UNIVERSIDADE FEDERAL DE OURO PRETO
Instituto de Ciências Exatas e Biológicas
Departamento de Matemática

Algumas estimativas assintóticas sobre números primos

Allan Apolinário
Orientador:
Sávio Ribas

Ouro Preto - MG
Fevereiro - 2021

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DE OURO PRETO
REITORIA
INSTITUTO DE CIENCIAS EXATAS E BIOLOGICAS
COLEGIADO DO CURSO DE BACHARELADO EM MATEMATICA

FOLHA DE APROVAÇÃO

Allan Pereira Apolinário

Algumas estimativas assintóticas sobre números primos

Monografia apresentada ao Curso de Bacharelado em Matemática da Universidade Federal de Ouro Preto como requisito parcial para obtenção do título de bacharel em Matemática

Aprovada em 05 de março de 2021

Membros da banca

Dr. Sávio Ribas - Orientador - Universidade Federal de Ouro Preto
Dr.ª Ana Paula da Silva Cota - Universidade Federal de Ouro Preto
Dr. Wanderson Costa e Silva - Universidade Federal de Ouro Preto

Sávio Ribas, orientador do trabalho, aprovou a versão final e autorizou seu depósito na Biblioteca Digital de Trabalhos de Conclusão de Curso da UFOP em 22/04/2021

Documento assinado eletronicamente por **Savio Ribas**, **PROFESSOR DE MAGISTERIO SUPERIOR**, em 22/04/2021, às 12:53, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site http://sei.ufop.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **0136000** e o código CRC **5C8D9902**.

Referência: Caso responda este documento, indicar expressamente o Processo nº 23109.001482/2021-45 SEI nº 0136000

R. Diogo de Vasconcelos, 122, - Bairro Pilar Ouro Preto/MG, CEP 35400-000
Telefone: - www.ufop.br

Agradecimentos

- Agradeço primeiramente a Deus.
- À meus pais, Maria Helena Pereira Apolinário e Marcos Apolinário, que me proporcionaram a oportunidade de iniciar meu sonho.
- À meus irmãos, Samuel e Gustavo, que são minha base.
- À minha namorada, Beatriz, que aceitou iniciar essa jornada comigo e sempre acreditar nas minhas capacidades.
- Ao meu orientador, Sávio, por ser um ótimo orientador, pelas horas dedicadas e pela paciência.
- Aos meus amigos, Cyndi e Igor.

Resumo

Nessa monografia, vamos apresentar alguns dos principais resultados envolvendo os números primos, tais como o Teorema de Chebyshev, o Postulado de Bertrand e as Fórmulas de Mertens. Exibiremos também algumas aplicações e consequências. Nosso principal objetivo é demonstrar o Teorema dos Números Primos e para isso necessitamos de algumas funções especiais, como a Função Zeta de Riemann e as funções multiplicativas (em particular, a Função de Möbius). Veremos também como o Teorema dos Números Primos pode ser generalizado para primos em progressão aritmética.

Palavras-chave: Números primos, Teorema dos números primos, Funções multiplicativas, Teorema de Chebyshev, Postulado de Bertrand, Fórmulas de Mertens, Função Zeta de Riemann.

Abstract

In this monograph, we will present some of the main results involving prime numbers, such as Chebyshev's Theorem, Bertrand's Postulate and Mertens' Formulas. We will also exhibit some applications and consequences. Our main goal is to prove the Prime Number Theorem, and for that we need some special functions, such as the Riemann Zeta Function and multiplicative functions (in particular, the Möbius Function). We will also see how the Prime Number Theorem can be generalized to primes in arithmetic progression.

Keywords: Prime numbers, Prime number theorem, multiplicative functions, Chebyshev's theorem, Bertrand's postulate, Mertens's theorems, Riemann Zeta Function.

