Universidade Federal de Uberlândia
Faculdade de Matemática

Bacharelado em Matemática

SOBRE A DISTRIBUIÇÃO DOS NÚMEROS PRIMOS

Lucas Vinnicius de Oliveira Gomes

Uberlândia-MG
2020

Lucas Vinnicius de Oliveira Gomes

SOBRE A DISTRIBUIÇÃO DOS NÚMEROS PRIMOS

Trabalho de conclusão de curso apresentado à Coordenação do Curso de Bacharelado em Matemática como requisito parcial para obtenção do grau de Bacharel em Matemática.

Orientador: Josimar Joao Ramirez Aguirre

Uberlândia-MG

2020

Universidade Federal de Uberlândia
Faculdade de Matemática

Coordenação do Curso de Bacharelado em Matemática

A banca examinadora, conforme abaixo assinado, certifica a adequação deste trabalho de conclusão de curso para obtenção do grau de Bacharel em Matemática.

Uberlândia, 04 de Dezembro de 2020.

BANCA EXAMINADORA

Josimar Joao Ramirez Aguirre

Victor Gonzalo Lopez Neumann

Luciana Aparecida Alves

Uberlândia-MG

2020

Agradecimentos

À minha mãe Maria Aparecida de Oliveira que sem sombra de dúvidas, foi essencial para que tudo isso tenha sido possível. Te amo mãe.

Ao meu pai Alessandro Isaias Marcelino Gomes por me proteger, me ensinar e me apoiar. Te amo pai.

Ao Prof. Dr. Josimar Joao Ramirez Aguirre pela orientação, confiança, dedicação pelo nosso projeto de pesquisa e acima de tudo pela nossa amizade. Agradeço por todos os ensinamentos nesses anos de pesquisa.

Aos meus colegas de turma e amigos pra vida toda Thiago Henrique e Pedro Augusto. Obrigado pelo apoio e pela jornada durante esses quatro anos.

Aos meus colegas do PET Matemática Gabriela, Alef, Ana Laura, Dhara, Fernanda, Gabriel, Julia, Leonardo, Tiago e Victor por todos os eventos, viagens e confraternizações. Com toda certeza foi uma experiência única de grande importância na minha vida.

À Profª. Drª. Elisa Regina dos Santos por todos os conselhos e ensinamentos.

A todas as outras pessoas que fizeram parte dessa jornada.

À Deus, pela vida e pela força nos momentos difíceis. Gratidão.

Resumo

Este trabalho tem como propósito o estudo de resultados acerca da distribuição dos números primos no qual, inicialmente serão definidas as funções aritméticas, o produto de Dirichlet, a fórmula de inversão de Mobius, a fórmula de soma de Euler, entre outros. Em seguida, serão estudados os conceitos básicos necessários para a prova do teorema dos números primos, como a função zeta de Riemann, as funções de Chebyshev, transformada de Laplace, entre outros. Além disso, será estudado o teorema de Dirichlet sobre primos em progressões aritméticas. Por fim, serão apresentados conceitos básicos sobre os métodos de crivos, tais como o crivo de Eratóstenes e Legendre e o truque de Rankin.

Palavras-chave: Funções Aritméticas, Produto de Dirichlet, Função Zeta de Riemann, Funções de Chebyshev, Teorema dos Números Primos, Crivo de Eratóstenes e Legendre.

Abstract

This work aims to study results about the distribution of prime numbers in which, initially, arithmetic functions, Dirichlet's product, Mobius inversion formula, Euler's sum formula, among others, will be defined. Then, the basic concepts necessary to prove the prime number theorem will be studied, such as the Riemann zeta function, the Chebyshev functions, Laplace transform, among others. Furthermore, Dirichlet's theorem about primes in arithmetic progressions will be studied. Finally, basic concepts about sieve methods will be presented, such as the sieve of Eratosthenes and Legendre and the Rankin's trick.

Keywords: Arithmetic Functions, Dirichlet's Product, Riemann's Zeta Function, Chebyshev's Functions, Prime Number Theorem, Eratosthenes' Sieve and Legendre..

Sumário

Introdução

Os gregos viam os números primos como "tijolos", a partir dos quais seria possível construir todos os outros números. A principal questão sobre números primos é compreender sua distribuição nos naturais, isto é, com que frequência eles aparecem. Desde Euclides sabemos a infinitude desses números, mas entender a ordem de aparição dos primos foi um verdadeiro desafio. Gauss foi o primeiro matemático a perceber um bom comportamento na quantidade de primos menores que um certo número dado, a partir das suas tabelas.

O Teorema dos Números Primos (TNP) é um dos grandes teoremas da matemática. Ele conecta o discreto e o contínuo com a elegante afirmação

$$\lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = 1,$$

em que $\pi(x)$ denota o número de primos menores ou iguais a x. Esse resultado foi primeiro conjecturado por Legendre por volta de 1798 e talvez alguns anos antes pelo jovem Gauss, sendo mais tarde provado independentemente por Hadamard [7] e de la Vallee Poussin [12] em 1896 com métodos de análise complexa, baseados no artigo de Riemann [9].

No Capítulo 2 apresentamos uma prova do TNP organizada da seguinte forma. Inicialmente, apresentamos uma equivalência assintótica ($\sim$) e a função zeta de Riemann $\zeta(s)$ junto com a fórmula do produto de Euler. Em seguida, provamos que a função zeta tem uma continuação analítica para $\operatorname{Re} s > 0$. Obtemos representações em série para $\log\zeta(s)$ e $\log|\zeta(s)|$. Estas são usadas para estabelecer que a função zeta não possui zeros na reta vertical $\operatorname{Re} s = 1$. Introduzimos a função de Chebyshev $\vartheta(x) = \sum_{p\le x} \log p$ e estabelecemos um limite superior para essa função. Provamos que uma função relacionada a $\log\zeta(s)$ se estende analiticamente a uma vizinhança aberta do semiplano fechado $\operatorname{Re} s \ge 1$. Em seguida, apresentamos um lema sobre a analiticidade das transformadas de Laplace. Apresentamos o teorema tauberiano de Newman e usamos para estabelecer a convergência de uma certa integral imprópria, que é utilizado para implicar $\vartheta(x) \sim x$. Por fim concluímos a prova do TNP.

Nota-se que são utilizados diversos resultados de análise complexa nessa demonstração. O leitor pode se referenciar por [2].

A progressão aritmética dos números ímpares $1, 3, 5, \ldots, 2n+1, \ldots$ contém infinitos primos. É natural perguntar se outras progressões aritméticas têm essa propriedade. Uma progressão aritmética com o primeiro termo h e diferença comum k consiste em todos os números da forma

$$kn + h, \quad n = 0, 1, 2, \ldots \tag{1}$$

Se h e k têm um fator comum d, cada termo da progressão é divisível por d e não é possível ter mais de um primo na progressão aritmética se $d > 1$. Em outras palavras, uma condição necessária para a existência de infinitos primos na progressão aritmética (1) é que $(h, k) = 1$. Dirichlet foi o primeiro a provar que essa condição também é suficiente. Ou seja, se $(h, k) = 1$, a progressão aritmética (1) contém infinitos primos. Este resultado, conhecido como teorema de Dirichlet, será provado no Capítulo 3.

As ideias de crivo certamente cresceram a partir de um processo chamado crivo de Eratóstenes proposto por volta do Século III a.C., cuja a ideia era eliminar, de uma tabela, aqueles elementos que por alguma razão eram considerados indesejaveis. Os processos atuais de crivos, no entanto, têm uma perspectiva diferente. Enquanto o crivo de Eratóstenes, na sua versão original, se preocupa em obter elementos atendendo a condições dadas, os crivos atuais se preocupam em contar o número de elementos atendendo a essas condições. A teoria moderna de crivos teve início com os trabalhos de Viggo Brun (1885-1978) e até 30 anos atrás, três métodos de crivos eram considerados como os principais pilares da teoria, a saber, crivo de Brun, crivo de Selberg e o grande crivo de Linnik. Segundo os autores de [3], a versão moderna do crivo de Eratóstenes (tambem conhecido como crivo de Eratóstenes-Legendre) quando associado ao truque de Rankin torna-se tão poderoso quanto o crivo de Brun. Desde o seu surgimento o crivo de Eratóstenes têm sido revisado e reinterpretado por vários matemáticos. No Capítulo 4 apresentamos a evolução dessas ideias desde sua origem até sua versão moderna e apresentamos, ao leitor, outras ideias comuns aos processos de crivo.

1. PRELIMINARES

1.1 FUNÇÕES ARITMÉTICAS

Uma função real ou complexa definida nos inteiros positivos é chamada de **função aritmética**. Em outras palavras, uma função aritmética é uma sequência de números reais ou complexos.

Neste capítulo vamos introduzir as propriedades de algumas funções aritméticas que desempenham um papel importante no estudo das propriedades de divisibilidade de inteiros e na distribuição de primos.

Vejamos alguns exemplos:

Função Identidade: Denotada como $I(n)$, definida por $I(1) = 1$ e $I(n) = 0$, para todo $n \geq 2$;

Função Unidade: Denotada como $u(n)$, definida por $u(n) = 1$ para todo n.

Função Divisor: Denotada como $d(n)$, representa o número de divisores positivos de n, considerando os divisores triviais 1 e n, ou seja, $d(n) = \sum_{d|n} 1$.

Função Mobius: Denotada como $\mu(n)$, definimos por $\mu(1) = 1$, $\mu(n) = 0$ se n é divisível por um primo ao quadrado e $\mu(n) = (-1)^k$ se n é produto de k fatores primos distintos.

Função Totiente de Euler: Conhecida como função phi de Euler e denotada como $\phi(n)$, representa o número de inteiros positivos $m \leq n$, onde m e n são primos entre si, ou seja, $\phi(n) = \sum_{m=1,(m,n)=1}^{n} 1$.

Função Mangoldt: Denotada como $\Lambda(n)$, definida por $\Lambda(n) = 0$ se n não é uma potência de primo e $\Lambda(n) = \log p$, se $n = p^m$ para algum primo p e um inteiro positivo m.

Algumas funções aritméticas apresentam a seguinte propriedade.

Definição 1. *Uma função aritmética f é chamada* ***multiplicativa*** *se f é não nula e se satisfaz*

$$f(mn) = f(m)f(n), \text{ sempre que } (m, n) = 1.$$

Uma função aritmética f é chamada ***completamente multiplicativa*** *se satisfaz*

$$f(mn) = f(m)f(n), \text{ para todo } m, n.$$

Por exemplo, temos que a função Mobius é multiplicativa, mas não é completamente multiplicativa, pois considere os inteiros m e n primos entre si. Se m ou n tem um fator primo ao quadrado, então o mesmo acontece com o produto mn e então $\mu(mn) = 0 = \mu(m)\mu(n)$. Caso contrário, seja $m = p_1 \dots p_s$ e $n = q_1 \dots q_t$ onde p_i e q_i são primos distintos. Então $\mu(m) = (-1)^s$ e $\mu(n) = (-1)^t$ e $\mu(mn) = (-1)^{s+t} = \mu(m)\mu(n)$, logo μ é multiplicativa. Agora $\mu(4) = 0$, mas $\mu(2)\mu(2) = 1$, logo μ não é completamente multiplicativa.

Teorema 1. *Se f é multiplicativa, então $f(1) = 1$.*

Demonstração. Temos $f(n) = f(1)f(n)$, pois $(n, 1) = 1$ para todo n. Como f é não nula temos $f(n) \neq 0$ para algum n, então $f(1) = 1$. □

Note que, como $\Lambda(1) = 0$, então a função Mangoldt não é multiplicativa. Da definição de função multiplicativa, temos os seguintes resultados.

Teorema 2. *Seja f tal que $f(1) = 1$. Então*

(a) f é multiplicativa se, e somente se,

$$f(p_1^{a_1} \dots p_r^{a_r}) = f(p_1^{a_1}) \dots f(p_r^{a_r})$$

para todo primo p_i e inteiros $a_i \geq 1$.

(b) Se f é multiplicativa, então f é completamente multiplicativa se, e somente se,

$$f(p^a) = f(p)^a.$$

para todo primo p e inteiros $a \geq 1$.

Vejamos agora algumas relações entre as funções aritméticas, que serão úteis no decorrer do trabalho.

Teorema 3. *Para todo $n \geq 1$, temos* $\displaystyle\sum_{d|n} \mu(d) = I(n)$.

Demonstração. Se $n = 1$, então $\sum_{d|n} \mu(d) = \mu(1) = 1 = I(1)$. Para $n > 1$, seja $n = \prod_{i=1}^{k} p_i^{a_i}$. Como $\mu(d) = 0$, se d é divisível por um primo ao quadrado, então os termos não nulos da soma são dados para $d = \prod_{i \in I} p_i$, onde $I \subset \{1, 2, 3, \dots, k\}$. Assim,

$$\sum_{d|n} \mu(d) = \mu(1) + \mu(p_1) + \dots + \mu(p_k) + \mu(p_1p_2) + \dots + \mu(p_{k-1}p_k) + \dots + \mu(p_1 \dots p_k) =$$

$$= 1 + \binom{k}{1}(-1) + \binom{k}{2}(-1)^2 + \dots + \binom{k}{k}(-1)^k = (1-1)^k = 0,$$

onde a penúltima igualdade é dada pelo teorema binomial. □

Teorema 4. *A função totiente de Euler satisfaz:*

(a) $\sum_{d|n} \phi(d) = n$, *para todo* $n \in \mathbb{N}$.

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

(c) $\phi(n) = n\prod_{p|n}\left(1 - \frac{1}{p}\right)$, *para todo* $n \in \mathbb{N}$.

Demonstração. (a) Seja $S = \{1, 2, \ldots, n\}$. Considere a partição $A_d = \{k : 1 \leq k \leq n, (k, n) = d\}$ de S. Se $k \in A_d$ é tal que $k = dk_0$, temos $A_d = \{dk_0 : 1 \leq k_0 \leq n/d, (k_0, n/d) = 1\}$ e então $|A_d| = \phi(n/d)$. Como $n = |S| = \sum_{d|n} |A_d|$, segue que $n = \sum_{d|n} \phi(n/d) = \sum_{d|n} \phi(d)$.

(b) Da definição da função $\phi(n)$ podemos escrever

$$\phi(n) = \sum_{k=1}^{n} \left\lfloor \frac{1}{(n,k)} \right\rfloor^{1},$$

onde k percorre todos os inteiros menores ou iguais a n. Agora, pelo teorema anterior, substituíndo n por (n, k) temos

$$\phi(n) = \sum_{k=1}^{n} \sum_{d|(n,k)} \mu(d) = \sum_{k=1}^{n} \sum_{\substack{d|n \\ d|k}} \mu(d).$$

Para um divisor fixo d de n, devemos somar todos os valores de k no intervalo $1 \leq k \leq n$ que são múltiplos de d. Se escrevermos $k = qd$, então $1 \leq k \leq n$ se e somente se $1 \leq q \leq n/d$. Portanto, podemos escrever

$$\phi(n) = \sum_{d|n} \sum_{q=1}^{n/d} \mu(d) = \sum_{d|n} \mu(d) \sum_{q=1}^{n/d} 1 = \sum_{d|n} \mu(d)\frac{n}{d}.$$

Isso prova o resultado.

(c) Seja p primo e $k \geq 1$, então

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

De fato, como p é um número primo os únicos valores possíveis de (p^k, m) são $1, p, p^2, \ldots, p^k$, e a única maneira de (p^k, m) não ser igual a 1 é para m múltiplo de p. Os múltiplos de p que são menores ou iguais a p^k são $p, 2p, 3p, ..., p^{k-1}p = p^k$, e há p^{k-1} deles. Portanto, os outros $p^k - p^{k-1}$ números são todos relativamente primos à p^k.

[1] A função parte inteira denotada por $\lfloor x \rfloor$ representa o maior inteiro menor ou igual a x.

Suponha, então, que $n > 1$ tal que $n = p_1^{k_1} \dots p_r^{k_r}$ onde $p_1 < \dots < p_r$ e cada $k_i > 1$. Usando de $\phi(n)$ ser multiplicativo e a fórmula para $\phi(p^k)$ temos

$$\begin{aligned}\phi(n) &= \phi(p_1^{k_1}) \dots \phi(p_r^{k_r}) \\ &= p_1^{k_1}\left(1 - \frac{1}{p_1}\right) \dots p_r^{k_r}\left(1 - \frac{1}{p_r}\right) \\ &= p_1^{k_1} \dots p_r^{k_r}\left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_r}\right) \\ &= n\left(1 - \frac{1}{p_1}\right) \dots \left(1 - \frac{1}{p_r}\right).\end{aligned}$$

□

Vamos apresentar agora alguns resultados sobre a função de Mangoldt.

Teorema 5. *Se $n \geq 1$, temos*

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

Demonstração. Para $n = 1$, ambos os membros são zero. Para $n > 1$, seja $n = \prod_{k=1}^{r} p_k^{a_k}$, considerando logaritmos, temos

$$\log n = \sum_{k=1}^{r} a_k \log p_k$$

Agora, considere a soma $\sum_{d|n} \Lambda(d)$. Os termos não nulos são os divisores d da forma p_k^m para $m = 1, 2, \dots, a_k$ e $k = 1, 2, \dots, r$. Então

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

como queríamos. □

1.2 O produto de Dirichlet

Vamos agora apresentar uma operação definida para funções aritméticas muito importante na teoria dos números. Foi desenvolvido por Johann Dirichlet. É proveitoso tratar essa operação como um novo tipo de multiplicação de funções aritméticas.

Definição 2. *Sejam f e g funções aritméticas. Definimos o **produto de Dirichlet**, denotado por $f * g$, sendo*

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

Uma motivação para introduzir essa operação é o fato de que a definição de muitas funções aritméticas têm a forma de um produto de Dirichlet e que muitas identidades entre funções aritméticas podem ser escritas como identidades envolvendo esse produto. Vejamos alguns exemplos.

(i) De $d(n) = \sum_{d|n} 1$, então $d = u * u$.

(ii) De $I(n) = \sum_{d|n} \mu(d)$, então $I = \mu * u$.

(iii) De $\log n = \sum_{d|n} \Lambda(d)$, então $\log = \Lambda * u$.

Apresentamos agora algumas propriedades do produto de Dirichlet.

Teorema 6. *O produto de Dirichlet é comutativo e associativo, ou seja, dados f, g e k funções aritméticas, temos*

$$f * g = g * f \quad e \quad (f * g) * k = f * (g * k).$$

Para mostrar essas propriedades, basta considerarmos o produto de Dirichlet da forma

$$(f * g)(n) = \sum_{ab=n} f(a)g(b)$$

onde a soma percorre todos os pares a e b de inteiros positivos cujo produto é igual a n.

Teorema 7. *Se f é uma função aritmética com $f(1) \neq 0$ então existe uma única função aritmética f^{-1}, chamado* ***inverso de*** *f (segundo o produto de Dirichlet) tal que*

$$f * f^{-1} = f^{-1} * f = I$$

onde I é a função identidade. Além disso, f^{-1} é dado por

$$f^{-1}(1) = \frac{1}{f(1)}$$

e

$$f^{-1}(n) = \frac{-1}{f(1)} \sum_{\substack{d|n \\ d<n}} f\left(\frac{n}{d}\right) f^{-1}(d)$$

para $n > 1$.

