i = 1, 2$. Podemos então concluir que a soma em (2.7) é

$$\leq \left(\frac{r_1 r_2 r_4}{r_5}\right)^{\frac{1}{2}} \varphi(r_4)^{-1}\varphi\left(\frac{r_4}{r_5}\right)^{-1} \sum_{\substack{k=1\\(k,r_4)=1}}^{\infty} \mu(k)^2\varphi(k)^{-1}\varphi\left(\frac{k}{(k,m)}\right)^{-1}. \tag{2.8}$$

Como os termos da soma em (2.8) são todos multiplicativos, a Proposição 1.5 nos diz que

$$\begin{aligned}
\sum_{\substack{k=1\\(k,r_4)=1}}^{\infty} \mu(k)^2\varphi(k)^{-1}\varphi\left(\frac{k}{(k,m)}\right)^{-1} &= \sum_{k=1}^{\infty} \mu(k)^2\varphi(k)^{-1}\varphi\left(\frac{k}{(k,m)}\right)^{-1}\left[\frac{1}{(k,r_4)}\right] \\
&= \prod_{\substack{p\nmid r_4\\p\nmid m}}\left(1+\frac{1}{(p-1)^2}\right)\prod_{\substack{p\nmid r_4\\p|m}}\left(1+\frac{1}{p-1}\right) \\
&\ll \prod_{\substack{p\nmid r_4\\p|m}}\left(1-\frac{1}{p}\right)^{-1}.
\end{aligned}$$

O outro fator de (2.8) pode ser escrito como $\Pi_1 \cdot \Pi_2$, onde

$$\Pi_1 := \frac{\left(\frac{r_4}{r_5}\right)^{\frac{1}{2}}}{\varphi\left(\frac{r_4}{r_5}\right)} \prod_{\substack{p|r_4\\p\nmid m}} p^{\frac{1}{2}a_1+\frac{1}{2}a_2-a_4}\left(1-\frac{1}{p}\right)^{-1} \ll \prod_{\substack{p|r_4\\p\nmid m}} p^{-\frac{1}{2}}\left(1-\frac{1}{p}\right)^{-2} \ll 1,$$

pois $a_4 = \max(a_1, a_2)$ e $p^{-\frac{1}{2}}\left(1-\frac{1}{p}\right)^{-2} \leq 1$, para p grande, e

$$\Pi_2 := \prod_{\substack{p|r_4\\p|m}} p^{\frac{1}{2}a_1+\frac{1}{2}a_2-a_4}\left(1-\frac{1}{p}\right)^{-1} \leq \prod_{p|r_5}\left(1-\frac{1}{p}\right)^{-1}.$$

Combinando as últimas três estimativas chegamos ao resultado desejado.

Capítulo 3

Sobre os Zeros das L-funções de Dirichlet

Neste capítulo trataremos da função Zeta de Riemann e das L-funções de Dirichlet, estabelecendo para estas regiões livres de zeros e estimativas para o número de zeros em retângulos $\alpha \leq \sigma \leq 1$, $|t| \leq T$. Usando estes resultados provaremos na última seção um resultado de Patrick X. Gallagher (Proposição 3.8) que será importante na prova do Teorema (Montgomery-Vaughan). A menos que seja dito o contrário, as demonstrações de todas as afirmações sem provas aqui encontradas podem ser vistas em [8]. Este capítulo é fortemente baseado em [10].

3.1 A função Zeta e as L-funções de Dirichlet

Relembramos que s é uma variável complexa da forma $\sigma + it$.

Definição 3.1. *Para $\sigma > 1$, definimos a função Zeta de Riemann pela soma*

$$\varsigma(s) = \sum_{n=1}^{\infty} n^{-s}.$$

Como a série acima converge uniformemente sobre compactos no semiplano $\sigma > 1$, temos pela Proposição A.7 que $\varsigma(s)$ é analítica neste semiplano. Além disso, pela Proposição 1.5

$$\varsigma(s) = \prod_{p} \left(1 - \frac{1}{p^s}\right)^{-1}. \tag{3.1}$$

Usando somas parciais, vemos que

$$\sum_{n \leq x} n^{-s} = \int_{1^-}^{x} t^{-s} d[t] = x^{-s}[x] + s \int_{1}^{x} t^{-(s+1)}[t]dt,$$

para todo $\sigma > 1$. Fazendo $x \longrightarrow \infty$ e escrevendo $[t] = t - \{t\}$, chegamos a

$$\varsigma(s) = \frac{s}{s-1} - s \int_{1}^{\infty} t^{-(s+1)}\{t\}dt, \tag{3.2}$$

para todo $\sigma > 1$. Repare que o lado direito de (3.2) é uma função meromorfa no semiplano $\sigma > 0$, com um único pólo simples em $s = 1$. Logo, a função Zeta pode ser estendida a uma função meromorfa em $\sigma > 0$ que satisfaz as mesmas propriedades da função à direita de (3.2). Mais ainda, $\varsigma(s)$ admite uma extensão meromorfa para todo o plano complexo, com um único pólo em $s = 1$. Pela Identidade (1.1) vemos que

$$\varsigma(s) \sum_{n=1}^{\infty} \mu(n) n^{-s} = \sum_{n=1}^{\infty} \sum_{d|n} \mu(d) n^{-s} = 1,$$

para todo $\sigma > 1$. Portanto a função Zeta não possui zeros no semiplano $\sigma > 1$ e $\varsigma(s)^{-1} = \sum_{n=1}^{\infty} \mu(n) n^{-s}$ nesta região.

A função $\xi(s) := \frac{1}{2}s(s-1)\pi^{-\frac{1}{2}s}\Gamma\left(\frac{1}{2}s\right)\varsigma(s)$, onde Γ é a função gama definida no Apêndice A, é inteira e satisfaz a equação funcional $\xi(s) = \xi(1-s)$. Como a função gama não se anula em nenhum ponto do plano complexo e tem pólos precisamente em $s = 0,\ -1,\ -2, \ldots$ (os quais são simples), a equação funcional acima nos diz que $\varsigma(s)$ possui zeros em $\sigma < 0$, somente nos inteiros pares negativos e tais zeros são simples. Nós os chamamos de zeros triviais.

Assim, a única região onde $\varsigma(s)$ pode ter zeros não triviais é na faixa $0 \leq \sigma \leq 1$. Sabemos, no entanto, que a função não se anula na fronteira desta faixa, portanto podemos nos restringir a assim chamada faixa crítica $0 < \sigma < 1$. Pela equação funcional e o fato que $\overline{\varsigma}(s) = \varsigma(\overline{s})$, vemos que os zeros nesta região são simétricos com relação a reta $\sigma = \frac{1}{2}$ e a reta real. Os zeros não triviais são comumente denotados por $\rho = \beta + i\gamma$.

Chamando de $N(T)$ o número de zeros não triviais com $|\gamma| \leq T$, temos a seguinte estimativa devida a von Mangoldt

$$N(T) = \frac{T}{\pi}\log\frac{T}{2\pi} - \frac{T}{\pi} + O(\log T), \tag{3.3}$$

em particular,

$$|\{\rho;\ |\gamma - t| \leq 1\}| \ll \log(|t| + 2), \tag{3.4}$$

para todo t real. Sobre a distribuição dos zeros não triviais, temos a famosa e importante conjectura formulada por Riemann,

Conjectura 3.2 (Riemann)**.** *Todos os zeros não triviais de $\varsigma(s)$ satisfazem $\beta = \frac{1}{2}$.*

Em 1899, de la Vallée Poussin provou que $\varsigma(s) \neq 0$ em uma região estreita à esquerda da reta $\sigma = 1$. Mais precisamente, temos a

Proposição 3.3. *Existe uma constante $c_1 > 0$ tal que $\varsigma(s)$ não possui zeros na região*

$$\begin{cases} \sigma \geq 1 - \dfrac{c_1}{\log|t|}, & se\ |t| > 2; \\ \\ 0 < \sigma < 1, & se\ |t| \leq 2. \end{cases}$$

A melhor região livre de zeros conhecida até o momento foi dada independentemente por Vinogradov e Korobov em 1958. Eles provaram que existe uma constante c_2 tal que $\varsigma(s) \neq 0$ em $\sigma \geq 1 - \dfrac{c_2}{(\log|t|)^{\frac{2}{3}}(\log\log|t|)^{\frac{1}{3}}}$, para $|t| > 3$. Uma prova deste fato pode ser encontrada em ([16], Capítulo 8).

Podemos dizer que a Teoria Analítica dos Números nasceu por volta de 1837 nos trabalhos de Dirichlet sobre a existência de primos em uma dada progressão aritmética, onde ele introduziu o que chamamos hoje de L-funções de Dirichlet.

Definição 3.4. *Para cada caráter χ módulo q, definimos a L-função associada a χ por*

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

para $\sigma > 1$.

Como os caracteres são completamente multiplicativos e a série acima converge absolutamente para $\sigma > 1$, obtemos pela Proposição 1.5 que

$$L(s,\chi) = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}. \tag{3.5}$$

Usando somas parciais chegamos a

$$\sum_{x<n\leq y} \chi(n)n^{-s} = \int_1^y t^{-s} d\left(\sum_{x<n\leq t}\chi(n)\right) = y^{-s}\sum_{x<n\leq y}\chi(n) + s\int_1^y t^{-(s+1)}\sum_{x<n\leq t}\chi(n)dt,$$

para $1 < x \leq y$. Agora, pelo Lema 2.3 chega-se a $\left|\sum_{x<n\leq t}\chi(n)\right| \leq \varphi(q)$, sempre que $\chi \neq \chi_0$ [1], logo

$$\sum_{x<n\leq y}\chi(n)n^{-s} \ll \varphi(q)\left(y^{-\sigma}+|s|\int_x^y t^{-(\sigma+1)}dt\right) \ll \varphi(q)\frac{|s|}{\sigma}x^{-\sigma}.$$

Daí resulta que, $\sum_{n=1}^{\infty}\chi(n)n^{-s}$ converge uniformemente sobre compactos no semiplano $\sigma > 0$ e, portanto, é analítica nesta região. Na verdade, $L(s,\chi)$ admite uma extensão inteira sempre que $\chi \neq \chi_0$.

Quando $\chi = \chi_0$, a extensão inteira não pode ser obtida, pois $L(s,\chi_0)$ tem um pólo em $s = 1$. De fato, por (3.1) e (3.5) obtemos

$$L(s,\chi_0) = \prod_{p\nmid q}\left(1-\frac{1}{p^s}\right)^{-1} = \varsigma(s)\prod_{p|q}\left(1-\frac{1}{p^s}\right).$$

Como o último produtório acima define uma função inteira e a função Zeta admite uma extensão meromorfa, segue-se que $L(s,\chi_0)$ também admite tal extensão, com um único pólo simples em $s = 1$.

Repare que $h(n) := \sum_{d|n}\mu(d)\chi(d)\chi\left(\frac{n}{d}\right) = \chi(n)\sum_{d|n}\mu(d)$. Assim, pela Identidade (1.1) chegamos a

$$h(n) = \begin{cases} 1, & \text{se } n = 1; \\ 0, & \text{se } n > 1, \end{cases}$$

portanto $L(s,\chi)\sum_{n=1}^{\infty}\mu(n)\chi(n)n^{-s} = \sum_{n=1}^{\infty}h(n)n^{-s} = 1$, para $\sigma > 1$. Como consequência, as L-funções não possuem zeros no semiplano $\sigma > 1$ e $L(s,\chi)^{-1} = \sum_{n=1}^{\infty}\mu(n)\chi(n)n^{-s}$ nesta região.

Seja χ^* o caráter primitivo módulo r que induz χ. Por (3.5), obtemos

$$L(s,\chi) = \prod_{p\nmid q}\left(1-\frac{\chi^*(p)}{p^s}\right)^{-1} = L(s,\chi^*)\prod_{\substack{p|q\\ p\nmid r}}\left(1-\frac{\chi^*(p)}{p^s}\right), \tag{3.6}$$

para $\sigma > 1$. Sendo o último produtório de (3.6) uma função inteira, a decomposição acima vale para todo $s \in \mathbb{C}$ e assim, quando tratamos de L-funções podemos nos restringir à classe das L-funções associadas a caracteres primitivos.

Para χ caráter primitivo módulo q, defina

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

A função $\xi(s,\chi) := \left(\frac{\pi}{q}\right)^{-\frac{1}{2}(s+\mathfrak{a})}\Gamma\left(\frac{1}{2}(s+\mathfrak{a})\right)L(s,\chi)$ é inteira e obedece a equação funcional

$$\xi(1-s,\overline{\chi}) = \frac{i^{\mathfrak{a}}q^{\frac{1}{2}}}{\tau(\chi)}\xi(s,\chi). \tag{3.7}$$

Pela localização dos pólos da função gama e a equação funcional (3.7), concluímos que os zeros de $L(s,\chi)$, para $\sigma < 0$, são precisamente $s = -1,\ -3,\ -5,\dots$, se $\mathfrak{a} = 1$ e $s = -2,\ -4,\ -6,\dots$, se $\mathfrak{a} = 0$, os quais chamamos de zeros triviais. Assim, a única região onde $L(s,\chi)$ pode ter zeros não triviais é na faixa $0 \leq \sigma \leq 1$. Sabemos, no entanto, que esta função não se anula na fronteira desta faixa, com exceção de um zero simples em $s = 0$, quando $\mathfrak{a} = 0$. Portanto podemos nos concentrar na também chamada faixa crítica $0 < \sigma < 1$ para L-funções. Os zeros não triviais de $L(s,\chi)$ serão denotados por $\rho = \beta + i\gamma$.

Chamando de $N(T,\chi)$ o número de zeros não triviais de $L(s,\chi)$, com $|\gamma| \leq T$, temos a seguinte estimativa

$$N(T,\chi) = \frac{T}{\pi}\log\frac{qT}{2\pi} - \frac{T}{\pi} + O(\log qT), \tag{3.8}$$

[1] Em 1918, Pólya e Vinogradov provaram independentemente que $\left|\sum_{x<n\leq t}\chi(n)\right| \leq q^{\frac{1}{2}}\log q$.

em particular,

$$|\{\rho;\ |\gamma - t| \leq 1\}| \ll \log q(|t|+2), \tag{3.9}$$

para todo t real. Sobre a distribuição dos zeros não triviais, temos a

Conjectura 3.5 (Riemann Generalizada). *Todos os zeros não triviais de $L(s,\chi)$, com χ primitivo, satisfazem $\beta = \frac{1}{2}$.*

Para L-funções contamos com um resultado análogo a Proposição 3.3, onde as regiões livres de zeros dependem explicitamente de q. Porém os resultados obtidos são melhores para caracteres complexos do que para caracteres reais.

Proposição 3.6. *Existe uma constante absoluta $c_3 > 0$ tal que se χ é um caráter módulo q, então $L(s,\chi)$ não tem zeros na região definida por*

$$\sigma \geq \begin{cases} 1 - \dfrac{c_3}{\log q|t|}, & se\ |t| \geq 1; \\ \\ 1 - \dfrac{c_3}{\log q}, & se\ |t| \leq 1, \end{cases} \tag{3.10}$$

com a possível exceção de um caráter real χ_1 não principal módulo q. Se este caráter existir, a L-função associada a ele possui um único zero β_1 em (3.10), sendo este real e simples .

Se analisarmos a região livre de zeros para a família de L-funções associadas a caracteres com módulo menor ou igual a T, obtemos a

Proposição 3.7. *Existe uma constante $c_4 > 0$ tal que $L(\sigma,\chi) \neq 0$, sempre que*

$$\sigma \geq 1 - \frac{c_4}{\log T},$$

para todo caráter primitivo χ de módulo $q \leq T$, com uma possível exceção de no máximo um caráter primitivo $\widetilde{\chi}\ (mod\ \widetilde{r})$. Se tal caráter existir, $\widetilde{\chi}$ é real, não principal e o (único) zero real excepcional $\widetilde{\beta}$ de $L(s,\widetilde{\chi})$ satisfaz

$$\frac{c_5}{\widetilde{r}^{\frac{1}{2}} \log^2 \widetilde{r}} \leq 1 - \widetilde{\beta} \leq \frac{c_4}{\log T}. \tag{3.11}$$

O caráter $\widetilde{\chi}\ (mod\ \widetilde{r})$ da Proposição 3.7 (se existir) é chamado de caráter excepcional de ordem T. A próxima proposição tem um papel importante no tratamento do termo de erro da estimativa para $R_1(n)$ obtida no Capítulo 4. No que se segue, usamos a notação $\displaystyle\sideset{}{^*}\sum_{\chi\ (mod\ q)}$ para indicar a soma sobre os caracteres primitivos módulo q.

Proposição 3.8. *Para constantes absolutas positivas c_6 e c_7 bem escolhidas, temos*

$$\sum_{q \leq P} \sideset{}{^*}\sum_{\chi\ (mod\ q)} \max_{x \leq N} \max_{h \leq N} \left(h + \frac{N}{P}\right)^{-1} \left| \sideset{}{^\sharp}\sum_{x-h<p\leq x} \chi(p)\log p \right| \ll \exp\left(-c_6 \frac{\log N}{\log P}\right), \tag{3.12}$$

sob a condição de que $\exp(\log^{\frac{1}{2}} N) \leq P \leq N^{c_7}$. Aqui $\sum^\sharp$ indica que o termo com $q = 1$ é

$$\sum_{x-h<p\leq x} \log p - \sum_{\substack{x-h<n\leq x \\ n>0}} 1,$$

e se existe o caráter excepcional $\widetilde{\chi}$ de ordem P, então o termo que lhe corresponde é

$$\sum_{x-h<p\leq x} \widetilde{\chi}(p)\log p + \sum_{\substack{x-h<n\leq x \\ n>0}} n^{\widetilde{\beta}-1}.$$

Além disso, se o caráter excepcional ocorre, o lado direito de (3.12) pode ser multiplicado pelo fator $(1-\widetilde{\beta})\log P$.

A proposição acima é basicamente o Teorema 7 de Gallagher [10], com duas modificações. Neste capítulo objetivamos apresentar uma demonstração da Proposição 3.8, a qual depende de uma série de resultados e métodos em Teoria Analítica dos Números, tais como: somas exponenciais, estimativas do grande crivo, método de somas de potências de Turán, fenômeno de Deuring-Heilbronn, etc. Finalizamos esta seção com um "roteiro"da demonstração da Proposição 3.8, este também servirá para contextualizar a proposição dentro do cenário da Teoria Analítica dos Números.

Dados a e q, com $(a,q)=1$, Dirichlet estabeleceu que há infinitos primos cumprindo a condição $p \equiv a \ (mod\ q)$. Além disso, sabemos que a distribuição de primos em classes de resíduos primitivos módulo q é uniforme. Assim, uma questão natural a ser feita é quão grande é o primeiro primo em uma dada classe.

Na direção de responder tal questão, Linnik em 1944 provou o seguinte resultado.

Teorema 3.9 (Linnik, Capítulo 18 de [16]). *Existem constantes absolutas $c_8 \geq 1$ e $L \geq 2$ tais que*

$$p(q,a) \leq c_8 q^L,$$

onde $p(q,a) := \min\{p;\ p \equiv a \ (mod\ q)\}$.

Este teorema é um dos grandes feitos em Teoria Analítica dos Números. O método desenvolvido por Linnik é efetivo, embora originalmente ele não tenha dado um valor numérico para L. No entanto, vários pesquisadores produziram valores para a constante de Linnik, por exemplo, Heath-Brown em 1992 demonstrou que podemos tomar $L = 5,5$.

Todas as provas do Teorema de Linnik usam, de uma forma ou outra, dois princípios sobre os zeros de L-funções de Dirichlet, os quais serão enunciados adiante. Antes porém, precisamos fixar alguma notação. Definimos

$$L_q(s) := \prod_{\chi \ (mod\ q)} L(s,\chi) \quad \text{e} \quad L_q^*(s) := \prod_{\chi \ (mod\ q)}^{*} L(s,\chi),$$

onde * no produtório significa que estamos nos restringindo aos caracteres primitivos. Como antes, um zero não trivial de $L(s,\chi)$ será representado por $\rho = \beta + i\gamma$ ou por $\rho_\chi = \beta_\chi + i\gamma_\chi$ se a dependência do caráter precisa ser exibida. Para $\frac{1}{2} \leq \alpha \leq 1$ e $T \geq 1$, denotamos por $N(\alpha,T,\chi)$ o número de zeros ρ_χ contados com multiplicidade no retângulo

$$\alpha \leq \sigma \leq 1, \qquad |t| \leq T. \tag{3.13}$$

Assim,

$$N_q(\alpha,T) := \sum_{\chi \ (mod\ q)} N(\alpha,T,\chi) \quad \text{e} \quad N_q^*(\alpha,T) := \sum_{\chi \ (mod\ q)}^{*} N(\alpha,T,\chi)$$

é o número de zeros de $L_q(s)$ e $L_q^*(s)$ (respectivamente) contados com multiplicidade no retângulo (3.13).