Sumário

Capítulo 1

Introdução

Um número natural p é dito *primo* se o conjunto dos seus divisores positivos possui apenas dois elementos: 1 e p. Os primeiros números primos menores que 100 são: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97. Existem números primos grandes, como por exemplo $2^{82,589,933} - 1$ (esse é o maior número primo conhecido, que foi descoberto em 2018 por Patrick Laroche e possui 24862048 dígitos). Para encontrar tal primo foi utilizado um software especial criado pelo projeto GIMPS (*Great Internet Mersenne Prime Search*) em 1996. O projeto GIMPS se baseia nos primos de Mersenne, que são primos da forma $M_p = 2^p - 1$. Notemos que se p é composto, digamos $p = ab$, então

$$M_p = (2^a)^b - 1 = (2^a - 1)[(2^a)^{b-1} + (2^a)^{b-2} + \cdots + 2^a + 1],$$

ou seja, M_p é composto. Por outro lado, se p primo então M_p pode ser primo ou composto ($M_3 = 7$ é primo, $M_{11} = 2047 = 23 \times 89$ é composto). Observe que utilizando os *primos de Mersenne* fica mais "fácil" achar primos, pois podemos restringir nossa busca ao expoente primo, diminuindo o trabalho computacional. Existem diversas formas de testar a primalidade de um número. Os dois tipos de testes de primalidade são: os testes determinísticos e os testes probabilísticos. Os testes determinísticos dizem se o número testado é primo ou não, já os testes probabilísticos dão como respostas: o número não é primo ou o número é provavelmente primo. Os testes probabilísticos levam a vantagem de serem mais rápidos que os testes determinísticos, em contrapartida os testes determinísticos são exatos. O teste probabilístico mais eficiente é o teste de Miller-Rabin que tem como base o seguintes teorema:

Teorema 1.0.1 (Pequeno Teorema de Fermat)**.** *Se p é um número primo, então para qualquer inteiro a, temos que*

$$a^p \equiv a \pmod{p}.$$

Podemos escrever o Pequeno Teorema de Fermat na seguinte forma: Se existe $1 < a < n$ tal que $a^n \not\equiv a \pmod{n}$, então n é composto. A ideia do teste de Miller-Rabin é selecionar ao acaso diversas bases a tal que $1 < a < n$ e verificar se vale o Pequeno Teorema de Fermat para cada uma delas. Se não valer, n é provavelmente primo (inconclusivo). Se n é composto e divide $a^{n-1} - 1$, dizemos que n é *pseudoprimo* na base a. Por exemplo, 341 é pseudoprimo na base 2, pois $2^{340} \equiv 1 \pmod{341}$ e $341 = 11 \times 31$. Um número composto n que passa no teste de Miller-Rabin para uma determinada base a é chamado *pseudoprimo forte* na base a. Por exemplo, o menor pseudoprimo forte na base 2 é 2047. De fato, 2047 é composto e $2^{2046} \equiv 1 \pmod{2047}$. Dizemos que n é um *número de Carmichael* se $a^n \equiv a \pmod{n}$ para todo inteiro a, isto é, se n é *pseudoprimo* em toda base. Por exemplo, o menor número de Carmichael é $561 = 3 \times 11 \times 17$. Existe um critério devido a Korselt (1899, ver [1]) que diz que n ímpar é número de Carmichael se, e somente se, n é livre de quadrados e $p - 1 \mid n - 1$ para todo primo $p \mid n$. Em 1994, Alford, Granville e Pomerance [1] provaram que existem infinitos números de Carmichael, o que significa que o teste de Miller-Rabin é de fato probabilístico.

Existem também primos com algumas características especiais, como exemplo podemos citar *primos gêmeos*, que advém da seguinte definição: Um par de primos é chamado de primos gêmeos se eles são dois números primos p e q tais que $q = p + 2$. Outro exemplo de primos especiais são os chamados de primos de Sophie Germain que resultam da definição: Um número primo p é um número *primo de Sophie Germain* se $2p + 1$ é também primo. A infinidade dos primos gêmeos e primos de Sophie Germain é uma conjectura. Os primos de Sophie Germain se relacionam com os primos de Mersenne através da seguinte proposição, que não será provada nesse texto.