Demonstração. Dado f, mostraremos que a equação $(f * f^{-1})(n) = I(n)$ tem uma solução única para os valores da função $f^{-1}(n)$. Para $n = 1$, temos que resolver a equação

$$(f * f^{-1})(1) = I(1)$$

no qual resulta em

$$f(1)f^{-1}(1) = 1$$

Como $f(1) \neq 0$ existe uma única solução, $f^{-1}(1) = 1/f(1)$. Suponha agora que os valores da função $f^{-1}(k)$ fosse determinados exclusivamente para todos $k < n$. Então temos que resolver a equação $(f * f^{-1})(n) = I(n)$, ou

$$\sum_{d|n} f\left(\frac{n}{d}\right) f^{-1}(d) = 0.$$

Podemos escrever como

$$f(1)f^{-1}(n) + \sum_{\substack{d|n \\ d<n}} f\left(\frac{n}{d}\right) f^{-1}(d) = 0.$$

Se os valores $f^{-1}(d)$ são conhecidos para todos os divisores $d < n$, existe um único determinado valor para $f^{-1}(n)$, ou seja,

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

Esse resultado estabelece a existência e unicidade de f^{-1} por indução. □

Já provamos que $\sum_{d|n} \mu(d) = I(n)$. Na notação de Dirichlet, temos

$$\mu * u = I.$$

Assim u e μ são inversos de Dirichlet um do outro, ou seja

$$u = \mu^{-1} \quad \text{e} \quad \mu = u^{-1}.$$

Esta propriedade simples da função Mobius, juntamente com a propriedade associativa do produto de Dirichlet, nos permite apresentar uma prova simples do próximo teorema.

Teorema 8 (**Fórmula de inversão de Mobius**). *Temos*

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

se, e somente se,

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

Demonstração. Por hipótese, temos $f = g * u$, onde u é a função unidade. Multiplicando por μ, temos $f * \mu = (g * u) * \mu = g * (u * \mu) = g * I = g$. Analogamente, para a condição necessária basta multiplicar $f * \mu = g$ por u. □

Agora, F denota uma função real ou complexa, definida nos reais positivos $(0, +\infty)$ tal que $F(x) = 0$, para $0 < x < 1$. Somas do tipo $\sum_{n \leq x} \alpha(n) F\left(\frac{x}{n}\right)$ são frequentes na Teoria dos Números, onde α é uma Função Aritmética. A soma define uma nova função G em $(0, +\infty)$, com $G(x) = 0$ para $0 < x < 1$. Denotamos essa função G por $\alpha \circ F$. Então

$$G(x) = (\alpha \circ F)(x) = \sum_{n \leq x} \alpha(n) F\left(\frac{x}{n}\right).$$

Se $F(x) = 0$ para todo x não inteiro, a restrição de F para os inteiros é uma Função Aritmética e temos $(\alpha \circ F)(m) = (\alpha * F)(x)$ para todo inteiro $m \geq 1$, então a operação $\circ$ pode ser considerada uma generalização do Produto de Dirichlet $*$. A operação $\circ$, em geral,

não é comutativa nem associativa. No entanto, a seguinte propriedade funciona como uma propriedade associativa relacionando $\circ$ e $*$.

Teorema 9. *Para quaisquer funções α e β temos*

$$\alpha \circ (\beta \circ F) = (\alpha * \beta) \circ F.$$

Demonstração. Para $x > 0$, temos

$$\begin{aligned}\{\alpha \circ (\beta \circ F)\}(x) &= \sum_{n\leq x} \alpha(n) \sum_{m\leq x/n} \beta(m) F\left(\frac{x}{mn}\right) = \sum_{mn\leq x} \alpha(n)\beta(m) F\left(\frac{x}{mn}\right) \\ &= \sum_{k\leq x} \left(\sum_{n|k} \alpha(n)\beta\left(\frac{k}{n}\right)\right) F\left(\frac{x}{k}\right) = \sum_{k\leq x} (\alpha * \beta)(k) F\left(\frac{x}{k}\right) \\ &= \{(\alpha * \beta) \circ F\}(x),\end{aligned}$$

como queríamos. □

Teorema 10 (**Fórmula de Inversão Generalizada**)**.** *Se α tem inverso α^{-1} pelo produto de Dirichlet, então a equação*

$$G(x) = \sum_{n\leq x} \alpha(n) F\left(\frac{x}{n}\right) \tag{1.1}$$

implica

$$F(x) = \sum_{n\leq x} \alpha^{-1}(n) G\left(\frac{x}{n}\right). \tag{1.2}$$

Reciprocamente, (1.2) implica (1.1).

Demonstração. Se $G = \alpha \circ F$, então

$$\alpha^{-1} \circ G = \alpha^{-1} \circ (\alpha \circ F) = (\alpha^{-1} * \alpha) \circ F = I \circ F = F.$$

Logo (1.1) implica (1.2). O recíproco é análogo. □

O caso especial a seguir é de particular importância.

Teorema 11 (**Fórmula de Inversão de Mobius Generalizada**)**.** *Se α é completamente multiplicativa, temos*

$$G(x) = \sum_{n\leq x} \alpha(n) F\left(\frac{x}{n}\right) \Leftrightarrow F(x) = \sum_{n\leq x} \mu(n)\alpha(n) G\left(\frac{x}{n}\right). \tag{1.3}$$

Demonstração. Nesse caso, tome $\alpha^{-1} = \mu(n)\alpha(n)$ no Teorema 10. □

1.3 ALGUMAS FÓRMULAS ASSINTÓTICAS ELEMENTARES

Às vezes, o valor assintótico de uma soma parcial pode ser obtido comparando com uma integral. Uma fórmula de soma de Euler fornece uma expressão exata para o erro cometido nessa aproximação.

Teorema 12 (**Fórmula de soma de Euler**). *Se f tem derivada contínua no intervalo $[y, x]$, onde $0 < y < x$, então*

$$\sum_{y<n\leq x} f(n) = \int_y^x f(t)dt + \int_y^x (t - \lfloor t \rfloor) f'(t)dt + f(x)(\lfloor x \rfloor - x) - f(y)(\lfloor y \rfloor - y). \tag{1.4}$$

Demonstração. Seja $m = \lfloor y \rfloor$, $k = \lfloor x \rfloor$. Para inteiros n e $n-1$ em $[y, x]$ temos

$$\begin{aligned}\int_{n-1}^{n} \lfloor t \rfloor f'(t)dt &= \int_{n-1}^{n} (n-1) f'(t)dt = (n-1)\{f(n) - f(n-1)\} \\ &= \{nf(n) - (n-1)f(n-1)\} - f(n).\end{aligned}$$

Somando para $n = m+1$ até $n = k$ temos

$$\begin{aligned}\int_m^k \lfloor t \rfloor f'(t)dt &= \sum_{n=m+1}^{k} \{nf(n) - (n-1)f(n-1)\} - \sum_{y<n\leq x} f(n) \\ &= kf(k) - mf(m) - \sum_{y<n\leq x} f(n),\end{aligned}$$

então

$$\begin{aligned}\sum_{y<n\leq x} f(n) &= -\int_m^k \lfloor t \rfloor f'(t)dt + kf(k) - mf(m) \\ &= -\int_y^x \lfloor t \rfloor f'(t)dt + kf(x) - mf(y).\end{aligned}$$

Integrando por partes,

$$\int_y^x f(t)dt = xf(x) - yf(y) - \int_y^x tf'(t)dt,$$

concluímos a demonstração. □

O próximo Teorema fornece algumas fórmulas assintóticas que são consequências da fórmula de soma de Euler. Na parte (a), $C = \lim_{n\to\infty} \left(1 + \frac{1}{2} + \cdots + \frac{1}{n} - \log n\right)$ representa a constante de Euler. Na parte (b), $\zeta(s)$ é definida por

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

se $s > 1$, e pela equação

$$\zeta(s) = \lim_{x\to\infty}\left(\sum_{n\leq x}\frac{1}{n^s} - \frac{x^{1-s}}{1-s}\right),$$

se $0 < s < 1$.

O caso em que $s \in \mathbb{C}$, a função $\zeta(s)$ é conhecida como *função Zeta de Riemann*, para Re $s > 1$ e será estudada com mais detalhes no Capítulo 2.

Teorema 13. *Se $x \geq 1$ temos:*

(a) $\displaystyle\sum_{n\leq x}\frac{1}{n} = \log x + C + O\left(\frac{1}{x}\right)$.[2]

(b) $\displaystyle\sum_{n\leq x}\frac{1}{n^s} = \frac{x^{1-s}}{1-s} + \zeta(s) + O\left(x^{-s}\right)$, se $s > 0, s \neq 1$.

Demonstração. Para provar (a), tome $f(t) = 1/t$ na fórmula de soma de Euler (1.4) e temos

$$\begin{aligned}\sum_{n\leq x}\frac{1}{n} &= \int_1^x \frac{dt}{t} - \int_1^x \frac{t-\lfloor t\rfloor}{t^2}dt + 1 - \frac{x-[x]}{x}\\ &= \log x - \int_1^x \frac{t-\lfloor t\rfloor}{t^2}dt + 1 - O\left(\frac{1}{x}\right)\\ &= \log x + 1 - \int_1^\infty \frac{t-\lfloor t\rfloor}{t^2}dt + \int_x^\infty \frac{t-\lfloor t\rfloor}{t^2}dt - O\left(\frac{1}{x}\right)\\ &= \log x + C + O\left(\frac{1}{x}\right).\end{aligned}$$

pois $C = 1 - \displaystyle\int_1^\infty \frac{t-\lfloor t\rfloor}{t^2}dt$ e $\displaystyle\int_x^\infty \frac{t-\lfloor t\rfloor}{t^2}dt < \int_x^\infty \frac{dt}{t^2} = O\left(\frac{1}{x}\right)$. Para provar (b), tome $f(x) = x^{-s}$, onde $s > 0, s \neq 1$ na fórmula de soma de Euler (1.4) e temos

$$\begin{aligned}\sum_{n\leq x}\frac{1}{n^s} &= \int_1^x \frac{dt}{t^s} - s\int_1^x \frac{t-\lfloor t\rfloor}{t^{s+1}}dt + 1 - \frac{x-\lfloor x\rfloor}{x^s}\\ &= \frac{x^{1-s}}{1-s} - \frac{1}{1-s} + 1 - s\int_1^\infty \frac{t-\lfloor t\rfloor}{t^{s+1}}dt + O\left(x^{-s}\right)\\ &= \frac{x^{1-s}}{1-s} + \zeta(s) + O\left(x^{-s}\right).\end{aligned}$$

□

1.4 Somas Parciais do Produto de Dirichlet

Algumas somas envolvendo o Produto de Dirichlet e o Produto de Dirichlet Generalizado são recorrente nos problemas de Teoria Analítica dos Números já que eles permitem estudar

[2] Dizemos que $f(x) = O(g(x))$ se, e somente se, existe uma constante positiva M e um número real x_0 tal que $|f(x)| \leq M|g(x)|$ para todo $x \geq x_0$.

casos de primos sobre subconjuntos específicos dos inteiros, como veremos no Capítulo 3 deste trabalho.

Teorema 14. *Se $h = f * g$, seja*

$$H(x) = \sum_{n\leq x} h(n), \qquad F(x) = \sum_{n\leq x} f(n), \quad e \quad G(x) = \sum_{n\leq x} g(n).$$

Então, temos

$$H(x) = \sum_{n\leq x} f(n)G\left(\frac{x}{n}\right) = \sum_{n\leq x} g(n)F\left(\frac{x}{n}\right). \tag{1.5}$$

Demonstração. Vamos usar a propriedade associativa do Teorema 9. Seja $U(x) = 0$, para $0 < x < 1$, e $U(x) = 1$, para $x \geq 1$. Então $F = f \circ U$, $G = g \circ U$, e temos

$$f \circ G = f \circ (g \circ U) = (f * g) \circ U = H,$$
$$g \circ F = g \circ (f \circ U) = (g * f) \circ U = H.$$

Isso completa a demonstração. □

Observação 1. *Um caso particular do último Teorema é dada por*

$$F(x) = \sum_{n\leq x} f(n), \qquad G(x) = \sum_{n\leq x} g(n), \quad e \quad H(x) = \sum_{n\leq x} (f * g)(n)$$

então

$$H(x) = \sum_{n\leq x} \sum_{d|n} f(d)g\left(\frac{n}{d}\right) = \sum_{\substack{q,d \\ qd\leq x}} f(d)g(q).$$

O último resultado desta seção será usado no capitulo 3.

Teorema 15. *Se a e b são reais positivos tais que $ab = x$, então*

$$\sum_{\substack{q,d \\ qd\leq x}} f(d)g(q) = \sum_{n\leq a} f(n)G\left(\frac{x}{n}\right) + \sum_{n\leq b} g(n)F\left(\frac{x}{n}\right) - F(a)G(b).$$

Demonstração. O resultado segue da observação anterior (ver Apostol [1], página 70). □

1.5 Grupo de Caracteres

Nesta seção, apresentamos os principais conceitos relacionados com a Teoria dos Caracteres de Grupos Abelianos que são necessários para a prova do Teorema de Dirichlet. As noções incluem caráter de um grupo e relações de ortogonalidade.

Definição 3. *Seja G um grupo. Um caráter de G é uma função $f : G \to \mathbb{C}^*$ tal que $f(ab) = f(a)f(b)$, para todo $a, b \in G$.*

Teorema 16. *Se f é um caráter de um grupo finito G, onde e representa o elemento identidade, então $f(e) = 1$ e cada valor de $f(a)$ é uma raiz da unidade. De fato, se $a^n = e$ então $f(a)^n = 1$.*

Demonstração. Seja $c \in G$ tal que $f(c) \neq 0$. Como $ce = c$, temos $f(c)f(e) = f(c)$ então $f(e) = 1$. Se $a^n = e$, então $f(a)^n = f(a^n) = f(e) = 1$. □

Um caráter f de um grupo G é chamado *caráter principal* se $f(n) = 1$, para todo $n \in G$. Denotamos o caráter principal por f_1.

Definição 4. *Classes residuais módulo k é um conjunto de $\varphi(k)$ inteiros $\{a_1, \ldots, a_{\varphi(k)}\}$ incongruentes módulo k, onde cada um dos elementos é relativamente primo a k. Para cada inteiro a, a classe residual correspondente é $\hat{a} = \{x : x \equiv a \pmod{k}\}$.*

Definindo a multiplicação de classes residuais por $\hat{a}.\hat{b} = \widehat{ab}$, o conjunto das classes residuais módulo k forma um grupo abeliano finito de ordem $\varphi(k)$[3]. A identidade é a classe $\hat{1}$. O inverso de $\hat{a}$ é a classe $\hat{b}$ tal que $ab \equiv 1 \pmod{k}$.

Definição 5 (Caracteres de Dirichlet)**.** *Seja G um grupo de classes residuais módulo k. Para cada caráter f de G definimos uma função aritmética $\chi = \chi_f$ tal que:*

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

A função χ é chamada Caráter de Dirichlet módulo k. O caráter principal χ_1 é tal que

$$\chi_1(n) = \begin{cases} 1 & se\ (n,k) = 1, \\ 0 & se\ (n,k) > 1. \end{cases}$$

A partir dessa definição, temos que existem $\varphi(k)$ caracteres de Dirichlet módulo k distintos, tais que $\chi(mn) = \chi(m)\chi(n)$ e $\chi(n+k) = \chi(n)$, para todos m, n inteiros. No Teorema de Dirichlet, usaremos a seguinte relação de ortogonalidade para caracteres módulo k.

Teorema 17. *Sejam $\chi_1, \ldots \chi_{\varphi(k)}$ os $\varphi(k)$ caracteres de Dirichlet módulo k. Sejam m e n inteiros tais que $(m,k) = 1$. Então*

$$\sum_{r=1}^{\varphi(k)} \chi_r(m)\overline{\chi}_r(n) = \begin{cases} \varphi(k) & se\ m \equiv n \pmod{k}, \\ 0 & se\ m \not\equiv n \pmod{k}, \end{cases} \tag{1.6}$$

onde $\overline{\chi}_r$ representa o conjugado complexo.

Demonstração. Se $m \equiv n \pmod{k}$ então $\chi_r(m)\overline{\chi_r}(n) = \chi_r(m)\overline{\chi_r}(m) = 1$, assim a soma sobre todos os caratéres resulta $\varphi(k)$. Agora, se $m \not\equiv n \pmod{k}$ existe um carater χ_s tal que

[3](ver Apostol [1] página 135)

$\chi_s(m)\overline{\chi_s}(n) \neq 1$. Logo

$$(1-\chi_s(m)\overline{\chi_s}(n))\sum_{r=1}^{\varphi(k)}\chi_r(m)\overline{\chi}_r(n) = \sum_{r=1}^{\varphi(k)}\chi_r(m)\overline{\chi}_r(n) - \sum_{r=1}^{\varphi(k)}\chi_s(m)\overline{\chi_s}(n)\chi_r(m)\overline{\chi}_r(n)$$
$$= \sum_{r=1}^{\varphi(k)}\chi_r(m)\overline{\chi}_r(n) - \sum_{r=1}^{\varphi(k)}\chi_{sr}(m)\overline{\chi}_{sr}(n) = 0$$

Como $\chi_s(m)\overline{\chi_s}(n) \neq 1$. segue o resultado. □

Teorema 18. *Seja $\chi \neq \chi_1$ um caráter módulo k e seja f uma função não negativa que tenha derivada negativa contínua para todo $x \geq x_0$. Então se $y \geq x \geq x_0$, temos*

$$\sum_{x<n\leq y}\chi(n)f(n) = O(f(x)). \tag{1.7}$$

Além disso, se $f(x) \to 0$ quando $x \to \infty$, então a série infinita

$$\sum_{n=1}^{\infty}\chi(n)f(n)$$

converge, e para $x \geq x_0$,

$$\sum_{n\leq x}\chi(n)f(n) = \sum_{n=1}^{\infty}\chi(n)f(n) + O(f(x)). \tag{1.8}$$

Demonstração. Seja $A(x) = \sum_{n\leq x}\chi(n)$. Como $\chi \neq \chi_1$, temos

$$A(k) = \sum_{n=1}^{k}\chi(n) = 0.$$

Por periodicidade, segue que $A(nk) = 0$ para $n = 2, 3, \ldots$, então $|A(x)| < \phi(k)$ para todo x, isto é, $A(x) = O(1)$.

Agora, utilizando a Identidade de Abel[4]

$$\sum_{x<n\leq y}\chi(n)f(n) = f(y)A(y) - f(x)A(x) - \int_x^y A(t)f'(t)dt$$
$$= O(f(y)) + O(f(x)) + O\left(\int_x^y(-f'(t))dt\right) = O(f(x)).$$

Isso prova (1.7). Se $f(x) \to 0$ quando $x \to \infty$, então (1.7) mostra que a série

$$\sum_{n=1}^{\infty}\chi(n)f(n)$$

[4](ver Apostol [1] página 77)

converge pelo critério de Cauchy. Para provar (1.8), note que

$$\sum_{n=1}^{\infty}\chi(n)f(n)=\sum_{n\leq x}\chi(n)f(n)+\lim_{y\to\infty}\sum_{x<n\leq y}\chi(n)f(n).$$

Mas de (1.7) o limite da direita é da ordem $O(f(x))$. Logo, o Teorema está provado. □

Agora, aplicando o Teorema 18 com $f(x)=1/x$, $f(x)=(\log x)/x$ e $f(x)=1/\sqrt{x}$ para $x\geq 1$, temos:

Teorema 19. *Se χ é um caráter não principal módulo k e se $x\geq 1$, temos*

$$\sum_{n\leq x}\frac{\chi(n)}{n}=\sum_{n=1}^{\infty}\frac{\chi(n)}{n}+O\left(\frac{1}{x}\right). \tag{1.9}$$

$$\sum_{n\leq x}\frac{\chi(n)\log(n)}{n}=\sum_{n=1}^{\infty}\frac{\chi(n)\log(n)}{n}+O\left(\frac{\log x}{x}\right). \tag{1.10}$$

$$\sum_{n\leq x}\frac{\chi(n)}{\sqrt{n}}=\sum_{n=1}^{\infty}\frac{\chi(n)}{\sqrt{n}}+O\left(\frac{1}{\sqrt{x}}\right). \tag{1.11}$$

Denotamos por $L(1,\chi)$ a seguinte série:

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

onde $\chi\neq\chi_1$. Na prova do Teorema de Dirichlet precisamos mostrar que $L(1,\chi)\neq 0$. Em primeiro lugar vamos provar esse resultado para um caráter não principal real.

Teorema 20. *Seja χ um caráter real módulo k e seja*

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

Então $A(n)\geq 0$ para todo n, e $A(n)\geq 1$ se n é um quadrado.