Princípio 3.10 (Estimativa para Densidade dos Zeros). *Existe uma constante c_9 tal que para $\frac{1}{2} \leq \alpha \leq 1$ e $T \geq 1$, temos*

$$N_q(\alpha,T) \ll (qT)^{c_9(1-\alpha)}.$$

Princípio 3.11 (Repulsão do Zero Excepcional). *Temos $L(s,\chi) \neq 0$ na região*

$$\sigma \geq 1 - \frac{c_4}{\log T}, \quad |t| \leq T, \tag{3.14}$$

para todo caráter primitivo χ de módulo menor ou igual a T, com a possível exceção do caráter excepcional $\widetilde{\chi}$ $(mod\ \widetilde{r})$ de ordem T. Se tal caráter existir, $L(s,\widetilde{\chi})$ possui um único zero $\widetilde{\beta}$ em (3.14), sendo este real e simples. Além disso, existe uma constante c_{10} tal que se o caráter excepcional ocorrer, então podemos melhorar a região (3.14) para

$$\sigma \geq 1 - c_{10} \frac{\log\left(\frac{ec_4}{(1-\widetilde{\beta})\log T}\right)}{\log T}, \quad |t| \leq T, \tag{3.15}$$

sendo $\widetilde{\beta}$ ainda a única exceção.

O Princípio 3.10 foi demonstrado por Linnik em [18] e o Princípio 3.11 é uma versão quantitativa do fenômeno de Deuring-Heilbronn e foi também provado por Linnik em [19]. Gallagher e Bombieri estabeleceram o seguinte resultado que implica os princípios acima.

Teorema 3.12 (Gallagher-Bombieri). *Existe uma constante c_{11} tal que para $\frac{1}{2} \leq \alpha \leq 1$ e $T > 1$, temos*

$$\sum_{q \leq T} N_q^*(\alpha,T) \ll T^{c_{11}(1-\alpha)}. \tag{3.16}$$

Agora, se existe o caráter excepcional $\widetilde{\chi}$ de ordem T, com zero excepcional $\widetilde{\beta}$, temos

$$\sum_{q \leq T} \widetilde{N}_q^*(\alpha,T) \ll T^{c_{11}(1-\alpha)}(1-\widetilde{\beta})\log T. \tag{3.17}$$

Aqui $\sim$ em $\widetilde{N}_q^*$ significa que $\widetilde{\beta}$ é excluído.

A estimativa (3.16) foi provada por Gallagher em [10], enquanto (3.17) é um resultado posterior devido a Enrico Bombieri. Por (3.6), vemos que (3.16) implica o Princípio 3.10. De fato,

$$N_q(\alpha, T) = \sum_{\chi \ (mod\ q)} N(\alpha, T, \chi) \leq \sum_{r \leq q} \sum_{\chi \ (mod\ r)}^{*} N(\alpha, T, \chi) \leq \sum_{r \leq qT} N_r^*(\alpha, qT) \ll (qT)^{c_{11}(1-\alpha)}.$$

Por fim, demonstraremos que (3.17) implica o Princípio 3.11. A primeira parte do princípio segue diretamente das Proposições 3.6 e 3.7. Agora, se existe o caráter excepcional $\widetilde{\chi}$, a estimativa (3.17) assegura a existência de uma constante c_{12} tal que

$$\sum_{q \leq T} \widetilde{N}_q^*(\alpha, T) \leq c_{12} T^{c_{11}(1-\alpha)}(1 - \widetilde{\beta}) \log T. \tag{3.18}$$

Portanto, se α satisfaz a desigualdade

$$c_{11}(1-\alpha)\log T + \log\Big(c_{12}(1-\widetilde{\beta})\log T\Big) < 0, \tag{3.19}$$

a estimativa (3.18) implica

$$\sum_{q \leq T} \widetilde{N}_q^*(\alpha, T) < 1.$$

Ou seja, $L(s, \chi)$ não possui zeros diferentes de $\widetilde{\beta}$ no retângulo $\alpha \leq \sigma \leq 1$, $|t| \leq T$, para todo caráter χ com módulo menor ou igual a T. Porém, a desigualdade (3.19) é equivalente a

$$\alpha > 1 - \frac{\log\left(\frac{1}{c_{12}\left(1-\widetilde{\beta}\right)\log T}\right)}{c_{11}\log T}.$$

Assim, tomando c_4 suficientemente pequeno, obtemos (3.15). O que conclui a prova do Princípio 3.11, com base no Teorema 3.12.

Usando (3.16) e o fenômeno de Deuring-Heilbronn, Gallagher provou a Proposição 3.8. Neste capítulo seguiremos os passos de Gallagher [10]. Isto é, primeiramente daremos uma demonstração do Teorema 3.12 e só então, na última seção deste capítulo, apresentaremos uma prova da Proposição 3.8.

3.2 Valor médio de somas exponenciais

Seja

$$S(t) := \sum c(v)e(vt) \tag{3.20}$$

uma soma exponencial absolutamente convergente. Aqui as frequências v percorrem uma sequência arbitrária de números reais e os coeficientes $c(v)$ são complexos.

Proposição 3.13. *Seja* $\delta = \frac{\epsilon}{T}$, *com* $0 < \epsilon < 1$. *Então*

$$\int_{-T}^{T} |S(t)|^2 dt \ll_\epsilon \int_{-\infty}^{\infty} \left| \delta^{-1} \sum_{x \leq v \leq x+\delta} c(v) \right|^2 dx. \tag{3.21}$$

Prova: Podemos escrever a integral à direita em (3.21) como

$$\int_{-\infty}^{\infty} |C_\delta(x)|^2 dx, \text{ com } \ C_\delta(x) = \delta^{-1} \sum_{|v-x| \leq \frac{\delta}{2}} c(v).$$

Definindo $F_\delta(x) = \delta^{-1}$, se $|x| \leq \frac{\delta}{2}$ e 0, em caso contrário, temos

$$C_\delta(x) = \sum c(v) F_\delta(v - x).$$

Como a série (3.20) converge absolutamente, $C_\delta(x)$ é uma função limitada em $L^1(\mathbb{R})$, portanto pertence a $L^2(\mathbb{R})$.

Assim, pelo Teorema de Plancherel (ver Teorema A.2)

$$\int_{-\infty}^{\infty} |C_\delta(x)|^2 dx = \int_{-\infty}^{\infty} |\widehat{C}_\delta(t)|^2 dt,$$

mas $\widehat{C}_\delta(t)$ é igual a

$$\int_{-\infty}^{\infty} \sum c(v) F_\delta(v-x) e(-xt) dx = \sum c(v) \int_{-\infty}^{\infty} F_\delta(v-x) e(-xt) dx = S(-t)\widehat{F}_\delta(-t),$$

logo

$$\int_{-\infty}^{\infty} |C_\delta(x)|^2 dx = \int_{-\infty}^{\infty} |S(t)\widehat{F}_\delta(t)|^2 dt \geq \int_{-T}^{T} |S(t)\widehat{F}_\delta(t)|^2 dt.$$

Como

$$\widehat{F}_\delta(t) = \frac{\sin \pi\delta t}{\pi \delta t} \gg_\epsilon 1, \text{ para } \quad |t| \leq T,$$

concluímos a demonstração.

Se v percorre a sequência $\left\{\frac{\log n}{2\pi};\ n \in \mathbb{N}\right\}$, temos que $S(t) = \sum_{n=1}^{\infty} a_n n^{it}$. Ou seja, $S(t)$ é uma Série de Dirichlet absolutamente convergente. Tomando $\epsilon = \frac{1}{2\pi}$ e fazendo a mudança de variável $\log y = 2\pi x$ na Proposição 3.13 chegamos ao

Corolário 3.14. *Para $\tau = \exp\left(\frac{1}{T}\right)$, temos*

$$\int_{-T}^{T} |S(t)|^2 dt \ll T^2 \int_{0}^{\infty} \left| \sum_{y \leq n \leq y\tau} a_n \right|^2 \frac{dy}{y}.$$

Vamos aplicar o Corolário 3.14 para somas da forma

$$S(\chi, t) := \sum_{n=1}^{\infty} a_n \chi(n) n^{it},$$

onde χ é um caráter de Dirichlet. O seguinte lema é um resultado dado por Bombieri e Davenport em [4], a prova depende essencialmente de uma desigualdade da Teoria do Grande Crivo (ver Apêndice B).

Lema 3.15. *Assuma que $a_n = 0$, se n tem algum fator primo $\leq Q$. Então*

$$\sum_{q \leq Q} \log \frac{Q}{q} \sum_{\chi\,(mod\,q)}^{*} \left| \sum_{y \leq n \leq y+z} a_n \chi(n) \right|^2 \ll \left(Q^2 + z\right) \sum_{y \leq n \leq y+z} |a_n|^2.$$

Prova: Para cada caráter χ módulo q, a Identidade (2.1) nos diz que

$$\tau(\overline{\chi})\chi(n) = \sum_{a=1}^{q} \overline{\chi}(a) e\left(\frac{an}{q}\right),$$

sempre que $(n, q) = 1$. Seja

$$S(\chi) := \sum_{y \leq n \leq y+z} a_n \chi(n) \text{ e } S(\alpha) := \sum_{y \leq n \leq y+z} a_n e(n\alpha).$$

Usando a hipótese do lema, obtemos para todo caráter χ com módulo menor ou igual a Q e $n \geq 1$, a seguinte igualdade

$$\tau(\overline{\chi}) a_n \chi(n) = \sum_{a=1}^{q} \overline{\chi}(a) a_n e\left(\frac{an}{q}\right),$$

somando a última igualdade sobre $y \le n \le y+z$, chegamos a

$$\tau(\overline{\chi})S(\chi) = \sum_{a=1}^{q} \overline{\chi}(a) S\left(\frac{a}{q}\right).$$

Pela relação de ortogonalidade dos caracteres (ver Proposição 2.7), temos

$$\begin{aligned}
\sum_{\chi\,(mod\,q)} |\tau(\overline{\chi})S(\chi)|^2 &= \sum_{\chi\,(mod\,q)} \sum_{1\le a_1,a_2\le q} \overline{\chi}(a_1)\chi(a_2) S\left(\frac{a_1}{q}\right)\overline{S}\left(\frac{a_2}{q}\right) \\
&= \sum_{1\le a_1,a_2\le q} S\left(\frac{a_1}{q}\right)\overline{S}\left(\frac{a_2}{q}\right) \sum_{\chi\,(mod\,q)} \overline{\chi}(a_1)\chi(a_2) \\
&= \varphi(q) \sum_{a=1}^{q}{}' \left|S\left(\frac{a}{q}\right)\right|^2,
\end{aligned}$$

para todo $q \le Q$. Usando a desigualdade de Bombieri do Grande Crivo (ver Teorema B.3), encontramos

$$\sum_{q\le Q} \frac{1}{\varphi(q)} \sum_{\chi\,(mod\,q)} |\tau(\overline{\chi})S(\chi)|^2 = \sum_{q\le Q} \sum_{a=1}^{q}{}' \left|S\left(\frac{a}{q}\right)\right|^2 \ll \left(Q^2+z\right) \sum_{y\le n\le y+z} |a_n|^2. \tag{3.22}$$

Seja r o condutor de χ. Então $q = rk$ e pelos Lemas 2.15 e 2.16 temos $|\tau(\overline{\chi})|^2 = r$, se k é livre de quadrados e primo com r e 0, em caso contrário. Também pela hipótese do lema, $S(\chi) = S(\chi^*)$, onde χ^* é o caráter primitivo módulo r que induz χ. Assim, o lado esquerdo de (3.22) é igual a

$$\sum_{r\le Q} \frac{r}{\varphi(r)} \left(\sum_{\substack{k\le \frac{Q}{r} \\ (r,k)=1}} \frac{\mu^2(k)}{\varphi(k)} \right) \left(\sum_{\chi\,(mod\,r)}^{*} |S(\chi)|^2 \right). \tag{3.23}$$

Agora, o Lema 3.1 de [11] nos diz que

$$\sum_{\substack{k\le x \\ (r,k)=1}} \frac{\mu^2(k)}{\varphi(k)} \ge \frac{\varphi(r)}{r}\log x,$$

para todo $x \ge 1$. Usando esta estimativa em (3.23), concluímos a prova.

Com os resultados acima, demonstraremos o

Teorema 3.16. *Sob a mesma hipótese do Lema 3.15, temos*

$$\sum_{q\le Q} \log\frac{Q}{q} \sum_{\chi\,(mod\,q)}^{*} \int_{-T}^{T} |S(\chi,t)|^2\,dt \ll \sum_{n=1}^{\infty} \left(Q^2T+n\right)|a_n|^2,$$

para todo $T \ge 1$.

Prova: Usando o Corolário 3.14 e o Lema 3.15, obtemos

$$\begin{aligned}
\sum_{q\le Q} \log\frac{Q}{q} \sum_{\chi\,(mod\,q)}^{*} \int_{-T}^{T} |S(\chi,t)|^2\,dt &\overset{3.14}{\ll} T^2 \int_0^\infty \sum_{q\le Q}\log\frac{Q}{q} \sum_{\chi\,(mod\,q)}^{*} \left| \sum_{y\le n\le y\tau} a_n\chi(n)\right|^2 \frac{dy}{y} \\
&\overset{3.15}{\ll} T^2 \int_0^\infty \left(Q^2 + y(\tau-1)\right) \sum_{y\le n\le y\tau} |a_n|^2 \frac{dy}{y}.
\end{aligned} \tag{3.24}$$

Definindo $F_y(x) = 1$, se $y \le x \le y\tau$ e 0, em caso contrário, vemos que $\sum_{y\le n\le y\tau} |a_n|^2 = \sum_{n=1}^{\infty} |a_n|^2 F_y(n)$. Assim, pelo Teorema da Convergência Monótona, concluímos que o lado esquerdo de (3.24) é

$$\ll T^2 \sum_{n=1}^{\infty} |a_n|^2 \int_0^\infty \left(Q^2 + y(\tau-1)\right) F_y(n) \frac{dy}{y} = T^2 \sum_{n=1}^{\infty} |a_n|^2 \int_{\frac{n}{\tau}}^{n} \left(Q^2 + y(\tau-1)\right) \frac{dy}{y}.$$

Mas o coeficiente de $|a_n|^2$ na série acima é igual a

$$(TQ)^2 \int\limits_{\frac{n}{\tau}}^{n} \frac{dy}{y} + T^2(\tau - 1) \int\limits_{\frac{n}{\tau}}^{n} dy = TQ^2 + T^2(\tau-1)(1-\tau^{-1})n,$$

o qual é $\ll Q^2T + n$, pois $T \geq 1$ implica em $(\tau-1)(1-\tau^{-1}) \ll T^{-2}$, de onde segue o resultado.

3.3 O método de Turán para detecção de zeros

Sabemos que $\log\left(1 - \frac{1}{p^s}\right) \ll p^{-\sigma}$, para $\sigma > 1$, onde log é o ramo principal do logaritmo. Assim, o produto de Euler para a função Zeta (ver (3.1)) implica $\varsigma(s) = exp\left(-\sum_p \log\left(1 - \frac{1}{p^s}\right)\right)$, para $\sigma > 1$. Além disso, $\log\varsigma(s) := -\sum_p \log\left(1 - \frac{1}{p^s}\right)$ converge absolutamente sobre compactos no semiplano $\sigma > 1$, consequentemente é analítica nesta região. Portanto,

$$\frac{\varsigma'(s)}{\varsigma(s)} = \frac{d}{ds}\log\varsigma(s) = -\sum_p \frac{(\log p)p^{-s}}{1-p^{-s}} = -\sum_p \log p \sum_{n=1}^{\infty} p^{-ns} = -\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s},$$

para $\sigma > 1$. Analogamente chega-se a seguinte identidade

$$\frac{L'(s,\chi)}{L(s,\chi)} = -\sum_{n=1}^{\infty} \frac{\Lambda(n)\chi(n)}{n^s}, \tag{3.25}$$

para todo χ caráter de Dirichlet e $\sigma > 1$.

Sejam $L(s,\chi)$ a L-função associada a um caráter χ módulo q, com q menor ou igual a T, $w = 1 + iv$, com $|v| \leq T$ e $r > 0$. Se $\chi = \chi_0$, adicionamos a condição $|v| \geq 2$ (em função do pólo de $L(s,\chi_0)$ em $s = 1$). Definimos $\mathcal{L} = \log T$ e $Q(r,v)$ como sendo o número de zeros de $L(s,\chi)$, contados com multiplicidade, no disco $|s - w| \leq r$. O seguinte lema apresenta uma estimativa para $Q(r,v)$.

Lema 3.17 (Linnik). *Seja $\mathcal{L}^{-1} \leq r \leq 1$, então $Q(r,v) \ll r\mathcal{L}$.*

Prova: Pela relação (3.6) e a discussão que a segue, podemos supor sem perda de generalidade que χ é primitivo. Por ([8], páginas 99 e 102), temos

$$\frac{L'(s,\chi)}{L(s,\chi)} = \sum_{\substack{\rho \\ |\gamma - t| \leq 1}} \frac{1}{s-\rho} + O(\log q(|t|+2)), \tag{3.26}$$

para $-1 \leq \sigma \leq 2$, com $|t| \geq 1$ se $\chi = \chi_0$.

De (3.25) e do fato que a função Zeta possui um pólo simples em $s = 1$, obtemos

$$\Re\frac{L'(s,\chi)}{L(s,\chi)} \leq \left|\frac{L'(s,\chi)}{L(s,\chi)}\right| \leq \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^\sigma} = -\frac{\varsigma'(\sigma)}{\varsigma(\sigma)} \ll \frac{1}{\sigma - 1}, \tag{3.27}$$

para $\sigma > 1$. Tomando $s = w + r$, temos $\Re\frac{1}{s-\rho} = \frac{1+r-\beta}{|s-\rho|^2} > 0$, para todo ρ. Assim,

$$\Re \sum_{\substack{\rho \\ |\gamma - v| \leq 1}} \frac{1}{s-\rho} \geq \Re \sum_{\substack{\rho \\ |\rho - w| \leq r}} \frac{1}{s-\rho},$$

mas $\Re\frac{1}{s-\rho} = \frac{1+r-\beta}{|s-\rho|^2} \geq \frac{r}{(|s-w|+|\rho-w|)^2} \geq \frac{r}{(2r)^2} = \frac{1}{4r}$, para todo ρ na última soma acima. Logo

$$\Re \sum_{\substack{\rho \\ |\gamma - v| \leq 1}} \frac{1}{s-\rho} \gg \frac{Q(r,v)}{4r}, \tag{3.28}$$

portanto (3.26), (3.27) e (3.28) implicam $\dfrac{Q(r,v)}{4r} \ll \dfrac{1}{r} + \mathcal{L}$. Como, por hipótese, $\mathcal{L}^{-1} \leq r$, concluímos que $Q(r,v) \ll r\mathcal{L}$.

Usaremos agora os resultados de Turán sobre somas de potências (ver Apêndice C) e o Lema de Linnik para provar que se $L(s,\chi)$ tem um zero próximo de w, então para x e y bem escolhidos, a soma

$$S_{x,y}(\chi, v) := \sum_{x \leq p \leq y} \frac{\chi(p)\log p}{p^w}$$

é "grande". Mais precisamente, provaremos a seguinte proposição.

Proposição 3.18. *Existem constantes positivas c_{13}, c_{14}, c_{15} e c_{16} tais que se $L(s,\chi)$ tem um zero no disco $|s-w| \leq r$, com $\mathcal{L}^{-1} \leq r \leq c_{13}$, então, para cada $x \geq T^{c_{14}}$, temos*

$$\int_x^{x^{c_{15}}} |S_{x,y}(\chi, v)| \frac{dy}{y} \gg x^{-c_{16}\cdot r} \log^2 x.$$

Prova: Se χ é primitivo, por (3.26) e a estimativa (3.9), obtemos

$$\frac{L'(s,\chi)}{L(s,\chi)} = \sum_{\substack{\rho \\ |\gamma - t| \leq 2}} \frac{1}{s-\rho} + O(\log q(|t|+2)), \tag{3.29}$$

para $-1 \leq \sigma \leq 2$, com $|t| \geq 1$ se $\chi = \chi_0$. Agora, se χ é um caráter módulo q (não necessariamente primitivo) induzido pelo caráter primitivo χ^*, então por (3.6), temos

$$\frac{L'(s,\chi)}{L(s,\chi)} = \frac{L'(s,\chi^*)}{L(s,\chi^*)} + \sum_{p|q} \frac{\chi^*(p)p^{-s}\log p}{1-\chi^*(p)p^{-s}},$$

para todo $s \in \mathbb{C}$. Adicionando a condição $\sigma \geq \frac{1}{4}$, temos que

$$\sum_{p|q} \frac{\chi^*(p)p^{-s}\log p}{1-\chi^*(p)p^{-s}} \ll \sum_{p|q} \log p \ll \log q,$$

o qual é absorvido no termo de erro de (3.29). Assim, para qualquer χ módulo q, temos

$$\frac{L'(s,\chi)}{L(s,\chi)} = \sum_{\substack{\rho \\ |\gamma - t| \leq 2}} \frac{1}{s-\rho} + O(\log q(|t|+2)), \tag{3.30}$$

para $\frac{1}{4} \leq \sigma \leq 2$, com $|t| \geq 1$ se $\chi = \chi_0$, onde a soma é sobre os zeros de $L(s,\chi)$ na faixa crítica.