Proposição 1.0.2 ([2, Proposição 7.27])**.** *Seja p primo, $p \equiv 3 \pmod{4}$. Então $2p + 1$ é primo se, e somente se, $2p + 1$ divide M_p.*

Não se conhece nenhuma fórmula "útil" que gere todos e apenas números primos na ordem correta. Por outro lado, podemos citar dois exemplos de fórmulas que não são muito úteis computacionalmente, que são

$$p_n = \left[1 - \frac{1}{\log 2} \log \left(-\frac{1}{2} + \sum_{d \mid P_n - 1} \frac{\mu(d)}{2^d - 1} \right) \right],$$

em que $P_{n-1} = p_1 p_2 \ldots p_{n-1}$, (ou seja, é necessário conhecer todos os primos anteriores a p_n), outra fórmula é a seguinte

$$p_n = \lfloor 10^{2^n} c \rfloor - 10^{2^{n-1}} \lfloor 10^{2^{n-1}} c \rfloor,$$

em que

$$c = \sum_{n=1}^{\infty} \frac{p_n}{10^{2^n}} = 0.2030\ldots$$

(ou seja, precisamos saber todos os primos para utilizar a última fórmula). Em algum momento achou-se que a fórmula $x^2 - x + 41$ daria conta de gerar primos e realmente tal fórmula gera primos mas apenas para valores naturais de $x \leq 40$. Para $x = 41$ temos um número composto: 41^2. Os primos de Mersenne também se relacionam aos números perfeitos. Um número n é *perfeito* se a soma dos seus divisores positivos é igual a $2n$. Por exemplo, 6 e 28 são perfeitos, pois a soma dos divisores de 6 é $1 + 2 + 3 + 6 = 12$ e a soma dos divisores de 28 é $1 + 2 + 4 + 7 + 14 + 28 = 56$. Os números perfeitos são da forma $2^{p-1}M_p$, onde M_p é primo (ver [2, Proposição 7.2.3]). Conjectura-se que não existem números perfeitos ímpares.

Por volta dos anos $300a.C.$, Euclides deu a seguinte demonstração para a existência de infinitos números primos: Suponha que não existam infinitos números primos. Consequentemente, podemos concluir que existe um maior número primo p. Considere o número

$$p(p-1)(p-2)\cdots 1 + 1 = N$$

Note que se q é um divisor primo de N, então $q \leq p$, por suposição, e daí $q|p!$. Portanto $q \mid N - p! = 1$, absurdo! Isso completa a prova.

Os números primos têm grande importância na matemática, tanto teórica como prática. O primeiro resultado teórico sobre os números primos é o Teorema Fundamental da Aritmética, o qual afirma que todo número natural pode ser escrito de forma única (a menos da ordem dos fatores) como produto de primos. Resultados práticos são fornecidos, por exemplo, pela criptografia (ver [3], onde o sistema criptográfico RSA, que é o mais usado atualmente, depende fortemente da dificuldade computacional de se fatorar números que possuem fatores primos grandes). Os números primos também são usados na teoria de códigos corretores de erros usado em corpos finitos: a cardinalidade de qualquer corpo finito é sempre uma potência de um primo (ver [6]). Nessa monografia, vamos estudar o comportamento assintótico dos números primos. Em particular, daremos outra demonstração do Teorema de Euclides. Veremos diversas expressões que envolvem números primos, juntamente com o comportamento dessas expressões. Nosso principal objetivo é demonstrar o Teorema dos Números Primos, que afirma basicamente que o número de primos até x é aproximadamente $\frac{x}{\log x}$. A principal ferramenta para provar esse teorema vem da função Zeta de Riemann, que é uma função sobre os números complexos.

No Capítulo 2, vamos estudar as principais funções aritméticas multiplicativas (entre elas, a função phi de Euler e a função de Möbius) e suas propriedades. Veremos que a

fatoração dos números ajudará a calcular o valor dessas funções. No Capítulo 3, veremos o comportamento dos números primos de forma mais elementar. Vamos apresentar o Teorema de Chebyshev (que é uma versão mais fraca porém assintoticamente correta do Teorema dos Números Primos), o Postulado de Bertrand (que afirma que entre n e $2n$ sempre há um primo) e as Fórmulas de Mertens (que determinam algumas expressões envolvendo primos). No Capítulo 4, vamos provar (a menos de alguns pormenores envolvendo as transformadas de Laplace e Mellin) o Teorema dos Números Primos, que é o principal resultado dessa monografia. Além disso, exibiremos algumas consequências desses teoremas e enunciaremos os análogos de alguns dos resultados dessa monografia para primos em progressão aritmética.