Demonstração. Seja n uma potência de um primo p. Então

$$A(p^a)=\sum_{t=0}^{a}\chi(p^t)=1+\sum_{t=1}^{a}\chi(p^t).$$

Como χ é um caráter real, os únicos possíveis valores para $\chi(p)$ são 0,1 e -1. Se $\chi(p)=0$, então $A(p^a)=1$. Se $\chi(p)=1$, então $A(p^a)=a+1$ e se $\chi(p)=-1$, então $A(p^a)=0$ se a é ímpar e $A(p^a)=1$ se a é par. Em qualquer caso, $A(p^a)\geq 1$ se a for par.

Agora, seja $n=p_1^{a_1}\dots p_r^{a_r}$ então $A(n)=A(p_1^{a_1})\dots A(p_r^{a_r})$, pois A é multiplicativo. Cada fator $A(p_i^{a_i})\geq 0$, logo $A(n)\geq 0$. Além disso, se n for um quadrado, então cada expoente a_i é par, então cada fator $A(p_i^{a_i})\geq 1$, logo $A(n)\geq 1$. □

Teorema 21. *Para qualquer caráter real χ não principal módulo k, seja*

$$A(n) = \sum_{d|n} \chi(d) \text{ e } B(x) = \sum_{n\leq x} \frac{A(n)}{\sqrt{n}}.$$

Então:

(a) $B(x) \to \infty$, *quando* $x \to \infty$.

(b) $B(x) = 2\sqrt{x}L(1,\chi) + O(1)$, *para todo* $x \geq 1$.

Demonstração. (a) Do Teorema 20 temos

$$B(x) \geq \sum_{\substack{n\leq x,\\ n=m^2}} \frac{1}{\sqrt{n}} = \sum_{m\leq\sqrt{x}} \frac{1}{m},$$

onde a última soma representa a série harmônica que é divergente. Portanto, o resultado segue do critério da comparação.

(b) Escrevemos

$$B(x) = \sum_{n\leq x} \frac{1}{\sqrt{n}} \sum_{d|n} \chi(d) = \sum_{\substack{q,d\\ qd\leq x}} \frac{\chi(d)}{\sqrt{qd}}.$$

Agora, pelo Teorema 15, tome $a = b = \sqrt{x}$, $f(n) = \dfrac{\chi(n)}{\sqrt{n}}$ e $g(n) = \dfrac{1}{\sqrt{n}}$. Então

$$B(x) = \sum_{\substack{q,d\\ qd\leq x}} \frac{\chi(d)}{\sqrt{qd}} = \sum_{n\leq\sqrt{x}} \frac{\chi(n)}{\sqrt{n}} G\left(\frac{x}{n}\right) + \sum_{n\leq\sqrt{x}} \frac{1}{\sqrt{n}} F\left(\frac{x}{n}\right) - F(\sqrt{x})G(\sqrt{x}). \tag{1.12}$$

Pelo Teorema 13 temos

$$G(x) = \sum_{n\leq x} \frac{1}{\sqrt{n}} = 2\sqrt{x} + A + O\left(\frac{1}{\sqrt{x}}\right),$$

onde A é constante, e pelo Teorema 19 temos

$$F(x) = \sum_{n\leq x} \frac{\chi(n)}{\sqrt{n}} = B + O\left(\frac{1}{\sqrt{x}}\right),$$

onde $B = \sum_{n=1}^{\infty} \chi(n)/\sqrt{n}$. Como $F(\sqrt{x})G(\sqrt{x}) = 2Bx^{1/4} + O(1)$, por (1.12) temos

$$\begin{aligned}
B(x) =& \sum_{n\leq\sqrt{x}} \frac{\chi(n)}{\sqrt{n}} \left[2\sqrt{\frac{x}{n}} + A + O\left(\sqrt{\frac{n}{x}}\right)\right] \\
&+ \sum_{n\leq\sqrt{x}} \frac{1}{\sqrt{n}} \left[B + O\left(\sqrt{\frac{n}{x}}\right)\right] - 2Bx^{1/4} + O(1) \\
=& 2\sqrt{x} \sum_{n\leq\sqrt{x}} \frac{\chi(n)}{n} + A \sum_{n\leq\sqrt{x}} \frac{\chi(n)}{\sqrt{n}} + O\left(\frac{1}{\sqrt{x}} \sum_{n\leq\sqrt{x}} |\chi(n)|\right) \\
&+ B \sum_{n\leq\sqrt{x}} \frac{1}{\sqrt{n}} + O\left(\frac{1}{\sqrt{x}} \sum_{n\leq\sqrt{x}} 1\right) - 2Bx^{1/4} + O(1) \\
=& 2\sqrt{x}L(1,\chi) + O(1).
\end{aligned}$$

Isso prova a parte (b).

□

Dessa forma, de *(a)* e *(b)* concluímos que $L(1,\chi) \neq 0$.

2. O Teorema dos Números Primos

Sejam $f(x)$ e $g(x)$ funções reais não nulas para x suficientemente grande. Se

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

dizemos que f é *assintoticamente equivalente a* g, e escrevemos $f(x) \sim g(x)$.

O seguinte resultado foi primeiro conjecturado por Legendre por volta de 1798 e talvez alguns anos antes pelo jovem Gauss, sendo mais tarde provado independentemente por Hadamard [7] e de la Vallee Poussin [12] em 1896 com métodos de análise complexa, baseados no artigo de Riemann [9]. Este capítulo está baseado no artigo [6].

Teorema 22 (**Teorema dos Números Primos (TNP)**). *Seja $\pi(x)$ uma função que determina o número de primos menores ou iguais a x. Então*

$$\pi(x) \sim Li(x),$$

onde

$$Li(x) = \int_2^x \frac{dt}{\log t}$$

é a integral logarítmica.

A integral logarítmica fornece aproximações surpreendentes, mas infelizmente não pode ser avaliada de forma fechada. Desse modo, é conveniente substituir $Li(x)$ por uma função mais simples que seja assintoticamente equivalente a ela. A regra de L'Hopital e o Teorema Fundamental do Cálculo implicam que

$$\lim_{x\to\infty} \frac{Li(x)}{x/\log x} = \lim_{x\to\infty} \frac{\dfrac{1}{\log x}}{\dfrac{\log x - x\dfrac{1}{x}}{(\log x)^2}} = \lim_{x\to\infty} \frac{1}{1-\dfrac{1}{\log x}} = 1.$$

Logo $Li(x) \sim \dfrac{x}{\log x}$.

No entanto, a integral logarítmica fornece uma melhor aproximação para $\pi(x)$. Vamos provar o TNP na seguinte forma equivalente:

Teorema 23 (**Teorema dos Números Primos**). $\pi(x) \sim \dfrac{x}{\log x}$.

A prova possui simplificações modernas devido a Newman e Zagier, no entanto ainda é difícil e envolve técnicas e ferramentas de análise complexa. Em 1948, Erdos [5] e Selberg [11] encontraram independentemente provas do Teorema dos Números Primos que não faz uso de análise complexa. Essas provas elementares são mais difíceis que a abordagem apresentada aqui.

Observação 2. *O TNP implica que $p_n \sim n \log n$, onde p_n denota o n-ésimo número primo. De fato, como $\pi(p_n) = n$, substituindo $q = p_n$ temos*

$$\lim_{n\to\infty} \frac{n \log n}{p_n} = \lim_{n\to\infty} \frac{\pi(p_n) \log p_n}{p_n} \left(\frac{\log n}{\log p_n}\right) = \lim_{q\to\infty} \frac{\log \pi(q)}{\log q} = \lim_{q\to\infty} \left(\frac{\log 1}{\log q} + 1 - \frac{\log \log q}{\log q}\right) = 1.$$

2.1 A função Zeta de Riemann

Ao estudar a distribuição dos números primos em seus trabalhos, Euler mostrou que a série dos inversos dos números primos é divergente, baseando-se na identidade que será apresentada a seguir, conhecida como *Produto de Euler*.

Euler e Chebyshev usaram essa identidade considerando s uma variável real. Riemann, em 1858, tratou s como uma variável complexa e estudou a série com base na teoria das funções analíticas. Usou a letra grega zeta para denotar a função, e com base nisso ficou conhecida como *função Zeta de Riemann*. O matemático anunciou algumas propriedades importantes desta função, porém suas provas eram incompletas. Mais tarde, seu trabalho foi completado por Hadamard, em 1893, e por Mangoldt, em 1894.

A função Zeta de Riemann é definida por

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \tag{2.1}$$

para $\operatorname{Re} s > 1$. Suponha que $\operatorname{Re} s \geq \sigma > 1$. Como

$$|n^s| = |e^{s \log n}| = e^{Re\,(s \log n)} = n^{Re\, s} \geq n^{\sigma}$$

segue que

$$\left|\sum_{n=1}^{\infty} \frac{1}{n^s}\right| \leq \sum_{n=1}^{\infty} \frac{1}{n^{\sigma}} < \infty.$$

Pelo teste M de Weierstrass, temos que (2.1) converge absolutamente e uniformemente em $\operatorname{Re} s \geq \sigma$. Como $\sigma > 1$ é arbitrário e cada soma em (2.1) é analítica em $\operatorname{Re} s > 1$, concluímos que (2.1) converge de forma uniforme localmente em $\operatorname{Re} s > 1$ para uma função analítica.

No que segue, p denota um número primo e uma soma ou produto indexado por p percorre todos os números primos. Aqui está a conexão entre a função zeta e os primos.

Teorema 24 (**Fórmula do Produto de Euler**). *Se* $\operatorname{Re} s > 1$, *então* $\zeta(s) \neq 0$ *e*

$$\zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}. \tag{2.2}$$

A convergência é localmente uniforme em $\operatorname{Re} s > 1$.

Demonstração. Como $|p^{-s}| = p^{-\operatorname{Re} s} < 1$ para $\operatorname{Re} s > 1$, temos que a série geométrica

$$\left(1 - \frac{1}{p^s}\right)^{-1} = \sum_{n=0}^{\infty} \left(\frac{1}{p^s}\right)^n = \sum_{n=0}^{\infty} \frac{1}{p^{ns}},$$

é absolutamente convergente. Uma vez que um número finito de séries absolutamente convergentes pode ser multiplicado termo a termo, segue que

$$\begin{aligned}\left(1 - \frac{1}{2^s}\right)^{-1}\left(1 - \frac{1}{3^s}\right)^{-1} &= \left(1 + \frac{1}{2^s} + \frac{1}{2^{2s}} + \dots\right)\left(1 + \frac{1}{3^s} + \frac{1}{3^{2s}} + \dots\right) \\ &= 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{6^s} + \frac{1}{8^s} + \frac{1}{9^s} + \frac{1}{12^s} + \dots,\end{aligned}$$

em que aparecem apenas os números naturais divisíveis pelos primos 2 ou 3. Similarmente,

$$\begin{aligned}\prod_{p\leq 5}\left(1 - \frac{1}{p^s}\right)^{-1} &= \left(1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{6^s} + \frac{1}{8^s} + \frac{1}{9^s} + \frac{1}{12^s} + \dots\right)\left(1 + \frac{1}{5^s} + \frac{1}{5^{2s}} + \dots\right) \\ &= 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \frac{1}{6^s} + \frac{1}{8^s} + \frac{1}{9^s} + \frac{1}{10^s} + \frac{1}{12^s} + \dots,\end{aligned}$$

em que aparecem apenas os números naturais divisíveis pelos primos 2, 3 ou 5. Como os fatores primos de cada $n \leq N$ são no máximo N, e como a cauda de uma série convergente tende a 0, segue que para $\operatorname{Re} s \geq \sigma > 1$

$$\left|\zeta(s) - \prod_{p\leq N}\left(1 - \frac{1}{p^s}\right)^{-1}\right| \leq \sum_{n>N}\left|\frac{1}{n^s}\right| \leq \sum_{n=N}^{\infty}\frac{1}{n^\sigma} \to 0$$

para $N \to \infty$. Isso prova (2.2) e prova que a convergência é localmente uniforme em $\operatorname{Re} s > 1$. Como cada produto parcial é não nulo em $\operatorname{Re} s > 1$ e o limite $\zeta(s)$ não é zero, o Teorema de Hurwitz[1] garante que $\zeta(s) \neq 0$ para $\operatorname{Re} s > 1$. □

Observação 3. *O Produto de Euler implica no Teorema de Euclides sobre a infinidade dos primos. De fato, se houvesse finitos primos, então o lado direito de* (2.2) *convergiria para um limite finito quando* $s \to 1^+$. *No entanto, o lado esquerdo de* (2.2) *diverge quando* $s \to 1^+$ *visto que seus termos tendem aos da série harmônica.*

Agora, vamos provar que a função zeta de Riemann pode ser prolongada analiticamente até $\operatorname{Re} s > 0$, com exceção de $s = 1$, onde $\zeta(s)$ tem um polo simples.

[1] (ver Bak [2] página 139)

Teorema 25. *$\zeta(s)$ pode ser prolongada analiticamente para $\operatorname{Re} s > 0$ exceto para um polo simples em $s = 1$ com resíduo 1.*

Demonstração. Seja $\lfloor x \rfloor$ o único número inteiro tal que $\lfloor x \rfloor \leq x < \lfloor x \rfloor + 1$, em particular, $0 \leq x - \lfloor x \rfloor < 1$. Para $\operatorname{Re} s > 2$,

$$\begin{aligned}
\zeta(s) &= \sum_{n=1}^{\infty} \frac{1}{n^s} = \sum_{n=1}^{\infty} \frac{n-(n-1)}{n^s} \\
&= \sum_{n=1}^{\infty} \frac{n}{n^s} - \sum_{n=2}^{\infty} \frac{n-1}{n^s} \\
&= \sum_{n=1}^{\infty} \frac{n}{n^s} - \sum_{n=1}^{\infty} \frac{n}{(n+1)^s} \\
&= \sum_{n=1}^{\infty} n \left(s \int_n^{n+1} \frac{dx}{x^{s+1}} \right) \\
&= s \sum_{n=1}^{\infty} \int_n^{n+1} \frac{\lfloor x \rfloor dx}{x^{s+1}} = s \int_1^{\infty} \frac{\lfloor x \rfloor dx}{x^{s+1}}.
\end{aligned}$$

Observe que para $\operatorname{Re} s > 0$,

$$\int_1^{\infty} \frac{dx}{x^s} = \frac{1}{s-1} \implies \frac{1}{s-1} + 1 - s \int_1^{\infty} \frac{x dx}{x^{s+1}} = 0$$

e portanto

$$\begin{aligned}
\zeta(s) &= s \int_1^{\infty} \frac{\lfloor x \rfloor dx}{x^{s+1}} \\
&= \left(\frac{1}{s-1} + 1 - s \int_1^{\infty} \frac{x dx}{x^{s+1}} \right) + s \int_1^{\infty} \frac{\lfloor x \rfloor dx}{x^{s+1}} \\
&= \frac{1}{s-1} + 1 - s \int_1^{\infty} \frac{x - \lfloor x \rfloor}{x^{s+1}} dx.
\end{aligned}$$

Se mostrarmos que a integral acima define uma função analítica em $\operatorname{Re} s > 0$, então $\zeta(s)$ pode ser prolongada analiticamente para $\operatorname{Re} s > 0$, exceto para um pólo simples em $s = 1$ com resíduo 1. Para $n = 1, 2, 3, \ldots$, seja

$$f_n(s) = \int_n^{n+1} \frac{x - \lfloor x \rfloor}{x^{s+1}} dx.$$

Para qualquer curva fechada simples γ em $\operatorname{Re} s > 0$, o Teorema de Fubini e o Teorema de

Cauchy[2] implicam que

$$\begin{aligned}\int_\gamma f_n(s) &= \int_\gamma \int_n^{n+1} \frac{x-\lfloor x\rfloor}{x^{s+1}} dx ds \\ &= \int_n^{n+1} (x-\lfloor x\rfloor)\left(\int_\gamma \frac{ds}{x^{s+1}}\right) dx = 0.\end{aligned}$$

O Teorema de Morera[3] garante que cada f_n é analítica em $\operatorname{Re} s > 0$. Se $\operatorname{Re} s \geq \sigma > 0$, então

$$\begin{aligned}\sum_{n=1}^{\infty} |f_n(s)| &= \sum_{n=1}^{\infty} \left| \int_n^{n+1} \frac{x-\lfloor x\rfloor}{x^{s+1}} dx \right| \\ &\leq \sum_{n=1}^{\infty} \int_n^{n+1} \left| \frac{x-\lfloor x\rfloor}{x^{s+1}} \right| dx \\ &\leq \sum_{n=1}^{\infty} \int_n^{n+1} \frac{dx}{x^{Re\ (s+1)}} \\ &\leq \int_1^{\infty} \frac{dx}{x^{\sigma+1}} = \frac{1}{\sigma} < \infty.\end{aligned}$$

Consequentemente, o Teste M de Weierstrass implica que

$$\sum_{n=1}^{\infty} f_n(s) = \int_1^{\infty} \frac{x-\lfloor x\rfloor}{x^{s+1}} dx \tag{2.3}$$

converge absolutamente e uniformemente em $\operatorname{Re} s \geq \sigma$. Como $\sigma > 0$ é arbitrário, segue que a série converge localmente uniforme em $\operatorname{Re} s > 0$. Sendo o limite localmente uniforme de funções analíticas em $\operatorname{Re} s > 0$, concluímos que (2.3) é analítico. □

Observação 4. *Acontece que $\zeta(s)$ pode ser prolongada analiticamente até $\mathbb{C}\backslash\{1\}$. O argumento envolve a introdução da função gama para obter a equação funcional*

$$\zeta(s) = 2^s \pi^{s-1} \operatorname{sin}\left(\frac{\pi s}{2}\right) \Gamma(1-s)\zeta(1-s). \tag{2.4}$$

A função zeta estendida tem zeros em -2, -4, -6,... (os zeros triviais), junto com infinitos zeros na faixa crítica $0 < Re\, s < 1$ (os zeros não triviais).

Os primeiros 10^{13} zeros não triviais encontram-se na linha crítica $Re\, s = \frac{1}{2}$. A famosa Hipótese de Riemann afirma que todos os zeros na faixa crítica estão na linha crítica. Este problema foi colocado pela primeira vez por Riemann em 1859 e permanece sem solução. É considerado o problema aberto mais importante na matemática por causa do impacto que teria sobre a distribuição dos números primos.

Observação 5. *O erro na estimativa fornecida pelo Teorema dos Números Primos está vinculado aos zeros da função Zeta. Pode-se mostrar que se $\zeta(s) \neq 0$ para $Re\, s > \Theta$, então existe*

[2](ver Bak [2] página 111)
[3](ver Bak [2] página 98)

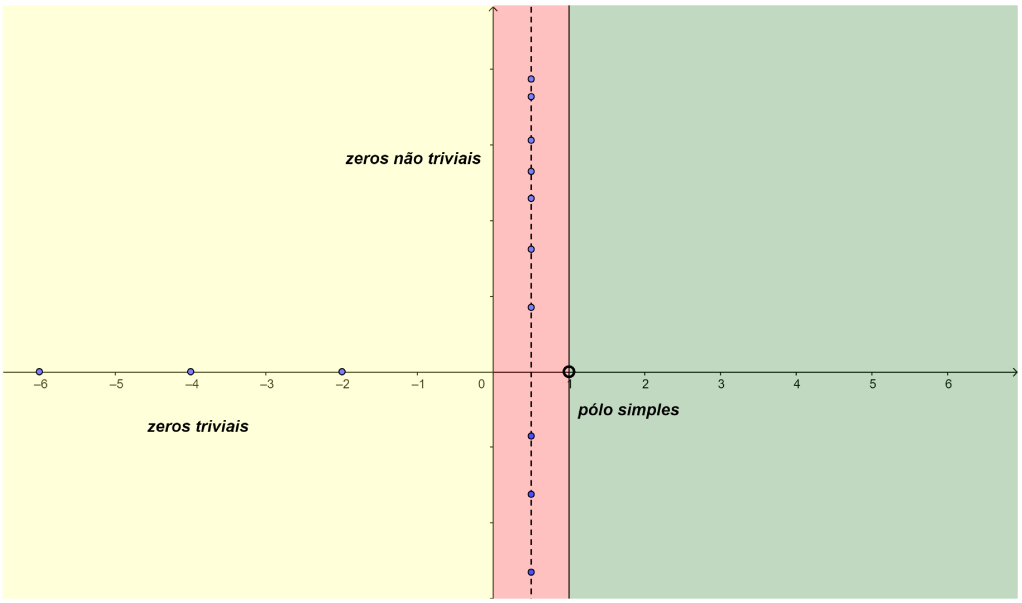

Figura 2.1: Prolongamento analítico da função $\zeta(s)$ para $\mathbb{C}\backslash\{1\}$. Os zeros não triviais da função zeta encontram-se na *faixa crítica* $0 < \operatorname{Re} s < 1$.

uma constante C_Θ *tal que*

$$|\pi(x) - Li(x)| \leq C_\Theta x^\theta \log x$$

para todo $x \geq 2$ *[10]. Uma vez que se sabe que a função zeta possui infinitos zeros na linha crítica* $Re\ s = \frac{1}{2}$*, devemos ter* $\Theta \geq \frac{1}{2}$.