Tome s satisfazendo $|s-w| \leq \frac{1}{2}$. Então $|\rho - w| \leq 1$ implica $|s-\rho| \leq |\rho - w| + |w-s| \leq 2$, logo

$$\sum_{\substack{\rho \\ |\gamma - t| \leq 2}} \frac{1}{s-\rho} = \sum_{\substack{\rho \\ |\rho - w| \leq 1}} \frac{1}{s-\rho} + \sum_{\substack{\rho \\ |\rho - w| > 1 \\ |\gamma - t| \leq 2}} \frac{1}{s-\rho}.$$

Como $|\rho - w| > 1$ implica $|s-\rho| \geq |\rho - w| - |s-w| \geq \frac{1}{2}$, conclui-se que

$$\sum_{\substack{\rho \\ |\rho - w| > 1 \\ |\gamma - t| \leq 2}} \frac{1}{s-\rho} \ll \sum_{\substack{\rho \\ |\gamma - t| \leq 2}} 1 \overset{(3.9)}{\ll} \mathcal{L}.$$

Portanto,

$$\frac{L'(s,\chi)}{L(s,\chi)} = \sum_{\substack{\rho \\ |\rho - w| \leq 1}} \frac{1}{s-\rho} + O(\mathcal{L}),$$

para $|s-w| \leq \frac{1}{2}$. Pela Fórmula Integral de Cauchy (ver Teorema A.4 e a relação (A.2)) segue-se que

$$\frac{(-1)^k}{k!} \left(\frac{d}{ds}\right)^k \frac{L'(s,\chi)}{L(s,\chi)} = \sum_{\substack{\rho \\ |\rho - w| \leq 1}} \frac{1}{(s-\rho)^{k+1}} + O(4^k \mathcal{L}),$$

para $|s-w| \le \frac{1}{4}$ e $k \ge 0$. Escolhendo $s = w + r$ acima, estimamos a contribuição dos termos da última soma que correspondem aos ρ que satisfazem $|\rho - w| > \lambda$, onde $r \le \lambda \le 1$. Pelo Lema 3.17, há $\ll 2^j\lambda\mathcal{L}$ zeros no anel $2^j\lambda < |\rho - w| \le 2^{j+1}\lambda$ e para cada um destes zeros vale $\left|\frac{1}{(s-\rho)^{k+1}}\right| \le \left(2^j\lambda\right)^{-(k+1)}$. Portanto, para $k \ge 1$, temos

$$\sum_{\substack{\rho \\ |\rho-w|>\lambda}} \frac{1}{(s-\rho)^{k+1}} \ll \sum_{0 \le j \le \left\lfloor \frac{\log\lambda}{\log 2}\right\rfloor} \sum_{\substack{\rho \\ 2^j\lambda < |\rho-w| \le 2^{j+1}\lambda}} \left(2^j\lambda\right)^{-(k+1)} \ll \sum_{j=0}^{\infty} \left(2^j\lambda\right)^{-(k+1)} 2^j\lambda\mathcal{L} \ll \sum_{j=0}^{\infty} \left(2^j\lambda\right)^{-k}\mathcal{L} \ll \lambda^{-k}\mathcal{L}.$$

Então, para $\mathcal{L}^{-1} \le r \le \lambda \le \frac{1}{4}$, temos

$$\frac{(-1)^k}{k!}\left(\frac{d}{ds}\right)^k \frac{L'(s,\chi)}{L(s,\chi)} = \sum_{\substack{\rho \\ |\rho-w| \le \lambda}} \frac{1}{(s-\rho)^{k+1}} + O(\lambda^{-k}\mathcal{L}), \tag{3.31}$$

Pelo Lema 3.17, a quantidade de zeros com $|\rho - w| \le \lambda$ é menor ou igual a $A_1\lambda\mathcal{L}$ e pela hipótese da proposição $\min\limits_{\substack{\rho \\ |\rho-w|\le\lambda}} |s-\rho| \le 2r$. Assim, pelo Corolário C.3 (ver Apêndice C), para todo $K \ge A_1\lambda\mathcal{L}$ existe um inteiro $k \in [K, 2K]$, tal que

$$\left|\sum_{\substack{\rho \\ |\rho-w| \le \lambda}} \frac{1}{(s-\rho)^{k+1}}\right| \ge (Dr)^{-(k+1)},$$

onde D é uma constante fixa.

Escolhendo $\lambda = A_2Dr$, onde A_2 é uma constante escolhida de modo que $r \le \lambda \le \frac{1}{4}$ (repare que tomando r pequeno podemos supor A_2 suficientemente grande), a soma em (3.31) domina o termo de erro. De fato, para qualquer constante $C_0 > 0$, temos $(Dr)^{-(k+1)} \ge C_0(A_2Dr)^{-k}\mathcal{L}$ se $A_2^k \ge C_0Dr\mathcal{L}$ e esta última desigualdade vale se tomarmos $K \ge A_1A_2Dr\mathcal{L}$, com A_2 grande. Portanto existe $E > 0$, tal que

$$\frac{1}{k!}\left(\frac{d}{ds}\right)^k \frac{L'(s,\chi)}{L(s,\chi)} \gg (Dr)^{-(k+1)}, \tag{3.32}$$

para algum inteiro $k \in [K, 2K]$, sob a condição de $K \ge Er\mathcal{L}$. Usando (3.25) e o fato que $s = w + r$, podemos escrever (3.32) como

$$\sum_{n=1}^{\infty} \frac{\Lambda(n)\chi(n)}{n^w} p_k(r\log n) \gg \frac{D^{-k}}{r}, \tag{3.33}$$

onde $p_k(u) := \dfrac{e^{-u}u^k}{k!}$.

Observamos agora que existem constantes B_1 e B_2 tais que

$$\begin{aligned} p_k(u) &\le (2D)^{-k}, && \text{para } u \le B_1k; \\ p_k(u) &\le (2D)^{-k}e^{-\frac{1}{2}u}, && \text{para } u \ge B_2k. \end{aligned} \tag{3.34}$$

Ora, escrevendo $u = vk$ e usando a desigualdade $k! \ge \left(\frac{k}{e}\right)^k$, chegamos a $p_k(u) \le (ve^{1-v})^k$, porém $ve^{1-v} \longrightarrow 0$ quando v vai para 0 e $ve^{1-\frac{v}{2}} \longrightarrow 0$ quando v vai ao infinito, de onde segue as desigualdades (3.34).

Dado $x \ge T^A$, com $A \ge B_1E$, tomamos $K = B_1^{-1}r\log x$. Logo $K \ge Er\mathcal{L}$. Portanto existe $k \in [K, 2K]$ satisfazendo (3.33). Defina agora $B = \frac{2B_2}{B_1}$. Para $n \le x$, temos $r\log n \le r\log x \le B_1K \le B_1k$, logo

$$\sum_{n\le x} \frac{\Lambda(n)\chi(n)}{n^w} p_k(r\log n) \overset{(3.34)}{\ll} (2D)^{-k} \sum_{n \le x} \frac{\Lambda(n)}{n} \overset{(1.11)}{\ll} (2D)^{-k}\frac{k}{r}.$$

Agora, para $n > x^B$, temos $r\log n \ge Br\log x \ge 2B_2K \ge B_2k$, portanto

$$\sum_{n>x^B} \frac{\Lambda(n)\chi(n)}{n^w} p_k(r\log n) \overset{(3.34)}{\ll} (2D)^{-k} \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^{1+\frac{1}{2}r}} \overset{(3.27)}{\ll} \frac{(2D)^{-k}}{r}.$$

Usando as últimas estimativas em (3.33), chegamos em

$$\sum_{x \le n \le x^B} \frac{\Lambda(n)\chi(n)}{n^w} p_k(r\log n) \gg \frac{D^{-k}}{r}, \tag{3.35}$$

para k suficientemente grande, o que é possível se tomarmos A grande. Como $p_k(u) \leq 1$, para todo $u \geq 0$, um argumento semelhante ao feito em (1.19) nos diz que a contribuição das potências de primos p^m, com $m \geq 2$, em (3.35) é $\ll x^{-\frac{1}{2}}$, a qual pode ser ignorada, desde que

$$D^{-k} \geq \exp\left(-2(\log D)B_1^{-1} r \log x\right) = x^{-\frac{C}{2}r}, \tag{3.36}$$

para alguma constante $C > 0$. Assim, podemos substituir (3.35) por

$$\sum_{x \leq p \leq x^B} \frac{(\log p)\chi(p)}{p^w} p_k(r \log p) \gg \frac{D^{-k}}{r}. \tag{3.37}$$

Definindo $S(y) = S_{x,y}(\chi, v)$, temos que (3.37) é igual a

$$\int_{x^-}^{x^B} p_k(r \log y) dS(y) = p_k\left(r \log x^B\right) S\left(x^B\right) - \int_{x}^{x^B} S(y) p_k'(r \log y) r \frac{dy}{y}.$$

Por (3.34), o primeiro termo à direita da igualdade acima tem ordem

$$(2D)^{-k} \sum_{n \leq x^B} \frac{\Lambda(n)}{n} \overset{(1.11)}{\ll} (2D)^{-k} \frac{k}{r},$$

como estamos supondo k suficientemente grande, obtemos

$$\int_{x}^{x^B} S(y) p_k'(r \log y) \frac{dy}{y} \gg \frac{D^{-k}}{r^2}. \tag{3.38}$$

Fazendo alguns cálculos, chegamos a $p_k' = p_{k-1} - p_k \ll 1$, usando isso em (3.38), conclui-se que

$$\int_{x}^{x^B} |S(y)| \frac{dy}{y} \gg \frac{D^{-k}}{r^2} \gg x^{-Cr} \log^2 x,$$

onde C é o mesmo que aparece em (3.36). Finalizando a demonstração.

Suponhamos agora que existe o caráter excepcional $\widetilde{\chi}$ $(mod\ \widetilde{r})$ de ordem T, com zero excepcional $\widetilde{\beta}$ satisfazendo

$$1 - \widetilde{\beta} \leq \frac{c_4}{\log T}$$

(ver Proposição 3.7 e a discussão que a segue). Para todo caráter χ com módulo menor ou igual a T, definimos:

$$\widetilde{S}_{x,y}(\chi, v) := \sum_{x \leq p \leq y} \frac{\chi(p)\left(1 + \frac{\widetilde{\chi}(p)}{p^{1-\widetilde{\beta}}}\right) \log p}{p^w}.$$

Proposição 3.19. *Se $L(s, \chi)$ tem um zero diferente de $\widetilde{\beta}$ no disco $|s - w| \leq r$, com $\mathcal{L}^{-1} \leq r \leq c_{13}$, então, para cada $x \geq T^{c_{14}}$, temos*

$$\int_{x}^{x^{c_{15}}} \left|\widetilde{S}_{x,y}(\chi, v)\right| \frac{dy}{y} \gg x^{-c_{16} \cdot r} \log^2 x.$$

Prova: Defina $F(s, \chi) := L(s, \chi) L(s + 1 - \widetilde{\beta}, \chi\widetilde{\chi})$. Para χ não induzido por $\widetilde{\chi}$, a demonstração segue repetindo a prova da Proposição 3.18, com $F(s, \chi)$ no lugar de $L(s, \chi)$, observando que

$$\frac{F'(s, \chi)}{F(s, \chi)} = \frac{L'(s, \chi)}{L(s, \chi)} + \frac{L'\left(s + 1 - \widetilde{\beta}, \chi\widetilde{\chi}\right)}{L\left(s + 1 - \widetilde{\beta}, \chi\widetilde{\chi}\right)} \overset{(3.25)}{=} -\sum_{n=1}^{\infty} \frac{\Lambda(n)\chi(n)\left(1 + \frac{\widetilde{\chi}(n)}{n^{1-\widetilde{\beta}}}\right)}{n^s}, \tag{3.39}$$

para $\sigma > 1$.

Para χ induzido por $\widetilde{\chi}$, vemos que $F(s,\chi) = L(s,\chi)L(s+1-\widetilde{\beta},\chi_0)$, onde χ_0 é um caráter principal módulo q, com $q \le T$. Como o pólo da função Zeta tem resíduo 1 e a mesma não tem zeros no retângulo $0 < \sigma < 1$, $|t| \le 2$ (ver Proposição 3.3), podemos escrever (3.30), no caso em que $\chi = \chi_0$, da seguinte forma

$$\frac{L'(s,\chi_0)}{L(s,\chi_0)} = -\frac{1}{s-1} + \sum_{\substack{\rho \\ |\gamma - t| \le 2}} \frac{1}{s-\rho} + O(\log q(|t|+2)),$$

para $\frac{1}{4} \le \sigma \le 2$. Assim,

$$\begin{aligned}
\frac{F'(s,\chi)}{F(s,\chi)} &= \frac{L'(s,\chi)}{L(s,\chi)} + \frac{L'\left(s+1-\widetilde{\beta},\chi_0\right)}{L\left(s+1-\widetilde{\beta},\chi_0\right)} \\
&= \frac{1}{s-\widetilde{\beta}} + \sum_{\substack{\rho \ne \widetilde{\beta} \\ L(\rho,\widetilde{\chi})=0 \\ |\gamma - t| \le 2}} \frac{1}{s-\rho} - \frac{1}{(s+1-\widetilde{\beta})-1} + \sum_{\substack{\rho \\ \zeta(\rho)=0 \\ |\gamma - t| \le 2}} \frac{1}{(s+1-\widetilde{\beta})-\rho} + O(\log q(|t|+2)) \\
&= \sum_{\substack{\rho \ne \widetilde{\beta} \\ F(\rho,\chi)=0 \\ |\gamma - t| \le 2}} \frac{1}{s-\rho} + O(\log q(|t|+2)),
\end{aligned} \tag{3.40}$$

para $\frac{1}{4} \le \sigma \le 2$. Repetindo a prova da Proposição 3.18 com $F(s,\chi)$ no lugar de $L(s,\chi)$, (3.40) no lugar de (3.30) e observando (3.39), concluímos a prova da proposição.

3.4 Demonstração do Teorema 3.12

Nesta seção usaremos os resultados das últimas duas seções para provar o Teorema 3.12. Iniciamos com o seguinte lema.

Lema 3.20. *Dados $a > 0$ e $0 < \lambda < c$, temos*

$$I(a,\lambda) := \frac{1}{2\pi i} \int_{(c)} \frac{a^s}{s(s-\lambda)} ds = \begin{cases} \dfrac{a^\lambda - 1}{\lambda}, & se\ a > 1; \\ 0, & se\ 0 < a \le 1, \end{cases}$$

onde (c) significa que estamos integrando sobre a reta $\sigma = c$.

Prova: **Caso 1.** Suponhamos que $a > 1$. Para $T > 0$ e $\eta > 0$, seja $R(\eta, T)$ o retângulo com vértices nos pontos $\{c \pm iT, -\eta \pm iT\}$, então pelo Teorema dos Resíduos (ver Teorema A.6), temos

$$\frac{1}{2\pi i} \int_{R(\eta,T)} \frac{a^s}{s(s-\lambda)} ds = \frac{a^\lambda - 1}{\lambda}. \tag{3.41}$$

A função $s \longmapsto \frac{a^s}{s(s-\lambda)}$ tende a 0, uniformemente em t, quando $\sigma \longrightarrow -\infty$. Portanto, fazendo $\eta \longrightarrow \infty$ em (3.41), chegamos a

$$\int_{c-iT}^{c+iT} \frac{a^s}{s(s-\lambda)} ds = \frac{a^\lambda - 1}{\lambda} + \int_{-\infty+iT}^{c+iT} \frac{a^s}{s(s-\lambda)} ds - \int_{-\infty-iT}^{c-iT} \frac{a^s}{s(s-\lambda)} ds, \tag{3.42}$$

mas

$$\int_{-\infty \pm iT}^{c \pm iT} \frac{a^s}{s(s-\lambda)} ds \ll T^{-2} \int_{-\infty}^{c} a^\sigma d\sigma \longrightarrow 0, \ \text{quando } T \longrightarrow \infty.$$

Assim, fazendo $T \longrightarrow \infty$ em (3.42), obtemos $I(a,\lambda) = \dfrac{a^\lambda - 1}{\lambda}$.

Caso 2. Para $a = 1$, basta observar que

$$2\pi i I(1,\lambda) = \frac{1}{\lambda} \log\left(\frac{s-\lambda}{s}\right)\Bigg|_{c-i\infty}^{c+i\infty} = 0.$$

Caso 3. Suponhamos que $0 < a < 1$. Dados $T > 0$ e $\eta > c$, seja $R(\eta, T)$ o retângulo com vértices nos pontos $\{c \pm iT, \eta \pm iT\}$, então pelo Teorema de Cauchy, temos

$$\frac{1}{2\pi i} \int\limits_{R(\eta,T)} \frac{a^s}{s(s-\lambda)} ds = 0. \tag{3.43}$$

Como a função $s \longmapsto \frac{a^s}{s(s-\lambda)}$ tende a 0, uniformemente em t, quando $\sigma \longrightarrow \infty$, podemos proceder como no **Caso 1** para concluir que, neste caso, $I(a, \lambda) = 0$.

Agora estamos prontos para dar uma demonstração ao Teorema 3.12. Para facilitar a leitura o enunciamos aqui novamente.

Teorema 3.12. *Existe uma constante c_{11} tal que para $\frac{1}{2} \leq \alpha \leq 1$ e $T > 1$, temos*

$$\sum_{q \leq T} N_q^*(\alpha, T) \ll T^{c_{11}(1-\alpha)}. \tag{3.44}$$

Agora, se existe o caráter excepcional $\widetilde{\chi}$ de ordem T, com zero excepcional $\widetilde{\beta}$, temos

$$\sum_{q \leq T} \widetilde{N}_q^*(\alpha, T) \ll T^{c_{11}(1-\alpha)}(1 - \widetilde{\beta}) \log T. \tag{3.45}$$

Aqui $\sim$ em $\widetilde{N}_q^*$ significa que $\widetilde{\beta}$ é excluído.

Prova: Por (3.8), obtemos $N(\alpha, T, \chi) \ll T \log T$, para todo caráter χ com módulo menor ou igual a T, logo

$$\sum_{q \leq T} N_q^*(\alpha, T) = \sum_{q \leq T} \sideset{}{^*}\sum_{\chi\ (mod\ q)} N(\alpha, T, \chi) \ll \sum_{q \leq T} \sideset{}{^*}\sum_{\chi\ (mod\ q)} T \log T \ll T^3 \log T.$$

Assim, observando que (3.11) implica $1 - \widetilde{\beta} \gg T^{-\frac{2}{3}}$ e tomando c_{11} no Teorema 3.12 suficientemente grande, podemos supor sem perda de generalidade que $1 - \alpha$ é suficientemente pequeno. Usando as Proposições 3.6 e 3.7 e o fato que o lado direito de (3.44) é maior ou igual a 1, podemos tomar $1 - \alpha \gg \mathcal{L}^{-1}$.