Nossa principal referência é o livro [2].

1.1 Notações

Denotaremos o conjunto dos números naturais como $\mathbb{N} = \{1, 2, 3, \dots\}$. Sejam as funções $f : \mathbb{N} \to \mathbb{R}$ e $g : \mathbb{N} \to (0, \infty)$. Escrevemos

- $f(n) = o(g(n))$ se $\lim_{n\to\infty} \frac{f(n)}{g(n)} = 0$.
- $f(n) = O(g(n))$ se existe $C > 0$ com $|f(n)| < Cg(n)$ para todo n grande.

Seja $x \in \mathbb{R}$. Então $\lfloor x \rfloor = \max\{n \in \mathbb{Z}; n \leq x\}$ (*função piso*) . Além disso, a *parte fracionária* de x é $\{x\} = x - \lfloor x \rfloor$. No decorrer do texto denotaremos log como o logaritmo natural. Ao citarmos o divisor de um número natural estaremos os referindo ao divisor positivo do mesmo. Além disso, as incógnitas $p, p_1, p_2 \dots$ sempre denotarão números primos.

Capítulo 2

Funções Aritméticas

Nesse capítulo, vamos apresentar algumas das principais funções multiplicativas e suas propriedades. Em particular, veremos que para avaliar uma função multiplicativa basta conhecer seus valores em potências de primos.

2.1 Funções Multiplicativas

Definição 2.1.1. *Diz-se que uma função f definida sobre $\mathbb{N}$ é* multiplicativa *se dados dois números naturais a e b tais que $mdc(a,b) = 1$ então $f(ab) = f(a)f(b)$, e* totalmente multiplicativa *se $f(ab) = f(a)f(b)$ para todo a e b.*

A seguir, veremos a definição da função φ e algumas outras funções multiplicativas importantes. Pela definição de função multiplicativa, se $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ é a fatoração de n em primos, obtida pelo Teorema Fundamental da álgebra, e se f é multiplicativa, então $f(n) = f(p_1^{\alpha_1}) \dots f(p_k^{\alpha_k})$, ou seja, basta saber o valor de f nas potências de primos. No caso em que f é totalmente multiplicativa, teremos $f(n) = f(p_1)^{\alpha_1} \dots f(p_k)^{\alpha_k}$, logo basta saber o valor de f nos primos.

Definição 2.1.2. *A função*

$$\varphi(n) = \#\{a \in \mathbb{N}; 1 \leq a \leq n \text{ e } mdc(a,n) = 1\}$$

é denominada função phi de Euler*, onde # denota a cardinalidade do referido conjunto.*

Exemplo 2.1.3. *$\varphi(4) = 2$, pois existem apenas dois números inteiros positivos até 4 que são primos com 4 (1 e 3) e $\varphi(10) = 4$ pois $1, 3, 7$ e 9 são os únicos números inteiros positivos até 10 que são primos com 10.*

Proposição 2.1.4. *Se $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ a fatoração de n em primos, então $\varphi(n) = n \prod_{1 \leq i \leq k} \left(1 - \frac{1}{p_i}\right)$. Em particular, φ é multiplicativa.*

Demonstração. Temos $\varphi(1) = \varphi(2) = 1$. Caso p seja primo, $\varphi(p) = p - 1$. Além disso, $mdc(a, p^k) = 1$ se, e somente se, p não divide a. Como existem p^{k-1} múltiplos de p entre 1 e p^k, temos $\varphi(p^k) = p^k - p^{k-1}$. Vamos mostrar agora que φ é multiplicativa. Sejam m, n naturais primos entre si e olhamos para o seguinte arranjo matricial:

$$\begin{array}{ccccc} 1 & 2 & 3 & \cdots & n \\ n+1 & n+2 & n+3 & \cdots & 2n \\ 2n+1 & 2n+2 & 2n+3 & \cdots & 3n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ n(m-1)+1 & n(m-1)+2 & n(m-1)+3 & \cdots & n(m-1)+n \end{array}$$