Agora, iremos estabelecer uma representação em série do logaritmo da função zeta. Vamos usar isso para estabelecer $\zeta(s) \neq 0$ em $\operatorname{Re} s = 1$ e em seguida para obter uma prolongação analítica de uma função intimamente relacionada.

Lema 1. *Se* $Re\, s > 1$*, então* $\log \zeta(s) = \sum_{n=1}^{\infty} \frac{c_n}{n^s}$*, no qual* $c_n \geq 0$ *para* $n \in \mathbb{N}$.

Demonstração. O semiplano aberto $\operatorname{Re} s > 1$ é simplesmente conexo e pelo Teorema 24 $\zeta(s) \neq 0$ nessa região. Assim, podemos definir um ramo de $\log \zeta(s)$ para $\operatorname{Re} s > 1$ tal que $\log \zeta(\sigma) \in \mathbb{R}$ para $\sigma > 1$. Lembre que

$$\log\left(\frac{1}{1-z}\right) = \sum_{k=1}^{\infty} \frac{z^k}{k} \tag{2.5}$$

para $|z| < 1$ e observe que $\operatorname{Re} s > 1$ implica $|p^{-s}| = p^{-Re\ s} < 1$, que permite considerar $z = p^{-s}$ em (2.5). Na fórmula do produto de Euler, a função $\zeta(s)$ não é identicamente nula para $\operatorname{Re} s > 1$, e a continuidade do logaritmo implicam que

$$\log \zeta(s) = \log \prod_p \left(\frac{1}{1-p^{-s}}\right) = \sum_p \log\left(\frac{1}{1-p^{-s}}\right) \tag{2.6}$$

$$= \sum_p \sum_{k=1}^{\infty} \frac{(p^{-s})^k}{k} = \sum_p \sum_{k=1}^{\infty} \frac{1/k}{(p^k)^s} = \sum_{n=1}^{\infty} \frac{c_n}{n^s}, \tag{2.7}$$

no qual $c_n = 1/k$ se $n = p^k$, e $c_n = 0$ caso contrário. □

Lema 2. *Se $s = \sigma + it$, no qual $\sigma > 1$ e $t \in \mathbb{R}$, então*

$$\log|\zeta(s)| = \sum_{n=1}^{\infty} \frac{c_n \cos(t \log n)}{n^{\sigma}},$$

para $c_n = 1/k$ se $n = p^k$, e $c_n = 0$ caso contrário.

Demonstração. Como $\sigma = \mathrm{Re}\, s > 1$, do Lema anterior e do produto de Euler temos

$$\log|\zeta(s)| = Re\,(\log\zeta(s)) = Re \sum_{n=1}^{\infty} \frac{c_n}{n^{\sigma+it}} = Re \sum_{n=1}^{\infty} \frac{c_n}{e^{(\sigma+it)\log n}} = \sum_{n=1}^{\infty} \frac{c_n \cos t \log n}{n^{\sigma}}.$$

□

Observação 6. *Uma consequência de (2.6) é que a série dos inversos dos primos diverge. Suponha por contradição que $\sum_p p^{-1}$ converge. Para $|z| < \frac{1}{2}$, (2.5) implica*

$$\left|\log\left(\frac{1}{1-z}\right)\right| = \left|\sum_{k=1}^{\infty} \frac{z^k}{k}\right| \leq \sum_{k=1}^{\infty} |z|^k = \frac{|z|}{1-|z|} \leq 2|z|. \tag{2.8}$$

Para $s > 1$, (2.6) e a desigualdade anterior implicam

$$\log\zeta(s) = \sum_p \log\left(\frac{1}{1-p^{-s}}\right) < 2\sum_p \frac{1}{p^s} \leq 2\sum_p \frac{1}{p} < \infty.$$

Isso contradiz o fato de que $\zeta(s)$ tem um pólo em $s = 1$. Logo $\sum_p p^{-1}$ diverge.

O seguinte resultado nos diz que a função Zeta estendida é não nula na linha vertical Re $s = 1$. Pode-se mostrar que esta afirmação é equivalente ao Teorema dos Números Primos, embora nosso objetivo é apenas derivar o Teorema dos Números Primos a partir dela.

Teorema 26. *$\zeta(s)$ não tem zeros sobre $Re\, s = 1$.*

Demonstração. Lembre que $\zeta(s)$ tem um pólo simples em $s = 1$. Em particular, $\zeta(s)$ é não nula para $s = 1$. Suponha por contradição que $\zeta(1 + it) = 0$ para algum $t \in \mathbb{R}\backslash\{0\}$ e considere

$$f(s) = \zeta^3(s)\zeta^4(s + it)\zeta(s + 2it).$$

Observe que

(i) $\zeta^3(s)$ tem um pólo de ordem três em $s = 1$, pois $\zeta(s)$ tem um pólo simples em $s = 1$.

(ii) $\zeta^4(s + it)$ tem um zero de ordem pelo menos quatro em $s = 1$, pois $\zeta(1 + it) = 0$.

(iii) $\zeta(s + 2it)$ não tem polo em $s = 1$, pois $t \in \mathbb{R}\backslash\{0\}$ e $s = 1$ é o único pólo de $\zeta(s)$ em $Re\, s = 1$.

Assim, a singularidade de f em $s = 1$ é removível e $f(1) = 0$. Portanto

$$\lim_{s\to 1} \log|f(s)| = -\infty. \tag{2.9}$$

Por outro lado, pelo Lema 2 temos

$$\begin{aligned}\log|f(s)| &= 3\log|\zeta(s)| + 4\log|\zeta(s+it)| + \log|\zeta(s+2it)| \\ &= 3\sum_{n=1}^{\infty}\frac{c_n}{n^\sigma} + 4\sum_{n=1}^{\infty}\frac{c_n\cos(t\log n)}{n^\sigma} + \sum_{n=1}^{\infty}\frac{c_n\cos(2t\log n)}{n^\sigma} \\ &= \sum_{n=1}^{\infty}\frac{c_n}{n^\sigma}(3 + 4\cos(t\log n) + \cos(2t\log n)) \geq 0,\end{aligned}$$

pois $c_n \geq 0$ para todo $n \in \mathbb{N}$ e $3 + 4\cos x + \cos 2x = 2(1+\cos x)^2 \geq 0$, para todo $x \in \mathbb{R}$.

Logo, isso contradiz (2.9). Portanto $\zeta(s)$ não tem zeros sobre $\operatorname{Re} s = 1$. □

2.2 Funções de Chebyshev

É conveniente abordar problemas relacionados a números primos com somas ponderadas logaritmicamente. Em vez de trabalhar com $\pi(x) = \sum_{p\leq x} 1$, consideramos

$$\vartheta(x) = \sum_{p\leq x}\log p. \tag{2.10}$$

Vamos provar que o TNP é equivalente à afirmação $\vartheta(x) \sim x$. Já que essa equivalência assintótica é difícil de estabelecer, primeiro nos contentamos com um limite superior.

Lema 3 (**Lema de Chebyshev**).

$$\vartheta(x) \leq 3x.$$

Demonstração. O Teorema Binomial implica que

$$\begin{aligned}2^{2n} = (1+1)^{2n} &= \sum_{k=0}^{2n}\binom{2n}{k}1^k 1^{2n-k} \geq \binom{2n}{n} \geq \prod_{n<p\leq 2n} p \\ &= \prod_{n<p\leq 2n} e^{\log p} = \exp\left(\sum_{n<p\leq 2n}\log p\right) = \exp(\vartheta(2n) - \vartheta(n)).\end{aligned}$$

Portanto, $\vartheta(2n) - \vartheta(n) \leq 2n\log 2$. Tome $n = 2^{k-1}$. Como $\vartheta(1) = 0$, por série telescópica e a fórmula de soma para uma série geométrica finita temos

$$\begin{aligned}\vartheta(2^k) = \vartheta(2^k) - \vartheta(2^0) &= \sum_{i=1}^{k}(\vartheta(2^i) - \vartheta(2^{i-1})) \\ &\leq \sum_{i=1}^{k} 2^i\log 2 < (1 + 2 + 2^2 + \cdots + 2^k)\log 2 < 2^{k+1}\log 2.\end{aligned}$$

Se $x \geq 1$, então tome $2^k \leq x < 2^{k+1}$, isto é, tome $k = \lfloor \log x / \log 2 \rfloor$. Então

$$\vartheta(x) \leq \vartheta(2^{k+1}) \leq 2^{k+2} \log 2 = 4.2^k \log 2 \leq x(4 \log 2) < 3x.$$

□

Introduzimos agora uma função cuja relevância para os números primos é evidente a partir de sua definição.

$$\Phi(s) = \sum_p \frac{\log p}{p^s}. \tag{2.11}$$

Se $\operatorname{Re} s \geq \sigma > 1$, então

$$\sum_p \left| \frac{\log p}{p^s} \right| \leq \sum_p \frac{\log p}{p^{Re\, s}} \leq \sum_p \frac{\log p}{p^\sigma} < \sum_{n=1}^{\infty} \frac{\log n}{n^\sigma} < \infty$$

pelo Teste da Integral. O Teste M de Weierstrass garante que (2.11) converge uniformemente em $\operatorname{Re} s \geq \sigma$. Como as somas em (2.11) são analíticas em $\operatorname{Re} s > 1$ e $\sigma > 1$ é arbitrário, a série (2.11) converge localmente de forma uniforme em $\operatorname{Re} s > 1$ então $\Phi(s)$ é analítica em $\operatorname{Re} s > 1$. Para o Teorema dos Números Primos, precisamos de um pouco mais.

Teorema 27. $\Phi(s) - \dfrac{1}{s-1}$ *é analítica em um aberto que contém* $Re\, s \geq 1$.

Demonstração. Para $\operatorname{Re} s > 1$, temos

$$\log \zeta(s) = \log \left(\prod_p (1 - p^{-s})^{-1} \right) = -\sum_p \log\left(1 - p^{-s}\right). \tag{2.12}$$

Por (2.8), temos $\log |1 - p^{-s}| \leq \dfrac{2}{p^{Re\, s}}$, o que implica que a convergência em (2.12) é localmente uniforme em $\operatorname{Re} s > 1$. Consequentemente, podemos tomar a derivada de (2.12) termo a termo e obter

$$\begin{aligned} -\frac{\zeta'(s)}{\zeta(s)} &= \sum_p \frac{(\log p) p^{-s}}{1 - p^{-s}} = \sum_p \log p \left(\frac{1}{p^s - 1} \right) \\ &= \sum_p \log p \left(\frac{1}{p^s} + \frac{1}{p^s(p^s - 1)} \right) = \Phi(s) + \sum_p \frac{\log p}{p^s(p^s - 1)}. \end{aligned}$$

Se $\operatorname{Re} s \geq \sigma > \frac{1}{2}$, então pelo Teste de Comparação e o Teste da Integral temos

$$\sum_p \left| \frac{\log p}{p^s(p^s - 1)} \right| \leq \sum_{n=2}^{\infty} \frac{\log n}{(n^{Re\, s} - 1)^2} \leq \sum_{n=2}^{\infty} \frac{\log n}{(n^\sigma - 1)^2} < \sum_{n=2}^{\infty} \frac{\log n}{n^{2\sigma}} < \int_2^{\infty} \frac{\log t}{t^{2\sigma}} < \infty.$$

O Teste M de Weierstrass garante que

$$\sum_p \frac{\log p}{p^s(p^s - 1)}$$

converge localmente uniforme em $\operatorname{Re} s > \frac{1}{2}$ e é analítica nesta região. O Teorema 25 implica

$$\Phi(s) = -\frac{\zeta'(s)}{\zeta(s)} - \sum_p \frac{\log p}{p^s(p^s-1)}$$

estende-se meromorficamente para $\operatorname{Re} s > \frac{1}{2}$ com pólos apenas em $s = 1$ e os zeros de $\zeta(s)$. O Teorema 25 implica que $\zeta(s) = (s-1)^{-1}Z(s)$, com $Z(1) = 1$, onde $Z(s)$ é analítica próximo de $s = 1$. Consequentemente,

$$\frac{\zeta'(s)}{\zeta(s)} = \frac{-1(s-1)^{-2}Z(s) + (s-1)^{-1}Z'(s)}{(s-1)^{-1}Z(s)} = -\frac{1}{s-1} + \frac{Z'(s)}{Z(s)}$$

e então

$$\Phi(s) - \frac{1}{s-1} = -\frac{Z'(s)}{Z(s)} - \sum_p \frac{\log p}{p^s(p^s-1)},$$

no qual o lado direito é meromorfo em $\operatorname{Re} s > \frac{1}{2}$ com pólos apenas nos zeros de $\zeta(s)$. O Teorema 26 garante que ζ não tem zeros sobre $\operatorname{Re} s = 1$, então o lado direito se estende analiticamente para alguma vizinhança aberta de $\operatorname{Re} s \geq 1$. □

2.3 Transformada de Laplace

Os métodos de transformação de Laplace são comumente usados para estudar equações diferenciais e muitas vezes aparecem com destaque em textos de variáveis complexas. Precisamos apenas da definição básica e um resultado de convergência simples. O seguinte Teorema não é declarado com a maior generalidade possível, mas é suficiente para nossos propósitos.

Teorema 28. *Seja $f : [0, \infty) \to \mathbb{C}$ contínua por partes em $[0, a]$ para todo $a > 0$ e*

$$|f(t)| \leq Ae^{Bt}$$

para $t \geq 0$. Então a transformada de Laplace

$$g(z) = \int_0^\infty f(t)e^{-zt}dt \tag{2.13}$$

de f está bem definida e é analítica em $\operatorname{Re} z > B$.

Demonstração. Para $\operatorname{Re} z > B$, a integral (2.13) converge pelo Teste da Comparação. De fato,

$$\int_0^\infty |f(t)e^{-zt}|dt \leq \int_0^\infty Ae^{Bt}e^{-t(\operatorname{Re} z)}dt = A\int_0^\infty e^{t(B-\operatorname{Re} z)}dt = \frac{A}{\operatorname{Re} z - B} < \infty.$$

Se γ é uma curva fechada simples em $\operatorname{Re} z > B$, então existe um $\sigma > B$ tal que $\operatorname{Re} z \geq \sigma$ para todo $z \in \gamma$. Então

$$\int_0^\infty |f(t)e^{-zt}|dt \leq \frac{A}{\sigma - B}$$

é uniformemente limitado para $z \in \gamma$. O Teorema de Fubini e o Teorema de Cauchy implicam

$$\int_\gamma g(z)dz = \int_\gamma \int_0^\infty f(t)e^{-zt}dtdz = \int_0^\infty f(t)\left(\int_\gamma e^{-zt}dz\right) = \int_0^\infty f(t).0dt = 0.$$

O Teorema de Morera garante que g é analítica em $\operatorname{Re} z > B$. □

Teorema 29 (**Representação de Laplace de Φ**). *Para $Re\, s > 1$*

$$\frac{\Phi(s)}{s} = \int_0^\infty \vartheta(e^t)e^{-st}dt. \tag{2.14}$$

Demonstração. Para $\operatorname{Re} s > 2$ e pelo Lema de Chebyshev, temos

$$\sum_{n=1}^\infty \left|\frac{\vartheta(n-1)}{n^s}\right| \leq \sum_{n=1}^\infty \left|\frac{\vartheta(n)}{n^s}\right| \leq \sum_{n=1}^\infty \frac{3n}{n^{Re\, s}} = 3\sum_{n=1}^\infty \frac{1}{n^{(Re\, s)-1}} < \infty. \tag{2.15}$$

Consequentemente,

$$\begin{aligned}
\Phi(s) &= \sum_p \frac{\log p}{p^s} \\
&= \sum_{n=1}^\infty \frac{\vartheta(n) - \vartheta(n-1)}{n^s} \\
&= \sum_{n=1}^\infty \frac{\vartheta(n)}{n^s} - \sum_{n=2}^\infty \frac{\vartheta(n-1)}{n^s} && \text{(por (2.15))} \\
&= \sum_{n=1}^\infty \frac{\vartheta(n)}{n^s} - \sum_{n=1}^\infty \frac{\vartheta(n)}{(n+1)^s} \\
&= \sum_{n=1}^\infty \vartheta(n)\left(\frac{1}{n^s} - \frac{1}{n^{s+1}}\right) \\
&= \sum_{n=1}^\infty \vartheta(n)\left(s\int_n^{n+1} \frac{dx}{x^{s+1}}\right) \\
&= s\sum_{n=1}^\infty \int_n^{n+1} \frac{\vartheta(x)dx}{x^{s+1}} && \text{(pois } \vartheta(x) = \vartheta(n) \text{ para } x \in [n, n+1)) \\
&= s\int_1^\infty \frac{\vartheta(x)dx}{x^{s+1}} \\
&= s\int_0^\infty \frac{\vartheta(e^t)e^t dt}{e^{st+t}} && \text{(mudança de variável } x = e^t) \\
&= s\int_0^\infty \vartheta(e^t)e^{-st}dt.
\end{aligned}$$

Isso estabelece a identidade desejada para $\operatorname{Re} s > 2$. O Teorema 3 implica $\vartheta(e^t) \leq 3e^t$, Teorema 28 (com $A = 3$ e $B = 1$) garante que a última integral é analítica em $\operatorname{Re} s > 1$. Por outro lado, $\Phi(s)$ é analítica em $\operatorname{Re} s > 1$, então o Princípio de Identidade implica que a representação desejada (2.14) vale para $\operatorname{Re} s > 1$. □

No Teorema a seguir, observe que g é a Transformada de Laplace de f. As hipóteses sobre f garantem que seremos capazes de aplicar o Teorema à função Theta de Chebyshev.