Sejam $w = 1 + iv$, com $|v| \leq T$ (e $|v| \geq 2$ se $\chi = \chi_0$) e $r = 2(1 - \alpha)$. Pela discussão feita acima basta provar o teorema sob a condição $\mathcal{L}^{-1} \leq r \leq c_{13}$, e assim podemos aplicar a Proposição 3.18 para concluir que, se $L(s, \chi)$ tem um zero no disco $|s - w| \leq r$, vale

$$\int\limits_x^{x^{c_{15}}} |S_{x,y}(\chi, v)| \frac{dy}{y} \gg x^{-c_{16} \cdot r} \log^2 x, \tag{3.46}$$

para todo $x \geq T^{c_{14}}$. Escolhendo $x = T^{\max\{c_{14},\, 5\}}$ e aplicando a Desigualdade de Cauchy-Schwarz no lado esquerdo de (3.46), chegamos a

$$T^{c(1-\alpha)} \mathcal{L}^{-3} \int\limits_x^{x^{c_{15}}} |S_{x,y}(\chi, v)|^2 \frac{dy}{y} \gg 1, \tag{3.47}$$

onde $c = 4c_{16} \max\{c_{14}, 5\}$. Como $Q(r, v) \ll r\mathcal{L}$ (ver Lema 3.17) e cada zero $\rho_\chi = \beta_\chi + i\gamma_\chi$, com $\beta_\chi \geq \alpha$ e $|\gamma_\chi| \leq T$, é detectado por (3.47) quando v varia em um intervalo de comprimento $\gg r$ contido em $[-T, T]$ (pela Proposição 3.3, podemos tomar os intervalos com $|v| \geq 2$ quando $\chi = \chi_0$), segue-se que

$$N(\alpha, T, \chi) \ll T^{c(1-\alpha)} \mathcal{L}^{-2} \int\limits_x^{x^{c_{15}}} \int\limits_{-T}^{T} |S_{x,y}(\chi, v)|^2 \, dv \frac{dy}{y},$$

portanto

$$\sum_{q \leq T} N_q^*(\alpha, T) \ll T^{c(1-\alpha)} \mathcal{L}^{-2} \int\limits_x^{x^{c_{15}}} \left(\sum_{q \leq T} \sideset{}{^*}\sum_{\chi\ (mod\ q)} \int\limits_{-T}^{T} |S_{x,y}(\chi, v)|^2 \, dv \right) \frac{dy}{y}.$$

O termo entre parênteses é uma função escada limitada em y, logo existe $y \in [x, x^{c_{15}}]$ tal que

$$\sum_{q \leq T} N_q^*(\alpha, T) \ll T^{c(1-\alpha)} \mathcal{L}^{-1} \sum_{q \leq T} \sideset{}{^*}\sum_{\chi\ (mod\ q)} \int\limits_{-T}^{T} |S_{x,y}(\chi, v)|^2 \, dv. \tag{3.48}$$

Estimamos agora a soma dupla em (3.48). Desde que $x \geq T^5$, a hipótese do Teorema 3.16 é satisfeita com $Q = T^2$ e $S(\chi, t) = S_{x,y}(\chi, v)$, portanto

$$\sum_{q \leq T^2} \log\left(\frac{T^2}{q}\right) \sum_{\chi \, (mod\, q)}^{*} \int_{-T}^{T} |S_{x,y}(\chi, v)|^2 \, dv \ll \sum_{x \leq p \leq y} \left(T^5 + p\right) \frac{\log^2 p}{p^2} \overset{(1.11)}{\ll} \mathcal{L}^2. \tag{3.49}$$

Porém, para $q \leq T$, temos $\log\left(\frac{T^2}{q}\right) \geq \log T$ e, portanto, (3.49) implica que a soma dupla em (3.48) é $\ll \mathcal{L}$. Assim, o lado direito de (3.48) é $\ll T^{c(1-\alpha)}$, o que prova (3.44).

Se o caráter excepcional existir, repetimos os passos acima com a Proposição 3.19 no lugar da Proposição 3.18, para concluir que se $x = T^{\max\{c_{14}, 5\}}$, existe $y \in [x, x^{c_{15}}]$ tal que

$$\sum_{q \leq T} \widetilde{N}_q^*(\alpha, T) \ll T^{c(1-\alpha)} \mathcal{L}^{-1} \sum_{q \leq T} \sum_{\chi \, (mod\, q)}^{*} \int_{-T}^{T} \left|\widetilde{S}_{x,y}(\chi, v)\right|^2 dv. \tag{3.50}$$

Estimamos agora a soma dupla em (3.50). Como $x \geq T^5$, o Teorema 3.16 nos diz que

$$\begin{aligned} \sum_{q \leq T^2} \log\left(\frac{T^2}{q}\right) \sum_{\chi \, (mod\, q)}^{*} \int_{-T}^{T} \left|\widetilde{S}_{x,y}(\chi, v)\right|^2 dv &\ll \sum_{x \leq p \leq y} \left(T^5 + p\right) \frac{\left(a_p \log p\right)^2}{p^2} \\ &\ll \sum_{x \leq p \leq x^{c_{15}}} \frac{\left(a_p \log p\right)^2}{p}, \end{aligned} \tag{3.51}$$

onde $a_p = 1 + \frac{\widetilde{\chi}(p)}{p^{1-\widetilde{\beta}}}$. Assim, por (3.50) e (3.51), chegamos em (3.45) se provarmos que

$$\sum_{x \leq p \leq x^{c_{15}}} \frac{\left(a_p \log p\right)^2}{p} \ll (1 - \widetilde{\beta}) \mathcal{L}^3. \tag{3.52}$$

Finalizamos demonstrando (3.52). Pelo Teorema do Valor Médio temos que $1 - p^{\widetilde{\beta}-1} \leq (1 - \widetilde{\beta}) \log p$, para todo p primo, portanto

$$a_p \log p = (1 + \widetilde{\chi}(p)) \log p + \left(p^{\widetilde{\beta}-1} - 1\right) \widetilde{\chi}(p) \log p = (1 + \widetilde{\chi}(p)) \log p + O\left((1 - \widetilde{\beta}) \log^2 p\right).$$

Agora, para $x \leq p \leq x^{c_{15}}$, a Desigualdade (3.11) implica $(1 - \widetilde{\beta}) \log p \ll 1$, logo

$$(a_p \log p)^2 \ll (1 + \widetilde{\chi}(p)) \log^2 p + (1 - \widetilde{\beta}) \log^3 p.$$

Repare que

$$\sum_{x \leq p \leq x^{c_{15}}} \frac{(1 - \widetilde{\beta}) \log^3 p}{p} \ll (1 - \widetilde{\beta}) \log^2 x \sum_{x \leq p \leq x^{c_{15}}} \frac{\log p}{p} \overset{(1.11)}{\ll} (1 - \widetilde{\beta}) \log^3 x$$

e

$$\sum_{x \leq p \leq x^{c_{15}}} \frac{(1 + \widetilde{\chi}(p)) \log^2 p}{p} \ll \log^2 x \sum_{x \leq p \leq x^{c_{15}}} \frac{1 + \widetilde{\chi}(p)}{p}.$$

Assim, basta provar que

$$\sum_{x \leq p \leq x^{c_{15}}} \frac{1 + \widetilde{\chi}(p)}{p} \ll (1 - \widetilde{\beta}) \log x. \tag{3.53}$$

Definindo $b_n = \sum_{d|n} \widetilde{\chi}(d)$. Temos, para todo p primo, que $b_p = 1 + \widetilde{\chi}(p)$, portanto (3.53) é equivalente a

$$\sum_{x \leq p \leq x^{c_{15}}} \frac{b_p}{p} \ll (1 - \widetilde{\beta}) \log x. \tag{3.54}$$

Sendo $\widetilde{\chi}$ multiplicativo, segue-se que $n \longmapsto b_n$ também o é. Assim, escrevendo $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$, obtemos

$$b_n = \prod_{i=1}^{k} \left(1 + \widetilde{\chi}(p_i) + \widetilde{\chi}(p_i)^2 + \ldots + \widetilde{\chi}(p_i)^{\alpha_i}\right) = \prod_{i=1}^{k} \frac{1 - \widetilde{\chi}(p_i)^{\alpha_i + 1}}{1 - \widetilde{\chi}(p_i)} \geq 0.$$

Além disso, para $\sigma > 1$, temos

$$G(s) := \zeta(s)L(s,\widetilde{\chi}) = \sum_{n=1}^{\infty}\frac{1}{n^s}\cdot\sum_{n=1}^{\infty}\frac{\widetilde{\chi}(n)}{n^s} = \sum_{n=1}^{\infty}\frac{b_n}{n^s}. \tag{3.55}$$

Seja $S := \sum_{n<x}\frac{b_n}{n}$, então

$$S\sum_{x\le p\le x^{c_{15}}}\frac{b_p}{p} \le \sum_{x\le n\le x^{c_{15}+1}}\frac{b_n}{n}, \tag{3.56}$$

pois os b_n são não negativos e multiplicativos.

Para $\kappa := 1+\frac{1}{\log x}$, considere a integral

$$I := \frac{1}{2\pi i}\int\limits_{(2)}\frac{x^s}{s}\left(\frac{\kappa-1}{s-\kappa}+\frac{1-\widetilde{\beta}}{s-\widetilde{\beta}}\right)G(s)ds. \tag{3.57}$$

Da representação (3.55) de $G(s)$ como uma série uniformemente convergente em semiplanos fechados de $\sigma > 1$, temos que

$$\begin{aligned} I &= \sum_{n=1}^{\infty}\frac{b_n}{2\pi i}\int\limits_{(2)}\frac{(x/n)^s}{s}\left(\frac{\kappa-1}{s-\kappa}+\frac{1-\widetilde{\beta}}{s-\widetilde{\beta}}\right)ds \\ &= (\kappa-1)\sum_{n=1}^{\infty}\frac{b_n}{2\pi i}\int\limits_{(2)}\frac{(x/n)^s}{s(s-\kappa)}ds + (1-\widetilde{\beta})\sum_{n=1}^{\infty}\frac{b_n}{2\pi i}\int\limits_{(2)}\frac{(x/n)^s}{s(s-\widetilde{\beta})}ds. \end{aligned}$$

Usando o Lema 3.20 na última igualdade, chegamos a

$$\begin{aligned} I &= \frac{\kappa-1}{\kappa}\sum_{n<x}b_n\left\{\left(\frac{x}{n}\right)^{\kappa}-1\right\}+\frac{1-\widetilde{\beta}}{\widetilde{\beta}}\sum_{n<x}b_n\left\{\left(\frac{x}{n}\right)^{\widetilde{\beta}}-1\right\} \\ &\le \frac{\kappa-1}{\kappa}x^{\kappa}\sum_{n<x}\frac{b_n}{n^{\kappa}}+\frac{1-\widetilde{\beta}}{\widetilde{\beta}}x\sum_{n<x}\frac{b_n}{n}. \end{aligned} \tag{3.58}$$

Por outro lado, movendo a linha de integração de (3.57) para a linha $\left(\frac{1}{2}\right)$ e observando que $G(\widetilde{\beta}) = 0$, enquanto o poló de $G(s)$ é cancelado pelo zero em $s = 1$ da função entre parênteses em (3.57), chegamos a seguinte igualdade via o Teorema dos Resíduos,

$$I = \frac{\kappa-1}{\kappa}x^{\kappa}G(\kappa)+\frac{1}{2\pi i}\int\limits_{(\frac{1}{2})}\frac{x^s}{s}\left(\frac{\kappa-1}{s-\kappa}+\frac{1-\widetilde{\beta}}{s-\widetilde{\beta}}\right)G(s)ds. \tag{3.59}$$

Agora, pelo Teorema 5.23 de [16], para todo χ caráter primitivo módulo q e $\sigma = \frac{1}{2}$, temos

$$L(s,\chi) \ll (q|s|)^{\frac{1}{4}},$$

portanto

$$\frac{1}{2\pi i}\int\limits_{(\frac{1}{2})}\frac{x^s}{s}\left(\frac{\kappa-1}{s-\kappa}+\frac{1-\widetilde{\beta}}{s-\widetilde{\beta}}\right)G(s)ds \ll (\widetilde{r}x)^{\frac{1}{2}} \ll x^{\frac{3}{5}},$$

usando esta última estimativa em (3.59), concluímos que

$$I = \frac{\kappa-1}{\kappa}x^{\kappa}G(\kappa)+O\left(x^{\frac{3}{5}}\right). \tag{3.60}$$

De (3.58) e (3.60), obtemos

$$\frac{\kappa-1}{\kappa}x^{\kappa}\sum_{n\ge x}\frac{b_n}{n^{\kappa}} \le \frac{1-\widetilde{\beta}}{\widetilde{\beta}}x\sum_{n<x}\frac{b_n}{n}+O\left(x^{\frac{3}{5}}\right),$$

de onde segue

$$\sum_{n\ge x}\frac{b_n}{n^{\kappa}} \ll (1-\widetilde{\beta})S\log x + x^{-\frac{2}{5}}\log x.$$

Assim,

$$\sum_{x\le n\le x^{c_{15}+1}} \frac{b_n}{n} \le e^{c_{15}+1} \sum_{n\ge x} \frac{b_n}{n^{\kappa}} \ll (1-\widetilde{\beta})S\log x + x^{-\frac{2}{5}}\log x. \tag{3.61}$$

Pela Desigualdade (3.11), temos que $1-\widetilde{\beta} \gg \dfrac{1}{x^{\frac{1}{10}}\log^2 x}$ e $S \ge b_1 = 1$, portanto a relação (3.61) implica

$$\sum_{x\le n\le x^{c_{15}+1}} \frac{b_n}{n} \ll (1-\widetilde{\beta})S\log x.$$

Utilizando esta última desigualdade em (3.56), obtemos

$$\sum_{x\le p\le x^{c_{15}}} \frac{b_p}{p} \ll (1-\widetilde{\beta})\log x.$$

Finalizando a demonstração do teorema.

3.5 Demonstração da Proposição 3.8

Nesta seção usaremos o Teorema de Densidade de Gallagher-Bombieri (Teorema 3.12) para provar a Proposição 3.8. Precisaremos ainda das chamadas Fórmulas Explícitas para somas parciais do produto da função de von Mangoldt com caracteres de Dirichlet. Para $x > 1$ e χ um caráter de Dirichlet, definimos

$$\psi(x,\chi) = \sum_{n\le x} \chi(n)\Lambda(n).$$

Podemos então relacionar $\psi(x,\chi)$ com os zeros de $L(s,\chi)$ da seguinte forma.

Proposição 3.21 (Fórmula Explícita). *Sejam χ um caráter módulo q, $T > 1$ e $x > 2$. Então*

$$\psi(x,\chi) = \delta_\chi x - \sum_{|\gamma|\le T}{}' \frac{x^\rho}{\rho} + R_q(x,T),$$

onde $R_q(x,T) \ll \dfrac{x\log^2 qxT}{T} + \log^2 qx + x^{\frac{1}{2}}\log x$,

$$\delta_\chi = \begin{cases} 1, & se\ \chi = \chi_0; \\ 0\,, & em\ caso\ contrário, \end{cases}$$

e a soma $\sum'$ *exclui o termo* $1-\beta_1$*, com* β_1 *definido como na Proposição 3.6.*

Uma prova da proposição acima pode ser encontrada em ([8], Capítulos 17 e 19).

Proposição 3.8. *Para constantes absolutas positivas* c_6 *e* c_7 *bem escolhidas, temos*

$$\sum_{q\le P} \sum_{\chi\ (mod\ q)}^{*} \max_{x\le N}\max_{h\le N} \left(h+\frac{N}{P}\right)^{-1} \left|\sum_{x-h<p\le x}^{\sharp} \chi(p)\log p\right| \ll \exp\left(-c_6\frac{\log N}{\log P}\right) \tag{3.62}$$

sob a condição de que $\exp(\log^{\frac{1}{2}} N) \le P \le N^{c_7}$*. Aqui* $\sum^\sharp$ *indica que o termo com* $q = 1$ *é*

$$\sum_{x-h<p\le x} \log p - \sum_{\substack{x-h<n\le x\\ n>0}} 1,$$

e se existe um caráter excepcional $\widetilde{\chi}$ *de ordem* P*, então o termo que lhe correspondente é*

$$\sum_{x-h<p\le x} \widetilde{\chi}(p)\log p + \sum_{\substack{x-h<n\le x\\ n>0}} n^{\widetilde{\beta}-1},$$

Além disso, se o caráter excepcional ocorre, então o lado direito de (3.62) pode ser multiplicado pelo fator $(1-\widetilde{\beta})\log P$*.*

Prova: Sejam $T > 1$, $x > 2$ e χ um caráter módulo q, com $q \leq T$. Da Proposição 3.21 e do Princípio 3.11, temos que

$$\sum_{n\leq x} \chi(n)\Lambda(n) = \delta_\chi x - \widetilde{\delta}_\chi \frac{x^{\widetilde{\beta}}}{\widetilde{\beta}} - \sum_{|\gamma|\leq T}^{\flat} \frac{x^\rho}{\rho} + O\left(\frac{x\log^2 xT}{T} + x^{\frac{1}{2}}\log^2 xT\right), \tag{3.63}$$

com δ_χ definido como na Proposição 3.21,

$$\widetilde{\delta}_\chi = \begin{cases} 1, & \text{se } \chi = \widetilde{\chi}; \\ 0\,, & \text{em caso contrário,} \end{cases}$$

e $\sum^{\flat}$ exclui os termos da soma que correspondem ao zero excepcional $\widetilde{\beta}$ de ordem T e $1-\widetilde{\beta}$.

Repetindo o argumento usado em (1.19), concluímos que os termos da soma à esquerda de (3.63) que correspondem aos $n = p^m$, $m \geq 2$, têm uma contribuição na ordem de $x^{\frac{1}{2}}$ para a soma em questão, logo podem ser absorvidos no termo de erro de (3.63). Assim,

$$\sum_{p\leq x} (\log p)\chi(p) = \delta_\chi x - \widetilde{\delta}_\chi \frac{x^{\widetilde{\beta}}}{\widetilde{\beta}} - \sum_{|\gamma|\leq T}^{\flat} \frac{x^\rho}{\rho} + O\left(\frac{x\log^2 xT}{T} + x^{\frac{1}{2}}\log^2 xT\right),$$

portanto, para $x \leq N$ e $h \leq N$, temos

$$\begin{aligned} \sum_{x-h\leq p\leq x} (\log p)\chi(p) &= \delta_\chi \min\{x,h\} - \widetilde{\delta}_\chi \left(\frac{x^{\widetilde{\beta}}}{\widetilde{\beta}} - \frac{(x-h)^{\widetilde{\beta}}}{\widetilde{\beta}}\right) - \sum_{|\gamma|\leq T}^{\flat} \left(\frac{x^\rho}{\rho} - \frac{(x-h)^\rho}{\rho}\right) \\ &\quad + O\left(\frac{x\log^2 xT}{T} + x^{\frac{1}{2}}\log^2 xT\right). \end{aligned} \tag{3.64}$$

Em (3.64) e no que se segue convencionamos que se $x \leq h$, os termos em $x - h$ desaparecem.