Observe que $mdc(ni + j, n) = mdc(j, n)$. Assim, se um número desta tabela é coprimo com n então todos os números dessa coluna também serão coprimos com n. Consequentemente, existem $\varphi(n)$ colunas tais que todos os números da coluna são coprimos com n. Em contrapartida, toda coluna representa um conjunto completo de restos módulo n, pois caso $ni_1 + j \equiv ni_2 + j \pmod{m}$ teremos $i_1 \equiv i_2 \pmod{m}$. Como $0 \leq i_1, i_2 < m$, devemos ter $i_1 = i_2$. Assim, cada coluna tem exatamente $\varphi(m)$ números coprimos com m. Logo, $\varphi(mn) = \varphi(m)\varphi(n)$. □

Definição 2.1.5. *Seja $n \in \mathbb{N}$. Definimos $d(n)$ como o número de divisores de n.*

Podemos expressar a função definida acima como $d(n) = \sum_{t|n} 1$.

Exemplo 2.1.6. *$d(10) = 4$ pois os divisores de 10 são $1, 2, 5$ e 10, $d(5) = 2$ pois os divisores de 5 são 1 e 5.*

Proposição 2.1.7. *Seja $n = p_1^{\alpha_1} \dots p_m^{\alpha_m}$ a fatoração de n em primos. Então $d(n) = \prod_{i=1}^{m} (\alpha_i + 1)$. Em particular, d é multiplicativa.*

Demonstração. Sejam $a, b \in \mathbb{N}$, com a e b coprimos, sendo $d(a) = s$ e $d(b) = t$, dessa forma os conjuntos de divisores de a e b são

$$D(a) = \{a_1 = 1, a_2, \dots, a_{s-1}, a_s = a\},$$
$$D(b) = \{b_1 = 1, b_2, \dots, b_{t-1}, b_t = b\}.$$

Como a e b são coprimos, qualquer divisor deste produto será da forma $a_i b_j$ com a_i e b_j coprimos, onde $a_i \in D(a)$ e $b_i \in D(b)$. Temos s possibilidades para os divisores de a e t

possibilidades para os divisores de b, logo existem st possibilidades para os divisores de $a_i b_j$. Dessa forma $d(ab) = st = d(a)d(b)$. Se $n = p^\alpha$, então seus divisores são p^β, onde $0 \leq \beta \leq \alpha$, logo temos $\alpha + 1$ divisores de n. Caso $n = p_1^{\alpha_1} \dots p_m^{\alpha_m}$, então o número de divisores é

$$(\alpha_1 + 1) \dots (\alpha_m + 1).$$

□

Definição 2.1.8. *Seja $n \in \mathbb{N}$. Definimos $\sigma(n)$ como a soma dos divisores de n.*

Podemos expressar a função acima como $\sigma(n) = \sum_{t|n} t$.

Exemplo 2.1.9. $\sigma(10) = 1 + 2 + 5 + 10 = 18$, $\sigma(5) = 1 + 5 = 6$, $\sigma(p) = p + 1$.

Proposição 2.1.10. *Seja $n = p_1^{\alpha_1} \dots p_m^{\alpha_m}$ a fatoração de n em primos. Então $\sigma(n) = \prod_{i=1}^m \frac{p_i^{\alpha_i+1}-1}{p_i-1}$. Em particular, σ é multiplicativa.*

Demonstração. Se t é divisor de n então $t = p_1^{\beta_1} \dots p_m^{\beta_m}$. Logo,

$$\begin{aligned}
\sigma(n) &= \sum_{t|n} t = \sum_{\substack{0 \leq \beta_1 \leq \alpha_1 \\ \vdots \\ 0 \leq \beta_m \leq \alpha_m}} p_1^{\beta_1} \dots p_m^{\beta_m} \\
&= \sum_{\substack{0 \leq \beta_1 \leq \alpha_1 \\ \vdots \\ 0 \leq \beta_m \leq \alpha_m}} \prod_{i=1}^m p_i^{\beta_i} = \prod_{i=1}^m \sum_{0 \leq \beta_i \leq \alpha_i} p_i^{\beta_i} \\
&= \prod_{i=1}^m (1 + p_i + p_i^2 + \dots + p_i^{\alpha_i}) \\
&= \prod_{i=1}^m \frac{p_i^{\alpha_i+1} - 1}{p_i - 1},
\end{aligned}$$