Teorema 30 (**Teorema Tauberiano de Newman**). *Seja $f : [0, \infty) \to \mathbb{C}$ uma função limitada e contínua por partes em $[0, a]$ para cada $a > 0$. Para $\operatorname{Re} z > 0$, seja*

$$g(z) = \int_0^\infty f(t)e^{-zt}dt$$

e suponha que g possui uma extensão analítica para uma vizinhança de $\operatorname{Re} z \geq 0$. Então

$$g(0) = \lim_{T\to\infty} \int_0^T f(t)dt.$$

Demonstração. Para cada $T \in (0, \infty)$, seja

$$g_T(z) = \int_0^T f(t)e^{-zt}dt. \tag{2.16}$$

A prova do Teorema 28 garante que cada $g_T(z)$ é uma função inteira e $g(z)$ é analítica em Re $z > 0$. Devemos mostrar que

$$\lim_{T\to\infty} g_T(0) = g(0). \tag{2.17}$$

De fato, seja $\|f\|_\infty = \sup_{t\geq 0} |f(t)|$ que é finito por suposição. Para $\operatorname{Re} z > 0$,

$$\begin{aligned} |g(z) - g_T(z)| &= \left| \int_0^\infty f(t)e^{-zt}dt - \int_0^T f(t)e^{-zt}dt \right| = \left| \int_T^\infty f(t)e^{-zt}dt \right| \\ &\leq \int_T^\infty |f(t)|e^{-Re\, zt}dt \leq \|f\|_\infty \int_T^\infty e^{-tRe\, z}dt \\ &= \|f\|_\infty \frac{e^{-TRe\, z}}{Re\, z}. \end{aligned}$$

Para $\operatorname{Re} z < 0$,

$$\begin{aligned} |g_T(z)| &= \left| \int_0^T f(t)e^{-zt}dt \right| \leq \int_0^T |f(t)|e^{-Re\, zt}dt \\ &\leq \|f\|_\infty \int_0^T e^{-tRe\, z}dt \leq \|f\|_\infty \int_{-\infty}^T e^{-tRe\, z}dt \\ &= \|f\|_\infty \frac{e^{-TRe\, z}}{|Re\, z|}. \end{aligned}$$

Suponha agora que g tem uma extensão analítica para uma região aberta Ω que contém o semiplano fechado $\operatorname{Re} z \geq 0$. Sejam $R > 0$ e $\delta_R > 0$ pequeno o suficiente para garantir que g seja analítica em uma região aberta que contém a curva C_R (e seu interior) formado pelo círculo $|z| = R$ com a reta vertical $\operatorname{Re} z = -\delta_R$ (veja figura a seguir).

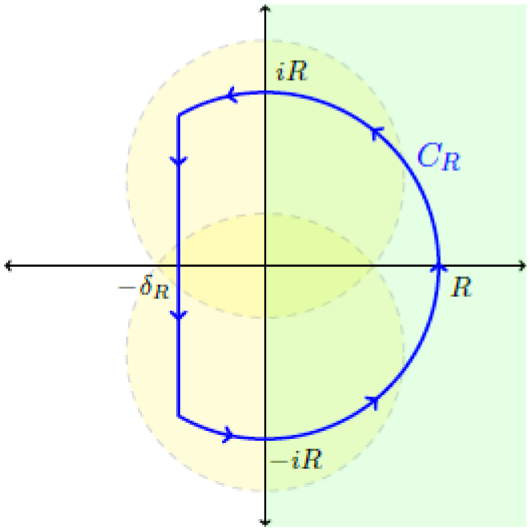

Figura 2.2: O contorno C_R. O segmento de linha imaginário $[-iR, iR]$ é compacto e pode ser coberto por um número finito de discos abertos (amarelo), onde g é analítico. Assim, existe um $\delta_R > 0$ tal que g é analítico em uma região aberta que contém a curva C_R.

Para cada $R > 0$, a Fórmula Integral de Cauchy[4] implica que

$$g_T(0) - g(0) = \frac{1}{2\pi i}\int_{C_R}(g_T(z) - g(z))e^{zT}\left(1 + \frac{z^2}{R^2}\right)\frac{dz}{z} \tag{2.18}$$

Examinamos as contribuições para esta integral nas duas curvas

$$C_R^+ = C_R \cap \{z : Re\, z \geq 0\} \quad \text{e} \quad C_R^- = C_R \cap \{z : Re\, z \leq 0\}.$$

Vamos examinar a contribuição de C_R^+ para (2.18). Para $z = Re^{it}$,

$$\begin{aligned}\left|\frac{1}{z}\left(1 + \frac{z^2}{R^2}\right)\right| &= \left|\frac{1}{z} + \frac{z}{R^2}\right| = \left|\frac{1}{Re^{it}} + \frac{Re^{it}}{R^2}\right| \\ &= \frac{1}{R^2}|Re^{-it} + Re^{it}| = \frac{1}{R^2}|\overline{z} + z| \\ &= \frac{2|Re\, z|}{R^2}.\end{aligned}$$

Para $z \in \mathbb{C}$,

$$|e^{zT}| = e^{TRe\, z} \tag{2.19}$$

temos

$$\begin{aligned}\left|\frac{1}{2\pi i}\int_{C_R^+}(g_T(z) - g(z))e^{zT}\left(1 + \frac{z^2}{R^2}\right)\frac{dz}{z}\right| &\leq \frac{1}{2\pi}\left(\|f\|_\infty \frac{e^{-TRe\, z}}{Re\, z}\right)(e^{TRe\, z})\left(\frac{2|Re\, z|}{R^2}\right)(\pi R) \\ &= \frac{\|f\|_\infty}{R}.\end{aligned}$$

[4](ver Bak [2] página 61)

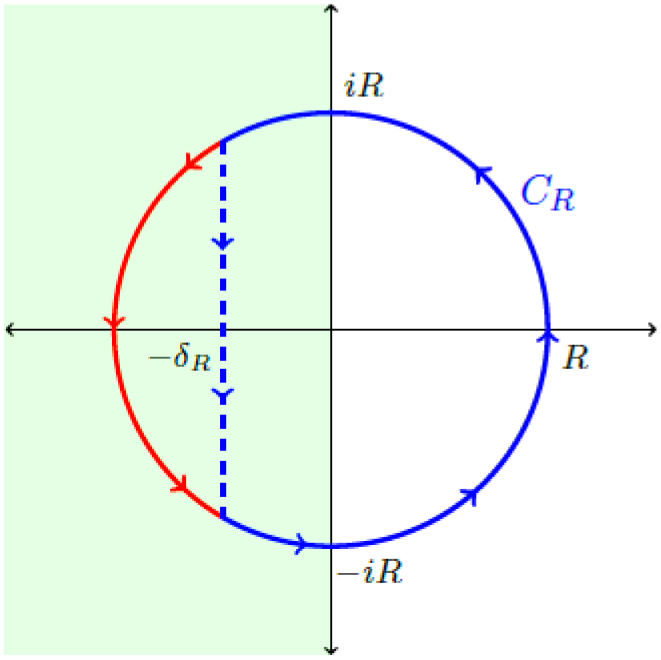

Figura 2.3: O Teorema de Cauchy garante que a integral sobre C_R^- é igual a integral sobre o semicírculo $\{z : |z| = R, Re\, z \leq 0\}$

.

Vamos examinar a contribuição de C_R^- em duas etapas. Como o integrando na integral seguinte é analítico em $Re\, z < 0$, podemos substituir o contorno C_R^- pelo lado esquerdo do círculo $|z| = R$ no cálculo

$$\begin{aligned}\left|\frac{1}{2\pi i}\int_{C_R^-} g_T(z)e^{zT}\left(1+\frac{z^2}{R^2}\right)\frac{dz}{z}\right| &= \left|\frac{1}{2\pi i}\int_{\substack{|z|=R\\ \mathrm{Re}\, z<0}} g_T(z)e^{zT}\left(1+\frac{z^2}{R^2}\right)\frac{dz}{z}\right| \\ &\leq \frac{1}{2\pi}\left(\|f\|_\infty \frac{e^{-TRe\, z}}{|Re\, z|}\right)(e^{TRe\, z})\left(\frac{2|Re\, z|}{R^2}\right)(\pi R) \\ &= \frac{\|f\|_\infty}{R}.\end{aligned}$$

Finalmente, a integral restante sobre C_R^- tende a 0 quando $T \to \infty$, porque o integrando é o produto da função $g(z)(1 + z^2/R^2)/z$, que é independente de T, e a função e^{zT}, que vai para 0 rapidamente de forma uniforme em conjuntos compactos quando $T \to \infty$ no semiplano Re $z < 0$. Portanto, como $R > 0$ é arbitrário segue que $\limsup_{T\to\infty} |g_T(0) - g(0)| = 0$.

□

2.4 Equivalências do TNP

Os resultados se juntam no seguinte lema. A prova desse lema equivale a uma série de aplicações estratégicas de resultados existentes. Requer a estimativa de Chebyshev para $\vartheta(x)$ (Teorema 3), a extensão analítica de $\Phi(s) - (s-1)^{-1}$ para uma vizinhança aberta de Re $s \geq 1$

(Teorema 27), a Transformada de Laplace de $\Phi(s)$ (Teorema 29), e o Teorema de Newman (Teorema 30).

Lema 4.

$$\int_1^\infty \frac{\vartheta(x)-x}{x^2}dx$$

converge.

Demonstração. Defina $f:[0,\infty)\to\mathbb{C}$ por $f(t)=\vartheta(e^t)e^{-t}-1$ e observe que é contínua por partes em $[0,a]$ para todo $a\geq 0$ e $|f(t)|\leq|\vartheta(e^t)|e^{-t}+1\leq 4$ para todo $t\geq 0$ pelo Teorema 3. O Teorema 28 com $A=4$ e $B=0$ garante que a Transformada de Laplace de f é analítica em $\operatorname{Re} z>0$. Consequentemente, para $\operatorname{Re} z>0$

$$\begin{aligned}\int_0^\infty f(t)e^{-zt}dt &= \int_0^\infty(\vartheta(e^t)e^{-t}-1)e^{-zt}dt\\ &= \int_0^\infty \vartheta(e^t)e^{-(z+1)t}dt-\int_0^\infty e^{-zt}dt\\ &= \int_0^\infty \vartheta(e^t)e^{-(z+1)t}dt-\frac{1}{z}\\ &= \frac{\Phi(z+1)}{z+1}-\frac{1}{z}. \qquad \text{(pelo Teorema 29)}\end{aligned}$$

Seja $z=s-1$ e note que o Teorema 27 implica que

$$g(z)=\frac{\Phi(z+1)}{z+1}-\frac{1}{z}=\frac{\Phi(s)}{s}-\frac{1}{s-1}$$

se estende analiticamente para uma vizinhança aberta de $\operatorname{Re} s\geq 1$, isto é, para uma vizinhança aberta do semiplano fechado $\operatorname{Re} z\geq 0$. O Teorema 30 garante que a integral imprópria

$$\int_0^\infty f(t)dt=\int_0^\infty(\vartheta(e^t)e^{-t}-1)dt=\int_1^\infty\left(\frac{\vartheta(x)}{x}-1\right)\frac{dx}{x}=\int_1^\infty\frac{\vartheta(x)-x}{x^2}dx$$

converge. □

Um ingrediente principal na prova do teorema dos números primos é a seguinte afirmação assintótica.

Teorema 31. $\vartheta(x)\sim x$.

Demonstração. Observe que

$$\underbrace{\int_1^\infty\frac{\vartheta(t)-t}{t^2}dt \quad existe}_{\text{pelo Lema 4}} \quad\Longrightarrow\quad \lim_{x\to\infty}\underbrace{\int_x^\infty\frac{\vartheta(t)-t}{t^2}dt}_{I(x)}=0. \tag{2.20}$$

Suponha por contradição que

$$\limsup_{x\to\infty}\frac{\vartheta(x)}{x}>1, \quad \text{e seja} \quad \limsup_{x\to\infty}\frac{\vartheta(x)}{x}>\alpha>1.$$

Então, existe $x > 1$ tal que $\vartheta(x) > \alpha x$. Para tal x,

$$\begin{aligned} I(\alpha x) - I(x) &= \int_x^{\alpha x} \frac{\vartheta(t) - t}{t^2} dt \geq \int_x^{\alpha x} \frac{\alpha x - t}{t^2} dt \qquad \text{(fazendo } t = xu\text{)} \\ &= \int_1^{\alpha} \frac{\alpha x - xu}{x^2 u^2} x du = \int_1^{\alpha} \frac{\alpha - u}{u^2} du \\ &= \alpha - 1 - \log \alpha > 0, \end{aligned}$$

pois calculando f'' de $f(\alpha) = \alpha - 1 - \log \alpha$ para $\alpha > 0$, temos que f é estritamente positiva em $(0, 1)$ e $(1, \infty)$. Como $\liminf_{x\to\infty}(I(\alpha x) - I(x)) > 0$, contradiz (2.20), concluímos que $\limsup_{x\to\infty} \frac{\vartheta(x)}{x} \leq 1$.

Agora, suponha por contradição que

$$\liminf_{x\to\infty} \frac{\vartheta(x)}{x} < 1, \quad \text{e seja} \quad \liminf_{x\to\infty} \frac{\vartheta(x)}{x} < \beta < 1.$$

Então, existe $x > 1$ tal que $\vartheta(x) < \beta x$. Para tal x,

$$\begin{aligned} I(x) - I(\beta x) &= \int_{\beta x}^{x} \frac{\vartheta(t) - t}{t^2} dt \leq \int_{\beta x}^{x} \frac{\alpha x - t}{t^2} dt \qquad \text{(fazendo } t = xu\text{)} \\ &= \int_{\beta}^{1} \frac{-xu}{x^2 u^2} x du = \int_{\beta}^{1} \frac{\beta - u}{u^2} du \\ &= 1 - \beta + \log \beta < 0. \end{aligned}$$

Como $\liminf_{x\to\infty}(I(x) - I(\beta x)) < 0$, contradiz (2.20), concluímos que $\liminf_{x\to\infty} \frac{\vartheta(x)}{x} \geq 1$.
Logo,

$$\limsup_{x\to\infty} \frac{\vartheta(x)}{x} \leq 1, \quad \text{e} \quad \liminf_{x\to\infty} \frac{\vartheta(x)}{x} \geq 1,$$

segue que $\lim_{x\to\infty} \vartheta(x)/x = 1$, isto é, $\vartheta(x) \sim x$. □

2.5 Conclusão da prova

Finalmente, estamos prontos para completar a prova do teorema dos números primos.

Teorema 32 (Teorema dos Números Primos). $\pi(x) \sim \dfrac{x}{\log x}$

Demonstração. Do Teorema 31, temos $\vartheta(x) \sim x$, isto é, $\lim_{x\to\infty} \vartheta(x)/x = 1$. Como

$$\vartheta(x) = \sum_{p \leq x} \log p \leq \sum_{p \leq x} \log x = \pi(x) \log x,$$

segue que

$$1 = \lim_{x\to\infty} \frac{\vartheta(x)}{x} = \liminf_{x\to\infty} \frac{\vartheta(x)}{x} \leq \liminf_{x\to\infty} \frac{\pi(x) \log x}{x}.$$

Para qualquer $\epsilon > 0$,

$$\begin{aligned}\vartheta(x) = \sum_{p \le x} \log p &\ge \sum_{x^{1-\epsilon} < p \le x} \log p \\ &\ge \sum_{x^{1-\epsilon} < p \le x} \log x^{1-\epsilon} \\ &\ge (1-\epsilon)(\pi(x) - x^{1-\epsilon}) \log x.\end{aligned}$$

Portanto,

$$\begin{aligned}1 = \lim_{x\to\infty} \frac{\vartheta(x)}{x} &= \limsup_{x\to\infty} \frac{\vartheta(x)}{x} \\ &\ge \limsup_{x\to\infty} \frac{(1-\epsilon)(\pi(x) - x^{1-\epsilon}) \log x}{x} \\ &= (1-\epsilon) \limsup_{x\to\infty} \frac{\pi(x) \log x}{x} - (1-\epsilon) \limsup_{x\to\infty} \frac{\log x}{x^{\epsilon}}.\end{aligned}$$

Como $\epsilon > 0$ é arbitrário,

$$\limsup_{x\to\infty} \frac{\pi(x) \log x}{x} \le 1.$$

Por fim,

$$1 \le \liminf_{x\to\infty} \frac{\pi(x)}{x/\log x} \le \limsup_{x\to\infty} \frac{\pi(x)}{x/\log x} \le 1,$$

logo

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

Isso concluí a prova do teorema dos números primos. □

Vários outros teoremas foram provados com relação aos números primos. Muitos grandes matemáticos abordaram problemas relacionados a primos, mas ainda existem muitos problemas em aberto, dos quais iremos mencionar alguns.

Conjectura 1 (Conjectura dos Primos Gêmeos)**.** *Existem infinitos pares de primos p e $p+2$.*

Conjectura 2 (Conjectura de Goldbach)**.** *Todo número inteiro positivo par maior que 2 pode ser escrito como a soma de dois primos.*

Conjectura 3 (Conjectura de Landau)**.** *Existem infinitos números primos na forma $n^2 + 1$, onde n é um número inteiro positivo.*

Em cada um desses casos, embora a maioria dos matemáticos acredite que essas conjecturas sejam verdadeiras, e haja uma boa quantidade de evidências empíricas para as conjecturas, a busca por uma prova completa continua.

Esse comportamento aparentemente obsessivo por parte dos matemáticos se deve parcialmente ao fato de a prova rigorosa ser um dos principais objetivos da matemática, mas também

porque qualquer prova da conjectura dos primos gêmeos, ou da hipótese de Riemann, provavelmente envolveria técnicas matemáticas radicalmente novas e percepções, potencialmente levando a novos caminhos de pesquisa e ideias a explorar.

Na matemática, muitas vezes acontece que a jornada para encontrar uma prova é pelo menos tão interessante quanto o próprio resultado.

3. Teorema de Dirichlet sobre Primos em Progressões Aritméticas

A distribuição dos números primos sempre foi um tópico central na teoria dos números. Sequências de números primos, geradas por funções e polinômios chamaram a atenção de grandes matemáticos, como Euler e Dirichlet. Em 1772, Euler notou que a equação quadrática $n^2 - n + 41$ sempre gerava primos, para n de 1 a 41. No entanto, já se sabe há mais tempo que não existe polinômios que sempre geram primos.

Em vista disso, ao invés de considerar polinômios que são sempre primos, os matemáticos voltaram sua atenção para polinômios que poderiam ser primos infinitamente. Este é o contexto para o *Teorema de Dirichlet*:

Se $(h, k) = 1$, então a sequência $kn + h, n = 0, 1, 2, \ldots$ contém infinitos primos.

O Teorema foi originalmente formulado em meados dos anos 1800 por Legendre e ficou conhecido como Conjectura de Legendre. Dirichlet foi o primeiro a provar esse resultado usando sua teoria de Caracteres e L-funções. Nesse trabalho, seguiremos o método de Dirichlet com algumas possíveis modificações para simplificar a prova original, que pode ser encontrada em [4].

Considere $k = 1$ e $h = 0$, a sequência $1, 2, 3, \ldots, n \ldots$ obviamente contém todos os números primos, porque contém todos os números inteiros positivos. Na seção seguinte vamos mostrar que existem infinitos primos se considerarmos $k = 4$ e $h = \pm 1$. Contudo, a prova para o caso geral é muito mais complicada e requer ferramentes da teoria analítica dos números.

3.1 Casos particulares do Teorema de Dirichlet

Proposição 1. *Existem infinitos primos da forma* $4n - 1$.

Demonstração. Suponha que exista um número finito de primos da forma $4n - 1$ e seja p o maior destes primos. Considere o inteiro $N = 2^2.3.5 \ldots p - 1$. O produto $3.5. \ldots . p$ contém todos os primos ímpares menores ou iguais a p. Como N é da forma $4n - 1$, temos que N não pode ser primo, pois $N > p$. Nenhum primo menor ou igual a p divide N, então todos os fatores primos de N são maiores que p. Mas não todos os fatores de N podem ser da forma $4n + 1$, pois o produto entre números da forma $4n + 1$ possuem essa forma. Logo, existe algum fator primo de N da forma $4n - 1$ maior que p. Absurdo. □

Proposição 2. *Existem infinitos primos da forma* $4n+1$.