Estimamos agora os termos da soma à direita de (3.64). Observe que $h \leq \frac{x}{2}$ implica

$$\frac{x^\rho}{\rho} - \frac{(x-h)^\rho}{\rho} = \int_{x-h}^{x} y^{\rho-1}dy \ll x^\beta \int_{x-h}^{x} y^{-1}dy \ll x^\beta \left|\log\left(1 - \frac{h}{x}\right)\right| \ll x^{\beta-1}\min\{x,h\}.$$

Agora, para $\frac{x}{2} < h$ e ρ um zero de $L(s,\chi)$ satisfazendo $|\rho| \geq \frac{1}{2}$, temos

$$\frac{x^\rho}{\rho} - \frac{(x-h)^\rho}{\rho} \ll \frac{x^\beta}{|\rho|} \ll x^\beta \ll x^{\beta-1}\min\{x,h\}.$$

Por fim, seja $\frac{x}{2} < h$ e ρ um zero diferente de $1-\widetilde{\beta}$, com $|\rho| \leq \frac{1}{2}$. Então, por (3.8), o número de tais zeros é $\ll \log q$ e cada um deles satisfaz $\frac{c_4}{\log T} \leq \beta \leq \frac{1}{2}$, portanto

$$\sum_{|\rho|\leq\frac{1}{2}}^{\flat} \left(\frac{x^\rho}{\rho} - \frac{(x-h)^\rho}{\rho}\right) \ll \sum_{|\rho|\leq\frac{1}{2}}^{\flat} \frac{x^\beta}{|\rho|} \ll x^{\frac{1}{2}}\log^2 T.$$

Assim,

$$\sum_{x-h\leq p\leq x} (\log p)\chi(p) - \delta_\chi \min\{x,h\} + \widetilde{\delta}_\chi \left(\frac{x^{\widetilde{\beta}}}{\widetilde{\beta}} - \frac{(x-h)^{\widetilde{\beta}}}{\widetilde{\beta}}\right) \ll \sum_{|\gamma|\leq T}^{\flat} x^{\beta-1}\min\{x,h\} + \frac{x\log^2 xT}{T} + x^{\frac{1}{2}}\log^2 xT.$$

Repare que

$$\min\{x,h\} = \sum_{\substack{x-h<n\leq x \\ n>0}} 1 + O(1),$$

e

$$\frac{x^{\widetilde{\beta}}}{\widetilde{\beta}} - \frac{(x-h)^{\widetilde{\beta}}}{\widetilde{\beta}} = \int_{\max\{x-h,0\}}^{x} y^{\widetilde{\beta}-1}dy = \int_{\max\{x-h,0\}}^{x} y^{\widetilde{\beta}-1}d[y] + \int_{\max\{x-h,0\}}^{x} y^{\widetilde{\beta}-1}d\{y\} = \sum_{\substack{x-h<n\leq x \\ n>0}} n^{\widetilde{\beta}-1} + O(1).$$

Portanto

$$\sum_{x-h<p\leq x}^{\sharp} \chi(p)\log p \ll \sum_{|\gamma|\leq T}^{\flat} x^{\beta-1}\min\{x,h\} + \frac{x\log^2 xT}{T} + x^{\frac{1}{2}}\log^2 xT.$$

Note que a condição $\exp(\log^{\frac{1}{2}} N) \le P$ implica

$$\max_{x\le N}\max_{h\le N}\left(h+\frac{N}{P}\right)^{-1}\left(\frac{x\log^2 xT}{T}+x^{\frac{1}{2}}\log^2 xT\right) \ll PT^{-1}\log^4 PT + PN^{-\frac{1}{2}}\log^4 PT$$

e

$$\max_{x\le N}\max_{h\le N}\left(h+\frac{N}{P}\right)^{-1} x^{\beta-1}\min\{x,h\} \ll \left(\frac{N}{P}\right)^{\beta-1},$$

logo, para $P \le T$, temos

$$\sum_{q\le P}\sideset{}{^*}\sum_{\chi\ (mod\ q)}\max_{x\le N}\max_{h\le N}\left(h+\frac{N}{P}\right)^{-1}\left|\sideset{}{^\sharp}\sum_{x-h<p\le x}\chi(p)\log p\right| \ll \sum_{q\le T}\sideset{}{^*}\sum_{\chi\ (mod\ q)}\sideset{}{^\flat}\sum_{|\gamma|\le T}\left(\frac{N}{P}\right)^{\beta-1}+$$
$$+P^3T^{-1}\log^4 PT + P^3N^{-\frac{1}{2}}\log^4 PT, \qquad (3.65)$$

A soma tripla à direita de (3.65) é igual a

$$-\int_0^1\left(\frac{N}{P}\right)^{\alpha-1} d_\alpha\left(\sum_{q\le T}\widetilde{N}_q^*(\alpha,T)\right) = \int_0^1\left(\frac{N}{P}\right)^{\alpha-1}\log\left(\frac{N}{P}\right)\sum_{q\le T}\widetilde{N}_q^*(\alpha,T)d\alpha + \left(\frac{N}{P}\right)^{-1}\sum_{q\le T}\widetilde{N}_q^*(0,T). \qquad (3.66)$$

Usando a estimativa (3.16) de Gallagher (ver Teorema 3.12) e a região livre de zeros do Princípio 3.11, e supondo que $T^{c_{11}} \le \left(\frac{N}{P}\right)^{\frac{1}{2}}$, vemos que (3.66) é igual a

$$\int_0^{1-\eta(T)}\left(\frac{N}{P}\right)^{\frac{1}{2}(\alpha-1)}\log\left(\frac{N}{P}\right)d\alpha + \left(\frac{N}{P}\right)^{-\frac{1}{2}} \ll \left(\frac{N}{P}\right)^{-\frac{1}{2}\eta(T)}, \qquad (3.67)$$

onde $\eta(T) = \frac{c_4}{\log T}$. Portanto, por (3.65), (3.66) e (3.67), obtemos

$$\sum_{q\le P}\sideset{}{^*}\sum_{\chi\ (mod\ q)}\max_{x\le N}\max_{h\le N}\left(h+\frac{N}{P}\right)^{-1}\left|\sideset{}{^\sharp}\sum_{x-h<p\le x}\chi(p)\log p\right| \ll \left(\frac{N}{P}\right)^{-\frac{1}{2}\eta(T)} + P^3T^{-1}\log^4 PT + P^3N^{-\frac{1}{2}}\log^4 PT. \qquad (3.68)$$

Escolhendo $T = P^5$ e c_7 tais que valem $P^3N^{-\frac{1}{2}}\log^4 P \le P^{-1}$ e $T^{c_{11}} \le \left(\frac{N}{P}\right)^{\frac{1}{2}}$. A expressão à direita de (3.68), em virtude de $\exp(\log^{\frac{1}{2}} N) \le P$, é

$$\ll \exp\left(-\frac{c_4}{10}\frac{\log\frac{N}{P}}{\log P}\right) + P^{-1} \ll \exp\left(-\frac{c_4}{10}\frac{\log N}{\log P}\right) + P^{-1} \ll \exp\left(-c_6\frac{\log N}{\log P}\right).$$

Se há um caráter excepcional de ordem P, repetimos os passos acima com a estimativa (3.17) de Bombieri no lugar da estimativa (3.16) de Gallagher, concluindo que a expressão à esquerda de (3.68) é

$$\ll \exp\left(-c_6\frac{\log N}{\log P}\right)(1-\widetilde{\beta})\log P.$$

Finalizando a demonstração da proposição.

Capítulo 4

Os Arcos Maiores

Na Seção 1.3 obtemos estimativas superiores para $R_2(n)$, para quase todo $n \leq X$. Neste capítulo, nos concentramos em $R_1(n)$, na tentativa de escrevê-lo como a soma de um termo principal mais um termo de erro que dependem explicitamente de n e X. Permitindo-nos assim, estabelecer cotas inferiores para $R_1(n)$, para quase todo $n \leq X$. A partir das estimativas obtidas, seguiremos as ideias contidas na Seção 1.2 para concluir, na última seção deste capítulo, a prova do Teorema (Montgomery-Vaughan).

Para $\alpha \in \mathfrak{M}(q,a)$, escrevemos $\alpha = \frac{a}{q} + \eta$, com $|\eta| \leq \frac{1}{qQ}$. Sendo $q \leq P$, a desigualdade $p > P$ implica em $(p,q) = 1$. Assim, usando a Ortogonalidade dos Caracteres (Proposição 2.7), temos

$$e(p\alpha) = \varphi(q)^{-1} \sum_{n=1}^{q} \left(\sum_{\chi\ (mod\ q)} \chi(pa)\overline{\chi}(n) e\left(\frac{n}{q}\right) \right) e(p\eta),$$

para todo $p > P$. Mudando a ordem dos somatórios, chegamos a

$$e(p\alpha) = \varphi(q)^{-1} \sum_{\chi\ (mod\ q)} \chi(pa)\tau(\overline{\chi}) e(p\eta).$$

Logo

$$S(\alpha) = \varphi(q)^{-1} \sum_{\chi\ (mod\ q)} \chi(a)\tau(\overline{\chi}) S(\chi,\eta),$$

onde $S(\chi,\eta) := \sum_{P<p\leq X} (\log p)\chi(p)e(p\eta)$. Note que a inocente condição $p > P$ assegura que $S(\chi,\eta) = S(\chi^*,\eta)$. Em geral, esperamos que $S(\chi,\eta)$ seja "pequeno", mas se $\chi = \chi_0$ ou $\chi = \chi_0\widetilde{\chi}$ (ou seja, χ é induzido por $\widetilde{\chi}$), onde χ_0 é o caráter principal módulo q e $\widetilde{\chi}$ o caráter excepcional de ordem P (este último podendo não existir), aproximamos $S(\chi,\eta)$ pelas correspondentes expressões

$$T(\eta) := \sum_{P<n\leq X} e(n\eta) \qquad e \qquad \widetilde{T}(\eta) := -\sum_{P<n\leq X} n^{\widetilde{\beta}-1} e(n\eta).$$

Essas aproximações justificam-se observando as chamadas Fórmulas Explícitas para L-funções (ver Proposição 3.21).

Claro que $\widetilde{T}(\eta)$ é definido se, e somente se, existe o zero excepcional $\widetilde{\beta}$ de ordem P. Escrevemos

$$S(\chi_0,\eta) = T(\eta) + W(\chi_0,\eta)\,, \qquad S(\chi_0\widetilde{\chi},\eta) = \widetilde{T}(\eta) + W(\chi_0\widetilde{\chi},\eta)$$

e

$$S(\chi,\eta) = W(\chi,\eta), \qquad se \qquad \chi \neq \chi_0,\ \chi \neq \chi_0\widetilde{\chi}.$$

Assim, também temos $W(\chi,\eta) = W(\chi^*,\eta)$. Com estas definições e o fato que $\tau(\chi_0) = \mu(q)$ (segue diretamente do Lema 2.16), podemos escrever

$$S(\alpha) = \frac{\mu(q)T(\eta)}{\varphi(q)} + \frac{1}{\varphi(q)} \sum_{\chi\ (mod\ q)} \chi(a)\tau(\overline{\chi}) W(\chi,\eta), \tag{4.1}$$

a menos que haja um caráter excepcional $\widetilde{\chi}$ $(mod\,\widetilde{r})$ de ordem P. Neste caso, se $\widetilde{r}|q$, adicionamos o termo

$$\frac{\widetilde{\chi}(a)\tau(\chi_0\widetilde{\chi})}{\varphi(q)}\widetilde{T}(\eta) \tag{4.2}$$

no lado direito de (4.1). Dividimos agora a nossa discussão sobre o arco maior em dois casos, levando em conta a existência ou não do caráter excepcional.

4.1 Sem caráter excepcional

Assumimos no momento que o caráter excepcional de ordem P não ocorre. Então, por (4.1), temos

$$S(\alpha)^2 = \left(\frac{\mu(q)T(\eta)}{\varphi(q)}\right)^2 + 2\mu(q)\varphi(q)^{-2}\sum_{\chi\ (mod\ q)}\chi(a)\tau(\overline{\chi})T(\eta)W(\chi,\eta) + \tag{4.3}$$
$$+\varphi(q)^{-2}\sum_{\chi,\,\chi'\ (mod\ q)}\chi\chi'(a)\tau(\overline{\chi})\tau(\overline{\chi'})W(\chi,\eta)W(\chi',\eta).$$

Assim,

$$\sum_{a=1}^{q}{}' \int_{\mathfrak{M}(q,a)} S(\alpha)^2e(-n\alpha)d\alpha = \mu(q)^2\varphi(q)^{-2}\sum_{a=1}^{q}{}'\int_{\mathfrak{M}(q,a)} T(\eta)^2e(-n\alpha)d\alpha +$$
$$+2\mu(q)\varphi(q)^{-2}\sum_{\chi\ (mod\ q)}\tau(\overline{\chi})\sum_{a=1}^{q}{}'\chi(a)\int_{\mathfrak{M}(q,a)}T(\eta)W(\chi,\eta)e(-n\alpha)d\alpha +$$
$$+\varphi(q)^{-2}\sum_{\chi,\chi'\ (mod\ q)}\tau(\overline{\chi})\tau(\overline{\chi'})\sum_{a=1}^{q}{}'\chi\chi'(a)\int_{\mathfrak{M}(q,a)}W(\chi,\eta)W(\chi',\eta)e(-n\alpha)d\alpha,$$

para todo $n \leq X$. Fazendo a mudança de variável $\alpha = \dfrac{a}{q} + \eta$ nas integrais acima, vemos que

$$\sum_{a=1}^{q}{}' \int_{\mathfrak{M}(q,a)} S(\alpha)^2e(-n\alpha)d\alpha = \mu(q)^2\varphi(q)^{-2}c_q(-n)\int_{-\frac{1}{qQ}}^{\frac{1}{qQ}}T(\eta)^2e(-n\eta)d\eta +$$
$$+2\mu(q)\varphi(q)^{-2}\sum_{\chi\ (mod\ q)}c_\chi(-n)\tau(\overline{\chi})\int_{-\frac{1}{qQ}}^{\frac{1}{qQ}}T(\eta)W(\chi,\eta)e(-n\eta)d\eta + \tag{4.4}$$
$$+\varphi(q)^{-2}\sum_{\chi,\chi'\ (mod\ q)}c_{\chi\chi'}(-n)\tau(\overline{\chi})\tau(\overline{\chi'})\int_{-\frac{1}{qQ}}^{\frac{1}{qQ}}W(\chi,\eta)W(\chi',\eta)e(-n\eta)d\eta.$$

Portanto, $R_1(n)$ é igual a

$$\sum_{q\leq P}\sum_{a=1}^{q}{}' \int_{\mathfrak{M}(q,a)} S(\alpha)^2e(-n\alpha)d\alpha = \sum_{q\leq P}\mu(q)^2\varphi(q)^{-2}c_q(-n)\int_{-\frac{1}{qQ}}^{\frac{1}{qQ}}T(\eta)^2e(-n\eta)d\eta +$$
$$+2\sum_{q\leq P}\mu(q)\varphi(q)^{-2}\sum_{\chi\ (mod\ q)}c_\chi(-n)\tau(\overline{\chi})\int_{-\frac{1}{qQ}}^{\frac{1}{qQ}}T(\eta)W(\chi,\eta)e(-n\eta)d\eta + \tag{4.5}$$
$$+\sum_{q\leq P}\varphi(q)^{-2}\sum_{\chi,\chi'\ (mod\ q)}c_{\chi\chi'}(-n)\tau(\overline{\chi})\tau(\overline{\chi'})\int_{-\frac{1}{qQ}}^{\frac{1}{qQ}}W(\chi,\eta)W(\chi',\eta)e(-n\eta)d\eta,$$

para todo $n \leq X$.

Aqui encaramos a primeira soma à direita de (4.5) como sendo o termo principal de $R_1(n)$, enquanto as outras como sendo o termo de erro. Vamos estimar este último agora. Suponha que $\chi\ (mod\, q)$ é induzido pelo caráter primitivo $\chi^*\ (mod\, r)$. Defina

$$W(\chi) = \left(\int_{-\frac{1}{rQ}}^{\frac{1}{rQ}} |W(\chi,\eta)|^2 d\eta \right)^{\frac{1}{2}}. \tag{4.6}$$

Note que $W(\chi) = W(\chi^*)$, pois $W(\chi,\eta) = W(\chi^*,\eta)$, então o termo de erro de $R_1(n)$ é limitado por

$$2X^{\frac{1}{2}} \sum_{q\leq P} \mu(q)^2\varphi(q)^{-2} \sum_{\chi\ (mod\, q)} |c_\chi(-n)\tau(\overline{\chi})| W(\chi^*) \ + \sum_{q\leq P} \varphi(q)^{-2} \sum_{\chi,\chi'\ (mod\, q)} |c_{\chi\chi'}(-n)\tau(\overline{\chi})\tau(\overline{\chi'})| W(\chi^*)W(\chi'^*). \tag{4.7}$$

Acima usamos a Desigualdade de Cauchy-Schwarz e o fato que

$$\int_{-\frac{1}{qQ}}^{\frac{1}{qQ}} |T(\eta)|^2 d\eta \leq \int_0^1 |T(\eta)|^2 d\eta = \sum_{P<n\leq X} 1 \leq X. \tag{4.8}$$

Agrupando os termos associados a cada par χ^* e χ'^*, obtemos que (4.7) é

$$\leq 2X^{\frac{1}{2}} \sum_{r\leq P} \sideset{}{^*}\sum_{\chi\ (mod\, r)} W(\chi) \sum_{\substack{q\leq P\\ r|q}} \varphi(q)^{-2} |c_{\chi\chi_0}(-n)\tau(\overline{\chi}\chi_0)| +$$

$$+ \sum_{r,r'\leq P} \sideset{}{^*}\sum_{\substack{\chi\ (mod\, r)\\ \chi'\ (mod\, r')}} W(\chi)W(\chi') \sum_{\substack{q\leq P\\ [r,r']|q}} \varphi(q)^{-2} |c_{\chi\chi'\chi_0}(-n)\tau(\overline{\chi}\chi_0)\tau(\overline{\chi'}\chi_0)|.$$

Pela Proposição 2.19, vemos que o termo de erro é

$$\ll \frac{n}{\varphi(n)} \left(WX^{\frac{1}{2}} + W^2 \right), \tag{4.9}$$

onde $W := \sum_{r\leq P} \sideset{}{^*}\sum_{\chi\ (mod\, r)} W(\chi)$.

Consideramos agora o primeiro termo à direita de (4.5). A integral que o acompanha satisfaz a limitação (4.8), no entanto precisamos de uma estimativa mais precisa. Para isso iniciamos estimando $T(\eta)$.

$$\begin{aligned} T(\eta) = \sum_{P<n\leq X} e(n\eta) = \sum_{[P]<n\leq [X]} e(n\eta) \ &= \ e(([P]+1)\eta) \sum_{n\leq [X]-[P]-1} e(n\eta) \\ &= \ e\left(\left([P]+1\right)\eta\right) \frac{e\left(\left([X]-[P]\right)\eta\right)-1}{e(\eta)-1} \\ &= \ e\left(\left(\frac{[X]+[P]+1}{2}\right)\eta\right) \frac{\sin\left(\pi([X]-[P])\eta\right)}{\sin \pi\eta}, \end{aligned}$$

para todo $\eta \notin \mathbb{Z}$. Usando a desigualdade $\sin \pi\eta \geq 2\eta$, válida para $0 \leq \eta \leq \frac{1}{2}$, e o fato que $T(\eta)$ e $T(\|\eta\|)$ possuem o mesmo módulo, chegamos a

$$T(\eta) \ll \min\{X-P, \|\eta\|^{-1}\} \ \text{ para todo } \eta \in \mathbb{R} \tag{4.10}$$

e, portanto,

$$\int_{\frac{1}{qQ}}^{\frac{1}{2}} |T(\eta)|^2 d\eta \ll \int_{\frac{1}{qQ}}^{\frac{1}{2}} \eta^{-2} d\eta \ll qQ. \tag{4.11}$$

Decorre daí que a integral em discussão é igual a

$$\begin{aligned} \int_{-\frac{1}{2}}^{\frac{1}{2}} T(\eta)^2 e(-n\eta) d\eta - \int_{\frac{1}{qQ}}^{\frac{1}{2}} T(\eta)^2 e(-n\eta) d\eta - \int_{-\frac{1}{2}}^{-\frac{1}{qQ}} T(\eta)^2 e(-n\eta) d\eta \ &= \ \int_0^1 T(\eta)^2 e(-n\eta) d\eta \ + \ O(qQ) \\ &= \ n \ + \ O(qQ), \end{aligned}$$

para $n \leq X$. Na última passagem acima usamos:

$$\int_0^1 T(\eta)^2 e(-n\eta)d\eta = \begin{cases} n - 2[P] - 1, & \text{se } 2P < n \leq X; \\ 0, & \text{se } n \leq 2P. \end{cases}$$

Assim, o termo principal de $R_1(n)$ é dado por

$$\sum_{q \leq P} \mu(q)^2 \varphi(q)^{-2} c_q(-n)(n + O(qQ)). \tag{4.12}$$

Pelo Lema 1.6 e (2.4), o termo de erro de (4.12) tem ordem

$$\begin{aligned} Q \sum_{q \leq P} q\varphi(q)^{-1} \varphi\left(\frac{q}{(q,n)}\right)^{-1} &\overset{(1.2)}{\ll} Q \sum_{q \leq P} (q,n)\varphi((q,n))^{-1} \left(\frac{q}{(q,n)} \varphi\left(\frac{q}{(q,n)}\right)^{-2}\right) \\ &\ll Q \sum_{d|n} d\varphi(d)^{-1} \sum_{r \leq P} r\varphi(r)^{-2} \\ &\overset{1.6}{\ll} Qn\varphi(n)^{-1} d(n) \log^2 P. \end{aligned} \tag{4.13}$$

O termo principal de (4.12) pode ser escrito como $n \sum_{q=1}^{\infty} \mu(q)^2 \varphi(q)^{-2} c_q(-n)$, com um erro de ordem

$$\begin{aligned} \left| n \sum_{q > P} \mu(q)^2 \varphi(q)^{-2} c_q(-n) \right| &\overset{(2.4)}{\ll} n \sum_{q > P} \varphi(q)^{-1} \varphi\left(\frac{q}{(q,n)}\right)^{-1} \\ &\overset{(1.2)}{\ll} n \sum_{q > P} \varphi((q,n))^{-1} \varphi\left(\frac{q}{(q,n)}\right)^{-2} \\ &\ll n \sum_{d|n} \varphi(d)^{-1} \sum_{r > \frac{P}{d}} \varphi(r)^{-2} \\ &\overset{1.6\,\textbf{(iii)}}{\ll} nP^{-1} \log P \sum_{d|n} d\varphi(d)^{-1} \\ &\overset{1.6\,\textbf{(i)}}{\ll} nP^{-1} d(n) n\varphi(n)^{-1} \log P, \end{aligned} \tag{4.14}$$

Das estimativas (1.3) e (1.4), vemos que

$$Qn\varphi(n)^{-1} d(n) \log^2 P \quad \text{e} \quad nP^{-1} d(n) n\varphi(n)^{-1} \log P$$

são $\ll X^{1+\delta} P^{-1}$, para todo $n \leq X$.

Então o primeiro termo à direita de (4.5) é igual a

$$\mathfrak{S}(n)\, n + O(X^{1+\delta} P^{-1}), \tag{4.15}$$

onde $\mathfrak{S}(n)$ é a série singular

$$\mathfrak{S}(n) := \sum_{q=1}^{\infty} \mu(q)^2 \varphi(q)^{-2} c_q(-n) = \prod_{p \nmid n} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{p|n} \left(1 + \frac{1}{p-1}\right). \tag{4.16}$$

Na última igualdade utilizamos a Proposição 1.5 e (2.4). Combinando (4.5), (4.9) e (4.15) chegamos a

$$R_1(n) = \mathfrak{S}(n) n + O\left(X^{1+\delta} P^{-1} + \frac{n}{\varphi(n)} \left(WX^{\frac{1}{2}} + W^2\right)\right), \tag{4.17}$$

para $n \leq X$, sob a condição de que o caráter excepcional de ordem P não ocorre.