Demonstração. Seja $N > 1$ um inteiro. Vamos mostrar que existe um número primo $p > N$ tal que $p \equiv 1 \pmod 4$. Considere o inteiro $m = (N!)^2 + 1$. Note que $m > 1$ é ímpar. Seja p o menor fator primo de m. Nenhum dos números $2, 3, \ldots, N$ divide m, logo $p > N$. Temos

$$(N!)^2 \equiv -1 \pmod p.$$

Elevando ambos os membros a $(p-1)/2$,

$$(N!)^{p-1} \equiv (-1)^{(p-1)/2} \pmod p.$$

Mas $(N!)^{p-1} \equiv 1 \pmod p$ pelo Pequeno Teorema de Fermat, então

$$(-1)^{(p-1)/2} \equiv 1 \pmod p.$$

Os possíveis valores para $(-1)^{(p-1)/2} - 1$ são 0 ou -2, mas não pode ser -2, uma vez que é divisível por p. Assim

$$(-1)^{(p-1)/2} = 1.$$

Mas isso significa que $(p-1)/2$ é par, isto é, $p \equiv 1 \pmod 4$. Em outras palavras, mostramos que para cada inteiro $N > 1$ existe um primo $p > N$ tal que $p \equiv 1 \pmod 4$. Logo existem infinitos primos da forma $4n+1$. □

3.2 O PLANO DA PROVA

Pela fórmula assintótica [1]

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

onde o somatório percorre todos os primos $p \le x$. Vamos provar o Teorema de Dirichlet como consequência do seguinte resultado:

Teorema 33. *Se* $k > 0$ *e* $(h,k) = 1$ *temos, para todo* $x > 1$,

$$\sum_{\substack{p \le x, \\ p \equiv h \pmod k}} \frac{\log p}{p} = \frac{1}{\varphi(k)} \log x + O(1).$$

Como $\log x \to \infty$ quando $x \to \infty$, esse Teorema implica que existem infinitos números primos $p \equiv h \pmod k$, isto é, existem infinitos primos na progressão aritmética $kn + h, n = 0, 1, 2, \ldots$ A prova do Teorema 33 será apresentada por uma sequência de lemas que reunimos nesta seção. Ao longo do capítulo, adotamos a seguinte notação: k é um inteiro positivo fixo que representa o módulo, e h é um inteiro fixo primo a k. Os $\varphi(k)$ caracteres de Dirichlet

[1] Este resultado pode ser encontrado em [1] *Teorema 4.10.*

módulo k serão denotados por $\chi_1, \ldots, \chi_{\varphi(k)}$, sendo χ_1 o caráter principal. Para $\chi \neq \chi_1$, temos que $L(1,\chi)$ e $L'(1,\chi)$ representam as séries

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

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

A convergência dessas séries foi provada no Teorema 19. Além disso, no Teorema 21 provamos que $L(1,\chi) \neq 0$, se χ é real. Vejamos o primeiro lema.

Lema 5. *Para $x > 1$ temos*

$$\sum_{\substack{p\leq x,\\ p\equiv h \pmod k}} \frac{\log p}{p} = \frac{1}{\varphi(k)}\log x + \frac{1}{\varphi(k)}\sum_{r=2}^{\varphi(k)} \overline{\chi}_r(h) \sum_{p\leq x} \frac{\chi_r(p)\log p}{p} + O(1).$$

Demonstração. Considere a fórmula assintótica

$$\sum_{p\leq x} \frac{\log p}{p} = \log x + O(1). \tag{3.1}$$

Dessa fórmula, vamos extrair do somatório os termos p primos tais que $p \equiv h \pmod k$. Para isso, vamos usar a ortogonalidade dos Caracteres de Dirichlet (1.6), tomando $m = p$ e $n = h$, $(h,k) = 1$, então multiplicando ambos os membros por $p^{-1}\log p$ e somando sobre todos $p \leq x$, temos

$$\sum_{p\leq x}\sum_{r=1}^{\varphi(k)} \chi_r(p)\overline{\chi}_r(h)\frac{\log p}{p} = \varphi(k) \sum_{\substack{p\leq x,\\ p\equiv h \pmod k}} \frac{\log p}{p}. \tag{3.2}$$

Agora, vamos isolar no somatório do lado esquerdo os termos envolvendo o caráter principal, então reescrevemos (3.2) na forma

$$\varphi(k) \sum_{\substack{p\leq x,\\ p\equiv h \pmod k}} \frac{\log p}{p} = \overline{\chi}_1(h)\sum_{p\leq x} \frac{\chi_1(p)\log p}{p} + \sum_{r=2}^{\varphi(k)} \overline{\chi}_r(h) \sum_{p\leq x} \frac{\chi_r(p)\log p}{p}. \tag{3.3}$$

Agora $\overline{\chi}_1(h) = 1$ e $\chi_1(p) = 0$ a menos que $(p,k) = 1$, caso em que $\chi_1(p) = 1$. Como o número de primos que dividem k é finito, o primeiro termo da direita em (3.3) é dado por

$$\sum_{\substack{p\leq x,\\ (p,k)=1}} \frac{\log p}{p} = \sum_{p\leq x} \frac{\log\ p}{p} - \sum_{\substack{p\leq x,\\ p\mid k}} \frac{\log\ p}{p} = \sum_{p\leq x} \frac{\log\ p}{p} + O(1). \tag{3.4}$$

De (3.4) e (3.3), obtemos

$$\varphi(k) \sum_{\substack{p\leq x,\\ p\equiv h \pmod{k}}} \frac{\log p}{p} = \sum_{p\leq x} \frac{\log\ p}{p} + \sum_{r=2}^{\varphi(k)} \overline{\chi}_r(h) \sum_{p\leq x} \frac{\chi_r(p)\log\ p}{p} + O(1). \tag{3.5}$$

Contudo, de (3.1) e dividindo por $\varphi(k)$, concluímos a prova. □

É claro que o Lema 5 implica no Teorema 33 se mostrarmos que

$$\sum_{p\leq x} \frac{\chi(p)\log p}{p} = O(1) \tag{3.6}$$

para $\chi \neq \chi_1$. O próximo Lema expressa essa soma de uma forma que não é estendida sobre primos.

Lema 6. *Para $x > 1$ e $\chi \neq \chi_1$ temos*

$$\sum_{p\leq x} \frac{\chi(p)\log p}{p} = -L'(1,\chi) \sum_{n\leq x} \frac{\mu(n)\chi(n)}{n} + O(1).$$

Demonstração. Considere o somatório

$$\sum_{n\leq x} \frac{\chi(n)\Lambda(n)}{n},$$

onde $\Lambda(n)$ é a função de Mangoldt. Vamos expressar esse somatório de dois modos. Primeiro, note que da definição da função $\Lambda(n)$ temos

$$\sum_{n\leq x} \frac{\chi(n)\Lambda(n)}{n} = \sum_{\substack{p\leq x\\ p^a\leq x}} \sum_{a=1}^{\infty} \frac{\chi(p^a)\log p}{p^a}. \tag{3.7}$$

Separando o termo $a = 1$

$$\sum_{n\leq x} \frac{\chi(n)\Lambda(n)}{n} = \sum_{p\leq x} \frac{\chi(p)\log p}{p} + \sum_{\substack{p\leq x\\ p^a\leq x}} \sum_{a=2}^{\infty} \frac{\chi(p^a)\log p}{p^a}. \tag{3.8}$$

Podemos controlar o segundo somatório da direita por

$$\sum_{p} \log p \sum_{a=2}^{\infty} \frac{1}{p^a} = \sum_{p} \frac{\log p}{p(p-1)} < \sum_{n=2}^{\infty} \frac{\log n}{n(n-1)} = O(1),$$

e de (3.8)

$$\sum_{p\leq x} \frac{\chi(p)\log p}{p} = \sum_{n\leq x} \frac{\chi(n)\Lambda(n)}{n} + O(1). \tag{3.9}$$

Lembrando que $\Lambda(n) = \sum_{d|n} \mu(d)\log(n/d)$, temos

$$\sum_{n\leq x} \frac{\chi(n)\Lambda(n)}{n} = \sum_{n\leq x} \frac{\chi(n)}{n} \sum_{d|n} \mu(d)\log\frac{n}{d}.$$

No último somatório, tome $n = cd$ e usando a propriedade multiplicativa de χ

$$\sum_{n\leq x} \frac{\chi(n)\Lambda(n)}{n} = \sum_{d\leq x} \frac{\mu(d)\chi(d)}{d} \left(\sum_{c\leq x/d} \frac{\chi(c)\log c}{c} \right). \tag{3.10}$$

Como $x/d \geq 1$, no somatório sobre c, usamos a fórmula (1.10) do Teorema 19 para obter

$$\sum_{c\leq x/d} \frac{\chi(c)\log c}{c} = -L'(1,\chi) + O\left(\frac{\log x/d}{x/d}\right).$$

Da equação (3.10) temos

$$\sum_{n\leq x} \frac{\chi(n)\Lambda n}{n} = -L'(1,\chi) \sum_{d\leq x} \frac{\mu(d)\chi(d)}{d} + O\left(\sum_{d\leq x} \frac{1}{d} \frac{\log x/d}{x/d} \right). \tag{3.11}$$

O somatório no termo O é

$$\frac{1}{x} \sum_{d\leq x} (\log x - \log d) = \frac{1}{x} \left([x]\log x - \sum_{d\leq x} \log d \right) = O(1),$$

uma vez que

$$\sum_{d\leq x} \log d = \log[x]! = x\log x + O(x).$$

Logo, de (3.11)

$$\sum_{n\leq x} \frac{\chi(n)\Lambda n}{n} = -L'(1,\chi) \sum_{d\leq x} \frac{\mu(d)\chi(d)}{d} + O(1),$$

e de (3.9), concluímos a prova. □

Dessa forma, o Lema 6 implica em (3.6) se mostrarmos que

$$\sum_{n\leq x} \frac{\mu(n)\chi(n)}{n} = O(1). \tag{3.12}$$

Isso, por sua vez, será deduzido no seguinte lema.

Lema 7. *Para $x > 1$ e $\chi \neq \chi_1$ temos*

$$L(1,\chi) \sum_{n\leq x} \frac{\mu(n)\chi(n)}{n} = O(1). \tag{3.13}$$

Demonstração. Vamos usar a Fórmula de Inversão de Mobius Generalizada, provada no Teo-

rema 11. Para $\alpha(n) = \chi(n)$ e $F(x) = x$ em (1.3),

$$x = \sum_{n \leq x} \mu(n)\chi(n) G\left(\frac{x}{n}\right) \tag{3.14}$$

onde

$$G(x) = \sum_{n \leq x} \chi(n)\frac{x}{n} = x \sum_{n \leq x} \frac{\chi(n)}{n}.$$

Pela Equação (1.9) do Teorema 19 podemos escrever $G(x) = xL(1,\chi) + O(1)$. Usando (3.14) temos

$$x = \sum_{n \leq x} \mu(n)\chi(n) \left\{\frac{x}{n} L(1,\chi) + O(1)\right\} = xL(1,\chi) \sum_{n \leq x} \frac{\mu(n)\chi(n)}{n} + O(x).$$

Dividindo por x, concluímos a prova. □

Se $L(1,\chi) \neq 0$, podemos cancelar $L(1,\chi)$ em (3.13) e obtemos (3.12). Portanto, a prova do Teorema de Dirichlet depende de $L(1,\chi)$ ser não nulo para $\chi \neq \chi_1$. Isso já foi provado para caracteres reais, no Teorema 21, então resta provar que $L(1,\chi) \neq 0$ para todo $\chi \neq \chi_1$ com valores complexos.

Para isso, seja $N(k)$ o número de caracteres χ não principais módulo k tais que $L(1,\chi) = 0$. Se $L(1,\chi) = 0$, então $L(1,\overline{\chi}) = 0$ e $\chi \neq \overline{\chi}$ para χ não real. Portanto, os caracteres χ tais que $L(1,\chi) = 0$ ocorrem em pares conjugados, então $N(k)$ é par. Nosso objetivo é provar que $N(k) = 0$, e isso será deduzido no Lema 9. Antes, vejamos o seguinte Lema.

Lema 8. *Se $\chi \neq \chi_1$ e $L(1,\chi) = 0$ temos*

$$L'(1,\chi) \sum_{n \leq x} \frac{\mu(n)\chi(n)}{n} = \log x + O(1).$$

Demonstração. Novamente vamos iniciar pela Fórmula de Inversão de Mobius Generalizada (Teorema 11). Desta vez, para $F(x) = x \log x$ temos

$$x \log x = \sum_{n \leq x} \mu(n)\chi(n) G\left(\frac{x}{n}\right) \tag{3.15}$$

onde

$$G(x) = \sum_{n \leq x} \chi(n)\frac{x}{n} \log\frac{x}{n} = x \log x \sum_{n \leq x} \frac{\chi(n)}{n} - x \sum_{n \leq x} \frac{\chi(n)\log n}{n}.$$

Agora, pelas equações (1.9) e (1.10) do Teorema 19

$$G(x) = x \log x \left\{L(1,\chi) + O\left(\frac{1}{x}\right)\right\} + x \left\{L'(1,\chi) + O\left(\frac{\log x}{x}\right)\right\} = xL'(1,\chi) + O(\log x)$$

assumindo que $L(1,\chi) = 0$. Assim, de (3.15)

$$x\log x = \sum_{n\le x}\mu(n)\chi(n)\left\{\frac{x}{n}L'(1,\chi)+O\left(\log\frac{x}{n}\right)\right\}$$

$$= xL'(1,\chi)\sum_{n\le x}\frac{\mu(n)\chi(n)}{n}+O\left(\sum_{n\le x}(\log x-\log n)\right).$$

No Lema 6 já provamos que o termo da ordem O é $O(x)$. Logo,

$$x\log x = xL'(1,\chi)\sum_{n\le x}\frac{\mu(n)\chi(n)}{n}+O(x),$$

e dividindo por x, concluímos a prova. □

Lema 9. *Para $x>1$ temos*

$$\sum_{\substack{p\le x,\\ p\equiv 1 \pmod k}}\frac{\log p}{p} = \frac{1-N(k)}{\varphi(k)}\log x+O(1). \tag{3.16}$$

Demonstração. Pelo Lema 5, para $h=1$ temos

$$\sum_{\substack{p\le x,\\ p\equiv 1 \pmod k}}\frac{\log p}{p} = \frac{1}{\varphi(k)}\log x+\frac{1}{\varphi(k)}\sum_{r=2}^{\varphi(k)}\sum_{p\le x}\frac{\chi_r(p)\log\ p}{p}+O(1). \tag{3.17}$$

Na somatório sobre p na direita, usamos o Lema 6 que afirma que

$$\sum_{p\le x}\frac{\chi_r(p)\log p}{p} = -L'(1,\chi_r)\sum_{n\le x}\frac{\mu(n)\chi_r(n)}{n}+O(1).$$

Se $L(1,\chi_r)\neq 0$, o Lema 7 mostra que o membro da direita de (3.17) é $O(1)$. Mas se $L(1,\chi_r)=0$, então o Lema 8 implica

$$-L'(1,\chi_r)\sum_{n\le x}\frac{\mu(n)\chi_r(n)}{n} = -\log x+O(1).$$

Portanto, o somatório da direita em (3.17) é

$$\frac{1}{\varphi(k)}\{-N(k)\log x+O(1)\},$$

então (3.17) é

$$\sum_{\substack{p\le x,\\ p\equiv 1 \pmod k}}\frac{\log p}{p} = \frac{1-N(k)}{\varphi(k)}\log x+O(1).$$

Isso conclui a prova. □

Se $N(k) \neq 0$, então $N(k) \geq 2$, uma vez que $N(k)$ é par. Portanto o coeficiente do $\log x$ em (3.16) é negativo e o membro da direita $\to -\infty$, para $x \to \infty$. Isso é uma contradição, pois todos os termos da esquerda são positivos. Portanto o Lema 9 implica que $N(k) = 0$, como queríamos. Logo o Teorema (33) está provado.

Como observado anteriormente, o Teorema 33 implica no Teorema de Dirichlet:

Teorema 34 (**Teorema de Dirichlet**). *Se $k > 0$ e $(h, k) = 1$, então existem infinitos primos na progressão aritmética $nk + h, n = 0, 1, 2, \ldots$*

A demonstração de Dirichlet é considerada como uma das primeiras aplicações importantes de métodos analíticos em Teoria dos Números e proporcionou novas linhas de desenvolvimento.

Até o século passado, um velho problema em aberto consistia em se determinar uma progressão aritmética arbitrariamente longa, porém finita em que todos os termos fossem números primos. Mais especificamente o **Teorema de Green-Tao**, demonstrado por Ben Green e Terence Tao em 2004, afirma que a sequência de números primos contém progressões aritméticas arbitrariamente longas. Em outras palavras, para cada número natural k, existe um progressão aritmética formada por k números primos. Este resultado, entre outros, rendeu à Terence Tao a Medalha Fields em 2006.

4. Uma introdução aos Métodos de Crivos

4.1 O Crivo de Eratóstenes e Legendre

Proposição 3. *Se n é um número natural composto, então n tem um divisor primo p tal que $p \leq \sqrt{n}$.*

Demonstração. Seja n um número natural composto, ou seja, existem números naturais a, b com $1 < a, b < n$, tais que $n = ab$. Sem perda de generalidade, suponha $a \leq b$, então $a^2 \leq ab = n$, e portanto, $a \leq \sqrt{n}$. Como $a > 1$, pelo Teorema Fundamental da Aritmética, existem primos $p_1, \ldots, p_r$ tais que $a = p_1 \ldots p_r$. Note que p_j divide a, logo também divide n, e além disso, temos $p_j \leq a \leq \sqrt{n}$, como queríamos. □

Apresentamos agora um algoritmo para encontrar números primos em uma lista até determinado valor limite, conhecido como **Crivo de Eratóstenes**.

Para exemplificá-lo, vamos encontrar os primos entre 1 e 40. Inicialmente, crie uma lista de todos os inteiros de 2 até o valor limite. Em seguida, determina-se o maior número a ser checado, dado pela raiz quadrada do valor limite, no caso $\sqrt{40} \simeq 6$. O primeiro número da lista, é primo, 2. Então remova todos os números múltiplos de 2 até 40. O próximo número da lista é o 3, primo. Então remova todos os números múltiplos de 3 até 40. O próximo número também é primo, 5, e é o último número a ser checado. Remova seus múltiplos. Assim, a lista encontrada contém somente números primos.

$$2, 3, \not{4}, 5, \not{6}, 7, \not{8}, \not{9}, \not{10}, 11, \not{12}, 13, \not{14}, \not{15}, \not{16}, 17, \not{18}, 19, \not{20}, \not{21}, \not{22},$$
$$23, \not{24}, \not{25}, \not{26}, \not{27}, \not{28}, 29, \not{30}, 31, \not{32}, \not{33}, \not{34}, \not{35}, \not{36}, 37, \not{38}, \not{39}, \not{40}$$

Ainda que os problemas de obter uma lista de primos e o de contar o número de primos menores do que um dado valor limite sejam diferentes, o matemático francês Legendre nos mostrou como aplicar o conceito do crivo de Eratóstenes para encontrar estimativas superiores e inferiores ao número de primos dado um conjunto de inteiros. Esse resultado é conhecido como **Crivo de Legendre**. Vamos agora introduzir uma formulação mais analítica do processo apresentado na seção anterior.

Seja A um conjunto finito de objetos e P um conjunto indexado de números primos tal que para cada $p \in P$ associamos um subconjunto A_p de A. O objetivo da teoria de Crivos é estimar o tamanho do conjunto

$$S(A,P) := A \setminus \bigcup_{p\in P} A_p.$$

Essa é a abordagem generelizada do problema. Para cada subconjunto I de P, denotamos

$$A_I := \bigcap_{p\in I} A_p,$$

onde para o conjunto vazio $\emptyset$ consideramos $A_\emptyset$ como sendo o próprio conjunto A. A estimativa do tamanho do conjunto $S(A,P)$ é dada pelo Princípio da Inclusão-Exclusão, que será apresentado a seguir.

Proposição 4 (Princípio da Inclusão-Exclusão)**.** *Considere um conjunto X finito. Sejam $A_1, A_2, \ldots, A_n$ subconjuntos de X. Então*

$$\left| X \setminus \bigcup_{i=1}^{n} A_i \right| = |X| - \sum_{i=1}^{n} |A_i| + \sum_{1\le i<j\le n} |A_i \cap A_j| - \sum_{1\le i<j<k\le n} |A_i \cap A_j \cap A_k| + \ldots + (-1)^n |A_1 \cap \ldots \cap A_n|.$$

Demonstração. A prova pode ser encontrada em Nascimento [8] página 23. □

Utilizando esse princípio, podemos escrever

$$|S(A,P)| = \sum_{I\subseteq P} (-1)^{|I|} |A_I|. \tag{4.1}$$

Ao longo do texto, o conjunto A irá representar os números naturais menores do que ou igual a x, o conjunto P os números primos menores do que ou igual a z e A_p o subconjunto de A dos números divisíveis por $p \in P$.

Utilizando a definição da função Mobius apresentada no primeiro capítulo, podemos reescrever o lado direito da igualdade (4.1) como

$$\begin{aligned} |S(A,P)| &= \sum_{I\subseteq P} (-1)^{|I|} |A_I| = \sum_{d|N} \mu(d) \left\lfloor \frac{x}{d} \right\rfloor \\ &= \lfloor x \rfloor - \sum_{p_1\le z} \left\lfloor \frac{x}{p_1} \right\rfloor + \sum_{p_2<p_1\le z} \left\lfloor \frac{x}{p_1 p_2} \right\rfloor - \sum_{p_1<p_2<p_3\le z} \left\lfloor \frac{x}{p_1 p_2 p_3} \right\rfloor + \ldots \end{aligned}$$

onde N denota o produto dos primos em P e $\lfloor x \rfloor$ denota a parte inteira de x. A relação entre o crivo de Eratóstenes e o crivo de Legendre é evidenciada: o primeiro termo representa o número de inteiros menores que x, o segundo termo remove os múltiplos de todos os primos, o terceiro acrescenta os múltiplos de dois primos (os quais estão sendo descontados porque foram "riscados duas vezes"), e assim sucessivamente todas as $2^{\pi(z)}$ combinações de primos são consideradas

pelo crivo de Legendre. Entende-se ainda que dado um limite no conjunto, a última parcial será a final.

Vamos denotar por $\pi(x)$ a quantidade de números primos entre 1 e x. Uma vez tendo sido calculados $S(A,P)$ nestes casos especiais, podem ser usado para limitar $\pi(x)$ usando a expressão

$$|S(A,P)| \geq \pi(x) - \pi(z) + 1 \tag{4.2}$$

que será provada na próxima seção.

Vamos ilustar com um exemplo numérico o algoritmo.

Suponha que queremos determinar a quantidade de primos menores que 100. Primeiramente, para obter a lista de todos primos p no intervalo $\sqrt{x} < p \leq x$ precisamos remover somente os múltiplos de primos menores do que ou iguais a $\sqrt{x}$. Em nosso exemplo, para $x = 100$ devemos retirar do intervalo $1 \leq n \leq 100$ os múltiplos de primos menores do que ou igual a $\sqrt{100} = 10$, ou seja, os múltiplos de $\{2,3,5,7\}$. Assim, a quantidade de primos no intervalo $1 \leq p \leq 100$ utilizando o princípio da inclusão-exclusão fornece

$$\begin{aligned}\pi(100) - \pi(10) + 1 = (-1)^0|A_\emptyset| &+ (-1)^1\left\lfloor\frac{100}{2}\right\rfloor + (-1)^1\left\lfloor\frac{100}{3}\right\rfloor + (-1)^1\left\lfloor\frac{100}{5}\right\rfloor + (-1)^1\left\lfloor\frac{100}{7}\right\rfloor \\ &+ (-1)^2\left\lfloor\frac{100}{6}\right\rfloor + (-1)^2\left\lfloor\frac{100}{10}\right\rfloor + (-1)^2\left\lfloor\frac{100}{14}\right\rfloor + (-1)^2\left\lfloor\frac{100}{15}\right\rfloor + (-1)^2\left\lfloor\frac{100}{21}\right\rfloor \\ &+ (-1)^2\left\lfloor\frac{100}{35}\right\rfloor + (-1)^3\left\lfloor\frac{100}{30}\right\rfloor + (-1)^3\left\lfloor\frac{100}{42}\right\rfloor + (-1)^3\left\lfloor\frac{100}{70}\right\rfloor \\ &+ (-1)^3\left\lfloor\frac{100}{105}\right\rfloor + (-1)^4\left\lfloor\frac{100}{210}\right\rfloor\end{aligned}$$

ou seja,

$$\begin{aligned}\pi(100) - 4 + 1 = 100 &- 50 - 33 - 20 - 14 + \\ &+ 16 + 10 + 7 + 6 + 4 \\ &+ 2 - 3 - 2 - 1 \\ &- 0 + 0 = 22.\end{aligned}$$

Logo o número de inteiros positivos que não são múltiplos de 2, 3, 5 ou 7 no intervalo $1 \leq p \leq 100$ é igual a 22. Portanto a quantidade de primos menores que 100 é $\pi(100) = 25$.

4.2 Estimativa para $\pi(x)$

Como uma aplicação do Crivo de Legendre, podemos tentar entender o crescimento da função $\pi(x)$. Voltando a igualdade (4.1)

$$S(A,P) := A \setminus \bigcup_{p\in B} A_p$$

no qual, com $z < \sqrt{x}$, segue que

$$|S(A,P)| \geq \pi(x) - \pi(z) + 1. \tag{4.3}$$

De fato, isso ocorre porque o termo à esquerda conta o número 1, não conta os primos $p \leq z$, conta os primos p com $z < p \leq x$ e também conta os números compostos que são produtos de primos maiores do que z.

Por outro lado, vimos que

$$|S(A,P)| = \sum_{d|N} \mu(d) \left\lfloor \frac{x}{d} \right\rfloor.$$

A parte fracionária de um número x, denotada $\{x\}$, é dada por $x - \lfloor x \rfloor$, então $\lfloor x \rfloor = x - \{x\}$. Assim, segue que

$$|S(A,P)| = \sum_{d|N} \mu(d) \left\lfloor \frac{x}{d} \right\rfloor = \sum_{d|N} \mu(d) \left(\frac{x}{d} - \left\{ \frac{x}{d} \right\} \right) = x \sum_{d|N} \frac{\mu(d)}{d} + \sum_{d|N} \mu(d) \left(- \left\{ \frac{x}{d} \right\} \right).$$

No entanto,

$$\left| \sum_{d|N} \mu(d) \left(- \left\{ \frac{x}{d} \right\} \right) \right| \leq \sum_{d|N} 1 = 2^{\pi(z)}.$$

Além disso, como μ é uma função multiplicativa, temos

$$\sum_{d|N} \frac{\mu(d)}{d} = \prod_{p<z} \left(1 + \frac{\mu(p)}{p} \right) = \prod_{p<z} \left(1 - \frac{1}{p} \right).$$

Logo,

$$|S(A,P)| = x \prod_{p<z} \left(1 - \frac{1}{p} \right) + O(2^{\pi(z)}). \tag{4.4}$$

Queremos agora controlar o produto $\prod_{p<z} \left(1 - \frac{1}{p} \right)$. Considere a desigualdade $1 - x \leq e^{-x}$, no qual é válida para todo $x \in \mathbb{R}$. Tome $x = \frac{1}{p}$, então

$$\prod_{p<z} \left(1 - \frac{1}{p} \right) \leq \exp \left(- \sum_{p<z} \frac{1}{p} \right).$$

Para tanto, usando o resultado (veja [8], Exemplo 1.3.9)

$$\prod_{p<z} \frac{1}{p} = \log\log z + O(1).$$

Assim,

$$\prod_{p<z}\left(1-\frac{1}{p}\right) \leq \exp\left(-\sum_{p<z}\frac{1}{p}\right) = \exp(-\log\log z - O(1)) = \frac{1}{e^{O(1)}\log z}$$

e para $0 < c < e^{O(1)}$ segue que

$$\prod_{p<z}\left(1-\frac{1}{p}\right) \leq \frac{1}{c\log z}. \tag{4.5}$$

De (4.3) temos

$$\pi(x) - \pi(z) + 1 \leq |S(A,P)| < \frac{x}{c\log z} + O(2^{\pi(z)})$$

ou seja,

$$\pi(x) < \frac{x}{c\log z} + O(2^{\pi(z)}) + z.$$

Para $z = \log x$, temos $2^{\pi(z)} < 2^{\log x} = x^{\log 2}$. Logo existe uma constante $k > 0$ tal que $O(2^{\pi(z)}) < kx^{\log 2}$. Daí

$$\pi(x) < \frac{x}{c\log\log x} + kx^{\log 2} + \log x.$$

Como $x/(\log\log x)$ cresce mais rápido do que $kx^{\log 2}$ e $\log x$, concluímos que

$$\pi(x) = O\left(\frac{x}{\log\log x}\right).$$

4.3 PROBLEMAS DE CRIVOS

Na Teoria dos Números dizemos que um par de números primos são gêmeos se a diferença entre eles é 2. Os primeiros pares de primos gêmeos são $(3,5),(5,7),(11,13),(17,19)$. O problema de saber se existe uma infinidade de números primos gêmeos é muito antigo e foi conjecturado por Euclides. Esta conjectura é chamada de conjectura dos primos gêmeos e é um dos problemas em aberto da Matemática. Vejamos esse problema em linguagem de crivo.

Exemplo 1 (Conjectura dos primos gêmeos)**.** *Seja B o conjunto de números primos menores do que ou iguais a z. Considere a sequência*

$$A = \{n(n+2) | z \leq n < z^2 - 2\}.$$

Se retirarmos os elementos da sequência A que são divisíveis por $p \in B$, temos que os elementos não são eliminados pelo processo se, e somente se, n e $n+2$ são ambos números primos. De fato, se $n.(n+2)$ têm somente fatores primos maiores do que ou iguais a z então sendo d um fator primo qualquer de $n.(n+2)$ devemos ter que $d \mid n.(n+2)$ se, e somente se $d \mid n$ ou $d \mid n+2$. Portanto os divisores primos de n e $n+2$ também devem ser maiores do que ou iguais a z.

Como $z < n < z^2$ e $z < n + 2 < z^2$, segue da proposição 3 que nem n e nem $n + 2$ podem ser números compostos.

Numericamente, seja $z = 11$, então

$$A = \{n(n + 2)|11 \leq n < 119\} \text{ e } B = \{2, 3, 5, 7, 11\}$$

Assim,

$$\begin{aligned} A = \{&143, 168, 195, 224, 255, 288, 323, 360, 399, 440, 483, 528, 575, 624, 675, 728, 783, 840, 899, 960, \\ &1023, 1088, 1155, 1224, 1295, 1368, 1443, 1520, 1599, 1680, 1763, 1848, 1935, 2024, 2115, 2208, \\ &2303, 2400, 2499, 2600, 2703, 2808, 2915, 3024, 3135, 3248, 3363, 3480, 3599, 3720, 3843, 3968, \\ &4095, 4224, 4355, 4488, 4623, 4760, 4899, 5040, 5183, 5328, 5475, 5624, 5775, 5928, 6083, 6240, \\ &6399, 6560, 6723, 6888, 7055, 7224, 7395, 7568, 7743, 7920, 8099, 8280, 8463, 8648, 8835, 9024, \\ &9215, 9408, 9603, 9800, 9999, 10200, 10403, 10608, 10815, 11024, 11235, 11448, 11663, 11880, \\ &12099, 12320, 12543, 12768, 12995, 13224, 13455, 13688, 13923, 14160, 14399\} \end{aligned}$$

Quando efetuamos o processo de crivo na sequência acima, isto é, quando retiramos os elementos da sequência A que deixam resto zero na divisão por $p \in B$, obtemos o conjunto

$$\{323, 899, 1763, 3599, 5183, 10403, 11663\} = \{17\times19, 29\times31, 41\times43, 59\times61, 71\times73, 101\times103, 107\times109\}.$$

Facilmente vemos que o número $(p \times (p + 2))$ têm como fatores os primos gêmeos p $p + 2$.

Exemplo 2 (Conjectura de Goldbach)**.** *Sejam $N > 2$ um inteiro par e B o conjunto de números primos menores do que $\sqrt{N}$. Considere a sequência*

$$A = \{n(N - n)|2 < n < N \text{ e } (n, N) = 1\}.$$

Utilizando o mesmo argumento apresentado no Exemplo 1, se $n.(N - n)$ tem somente divisores primos maiores do que $\sqrt{N}$ então necessariamente n e $N - n$ têm seus divisores primos maiores do que $\sqrt{N}$. Como o máximo entre n e $N - n$ é menor do que N, segue que $\sqrt{N} < n < N$ e $\sqrt{N} < N - n < N$. Portanto segue da Proposição 3, e pelo fato de que $(n, N) = 1$, que nem n e nem $N - n$ podem ser números compostos.

Mais uma vez ressaltamos que os problemas de obter uma tabela de números atendendo a uma certa condição e o problema de contar os números atendendo tal condição são problemas de natureza diferentes. Vimos acima dois exemplos em que sempre é possível obter os elementos desejados, utilizando a mesma ideia, embora não saibamos como contar o número de elementos atendendo a essas condições. Os métodos modernos de crivo foram fortemente inspirados na busca de uma solução para os exemplos acima.

No que segue, daremos uma perspectiva um pouco mais geral sobre as ideias envolvidas no crivo de Eratóstenes-Legendre, além de fornecer outros exemplos onde as ideias podem ser aplicadas.

Sejam A uma sequência finita de inteiros positivos menores do que ou igual a x, B um conjunto de números primos menores do que ou igual a $z < x$. Seja também $d > 1$ um inteiro livre de quadrados e composto por primos do conjunto B e defina,

$$A_d := \{a | a \in A, a \equiv 0 \pmod{d}\}, \tag{4.6}$$

ou seja, A_d representa o subconjunto de A cujos elementos são divisíveis por d. Para $d = 1$, definimos $A_1 := A$.

Considere $X > 1$ uma aproximação conveniente para $|A|$ e defina o erro da aproximação por

$$r_1 := |A| - X. \tag{4.7}$$

De maneira semelhante, para cada $p \in B$, podemos escolher $w(p)$ tal que $\dfrac{w(p)}{p}X$ seja uma aproximação para $|A_p|$ com erro de aproximação dado por

$$r_p := |A_p| - \frac{w(p)}{p}X, \tag{4.8}$$

para todo $p \in B$. Com estas escolhas de X e $w(p)$, agora definimos para cada inteiro d livre de quadrados e composto de primos em B, por $w(1) = 1$, $w(d) = \prod_{p|d} w(p)$, sendo assim $w(d)$ uma função multiplicativa. Introduzimos

$$r_d := |A_d| - \frac{w(d)}{d}X. \tag{4.9}$$

Obviamente essas escolhas podem ser feitas de várias formas, mas como podemos esperar ela irá revelar-se melhor quanto menor for $|r_d|$. Se estivermos interessados, como no crivo de Eratóstenes-Legendre, em estimar o número de elementos no conjunto

$$S(A, P) = A \setminus \bigcup_{p|P(z)} A_p \tag{4.10}$$

onde $P(z)$ denota o produto dos primos menores do que ou igual a z que pertencem a P, basta reescrever esse conjunto como,

$$S(A, P) = \{a | a \in A, (a, P(z)) = 1\},$$

considerar a sequência finita

$$a_n = \begin{cases} 1 & \text{se } n \in A, (n, P(z)) = 1, \\ 0 & \text{caso contrário.} \end{cases}$$

e utilizar as escolhas de X e $w(.)$ como segue.

Claramente,

$$|S(A,P)| = \sum_{\substack{(n,P(z))=1 \\ n\leq x}} a_n$$

e então

$$|S(A,P)| = \sum_{\substack{(n,P(z))=1 \\ n\leq x}} a_n = \sum_{n\leq x} a_n \left(\sum_{d|(n,P(z))} \mu(d) \right) = \sum_{d|P(z)} \mu(d) \sum_{\substack{d|n \\ n\leq x}} a_n = \sum_{d|P(z)} \mu(d)|A_d|.$$

Portanto,

$$|S(A,P)| = \sum_{d|P(z)} \mu(d)|A_d| \tag{4.11}$$

e por (4.9) temos,

$$|A_d| := \frac{w(d)}{d}X + r_d.$$

Segue que

$$|S(A,P)| = \sum_{d|P(z)} \mu(d) \left[\frac{w(d)}{d}X + r_d \right],$$

onde,

$$\sum_{d|P(z)} \mu(d)\frac{w(d)}{d} = \prod_{p\in B} \left(1 - \frac{w(p)}{p}\right)$$

e

$$\sum_{d|P(z)} \mu(d) r_d = O\left(\sum_{d|P(z)} r_d \right).$$

4.4 O crivo de Eratóstenes-Legendre associado ao Truque de Rankin

Nesta seção vamos descrever o Crivo de Eratóstenes-Legendre sob uma perspectiva moderna. No que segue, vamos considerar as notações da última seção e vamos definir a função $w(p)$, para cada primo $p \in P$, como o número de classes de resíduos distintas módulo p que estão A.

Vamos definir também $w(d)$, para cada inteiro d livre de quadrados e composto por primos em B, por $w(1) = 1$ e $w(d) = \prod_{p|d} w(p)$. Lembrando que $S(A,P)$ denota o conjunto dos primos menores ou iguais a z que estão em A e não pertencem a nenhum A_p com $p \in P$.

4.4.1 Uma versão moderna para o crivo de Eratóstenes-Legendre

Teorema 35. *Com as notações acima, suponha que as seguintes condições sejam satisfeitas:*

1. $|r_d| = O(w(d))$.

2. Para algum $k \geq 0$,

$$\sum_{\substack{p \leq z \\ p \in B}} \frac{w(p) \log p}{p} \leq k \log z + O(1).$$

3. Para algum número real positivo y, temos $|A_d| = 0$ para todo $d > y$.

Então,

$$|S(A, P, z)| = X.W(z) + O\left(X(\log z)^{k+1} \exp\left(-\frac{\log X}{\log z}\right)\right), \tag{4.12}$$

onde

$$W(z) := \prod_{\substack{p \in B \\ p \leq z}} \left(1 - \frac{w(p)}{p}\right).$$

Para demonstrar esse teorema precisamos de alguns resultados preliminares.