4.2 Com caráter excepcional

Suponhamos agora que o termo excepcional (4.2) ocorre. Nesta seção procedemos para determinar o efeito que este termo exerce sobre (4.17). No lado direito de (4.3) devemos acrescentar

$$\begin{aligned}\tau(\chi_0\widetilde{\chi})^2\varphi(q)^{-2}\widetilde{T}(\eta)^2 \;+\; 2\mu(q)\widetilde{\chi}(a)\tau(\chi_0\widetilde{\chi})\varphi(q)^{-2}T(\eta)\widetilde{T}(\eta) +\\ + 2\varphi(q)^{-2}\sum_{\chi\ (mod\ q)}\chi\widetilde{\chi}(a)\tau(\overline{\chi})\tau(\chi_0\widetilde{\chi})W(\chi,\eta)\widetilde{T}(\eta).\end{aligned} \tag{4.18}$$

Portanto, o lado direito de (4.5) deve ser acrescido com o seguinte termo

$$\begin{aligned}&\sum_{\substack{q\le P\\ \widetilde{r}|q}}\tau(\chi_0\widetilde{\chi})^2\varphi(q)^{-2}c_q(-n)\int_{-\frac{1}{qQ}}^{\frac{1}{qQ}}\widetilde{T}(\eta)^2e(-n\eta)d\eta \;+\; 2\sum_{\substack{q\le P\\ \widetilde{r}|q}}\mu(q)c_{\chi_0\widetilde{\chi}}(-n)\tau(\chi_0\widetilde{\chi})\varphi(q)^{-2}\int_{-\frac{1}{qQ}}^{\frac{1}{qQ}}T(\eta)\widetilde{T}(\eta)e(-n\eta)d\eta +\\ &+ 2\sum_{\substack{q\le P\\ \widetilde{r}|q}}\varphi(q)^{-2}\sum_{\chi\ (mod\ q)}c_{\chi\widetilde{\chi}}(-n)\tau(\overline{\chi})\tau(\chi_0\widetilde{\chi})\int_{-\frac{1}{qQ}}^{\frac{1}{qQ}}W(\chi,\eta)\widetilde{T}(\eta)e(-n\eta)d\eta.\end{aligned} \tag{4.19}$$

Tratamos o último termo de (4.19) da mesma forma que tratamos o segundo e terceiro termo à direita de (4.5). A contribuição deste termo não é maior que

$$2X^{\frac{1}{2}}\sum_{\substack{q\le P\\ \widetilde{r}|q}}\varphi(q)^{-2}\sum_{\chi\ (mod\ q)}|c_{\chi\widetilde{\chi}}(-n)\tau(\overline{\chi})\tau(\chi_0\widetilde{\chi})|W(\chi^*)\,, \tag{4.20}$$

pois

$$\int_{-\frac{1}{qQ}}^{\frac{1}{qQ}}|\widetilde{T}(\eta)|^2d\eta \le \int_0^1|\widetilde{T}(\eta)|^2d\eta = \sum_{P<n\le X}n^{\widetilde{\beta}-1}\le X.$$

Agrupando os termos correspondentes a cada χ^*, obtemos que (4.20) é

$$\le 2X^{\frac{1}{2}}\sum_{r\le P}\ \sideset{}{^*}\sum_{\chi\ (mod\ r)}W(\chi)\sum_{\substack{q\le P\\ [r,\widetilde{r}]|q}}\varphi(q)^{-2}|c_{\chi\widetilde{\chi}\chi_0}(-n)\tau(\chi_0\overline{\chi})\tau(\chi_0\widetilde{\chi})|,$$

aplicando a Proposição 2.19 como antes, concluímos que o último termo de (4.19) é

$$\ll \frac{n}{\varphi(n)}WX^{\frac{1}{2}},$$

o qual é absorvido por (4.9).

Investiguemos agora os dois primeiros termos em (4.19). Por (4.10) e somas parciais, vemos que

$$\widetilde{T}(\eta) = \int_1^X t^{\widetilde{\beta}-1}d\left(\sum_{P<n\le t}e(n\eta)\right) = X^{\widetilde{\beta}-1}\sum_{P<n\le X}e(n\eta) - (\widetilde{\beta}-1)\int_1^X t^{\widetilde{\beta}-2}\sum_{P<n\le t}e(n\eta)dt \ll \min(X-P,\|\eta\|).$$

Esta estimativa, a Desigualdade de Cauchy-Schwarz e (4.11) implicam

$$\int_{\frac{1}{qQ}}^{\frac{1}{2}}|\widetilde{T}(\eta)|^2 \ll qQ \qquad e \qquad \int_{\frac{1}{qQ}}^{\frac{1}{2}}|T(\eta)\widetilde{T}(\eta)| \ll qQ.$$

Portanto, como na seção anterior, podemos escrever as integrais dos dois primeiros termos de (4.19) como $\widetilde{I}(n)+O(qQ)$ e $\widetilde{J}(n)+O(qQ)$, onde

$$\widetilde{I}(n) := \int_0^1\widetilde{T}(\eta)^2e(-n\eta)d\eta \qquad e \qquad \widetilde{J}(n) := \int_0^1 T(\eta)\widetilde{T}(\eta)e(-n\eta)d\eta.$$

Pela Identidade de Parseval e a Desigualdade de Cauchy-Schwarz deduzimos que

$$\widetilde{I}(n) \ll X \qquad e \qquad \widetilde{J}(n) \ll X. \tag{4.21}$$

No final desta seção estimamos $\widetilde{I}(n)$ com mais cuidado. Logo devemos introduzir em (4.12) o seguinte termo

$$\sum_{\substack{q\leq P\\ \widetilde{r}|q}} \varphi(q)^{-2}\tau(\widetilde{\chi}\chi_0)^2 c_q(-n)\left(\widetilde{I}(n)+O(qQ)\right)+2\sum_{\substack{q\leq P\\ \widetilde{r}|q}}\mu(q)\varphi(q)^{-2}\tau(\widetilde{\chi}\chi_0)c_{\widetilde{\chi}\chi_0}(-n)\left(\widetilde{J}(n)+O(qQ)\right). \tag{4.22}$$

Da Proposição 2.18 e do Lema 2.15, as somas de Gauss correspondentes a q em (4.22) obedecem as seguintes limitações:

$$|\tau(\widetilde{\chi}\chi_0)| \leq \widetilde{r}^{\frac{1}{2}} \quad e \quad |c_{\widetilde{\chi}\chi_0}(-n)| \leq \widetilde{r}^{\frac{1}{2}}\frac{\varphi(q)}{\varphi\left(\frac{q}{(q,n)}\right)}, \tag{4.23}$$

podemos então concluir que os termos de erro de (4.22) têm ordem

$$\begin{aligned}
\widetilde{r}Q\sum_{\substack{q\leq P\\ \widetilde{r}|q}} q\varphi(q)^{-1}\varphi\left(\frac{q}{(n,q)}\right)^{-1} &\ll \widetilde{r}^2\varphi(\widetilde{r})^{-1}\varphi\left(\frac{\widetilde{r}}{(n,\widetilde{r})}\right)^{-1} Q\sum_{r\leq\frac{P}{\widetilde{r}}} r\varphi(r)^{-1}\varphi\left(\frac{r}{(n,r)}\right)^{-1}\\
&\overset{(4.13)}{\ll} \widetilde{r}^2\varphi(\widetilde{r})^{-1}\varphi\left(\frac{\widetilde{r}}{(n,\widetilde{r})}\right)^{-1} Qn\varphi(n)^{-1}d(n)\log^2 P\\
&\overset{(1.3)\,(1.4)}{\ll} X^{1+\delta}P^{-1}(n,\widetilde{r}),
\end{aligned} \tag{4.24}$$

para todo $n \leq X$.

Agora estendemos as somas dos termos principais de (4.22) para incluir todos os $q \geq 1$, com $\widetilde{r}|q$. Isto introduz mais dois termos de erro, os quais, em vista das desigualdades (4.23) e (4.21), têm ordem

$$\begin{aligned}
X\widetilde{r}\sum_{\substack{q>P\\ \widetilde{r}|q}} \varphi(q)^{-1}\varphi\left(\frac{q}{(q,n)}\right)^{-1} &\ll \widetilde{r}\varphi(\widetilde{r})^{-1}\varphi\left(\frac{\widetilde{r}}{(n,\widetilde{r})}\right)^{-1} X\sum_{r>\frac{P}{\widetilde{r}}} \varphi(r)^{-1}\varphi\left(\frac{r}{(n,r)}\right)^{-1}\\
&\overset{(4.14)}{\ll} \widetilde{r}^2\varphi(\widetilde{r})^{-1}\varphi\left(\frac{\widetilde{r}}{(n,\widetilde{r})}\right)^{-1} XP^{-1}d(n)n\varphi(n)^{-1}\log P\\
&\overset{(1.3)\,(1.4)}{\ll} X^{1+\delta}P^{-1}(n,\widetilde{r}).
\end{aligned} \tag{4.25}$$

A primeira e a segunda soma de (4.22), estendidas ao infinito, são respectivamente

$$\widetilde{\mathfrak{S}}(n) := \sum_{\substack{q=1\\ \widetilde{r}|q}}^{\infty} \tau(\widetilde{\chi}\chi_0)^2 c_q(-n)\varphi(q)^{-2} \;\text{ e }\; \sum_{\substack{q=1\\ \widetilde{r}|q}}^{\infty}\mu(q)\tau(\widetilde{\chi}\chi_0)c_{\widetilde{\chi}\chi_0}(-n)\varphi(q)^{-2}.$$

Como em (4.16), vamos escrever as séries acima como um produtório. Sejam $q \geq 1$ tal que $\widetilde{r}|q$ e χ_0 o caráter principal módulo q. Pelo Lema 2.16, temos

$$\tau(\widetilde{\chi}\chi_0) = \mu\left(\frac{q}{\widetilde{r}}\right)\widetilde{\chi}\left(\frac{q}{\widetilde{r}}\right)\tau(\widetilde{\chi}),$$

usando (2.2) do Lema 2.15 na última igualdade, obtemos

$$\tau(\widetilde{\chi}\chi_0)^2 = \widetilde{\chi}(-1)\widetilde{r}\mu\left(\frac{q}{\widetilde{r}}\right)^2\widetilde{\chi}\left(\frac{q}{\widetilde{r}}\right)^2. \tag{4.26}$$

Assim, escrevendo $q = \widetilde{r}t$, as relações (2.4) e (4.26) implicam

$$\begin{aligned}
\tau(\widetilde{\chi}\chi_0)^2 c_q(-n)\varphi(q)^{-2} &= \widetilde{\chi}(-1)\widetilde{r}\mu\left(\frac{q}{\widetilde{r}}\right)^2\mu\left(\frac{q}{(q,n)}\right)\widetilde{\chi}\left(\frac{q}{\widetilde{r}}\right)^2\varphi(q)^{-1}\varphi\left(\frac{q}{(q,n)}\right)^{-1}\\
&= \left(\widetilde{\chi}(-1)\mu\left(\frac{\widetilde{r}}{(\widetilde{r},n)}\right)\widetilde{r}\varphi(\widetilde{r})^{-1}\varphi\left(\frac{\widetilde{r}}{(\widetilde{r},n)}\right)^{-1}\right)\left(\widetilde{\chi}(t)^2\mu(t)^2\mu\left(\frac{t}{(t,n)}\right)\varphi(t)^{-1}\varphi\left(\frac{t}{(t,n)}\right)^{-1}\right),
\end{aligned}$$

portanto

$$\widetilde{\mathfrak{S}}(n) = \widetilde{\chi}(-1)\mu\left(\frac{\widetilde{r}}{(\widetilde{r},n)}\right)\widetilde{r}\varphi(\widetilde{r})^{-1}\varphi\left(\frac{\widetilde{r}}{(\widetilde{r},n)}\right)^{-1}\sum_{t=1}^{\infty}\widetilde{\chi}(t)^2\mu(t)^2\mu\left(\frac{t}{(t,n)}\right)\varphi(t)^{-1}\varphi\left(\frac{t}{(t,n)}\right)^{-1}.$$

Aplicando a Proposição 1.5 na última soma, chegamos a

$$\begin{aligned}
\widetilde{\mathfrak{S}}(n) &= \sum_{\substack{q=1\\ \widetilde{r}\mid q}}^{\infty} \tau(\widetilde{\chi}\chi_0)^2 c_q(-n)\varphi(q)^{-2}\\
&= \widetilde{\chi}(-1)\mu\left(\frac{\widetilde{r}}{(\widetilde{r},n)}\right)\widetilde{r}\varphi(\widetilde{r})^{-1}\varphi\left(\frac{\widetilde{r}}{(\widetilde{r},n)}\right)^{-1}\prod_{\substack{p\nmid\widetilde{r}\\ p\nmid n}}\left(1-\frac{1}{(p-1)^2}\right)\prod_{\substack{p\nmid\widetilde{r}\\ p\mid n}}\left(1+\frac{1}{p-1}\right).
\end{aligned}\tag{4.27}$$

Usando a Proposição 2.18 em $c_{\widetilde{\chi}\chi_0}(-n)$ e procedendo como acima, obtemos

$$\begin{aligned}
\sum_{\substack{q=1\\ \widetilde{r}\mid q}}^{\infty} \mu(q)\tau(\widetilde{\chi}\chi_0)c_{\widetilde{\chi}\chi_0}(-n)\varphi(q)^{-2} &= \mu(\widetilde{r})\widetilde{\chi}(n)\widetilde{r}\varphi(\widetilde{r})^{-2}\prod_{\substack{p\nmid\widetilde{r}\\ p\nmid n}}\left(1-\frac{1}{(p-1)^2}\right)\prod_{\substack{p\nmid\widetilde{r}\\ p\mid n}}\left(1+\frac{1}{p-1}\right)\\
&\overset{(1.2)}{\ll} \widetilde{\chi}(n)^2\widetilde{r}\varphi(\widetilde{r})^{-2}n\varphi(n)^{-1}.
\end{aligned}\tag{4.28}$$

Reunindo nossas estimativas (4.17) - (4.28), encontramos que se o termo excepcional ocorre, então ao invés de (4.17) teremos

$$R_1(n) = \mathfrak{S}(n)n + \widetilde{\mathfrak{S}}(n)\widetilde{I}(n) + O\left(\frac{\widetilde{\chi}(n)^2\widetilde{r}nX}{\varphi(\widetilde{r})^2\varphi(n)} + X^{1+\delta}P^{-1}(n,\widetilde{r}) + \frac{n}{\varphi(n)}\left(WX^{\frac{1}{2}}+W^2\right)\right), \tag{4.29}$$

para $n \le X$.

Para completar nossa descrição do termo principal de $R_1(n)$, daremos uma estimativa superior para $\widetilde{I}(n)$ mais refinada que (4.21). Claramente

$$\widetilde{I}(n) = \sum_{P<k<n-P}(k(n-k))^{\widetilde{\beta}-1} \le n.n^{\widetilde{\beta}-1} = n^{\widetilde{\beta}},$$

mas

$$\begin{aligned}
n - n^{\widetilde{\beta}} = \int_{\widetilde{\beta}}^{1} n^u(\log n)du &\ge \int_{\max\left(\widetilde{\beta},1-\frac{1}{\log X}\right)}^{1} n^u(\log n)du\\
&\ge \left(1-\max\left(\widetilde{\beta},1-\frac{1}{\log X}\right)\right)n\exp\left(-\frac{\log n}{\log X}\right)\log n\\
&\gg \begin{cases} (1-\widetilde{\beta})n\log n, & \text{se } \widetilde{\beta} \ge 1-\frac{1}{\log X};\\[2mm] n\dfrac{\log n}{\log X}, & \text{se } \widetilde{\beta} < 1-\frac{1}{\log X}.\end{cases}
\end{aligned}$$

Então, por (3.11), $n - n^{\widetilde{\beta}} > c_{17}\left(1-\widetilde{\beta}\right)n\log P$, para $\frac{1}{2}X < n \le X$. Assim

$$\widetilde{I}(n) \le n - c_{17}\left(1-\widetilde{\beta}\right)n\log P, \tag{4.30}$$

para todo $\frac{1}{2}X < n \le X$.

4.3 O termo de erro do arco maior

Para finalizarmos a discussão sobre o termo de erro de $R_1(n)$, precisaremos do seguinte resultado, o qual é uma consequência da Proposição 3.13.

Lema 4.1. *Sejam $u_1, u_2, \ldots, u_N$ números complexos arbitrários. Então, para todo $\theta > 0$, temos*

$$\int_{-\theta}^{\theta}\left|\sum_{n\le N}u_n e(n\eta)\right|^2 d\eta \ll \int_{-\infty}^{\infty}\left|\theta\sum_{x-(2\theta)^{-1}<n\le x}u_n\right|^2 dx.$$

Prova: Na Proposição 3.13 tome os v percorrendo a sequência $\{1, 2, \ldots, N\}$, $c(n) = u_n$ para $n \leq N$, $T = \theta$ e $\epsilon = \frac{1}{2}$.

Estimamos agora

$$W = \sum_{q \leq P} \sum_{\chi \, (mod \, q)}^{*} W(\chi),$$

com $W(\chi)$ definido em (4.6). Seja χ um caráter primitivo módulo q, com $q \leq P$, pelo Lema 4.1 vemos que

$$W(\chi) \ll \left(\int_{-\infty}^{\infty} \left| \frac{1}{qQ} \sum_{\substack{P < p \leq X \\ x - \frac{1}{2}qQ < p \leq x}}^{\sharp} \chi(p) \log p \right|^2 dx \right)^{\frac{1}{2}},$$

observe que o suporte do integrando está contido no intervalo $[P, 2X]$, logo

$$W(\chi) \ll \left(\int_{P}^{2X} \left| \frac{1}{qQ} \sum_{\substack{P < p \leq X \\ x - \frac{1}{2}qQ < p \leq x}}^{\sharp} \chi(p) \log p \right|^2 dx \right)^{\frac{1}{2}}. \tag{4.31}$$

Provamos agora que o integrando de (4.31) é

$$\ll \left(\max_{x \leq X} \max_{h \leq X} \left(h + \frac{X}{P} \right)^{-1} \left| \sum_{x-h<p\leq x}^{\sharp} \chi(p) \log p \right| \right)^2, \tag{4.32}$$

para isso, observe que fixado $x \in [P, 2X]$, temos:

- Se $P + \frac{1}{2}qQ < x \leq X$, defina $h_0 = \left[\frac{1}{2}qQ\right]$. Agora se $P < x \leq P + \frac{1}{2}qQ$, defina $h_0 = [x - P]$. Então $\frac{1}{qQ} \ll \left(h_0 + \frac{X}{P}\right)^{-1}$ (lembre-se que $\frac{X}{P} = Q$) e

$$\frac{1}{qQ} \sum_{\substack{P < p \leq X \\ x - \frac{1}{2}qQ < p \leq x}}^{\sharp} \chi(p) \log p \ll \max_{0 \leq a \leq 1} \left((h_0 + a) + \frac{X}{P} \right)^{-1} \left| \sum_{x-(h_0+a)<p\leq x}^{\sharp} \chi(p) \log p \right|;$$

- Se $X < x \leq 2X$, com $x - \frac{1}{2}qQ \leq X$ (em caso contrário a estimativa (4.32) é trivial), definimos $h_0 = [X - x + \frac{1}{2}qQ]$, então $\frac{1}{qQ} \ll \left(h_0 + \frac{X}{P}\right)^{-1}$ e

$$\frac{1}{qQ} \sum_{\substack{P < p \leq X \\ x - \frac{1}{2}qQ < p \leq x}}^{\sharp} \chi(p) \log p \ll \max_{0 \leq a \leq 1} \left((h_0 + a) + \frac{X}{P} \right)^{-1} \left| \sum_{X-(h_0+a)<p\leq X}^{\sharp} \chi(p) \log p \right|,$$

portanto

$$W(\chi) \ll X^{\frac{1}{2}} \max_{x \leq X} \max_{h \leq X} \left(h + \frac{X}{P} \right)^{-1} \left| \sum_{x-h<p\leq x}^{\sharp} \chi(p) \log p \right|,$$

logo

$$W \ll X^{\frac{1}{2}} \sum_{q \leq P} \sum_{\chi \, (mod \, q)}^{*} \max_{x \leq X} \max_{h \leq X} \left(h + \frac{X}{P} \right)^{-1} \left| \sum_{x-h<p\leq x}^{\sharp} \chi(p) \log p \right|. \tag{4.33}$$

Usando a Proposição 3.8 em (4.33) com $N = X$ e $P = X^{6\delta}$, onde $0 < \delta \leq \frac{c_7}{6}$, chegamos a

$$W \ll X^{\frac{1}{2}} \exp\left(-c_6 \frac{\log X}{\log P} \right), \tag{4.34}$$

na ausência do caráter excepcional de ordem P. Se o caráter excepcional existir, então

$$W \ll X^{\frac{1}{2}} \left(1 - \widetilde{\beta}\right) \exp\left(-c_6 \frac{\log X}{\log P} \right) \log P. \tag{4.35}$$

4.4 Demonstração do Teorema (Montgomery-Vaughan)

Recordando que $E(X)$ representa a quantidade dos números pares não excedendo X que não podem ser escritos como soma de dois primos, demonstraremos nesta seção o principal resultado desta dissertação, que consiste em:

Teorema (Montgomery-Vaughan). *Existe uma constante positiva δ (efetivamente computável) tal que para todo X suficientemente grande, temos*

$$E(X) < X^{1-\delta}.$$

Prova: Observamos na Seção 1.2 que $n \leq X$ é soma de dois primos se $R(n) > 0$, mas $R(n) \geq R_1(n) - |R_2(n)|$, então n é representável se

$$R_1(n) > |R_2(n)|.$$

Provaremos que esta desigualdade vale para todo n par, $\frac{1}{2}X < n \leq X$, com exceção de no máximo

$$\ll XP^{-\frac{1}{3}} \log^9 X = X^{1-2\delta} \log^9 X \tag{4.36}$$

valores de n, $\frac{1}{2}X < n \leq X$. Isto é suficiente para provar o Teorema (Montgomery-Vaughan), pois $(2, X] \subset \bigcup_{j=0}^{\left[\frac{\log X}{\log 2}\right]} \left(\frac{X}{2^{j+1}}, \frac{X}{2^j}\right]$, logo

$$E(X) \ll \sum_{j=0}^{\left[\frac{\log X}{\log 2}\right]} \left(\frac{X}{2^j}\right)^{1-2\delta} \log^9 X \ll X^{1-2\delta} \log^9 X \sum_{j=0}^{\infty} \frac{1}{2^{j(1-2\delta)}} \ll X^{1-2\delta} \log^9 X.$$

Da Proposição 1.12, sabemos que o número de $n \leq X$ para os quais $|R_2(n)| > XP^{-\frac{1}{3}}$ é no máximo $\ll XP^{-\frac{1}{3}} \log^9 X$, assim podemos descartar tais n, em vista de (4.36), sendo que aos n restantes vale $|R_2(n)| \leq XP^{-\frac{1}{3}}$. Demonstraremos agora que

$$R_1(n) > XP^{-\frac{1}{3}}, \tag{4.37}$$

para n par, $\frac{1}{2}X < n \leq X$, com exceção de no máximo $\ll XP^{-\frac{1}{3}}$ valores de n. Isto é suficiente para completar a prova, pois os valores de n para os quais a desigualdade (4.37) não é satisfeita podem ser absorvidos em (4.36).