Lema 10. *Com as hipóteses do Teorema 35, denotemos*

$$F(t, z) := \sum_{\substack{d \leq t \\ d | P(z)}} w(d);$$

Então,

$$F(t, z) = O\left(t(\log z)^k \exp\left(-\frac{\log t}{\log z}\right)\right).$$

Demonstração. É fácil ver que a função $w(.)$, definida para cada inteiro d livre de quadrados e composto por primos em P, é uma função multiplicativa. Podemos assim aplicar o truque de Rankin. A ideia do chamado truque de Rankin reside no fato de que se uma função f é multiplicativa e toma valores não negativos, então para $\delta > 0$ vale

$$\sum_{n \leq x} f(n) \leq \sum_{n \leq x} f(n) \left(\frac{x}{n}\right)^{\delta} \leq x^{\delta} \sum_{n \geq 1} \frac{f(n)}{n^{\delta}}.$$

Portanto,

$$F(t, z) = \sum_{\substack{d \leq t \\ d | P(z)}} w(d) \leq \sum_{\substack{d \leq t \\ d | P(z)}} w(d) \left(\frac{t}{d}\right)^{\delta} \leq t^{\delta} \sum_{d | P(z)} \frac{w(d)}{d^{\delta}}.$$

Observe agora que, como w é uma função multiplicativa, temos

$$\sum_{d | P(z)} \frac{w(d)}{d^{\delta}} = \prod_{\substack{p \leq z \\ p \in B}} \left(1 + \frac{w(p)}{p^{\delta}}\right) \quad \text{implicando} \quad F(t, z) \leq t^{\delta} \prod_{\substack{p \leq z \\ p \in B}} \left(1 + \frac{w(p)}{p^{\delta}}\right).$$

Usando agora a desigualdade $1 + x \leq e^x$, temos que para cada $x = \dfrac{w(p)}{p^{\delta}}$,

$$\left(1 + \frac{w(p)}{p^{\delta}}\right) \leq \exp\left(\frac{w(p)}{p^{\delta}}\right)$$

portanto fazendo o produto sobre os primos $p \in P$, temos

$$\prod_{\substack{p\leq z\\ p\in B}}\left(1+\frac{w(p)}{p^{\delta}}\right)\leq \exp\left(\sum_{\substack{p\leq z\\ p\in B}}\frac{w(p)}{p^{\delta}}\right)$$

além disso, fazendo $t^{\delta}=\exp\big(\log t^{\delta}\big)$

$$t^{\delta}\prod_{\substack{p\leq z\\ p\in B}}\left(1+\frac{w(p)}{p^{\delta}}\right)\leq \exp\left(\delta\log t+\sum_{\substack{p\leq z\\ p\in B}}\frac{w(p)}{p^{\delta}}\right)$$

e daí seque que,

$$F(t,z)\leq \exp\left(\delta\log t+\sum_{\substack{p\leq z\\ p\in B}}\frac{w(p)}{p^{\delta}}\right).$$

Colocando $\delta := 1-\eta$ e escrevendo $p^{-\delta}=p^{-1}\exp(\eta\log p)$, temos

$$\begin{aligned}\exp\left(\delta\log t+\sum_{\substack{p\leq z\\ p\in B}}\frac{w(p)}{p^{\delta}}\right) &= \exp\left((1-\eta)\log t+\sum_{\substack{p\leq z\\ p\in B}}\frac{w(p)}{p}\exp(\eta\log p)\right)\\ &= t\exp\left(-\eta\log t+\sum_{\substack{p\leq z\\ p\in B}}\frac{w(p)}{p}\exp(\eta\log p)\right).\end{aligned}$$

A desigualdade $e^{x}\leq 1+xe^{x}$ é válida para qualquer $x\in\mathbb{R}$. Pelo fato de que a função exp é monótona, temos

$$\begin{aligned}t\exp\left(-\eta\log t+\sum_{\substack{p\leq z\\ p\in B}}\frac{w(p)}{p}\exp(\eta\log p)\right) &\leq t\exp\left(-\eta\log t+\sum_{\substack{p\leq z\\ p\in B}}\frac{w(p)}{p}(1+\eta\log p\exp(\eta\log p)\right)\\ &= t\exp\left(-\eta\log t+\sum_{\substack{p\leq z\\ p\in B}}\frac{w(p)}{p}+\eta\sum_{\substack{p\leq z\\ p\in B}}\frac{w(p)\log p}{p}\exp(\eta\log p)\right)\\ &\leq t\exp\left(-\eta\log t+\sum_{\substack{p\leq z\\ p\in B}}\frac{w(p)}{p}+\eta\sum_{\substack{p\leq z\\ p\in B}}\frac{w(p)\log p}{p}\exp(\eta\log z)\right)\end{aligned}$$

e encontramos,

$$F(t,z) \leq t \exp\left(-\eta \log t + \sum_{\substack{p\leq z \\ p\in B}} \frac{w(p)}{p} +^{\eta} \sum_{\substack{p\leq z \\ p\in B}} \frac{w(p)\log p}{p} \right).$$

Agora pela segunda hipótese do Teorema 35, temos que para algum $k > 0$,

$$\sum_{\substack{p\leq z \\ p\in B}} \frac{w(p)\log p}{p} \leq kz + O(1).$$

Assim, fazendo $f(t) = 1/\log t$ e

$$c_n = \begin{cases} \dfrac{w(n)\log n}{n} & \text{se } n \in P, \\ 0 & \text{caso contrário.} \end{cases}$$

temos que,

$$C(z) = \sum_{\substack{p\leq z \\ p\in B}} \frac{w(p)\log p}{p} \leq k\log z + O(1).$$

Assim, por somas parciais seque que,

$$\begin{aligned} \sum_{\substack{p\leq z \\ p\in B}} \frac{w(p)}{p} &= \sum_{\substack{p\leq z \\ p\in B}} \frac{w(p)\log p}{p}\frac{1}{\log p} = C(z)\frac{1}{\log z} + \int_{n_0}^{z} \frac{C(u)}{u(\log u)^2}du \\ &\leq \frac{k\log z + O(1)}{\log z} \int_{n_0}^{z} \frac{k\log u + O(1)}{u(\log u)^2}du, \end{aligned}$$

onde $n_0 = \min\{P\}$.

Segue que

$$\sum_{\substack{p\leq z \\ p\in B}} \frac{w(p)}{p} \leq k + \frac{O(1)}{\log z} + k(\log\log z - \log\log n_0) + O(1).\left(-\frac{1}{\log z} + \frac{1}{\log n_0}\right),$$

assim,

$$\sum_{\substack{p\leq z \\ p\in B}} \frac{w(p)}{p} \leq k\log\log z + O(1).$$

Novamente usando o fato de que a função exp é monótona, temos

$$\begin{aligned} F(t,z) &\leq t \exp\left(-\eta \log t + \sum_{\substack{p\leq z \\ p\in B}} \frac{w(p)}{p} +^{\eta} \sum_{\substack{p\leq z \\ p\in B}} \frac{w(p)\log p}{p} \right) \\ &\leq t\exp(-\eta\log t + k\log\log z + O(1) + \eta z^{\eta}(k\log z + O(1))) \\ &= t\exp(-\eta\log t + k\log\log z + \eta z^{\eta} k\log z)\exp(O(1))\exp(\eta z^{\eta} O(1)). \end{aligned}$$

Escolhendo $\eta := \dfrac{1}{\log z}$, onde $z > e$, temos

$$\begin{aligned}
&t\exp(-\eta\log t + k\log\log z + \eta z^{\eta}k\log z)\exp(O(1))\exp(\eta z^{\eta}O(1))\\
&= t\exp\left(-\frac{\log t}{\log z} + \log(\log z)^k + z^{\frac{1}{\log z}k}\right)\exp(O(1))\exp\left(\frac{1}{\log z}O(1)z^{\frac{1}{\log z}}\right)\\
&= t\exp\left(-\frac{\log t}{\log z}(\log z)^k\exp(ek)\exp(O(1))\exp\left(\frac{e}{\log z}O(1)\right)\right)\\
&\leq t(\log z)^k\exp\left(-\frac{\log t}{\log z}\exp(ek)\exp(O(1))\exp(r)\right),
\end{aligned}$$

para alguma constante positiva r, uma vez que $\exp\left(\dfrac{e}{\log z}O(1)\right) \leq \exp(r)$. Logo

$$F(t,z) = O\left(t(\log z)^k\exp\left(-\frac{\log t}{\log z}\right)\right).$$

□

Lema 11. *Com as hipóteses do Teorema 35*

$$\sum_{\substack{d|P(z)\\ y<d}}\frac{w(d)}{d} = O\left((\log z)^{k+1}\exp\left(-\frac{\log y}{\log z}\right)\right).$$

Demonstração. Primeiramente temos,

$$\sum_{\substack{y<d\leq x\\ d|P(z)}}\frac{w(d)}{d} = \sum_{\substack{d\leq x\\ d|P(z)}}\frac{w(d)}{d} - \sum_{\substack{d\leq y\\ d|P(z)}}\frac{w(d)}{d}.$$

Através de somas parciais, usando $f(x) = 1/x$ e

$$c_d = \begin{cases} w(d) & \text{se } d\in P,\\ 0 & \text{caso contrário}\end{cases}$$

temos que,

$$\begin{aligned}
\sum_{\substack{y<d\leq x\\ d|P(z)}}\frac{w(d)}{d} &= F(x,z)\frac{1}{x} + \int_{n_0}^{x}\frac{F(t,z)}{t^2}dt - \left(F(y,z)\frac{1}{y} + \int_{n_0^y}\frac{F(t,z)}{t^2}dt\right)\\
&= F(x,z)\frac{1}{x} - F(y,z)\frac{1}{y} + \int_{y}^{x}\frac{F(t,z)}{t^2}dt.
\end{aligned}$$

Note que a soma $F(x,z)$ é no máximo $\sum_{d|P(z)}w(d)$. Assim, quando $x\to\infty$ temos que

$F(x,z)\frac{1}{x} \to 0, pois\ \frac{1}{x} \to 0$ quando $x \to \infty$, logo

$$\sum_{\substack{y<d \\ d|P(z)}} \frac{w(n)}{n} = -F(y,z)\frac{1}{y} + \int_y^\infty \frac{F(t,z)}{t^2}dt.$$

Como

$$\int_y^\infty \frac{F(t,z)}{t^2}dt = \int_y^\infty \frac{1}{t^2} O\left(t(\log z)^k \exp\left(-\frac{\log t}{\log z}\right)\right) dt \leq \int_y^\infty A\frac{1}{t}(\log z)^k \exp\left(-\frac{\log t}{\log z}\right) dt,$$

para alguma constante positiva A.

Fazendo agora uma substituição na última integral, $u = -\frac{\log t}{\log z}$, temos que $\frac{du}{dt} = -\frac{1}{\log z}\frac{1}{t}$, portanto,

$$\int_y^\infty \frac{1}{t} \exp\left(-\frac{\log t}{\log z}\right) dt = (-\log z) \lim_{x\to\infty} \int_y^x e^u du.$$

Segue que

$$\lim_{x\to\infty} \int_y^x e^u du = -\exp\left(-\frac{\log y}{\log z}\right).$$

Assim,

$$\int_y^\infty \frac{F(t,z)}{t^2}dt \leq A(\log z)^k(-\log z) \lim_{x\to\infty} \int_y^x e^u du = A(\log z)^{k+1} \exp\left(-\frac{\log y}{\log z}\right).$$

Sabemos também, pelo Lema 10, que

$$-F(y,z)\frac{1}{y} = \frac{1}{y} O\left(y(\log z)^k \exp\left(-\frac{\log y}{\log z}\right)\right),$$

assim, para alguma constante positiva B, temos

$$\left|-F(y,z)\frac{1}{y}\right| \leq B(\log z)^k \exp\left(-\frac{\log y}{\log z}\right) \leq B(\log z)^{k+1} \exp\left(-\frac{\log y}{\log z}\right).$$

Portanto, podemos concluir que

$$\sum_{\substack{y<d \\ d|P(z)}} \frac{w(d)}{d} = O\left((\log z)^{k+1} \exp\left(-\frac{\log y}{\log z}\right)\right).$$

□

Vejamos agora a demonstração do Teorema 35.

Pelo princípio de inclusão-exclusão temos,

$$|S(A,P,z)| = \sum_{\substack{d\leq y \\ d|P(z)}} \mu(d)|A_d| = \sum_{\substack{d\leq y \\ d|P(z)}} \mu(d)\left(X\frac{w(d)}{d} + r_d\right).$$

Como

$$\left|\sum_{\substack{d\leq y\\ d|P(z)}}\mu(d)r_d\right| \leq \sum_{\substack{d\leq y\\ d|P(z)}}|\mu(d)r_d| = \sum_{\substack{d\leq y\\ d|P(z)}}|r_d|.$$

Pela primeira hipótese, temos que $|r_d| = O(w(d))$, portanto existe uma menor constante $c_d > 0$ tal que $|r_d| \leq c_d w(d)$. Fazendo $C = \max_d\{c_d\}$ temos que

$$\sum_{\substack{d\leq y\\ d|P(z)}}|r_d| \leq C\sum_{\substack{d\leq y\\ d|P(z)}}w(d)$$

portanto,

$$|S(A,P,z)| = \sum_{\substack{d\leq y\\ d|P(z)}}\mu(d)X\frac{w(d)}{d} + O(F(y,z)). \tag{4.13}$$

Novamente, utilizando o fato de que w é uma função multiplicativa temos que

$$\sum_{d|P(z)}\mu(d)\frac{w(d)}{d} = \prod_{\substack{p<z\\ p\in B}}\left(1+\frac{\mu(p)w(p)}{p}\right) = \prod_{\substack{p<z\\ p\in B}}\left(1-\frac{w(p)}{p}\right).$$

Sabendo também que,

$$\sum_{d|P(z)}\mu(d)\frac{w(d)}{d} = \sum_{\substack{d\leq y\\ d|P(z)}}\mu(d)\frac{w(d)}{d} + \sum_{\substack{y<d\\ d|P(z)}}\mu(d)\frac{w(d)}{d}$$

segue que a equação (4.13) pode ser escrita como

$$|S(A,P,z)| = X\left(\sum_{d|P(z)}\mu(d)\frac{w(d)}{d} - \sum_{\substack{y<d\\ d|P(z)}}\mu(d)\frac{w(d)}{d}\right) + O(F(y,z)),$$

e, portanto,

$$|S(A,P,z)| = XW(z) - X\sum_{\substack{y<d\\ d|P(z)}}\mu(d)\frac{w(d)}{d} + O(F(y,z)).$$

Como d é um inteiro livre de quadrados e $w(d) > 0$, segue que

$$\left|\sum_{\substack{y<d\\ d|P(z)}}\mu(d)\frac{w(d)}{d}\right| \leq \sum_{\substack{y<d\\ d|P(z)}}\frac{w(d)}{d}.$$

Portanto

$$|S(A,P,z)| = XW(z) - XO\left(\sum_{\substack{y<d\\ d|P(z)}} \frac{w(d)}{d}\right) + O(F(y,z)).$$

Pelos Lemas 10 e 11 temos que

$$|S(A,P,z)| = XW(z) - XO\left((\log z)^{k+1}\exp\left(-\frac{\log y}{\log z}\right)\right) + O\left(y(\log z)^k \exp\left(-\frac{\log y}{\log z}\right)\right).$$

Fazendo $y = CX$ para alguma constante positiva C, temos que

$$y(\log z)^k \exp\left(-\frac{\log y}{\log z}\right) = O\left(X(\log z)^{k+1}\exp\left(-\frac{\log y}{\log z}\right)\right).$$

Portanto,

$$|S(A,P,z)| = XW(z) - O\left(X(\log z)^{k+1}\exp\left(-\frac{\log y}{\log z}\right)\right).$$

Por fim vamos mostrar que

$$X(\log z)^{k+1}\exp\left(-\frac{\log y}{\log z}\right) = O\left(X(\log z)^{k+1}\exp\left(-\frac{\log X}{\log z}\right)\right).$$

De fato, como $\exp\left(-\frac{\log C}{\log z}\right) \leq \exp(r)$ para alguma constante positiva r, temos

$$\begin{aligned}\left|X(\log z)^{k+1}\exp\left(-\frac{\log CX}{\log z}\right)\right| &= \left|X(\log z)^{k+1}\exp\left(-\frac{\log C}{\log z} - \frac{\log X}{\log z}\right)\right| \\ &\leq \exp(r)\left|X(\log z)^{k+1}\exp\left(-\frac{\log X}{\log z}\right)\right|.\end{aligned}$$

Portanto,

$$|S(A,P,z)| = XW(z) - O\left(X(\log z)^{k+1}\exp\left(-\frac{\log X}{\log z}\right)\right)$$

e isso conclui a demonstração.

Uma consequência imediata do último resultado é o corolário.

Corolário 1. *Se $\pi(X)$ denota o número de primos menores do que ou iguais a X, então*

$$\pi(x) = O\left(\frac{X}{\log X}\log\log X\right).$$

Demonstração. De fato, sejam A o conjunto dos inteiros menores do que X, P o conjunto dos números primos menores do que ou iguais a z, para algum z a ser escolhido futuramente.

Quando tomamos $w(d) = 1$, estamos contando uma classe de resíduo módulo d, no nosso caso queremos os inteiros na classe de resíduo 0 módulo d. Além disso, a função w definida desta forma, para todos os inteiros d livres de quadrados e compostos por primos em P, é multiplicativa. Com essa escolha vemos que as hipóteses do Teorema 35 satisfazem:

1. $|r_d| = O(1)$.

2. Para $k = 1$,
$$\sum_{p \leq z} \frac{\log p}{p} = \log z + O(1).$$

3. Para $C > 0$ e $y = CX$, temos $|A_d = 0|$ para todo $d > y$.

Então, pelo Teorema 35

$$|S(A, P, z)| = X.W(z) + O\left(X(\log z)^2 exp\left(-\frac{\log X}{\log z}\right)\right), \tag{4.14}$$

onde

$$W(z) = \prod_{p<z}\left(1 - \frac{1}{p}\right).$$

Vimos também que para alguma constante positiva

$$\prod_{p<z}\left(1 - \frac{1}{p}\right) < \frac{1}{c \log z}$$

e portanto,

$$|S(A, P, z)| < X\frac{1}{c \log z} + O\left(X(\log z)^2 exp\left(-\frac{\log X}{\log z}\right)\right).$$

Escolhendo $z = \exp\left(\frac{\log X}{3 \log\log X}\right)$, segue que $\log z = \frac{\log X}{3 \log\log X}$ e portanto temos

$$\begin{aligned} |S(A, P, z)| &< X\frac{1}{c\frac{\log X}{3 \log\log X}} + O\left(X\left(\frac{\log X}{3 \log\log X}\right)^2 exp\left(-\frac{\log X}{\frac{\log X}{3 \log\log X}}\right)\right) \\ &= X\frac{3 \log\log X}{C \log X} + O\left(\frac{X}{(3 \log\log X)^2 \log X}\right). \end{aligned}$$

Tome

$$f_1(X) = \frac{X}{(3 \log\log X)^2 \log X}.$$

Observe que

$$\left|X\frac{3 \log\log X}{C \log X} + f_1(X)\right| \leq \left|X\frac{3 \log\log X}{C \log X}\right| + A\left|\frac{X}{(3 \log\log X)^2 \log X}\right|,$$

observe também que a função

$$\left|X\frac{3 \log\log X}{C \log X}\right|$$

cresce mais rapidamente que a função

$$A\left|\frac{X}{(3 \log\log X)^2 \log X}\right|.$$

Portanto, podemos concluir que

$$|S(A,P,z)| = O\left(\frac{X}{\log X}\log\log X\right).$$

Observe no entanto que

$$\pi(X) - \pi(z) \leq |S(A,B,z)|,$$

uma vez que no conjunto $S(A,P,z)$ estão o número 1, todos os primos do intervalo $z < p < X$ e os números compostos que são produto de primos maiores do que z. Assim segue que

$$\pi(X) \leq |S(A,P,z)| + \pi(z) \leq |S(A,P,z)| + z.$$

Como $z = \exp\left(\frac{\log X}{3\log\log X}\right)$, temos

$$\pi(x) = O\left(\frac{X}{\log X}\log\log X\right).$$

□

Podemos notar que esta aproximação à função é melhor que a obtida na seção 4.2, confirmando uma “melhora"usando este crivo. Mesmo assim, estão longe da aproximação assintótica obtida no capitulo 2 deste trabalho.

Referências Bibliográficas

[1] Apostol, T. M.: *Introduction to analytic number theory.* Springer Science & Business Media, 2013.

[2] Bak, J., Newman, D. J. e Newman, D. J.: *Complex analysis.* Springer, 2010.

[3] Cojocaru, A. C., Murty, M. R. *et al.*: *An introduction to sieve methods and their applications*, vol. 66. Cambridge University Press, 2006.

[4] Dirichlet, P. G. L.: *There are infinitely many prime numbers in all arithmetic progressions with first term and difference coprime.* arXiv preprint arXiv:0808.1408, 2008.

[5] Erdös, P.: *On a new method in elementary number theory which leads to an elementary proof of the prime number theorem.* Proceedings of the National Academy of Sciences of the United States of America, 35(7):374, 1949.

[6] Garcia, S. R.: *The Prime Number Theorem as a Capstone in a Complex Analysis Course.* arXiv preprint arXiv:2005.12694, 2020.

[7] Hadamard, J.: *Sur la distribution des zéros de la fonction $\zeta(s)$ et ses conséquences arithmétiques.* Bulletin de la Societé mathematique de France, 24:199–220, 1896.

[8] Nascimento, M. V. S.: *Sobre o Crivo de Eratóstenes-Legendre.* Dissertação de Mestrado-UNICAMP, 2015.

[9] Riemann, B., Dedekind, R. e Weber, H.: *Gesammelte mathematische Werke und wissenschaftlicher Nachlass.* Ripol Classic, 1892.

[10] Rosser, J. B. e Schoenfeld, L.: *Sharper Bounds for the Chebyshev Functions $\theta(x)$ and $\psi(x)$.* Mathematics of computation, pp. 243–269, 1975.

[11] Selberg, A.: *An elementary proof of the prime-number theorem.* Annals of Mathematics, pp. 305–313, 1949.

[12] Vallée Poussin, C. J. De la: *Sur la fonction $\zeta(s)$ de Riemann et le nombre des nombres premiers inférieurs a une limite donnée.* Hayez, 1899.