Suponhamos primeiro que não há caráter excepcional, então de (4.17) e (4.34) segue-se que

$$R_1(n) = \mathfrak{S}(n)n + O\left(n\varphi(n)^{-1} X \exp\left(-c_{18}\delta^{-1}\right)\right),$$

para $n \leq X$. Agora, se $n \leq X$ for par, por (4.16), temos

$$\mathfrak{S}(n) \geq \prod_{p>2} \left(1 - \frac{1}{(p-1)^2}\right) \prod_{p|n} \left(1 + \frac{1}{p-1}\right) \gg n\varphi(n)^{-1}. \tag{4.38}$$

Assim, supondo δ suficientemente pequeno, chegamos a

$$R_1(n) \gg n\varphi(n)^{-1} X \gg X,$$

para n par, $\frac{1}{2}X < n \leq X$. Isto nos dá (4.37) sem exceções.

Se o caráter excepcional existir, usamos (4.29) e (4.35) para concluir que

$$R_1(n) = \mathfrak{S}(n)n + \widetilde{\mathfrak{S}}(n)\widetilde{I}(n) + O\left(\frac{\widetilde{\chi}(n)^2 \widetilde{r} n X}{\varphi(\widetilde{r})^2 \varphi(n)} + X^{1+\delta} P^{-1}(n, \widetilde{r}) + n\varphi(n)^{-1} X (1 - \widetilde{\beta}) \exp\left(-c_{18}\delta^{-1}\right) \log P\right). \tag{4.39}$$

Seja n par, $\frac{1}{2}X < n \leq X$, satisfazendo $(n, \widetilde{r}) = 1$. Então (4.27) implica

$$\widetilde{\mathfrak{S}}(n) \ll n\varphi(n)^{-1} \widetilde{r} \varphi(\widetilde{r})^{-2}.$$

Das desigualdades (3.11) obtemos $\widetilde{r} \gg \log P$. Esta última estimativa junto com (1.3) nos permite concluir que

$$n\varphi(n)^{-1} \widetilde{r} \varphi(\widetilde{r})^{-2} = o(1), \quad \text{quando } X \longrightarrow \infty.$$

Em particular, $\widetilde{\mathfrak{S}}(n) = o(1)$, quando $X \longrightarrow \infty$. Assim, (4.38), (4.39) e o fato de $\widetilde{I}(n) \leq X$ implicam $R_1(n) \gg n\varphi(n)^{-1}X \gg X$, para todo n par no intervalo $\left(\frac{1}{2}X, X\right]$, sob a condição $(n, \widetilde{r}) = 1$.

Seja n par, $\frac{1}{2}X < n \leq X$, satisfazendo $(n, \widetilde{r}) > 1$. Então o primeiro termo de erro de (4.39) é zero, mas agora o segundo termo de erro pode ser grande. Para solucionar este problema descartamos os n pares, para os quais $(n, \widetilde{r}) > P^{\frac{1}{2}}$. Desse modo, aos n restantes temos

$$X^{1+\delta}P^{-1}(n, \widetilde{r}) \ll X^{1+\delta}P^{-\frac{1}{2}} \ll XP^{-\frac{1}{3}}, \tag{4.40}$$

além disso, o número de termos descartados tem ordem

$$\sum_{\substack{d|\widetilde{r} \\ d>P^{\frac{1}{2}}}} \sum_{\substack{n\leq X \\ d|n}} 1 \ll \sum_{\substack{d|\widetilde{r} \\ d>P^{\frac{1}{2}}}} \frac{X}{d} \ll XP^{-\frac{1}{2}} \sum_{d|\widetilde{r}} 1 \overset{(1.4)}{\ll} XP^{-\frac{1}{3}},$$

o qual é admissível em vista de (4.36). Portanto nos resta tratar os n pares, $\frac{1}{2}X < n \leq X$, satisfazendo $1 < (n, \widetilde{r}) \leq P^{\frac{1}{2}}$. Para estes, (4.39) e (4.40) implicam

$$R_1(n) = \mathfrak{S}(n)n + \widetilde{\mathfrak{S}}(n)\widetilde{I}(n) + O\left(XP^{-\frac{1}{3}} + n\varphi(n)^{-1}(1-\widetilde{\beta})X\exp\left(-c_{18}\delta^{-1}\right)\log P\right). \tag{4.41}$$

Consideramos agora $\widetilde{\mathfrak{S}}(n)$. Repare que

$$\begin{aligned}
\left|\widetilde{\mathfrak{S}}(n)\right| \quad &\overset{(4.16)\,(4.27)}{\leq} \quad \mathfrak{S}(n)\widetilde{r}\varphi(\widetilde{r})^{-1}\varphi\left(\frac{\widetilde{r}}{(\widetilde{r}, n)}\right)^{-1} \prod_{\substack{p|\widetilde{r} \\ p\nmid n}} \left(1 - \frac{1}{(p-1)^2}\right)^{-1} \prod_{\substack{p|\widetilde{r} \\ p|n}} \left(1 + \frac{1}{p-1}\right)^{-1} \\
&\overset{(1.2)}{\leq} \quad \mathfrak{S}(n)\varphi\left(\frac{\widetilde{r}}{(\widetilde{r}, n)}\right)^{-1} \prod_{\substack{p|\widetilde{r} \\ p\nmid n}} \left(1 - \frac{1}{p-1}\right)^{-1} \\
&= \quad \mathfrak{S}(n) \prod_{\substack{p|\widetilde{r} \\ p\nmid n}} (p-2)^{-1}\, \varphi\left(\frac{\widetilde{r}}{(\widetilde{r}, n)}\right)^{-1} \prod_{\substack{p|\widetilde{r} \\ p\nmid n}} (p-1).
\end{aligned} \tag{4.42}$$

Agora, pelo Lema 2.15 sabemos que $\widetilde{r}/(4, \widetilde{r})$ é livre de quadrados, logo podemos escrever (4.42) como

$$|\widetilde{\mathfrak{S}}(n)| \leq \mathfrak{S}(n) \prod_{\substack{p|\widetilde{r} \\ p\nmid n \\ p>3}} (p-2)^{-1}. \tag{4.43}$$

Se o produto em (4.43) é não vazio, temos $|\widetilde{\mathfrak{S}}(n)| \leq \frac{1}{3}\mathfrak{S}(n)$. Assim, (4.38), (4.41) e o fato de $\widetilde{I}(n) \leq X$ implicam

$$R_1(n) \gg n\varphi(n)^{-1}X \gg X,$$

para n par, $\frac{1}{2}X < n \leq X$. Por outro lado, se o produto é vazio, o fato de $\widetilde{r}/(4, \widetilde{r})$ ser livre de quadrados implica $(n, \widetilde{r}) \geq \frac{1}{24}\widetilde{r}$. Mas os n sob consideração satisfazem $1 < (n, \widetilde{r}) \leq P^{\frac{1}{2}}$, assim o presente caso aparece somente se

$$\widetilde{r} \ll P^{\frac{1}{2}}. \tag{4.44}$$

Portanto, de (4.30), (4.38) e (4.43) deduzimos que

$$\mathfrak{S}(n)n + \widetilde{\mathfrak{S}}(n)\widetilde{I}(n) \geq \mathfrak{S}(n)\left(n - \widetilde{I}(n)\right) \geq c_{19}n\varphi(n)^{-1}(1-\widetilde{\beta})X\log P,$$

para n par, $\frac{1}{2}X < n \leq X$. O último termo de erro em (4.41) é menor que a metade deste tamanho se δ for suficientemente pequeno, dessa forma

$$R_1(n) \geq c_{20}n\varphi(n)^{-1}(1-\widetilde{\beta})X\log P - c_{21}XP^{-\frac{1}{3}},$$

porém

$$1 - \widetilde{\beta} \overset{(3.11)}{\gg} \widetilde{r}^{-\frac{1}{2}}\log^{-2}\widetilde{r} \overset{(4.44)}{\gg} P^{-\frac{1}{4}}\log^{-2}P,$$

portanto

$$R_1(n) \gg XP^{-\frac{1}{4}}\log^{-1}P > XP^{-\frac{1}{3}},$$

como desejado.

Apêndice A

Alguns Resultados de Análise

Neste apêndice, reunimos alguns resultados clássicos de Análise que foram utilizados no decorrer do texto. Aqui omitimos as provas de tais resultados, as quais se encontram em [6] e [24].

Seja $f : \mathbb{R} \longrightarrow \mathbb{C}$ uma função periódica de período 1 em $L^1([0,1])$, definimos o n-ésimo coeficiente de Fourier de f por

$$\widehat{f}(n) = \int_0^1 f(x)e(-nx)dx.$$

Teorema A.1 (Parseval). *Seja $f \in L^2([0,1])$. Então $\widehat{f} \in L^2(\mathbb{Z})$ e vale $\|f\|_{L^2([0,1])} = \|\widehat{f}\|_{L^2(\mathbb{Z})}$.*

Para uma função $f : \mathbb{R} \longrightarrow \mathbb{C}$ em $L^1(\mathbb{R})$, definimos a transformada de Fourier de f por

$$\widehat{f}(y) = \int_{\mathbb{R}} f(x)e(-xy)dx,$$

para todo $y \in \mathbb{R}$.

Teorema A.2 (Plancherel). *Seja $f \in L^1(\mathbb{R}) \cap L^2(\mathbb{R})$. Então $\widehat{f} \in L^2(\mathbb{R})$ e $\|f\|_{L^2(\mathbb{R})} = \|\widehat{f}\|_{L^2(\mathbb{R})}$.*

Enunciamos agora alguns resultados bem conhecidos em Análise Complexa. Iniciamos definindo o índice de uma curva com relação a um ponto.

Definição A.3. *Sejam γ uma curva complexa, fechada e retificável e $a \notin \gamma$. Definimos*

$$I(\gamma; a) = \frac{1}{2\pi i}\int_\gamma \frac{1}{z-a}dz,$$

como sendo o índice da curva γ com respeito ao ponto a.

Com esta definição podemos formular o seguinte teorema.

Teorema A.4 (Fórmula Integral de Cauchy). *Sejam G um aberto do plano complexo e f uma função analítica definida sobre G. Se γ é uma curva fechada e retificável em G tal que $I(\gamma; w) = 0$ para todo $w \notin G$, então para $a \in G - \gamma$, temos*

$$I(\gamma; a)f(a) = \frac{1}{2\pi i}\int_\gamma \frac{f(z)}{z-a}dz. \tag{A.1}$$

Tomando a k-ésima derivada em relação a variável a em (A.1), chegamos na seguinte igualdade

$$I(\gamma; a)f^{(k)}(a) = \frac{k!}{2\pi i}\int_\gamma \frac{f(z)}{(z-a)^{k+1}}dz, \tag{A.2}$$

válida sob as mesmas hipóteses do Teorema de Cauchy.

Dizemos que uma função f tem uma singularidade isolada em $z = a$ se existe $R > 0$, tal que f é definida e analítica em $0 < |z-a| < R$, mas não é analítica em $|z-a| < R$.

Definição A.5. *Suponhamos que f tem uma singularidade isolada em $z = a$ e seja*

$$f(z) = \sum_{n=-\infty}^{\infty} a_n (z-a)^n,$$

a série de Laurent de f centrada em a. Definimos o resíduo de f em $z = a$ como sendo o coeficiente a_{-1}, o qual denotamos por $Res(f; a)$.

Teorema A.6 (Teorema dos Resíduos)**.** *Seja f uma função analítica em um aberto convexo G, exceto pelas singularidades isoladas $a_1, \ldots, a_m$. Se γ é uma curva fechada e retificável em G que não passa pelos a_k, então*

$$\sum_{k=1}^{m} I(\gamma; a_k) Res(f; a_k) = \frac{1}{2\pi i} \int_\gamma f(z) dz.$$

A próxima proposição nos diz basicamente que o espaço das funções analíticas definidas sobre um aberto é completo com relação a métrica de convergência uniforme sobre compactos.

Proposição A.7. *Seja $\{f_n\}$ uma sequência de funções analíticas em um aberto G, tal que $f_n \longrightarrow f$ uniformemente sobre compactos de G, então f é analítica em G e vale $f_n' \longrightarrow f'$ uniformemente sobre compactos.*

Finalizamos este apêndice com uma breve discussão sobre a função gama. Para $|s| < 1$, o logaritmo principal é dado por

$$\log(1+s) = \sum_{k=1}^{\infty} (-1)^{k-1} \frac{s^k}{k}.$$

Então, para $n \geq 2|s|$, temos

$$-\frac{s}{n} + \log\left(1 + \frac{s}{n}\right) = -\frac{s}{n} + \left(\frac{s}{n} - \frac{1}{2}\frac{s^2}{n^2} + \frac{1}{3}\frac{s^3}{n^3} + \ldots\right) \ll \frac{s^2}{n^2},$$

logo, o produto $\prod_{n=1}^{\infty} \left(1 + \frac{s}{n}\right) e^{-\frac{s}{n}}$ converge absolutamente sobre compactos em $\mathbb{C}$. Assim, pela Proposição A.7, o produtório define uma função inteira com zeros simples precisamente em $s = -1, -2, \ldots$.

Definição A.8. *A função gama, representada por $\Gamma(s)$, é definida pela igualdade*

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

onde γ é a constante de Euler-Mascheroni, dada por $\gamma = \lim_{n\to\infty} \left(1 + \frac{1}{2} + \ldots + \frac{1}{n} - \log n\right)$.

Da definição e da discussão que a antecede, vemos que Γ é meromorfa com pólos simples em $s = 0, -1, -2, \ldots$. Quando $\sigma > 0$, podemos escrever

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

de onde segue que $\Gamma(1) = 1$ e $\Gamma(s+1) = s\Gamma(s)$. Em particular, $\Gamma(n+1) = n!$, para todo $n \in \mathbb{N}$. Podemos então considerar a função $\Gamma(s)$ como uma extensão do fatorial ao plano complexo.

Apêndice B

O Grande Crivo

Sejam $(a_n)_{M+1\leq n\leq M+N}$ números complexos arbitrários (aqui M e N são inteiros, com $N > 0$), $S(\alpha)$ o polinômio trigonométrico definido por

$$S(\alpha) = \sum_{n=M+1}^{M+N} a_n e(n\alpha) \tag{B.1}$$

e $\alpha_1, \ldots, \alpha_R$ reais (mod 1) δ-espaçados, ou seja, $\|\alpha_i - \alpha_j\| \geq \delta$, para todo $i \neq j$. O Grande Crivo (em seu aspecto analítico) consiste em desigualdades da forma

$$\sum_{r=1}^{R} |S(\alpha_r)|^2 \leq \Delta \sum_{n=M+1}^{M+N} |a_n|^2, \tag{B.2}$$

onde $\Delta = \Delta(N, \delta)$. O parâmetro M é irrelevante, pois para qualquer K inteiro, temos $T(\alpha) := \sum_{n=K+1}^{K+N} a_{M-K+n} e(n\alpha)$ $= e((K-M)\alpha)S(\alpha)$, assim $T(\alpha)$ tem frequências em $K+1 \leq n \leq K+N$ e $|T(\alpha)| = |S(\alpha)|$.

Nosso objetivo é determinar como Δ depende de N e δ. Nessa direção, Atle Selberg provou que $\Delta = N + \delta^{-1} - 1$ é um valor admissível e ótimo para a desigualdade do grande crivo, uma prova do resultado de Selberg pode ser vista em [21]. No entanto, ao nosso propósito um resultado mais fraco dado por Gallagher é o suficiente. Mais precisamente, provaremos que podemos tomar $\Delta = \pi N + \delta^{-1}$ na desigualdade (B.2).

Iniciamos com as seguintes desigualdades.

Lema B.1. *Suponhamos que $f \in C^1[0,1]$. Então, para $0 \leq x \leq 1$, temos*

$$|f(x)| \leq \int_0^1 (|f(t)| + |f'(t)|)dt$$

e

$$\left| f\left(\frac{1}{2}\right) \right| \leq \int_0^1 \left(|f(t)| + \frac{1}{2}|f'(t)| \right) dt.$$

Prova: Por integração por partes, vemos que

$$f(x) = \int_0^1 f(t)dt + \int_0^x tf'(t)dt + \int_x^1 (t-1)f'(t)dt.$$

Observe agora que os termos que multiplicam f' nas integrais acima têm módulo não excedendo 1 e quando $x = \frac{1}{2}$, estes têm módulo menor ou igual a $\frac{1}{2}$, de onde segue a prova do lema.

Com o Lema B.1, provaremos o

Teorema B.2 (Gallagher). *A desigualdade (B.2) é válida com $\Delta = \pi N + \delta^{-1}$.*

Prova: Sejam $f \in C^1(\mathbb{R})$ e β um real qualquer. Aplicando o Lema B.1 para a função $t \in [0,1] \longmapsto f\left(t\delta + \left(\beta - \frac{\delta}{2}\right)\right)$ juntamente com uma mudança de variável, chegamos à desigualdade

$$|f(\beta)| \leq \int\limits_{\beta-\frac{\delta}{2}}^{\beta+\frac{\delta}{2}} \left(\frac{1}{\delta}|f(t)| + \frac{1}{2}\,|f'(t)|\right) dt.$$

Escolhendo f como sendo o quadrado do polinômio trigonométrico (B.1) e $\beta = \alpha_j$, para $1 \leq j \leq R$, deduzimos que

$$|S(\alpha_j)|^2 \leq \int\limits_{\alpha_j-\frac{\delta}{2}}^{\alpha_j+\frac{\delta}{2}} \left(\frac{1}{\delta}|S(\alpha)|^2 + |S(\alpha)S'(\alpha)|\right) d\alpha. \tag{B.3}$$

Como $\{\alpha_j\}_{1\leq j\leq R}$ são δ-espaçados, segue-se que os intervalos $\left(\alpha_j - \frac{\delta}{2}, \alpha_j + \frac{\delta}{2}\right)$, com $1 \leq j \leq R$, são disjuntos (mod 1), logo somando (B.3) com relação a j, obtemos

$$\sum_{j=1}^{R} |S(\alpha_j)|^2 \leq \frac{1}{\delta}\int\limits_0^1 |S(\alpha)|^2 d\alpha + \int\limits_0^1 |S(\alpha)S'(\alpha)|\, d\alpha. \tag{B.4}$$

Pela Identidade de Parseval, o primeiro termo à direita de (B.4) é igual a $\displaystyle\frac{1}{\delta}\sum_{n=M+1}^{M+N} |a_n|^2$. Pela Desigualdade de Cauchy-Schwarz e a Identidade de Parseval, o segundo termo à direita de (B.4) é menor ou igual a

$$\begin{aligned}
\left(\int\limits_0^1 |S(\alpha)|^2 d\alpha\right)^{\frac{1}{2}} \left(\int\limits_0^1 \left|S'(\alpha)\right|^2 d\alpha\right)^{\frac{1}{2}} &= \left(\sum_{n=M+1}^{M+N} |a_n|^2\right)^{\frac{1}{2}} \left(\sum_{n=M+1}^{M+N} |2\pi i n a_n|^2\right)^{\frac{1}{2}} \\
&\leq 2\pi \left(\max_{M+1\leq n\leq M+N} |n|\right) \sum_{n=M+1}^{M+N} |a_n|^2.
\end{aligned}$$

Observamos anteriormente que $\Delta(N,\delta)$ é independente de M, assim podemos assumir que $M = -\left[\frac{N+1}{2}\right]$. Então $\max_{M+1\leq n\leq M+N} |n| \leq \frac{N}{2}$, logo

$$\sum_{j=1}^{R} |S(\alpha_j)|^2 \leq (\pi N + \delta^{-1}) \sum_{n=M+1}^{M+N} |a_n|^2,$$

como desejado.

Tome os pontos α_j como sendo as frações $\dfrac{a}{q}$, com $(a,q) = 1,\ q \leq Q$. Se $\dfrac{a}{q} \neq \dfrac{a'}{q'}$, temos

$$\left\|\frac{a}{q} - \frac{a'}{q'}\right\| = \left\|\frac{aq' - a'q}{qq'}\right\| \geq \frac{1}{qq'} \geq Q^{-2},$$

assim podemos tomar, neste caso, $\delta = Q^{-2}$. Consequentemente, estabelecemos o

Teorema B.3 (Bombieri)**.** *Com $S(\alpha)$ definida como em (B.1), temos*

$$\sum_{q\leq Q} \sideset{}{'}\sum_{a=1}^{q} \left|S\left(\frac{a}{q}\right)\right|^2 \ll \left(N + Q^2\right) \sum_{n=M+1}^{M+N} |a_n|^2.$$

Apêndice C

O Método de Turán

Dados $1 = |z_1| \geq |z_2| \geq \ldots \geq |z_n|$ e $b_j \in \mathbb{C}$, com $1 \leq j \leq n$. Definimos

$$g(v) = \sum_{j=1}^{n} b_j z_j^v,$$

para todo $v \in \mathbb{N}$.

Teorema C.1 (Segundo Teorema de Turán). *Para todo inteiro $m \geq 0$, temos*

$$\max_{\substack{m+1 \leq v \leq m+n \\ v \text{ } inteiro}} |g(v)| \geq 2\left(\frac{n}{8e(m+n)}\right)^n \min_{j=1,\ldots,n} |b_1 + \ldots + b_j|.$$

Do teorema acima segue imediatamente o

Corolário C.2. *Para todo inteiro $m \geq 0$ e complexos $\{z_j\}_{1 \leq j \leq n}$ existe um inteiro $m+1 \leq k \leq m+n$, tal que*

$$\left|z_1^k + \ldots + z_n^k\right| \geq 2\left(\frac{n}{8e(m+n)}\right)^n \left(\max_{j=1,\ldots,n} |z_j|\right)^k.$$

E deste último obtemos o seguinte resultado.

Corolário C.3. *Sejam $\{z_j\}_{1 \leq j \leq n}$ complexos e m um inteiro satisfazendo $m \geq n$, então existe $k \in (m, m+n]$, tal que*

$$\left|z_1^k + \ldots + z_n^k\right| \geq D^{-k} \left(\max_{j=1,\ldots,n} |z_j|\right)^k,$$

onde D é uma constante absoluta, positiva e efetivamente computável.

Para provar o Teorema C.1 precisamos de dois lemas auxiliares. O primeiro é um resultado clássico de Chebyshev, cuja demonstração pode ser encontrada em [23].

Lema C.4 (Desigualdade de Chebyshev). *Para $x < y$ e $P_n(z) = a_n z^n + a_{n-1} z^{n-1} + \ldots + a_0$, temos*

$$\max_{x \leq t \leq y} |P_n(t)| \geq 2\,|a_n| \left(\frac{y-x}{4}\right)^n.$$

Sejam $\xi_1, \xi_2, \ldots, \xi_n$ números complexos distintos e $y_1, y_2, \ldots, y_n$ números complexos arbitrários. Então existe um único polinômio $K(w) \in \mathbb{C}[w]$ de grau menor que n, com a propriedade $K(\xi_j) = y_j$, para todo $1 \leq j \leq n$ e este pode ser escrito de maneira única como

$$K(w) = e_0 + e_1(w - \xi_1) + e_2(w - \xi_1)(w - \xi_2) + \ldots + e_{n-1}(w - \xi_1)\ldots(w - \xi_{n-1}), \tag{C.1}$$

com $e_j \in \mathbb{C}$.

Suponhamos que $\xi_1, \xi_2, \ldots, \xi_n$ não pertencem ao disco $|s| \leq r$ e seja $h(w)$ uma função analítica em uma vizinhança de $|s| \geq r$, tal que

$$\lim_{w\to\infty} h(w) = 0$$

uniformemente. Se os valores de y_j são escolhidos tal que $y_j = h(\xi_j)$, com $j = 1, 2, \ldots, n$, temos o

Lema C.5 (Nörlund). *Os coeficientes e_j em (C.1) são dados por*

$$e_j = -\frac{1}{2\pi i} \int\limits_{|z|=r} \frac{h(z)}{(z-\xi_1)\ldots(z-\xi_{j+1})} dz,$$

para $j = 0, 1, \ldots, n-1$.

Prova: Iniciamos com a seguinte identidade

$$\frac{1}{z-\xi_1} + \frac{\xi_k - \xi_1}{(z-\xi_1)(z-\xi_2)} + \frac{(\xi_k-\xi_1)(\xi_k-\xi_2)}{(z-\xi_1)(z-\xi_2)(z-\xi_3)} + \ldots + \frac{(\xi_k-\xi_1)\ldots(\xi_k-\xi_{k-1})}{(z-\xi_1)\ldots(z-\xi_k)} = \frac{1}{z-\xi_k}, \tag{C.2}$$

válida para todo $k = 2, 3, \ldots, n$.

Seja $K_1(w)$ o polinômio construído a partir de (C.1), com e_j igual a

$$-\frac{1}{2\pi i} \int\limits_{|z|=r} \frac{h(z)}{(z-\xi_1)\ldots(z-\xi_{j+1})} dz,$$

então

$$K_1(w) = -\frac{1}{2\pi i} \int\limits_{|z|=r} h(z) \left(\frac{1}{z-\xi_1} + \frac{w-\xi_1}{(z-\xi_1)(z-\xi_2)} + \frac{(w-\xi_1)(w-\xi_2)}{(z-\xi_1)(z-\xi_2)(z-\xi_3)} + \ldots + \frac{(w-\xi_1)\ldots(w-\xi_{n-1})}{(z-\xi_1)\ldots(z-\xi_n)} \right) dz,$$

daí segue

$$K_1(\xi_k) = -\frac{1}{2\pi i} \int\limits_{|z|=r} h(z) \left(\frac{1}{z-\xi_1} + \frac{\xi_k-\xi_1}{(z-\xi_1)(z-\xi_2)} + \frac{(\xi_k-\xi_1)(\xi_k-\xi_2)}{(z-\xi_1)(z-\xi_2)(z-\xi_3)} + \ldots + \frac{(\xi_k-\xi_1)\ldots(\xi_k-\xi_{k-1})}{(z-\xi_1)\ldots(z-\xi_k)} \right) dz,$$

para $k = 1, 2, \ldots, n$. Usando a Identidade (C.2) na última igualdade, chegamos a

$$K_1(\xi_k) = -\frac{1}{2\pi i} \int\limits_{|z|=r} \frac{h(z)}{z-\xi_k} dz \ \text{ para } \ k = 1, 2, \ldots, n. \tag{C.3}$$

Agora, a hipótese $\lim_{w\to\infty} h(w) = 0$ juntamente com o Teorema de Cauchy (ver Teorema A.4) asseguram que o lado direito de (C.3) é igual a $h(\xi_k)$, portanto $K_1(\xi_k) = h(\xi_k)$, para todo $k = 1, 2, \ldots, n$. O que conclui a prova do lema.

Demonstraremos agora o Teorema de Turán enunciado no início deste apêndice. No que se segue, $\|\cdot\|$ é a norma sobre o espaço vetorial $\mathbb{C}[z]$, definida por $\|p(z)\| = |a_n| + |a_{n-1}| + \ldots + |a_0|$, para todo polinômio $p(z) = a_n z^n + a_{n-1} z^{n-1} + \ldots + a_0$.

Prova do Teorema C.1: Primeiramente suponhamos que

$$z_1 = 1,\ z_i \neq z_j,\ \text{para } i \neq j \ \text{ e } \ |z_n| > 0. \tag{C.4}$$

Sejam

$$\delta := \begin{cases} \frac{m}{m+n}, & \text{se } m > 0; \\ \\ 1 - \frac{1}{e}, & \text{se } m = 0, \end{cases}$$

e

$$f_0(z) := \prod_{j=1}^{n} (z - |z_j|).$$

Aplicando o Lema C.4 em $f_0(z)$ no intervalo $[\delta, 1]$, obtemos a existência de $\delta \leq \xi \leq 1$, tal que

$$|f_0(\xi)| \geq 2\left(\frac{1-\delta}{4}\right)^n. \tag{C.5}$$

Este último implica

$$\left|\prod_{j=1}^{n}(z-z_j)\right| \geq 2\left(\frac{1-\delta}{4}\right)^n, \text{ para } |z| = \xi.$$

Na esfera $|z| = \xi$ temos $||z| - |z_j|| \leq 1$, para todo $1 \leq j \leq n$, logo todos os subprodutos de $\prod_{j=1}^{n} |(z-z_j)|$ são estimados inferiormente por $2\left(\frac{1-\delta}{4}\right)^n$, em $|z| = \xi$.

Pela Desigualdade (C.5) temos que $\xi \neq |z_j|$, para todo $1 \leq j \leq n$. Assim, existe $1 \leq l \leq n$ tal que

$$(1 =)|z_1| \geq \ldots \geq |z_l| > \xi > |z_{l+1}| \geq \ldots \geq |z_n|.$$

Consideramos agora o primeiro polinômio auxiliar

$$f_1(z) := \prod_{j=l+1}^{n}(z-z_j) = \sum_{k=0}^{n-l} c_k^{(1)} z^k.$$

Como $|z_j| \leq 1$, temos que

$$\begin{aligned}
\|f_1\| &= 1 + \left|\sum_{1 \leq i_1 \leq n-l} z_{i_1+l}\right| + \left|\sum_{1 \leq i_1 < i_2 \leq n-l} z_{i_1+l} z_{i_2+l}\right| + \ldots + \left|\sum_{1 \leq i_1 < \ldots < i_{n-l} \leq n-l} z_{i_1+l} \ldots z_{i_{n-l}+l}\right| \\
&\leq \binom{n-l}{0} + \binom{n-l}{1} + \ldots + \binom{n-l}{n-l} \\
&= 2^{n-l}.
\end{aligned} \tag{C.6}$$

O segundo polinômio auxiliar $f_2(z)$ de grau menor ou igual a $l-1$ é definido por $f_2(z_j) = \dfrac{1}{z_j^{m+1} f_1(z_j)}$, para todo $1 \leq j \leq l$. Escrevemos

$$f_2(z) = c_0^{(2)} + c_1^{(2)}(z-z_1) + c_2^{(2)}(z-z_1)(z-z_2) + \ldots + c_{l-1}^{(2)}(z-z_1)\ldots(z-z_{l-1}).$$

De acordo com o Lema C.5, os coeficientes acima são dados pela seguinte fórmula

$$c_j^{(2)} = -\frac{1}{2\pi i}\int\limits_{|z|=\xi} \frac{dz}{z^{m+1} f_1(z)(z-z_1)\ldots(z-z_{j+1})},$$

assim

$$\left|c_j^{(2)}\right| \leq \frac{1}{2\pi}\int\limits_{|z|=\xi} \frac{|dz|}{\xi^{m+1}|f_1(z)(z-z_1)\ldots(z-z_{j+1})|}, \tag{C.7}$$

para todo $0 \leq j \leq l-1$. Pela construção dos polinômios auxiliares, vemos que $f_1(z)(z-z_1)\ldots(z-z_{j+1})$ é um subproduto de $\prod_{j=1}^{n}(z-z_j)$, logo

$$|f_1(z)(z-z_1)\ldots(z-z_{j+1})| \geq 2\left(\frac{1-\delta}{4}\right)^n, \tag{C.8}$$

em $|z| = \xi$. Desse modo, (C.7) e (C.8) implicam

$$\left|c_j^{(2)}\right| \leq \frac{\delta^{-m}}{2}\left(\frac{4}{1-\delta}\right)^n, \text{ para todo } 0 \leq j \leq l-1. \tag{C.9}$$

No entanto, precisamos estimar os coeficientes que nos dão

$$f_2(z) = c_0^{(3)} + c_1^{(3)} z + \ldots + c_{l-1}^{(3)} z^{l-1}.$$

Para isso, observe que

$$c_{l-1}^{(3)} = c_{l-1}^{(2)}$$

e

$$c_j^{(3)} = c_j^{(2)} - c_{j+1}^{(2)} \sum_{1 \le i_1 \le j+1} z_{i_1} + c_{j+2}^{(2)} \sum_{1 \le i_1 < i_2 \le j+2} z_{i_1} z_{i_2} + \ldots + (-1)^{l-j-1} c_{l-1}^{(2)} \sum_{1 \le i_1 < \ldots < i_{l-j-1} \le l-1} z_{i_1} \ldots z_{i_{l-j-1}},$$

para $0 \le j \le l-2$. Usando (C.9) nas igualdades acima, chegamos a

$$\begin{aligned} \left| c_j^{(3)} \right| &\le \frac{\delta^{-m}}{2} \left(\frac{4}{1-\delta} \right)^n \left\{ \binom{j}{0} + \binom{j+1}{1} + \binom{j+2}{2} + \ldots + \binom{l-1}{l-1-j} \right\} \\ &= \frac{\delta^{-m}}{2} \left(\frac{4}{1-\delta} \right)^n \binom{l}{j+1}, \end{aligned} \tag{C.10}$$

para $0 \le j \le l-1$, logo

$$\|f_2\| \le \frac{\delta^{-m}}{2} \left(\frac{4}{1-\delta} \right)^n \left\{ \binom{l}{1} + \binom{l}{2} + \ldots + \binom{l}{l} \right\} \le \frac{\delta^{-m}}{2} \left(\frac{4}{1-\delta} \right)^n 2^l. \tag{C.11}$$

Consideramos o terceiro e último polinômio auxiliar

$$f_3(z) := z^{m+1} f_1(z) f_2(z) = \sum_{v=m+1}^{m+n} c_v^{(4)} z^v.$$

Por construção, temos

$$\sum_{v=m+1}^{m+n} c_v^{(4)} z_j^v = \begin{cases} 1, & \text{se } 1 \le j \le l; \\ 0, & \text{se } l+1 \le j \le n. \end{cases}$$

Multiplicando por b_j e somando com relação a j, obtemos

$$\sum_{v=m+1}^{m+n} c_v^{(4)} g(v) = b_1 + \ldots + b_l,$$

de onde segue a desigualdade

$$\max_{\substack{m+1 \le v \le m+n \\ v \ inteiro}} |g(v)| \ge \frac{\min_{j=1,\ldots,n} |b_1 + \ldots + b_j|}{\|f_3\|}. \tag{C.12}$$

Por (C.6) e (C.11), temos

$$\|f_3\| \le \|f_1\| \cdot \|f_2\| \le \frac{\delta^{-m}}{2} \left(\frac{8}{1-\delta} \right)^n,$$

mas

$$\delta^{-m} = \left(\frac{m+n}{m} \right)^m < e^n, \text{ para todo } m \ge 0,$$

assim

$$\|f_3\| \le \frac{1}{2} \left(\frac{8e(m+n)}{n} \right)^n. \tag{C.13}$$

De (C.12) e (C.13) concluímos a prova do Teorema C.1 sob a condição (C.4). O caso geral segue deste por passagem ao limite.

Referências Bibliográficas

[1] Tom M. Apostol. *Modular Functions and Dirichlet Series in Number Theory*, volume 41. Springer-Verlag, 1976.

[2] Tom M. Apostol. *Introduction to analytic number theory.* Springer-Verlag, New York, Undergraduate Texts in Mathematics, 2013.

[3] Enrico Bombieri. Le grand crible dans la théorie analytique des nombres. *Soc. Math. de France, Asterisque*, 18, 1987.

[4] Enrico Bombieri and Harold Davenport. On the large sieve method. *Abhandlungen aus Zahlentheorie und Analysis*, 1968.

[5] Jingrun Chen and Chengdong Pan. The exceptional set of goldbach numbers. *Sci. Sinica*, 23:416–430, 1980.

[6] John B. Conway. *Functions of one complex variable I*, volume 11. Springer-Verlag, 1978.

[7] Nikolai G. Cudakov. The goldbach's problem. *Dokl. Akad. Nauk SSSR*, (17):331–334, 1937.

[8] Harold Davenport. *Multiplicative number theory*, volume 74 of Graduate Texts in Mathematics. Springer-Verlag, New York, third edition, 2000. Revised and with a preface by Hugh L. Montgomery.

[9] Theodor Estermann. On goldbach's problem: Proof that almost all even positive integers are sums of two primes. *Proceedings of the London Mathematical Society*, 2(44):307–314, 1938.

[10] Patrick X. Gallagher. A large sieve density estimate near $\sigma = 1$. *Inventiones mathematicae*, 11(4):329–339, 1970.

[11] Heine Halberstam and Hans-E. Richert. *Sieve methods.* Academic Press, 1974.

[12] Godfrey H. Hardy and John E. Littlewood. Some problems of 'partitio numerorum'; iii: On the expression of a number as a sum of primes. *Acta Mathematica*, 44(1):1–70, 1923.

[13] Godfrey H. Hardy and John E. Littlewood. Some problems of "partitio numerorum"(v): A further contribution to the study of goldbach's problem. *Proceedings of the London Mathematical Society*, 2(1):46–56, 1924.

[14] Harald A. Helfgott. Major arcs for goldbach's problem. *arXiv preprint arXiv:1305.2897*, 2013.

[15] Harald A. Helfgott. The ternary goldbach conjecture is true. *arXiv preprint arXiv:1312.7748*, 2013.

[16] Henryk Iwaniec and Emmanuel Kowalski. *Analytic number theory*, volume 53. American Mathematical Soc., 2004.

[17] Hongze Li. The exceptional set of goldbach numbers (ii). *Acta Arithmetica*, 92:71–88, 2000.

[18] Yu. V. Linnik. On the least prime in an arithmetic progression, i. the basic theorem. *Rec. Math. [Mat. Sbornik] N. S.*, 15(57):139–178, 1944.

[19] Yu. V. Linnik. On the least prime in an arithmetic progression, ii. the deuring–heilbronn phenomenon. *Rec. Math. [Mat. Sbornik] N. S.*, 15(57):347–368, 1944.

[20] Wen Chao Lu. Exceptional set of goldbach number. *Journal of Number Theory*, 10(130):2359–2392, 2010.

[21] Hugh L. Montgomery. The analytic principle of the large sieve. *Bulletin of the American Mathematical Society*, 84(4):547–567, 1978.

[22] Hugh L. Montgomery and Robert C. Vaughan. The exceptional set of goldbach's problem. *Acta Arithmetica*, 27(1):353–370, 1975.

[23] George Pólya and Gabor Szegö. *Problems and theorems in analysis II: Theory of functions. Zeros. Polynomials. Determinants. Number theory. Geometry.* Springer-Verlag, 1997.

[24] Walter Rudin. *Real and complex analysis.* McGraw-Hill, 1987.

[25] Johannes G. van der Corput. Sur l'hypothèse de goldbach. *Proc. Akad. Wet. Amsterdam*, (44):76–80, 1938.

[26] Robert C. Vaughan. On goldbach's problem. *Acta Arithmetica*, (22):21–48, 1972.

[27] Ivan M. Vinogradov. The method of trigonometric sums in the theory of numbers. 1954.