onde na segunda linha fatoramos a soma e da penúltima para a última passagem usamos a soma dos termos de uma progressão geométrica. Com isso, segue que se n e $k = q_1^{\gamma_1} \dots q_t^{\gamma_t}$ são coprimos (onde os primos p_i e q_j são todos distintos) então

$$\sigma(nk) = \prod_{i=1}^m \prod_{j=1}^t \frac{p_i^{\alpha_i+1} - 1}{p_i - 1} \frac{q_j^{\gamma_j+1} - 1}{p_j - 1} = \prod_{i=1}^m \frac{p_i^{\alpha_i+1} - 1}{p_i - 1} \cdot \prod_{j=1}^t \frac{q_j^{\gamma_j+1} - 1}{p_j - 1} = \sigma(n)\sigma(k),$$

portanto σ é multiplicativa. □

Definição 2.1.11. *A* Função de Möbius *é definida sobre* $\mathbb{N}$ *da seguinte forma*

$$\mu(n) = \begin{cases} 1, & se \quad n = 1, \\ 0, & se \quad a^2 \mid n \text{ para algum } a > 1, \\ (-1)^k, & se \quad n \text{ é produto de } k \text{ primos distintos.} \end{cases}$$

Exemplo 2.1.12. $\mu(1) = 1$, $\mu(8) = 0$ *pois* $2^2 \mid 8$, $\mu(6) = 1$ *pois* $6 = 2 \cdot 3$, $\mu(p) = -1$.

A função de Möbius atua como um "detector" de números livres de quadrados, isto é, números que não são divisíveis pelo quadrado de nenhum primo. Além disso, o sinal alternado $(-1)^k$ atua como se fosse uma espécie de Princípio da Inclusão e Exclusão. Como uma aplicação disso, citamos o Crivo de Brun [2, Seção 7.1.2].

Proposição 2.1.13. *A função de Möbius é multiplicativa.*

Demonstração. Se $s = 1$, $\mu(st) = \mu(t) = 1\mu(t) = \mu(s)\mu(t)$. Análogo se $t = 1$. Caso $s > 1$ e $t > 1$, se $n^2 \mid s$ ou $n^2 \mid t$, temos $\mu(s) = 0$ *ou* $\mu(t) = 0$, daí $\mu(st) = 0$, o que implica $\mu(st) = 0 = \mu(s)\mu(t)$. Por último, temos o caso em que s é produto de k primos distintos e t o produto de j primos distintos, digamos, $s = p_1 p_2 \dots p_k, t = q_1 q_2 \dots q_j$ *e* $mdc(s,t) = 1$. Essa última condição implica que st é livre de quadrados, logo $\mu(st) = \mu(p_1 p_2 \dots p_k q_1 q_2 \dots q_j) = (-1)^{k+j} = (-1)^k(-1)^j = \mu(s)\mu(t)$. □

Teorema 2.1.14. *Se* f *é uma função multiplicativa então a função*

$$F(n) = \sum_{d \mid n} f(d)$$

é também multiplicativa.

Demonstração. Sejam $a, b \in \mathbb{N}$ tais que $mdc(a,b) = 1$. Então

$$\begin{aligned} F(ab) &= \sum_{d \mid ab} f(d) = \sum_{d_1 \mid a, d_2 \mid b} f(d_1 d_2) = \sum_{d_1 \mid a, d_2 \mid b} f(d_1) f(d_2) \\ &= \sum_{d_1 \mid a} \sum_{d_2 \mid b} f(d_1) f(d_2) = \sum_{d_1 \mid a} f(d_1) \sum_{d_2 \mid b} f(d_2) \\ &= F(a)F(b), \end{aligned}$$

onde na segunda igualdade foi usado o fato de que se $d \mid ab$ então $d = d_1 d_2$, onde $d_1 \mid a$ e $d_2 \mid b$, portanto F é multiplicativa. □

Lema 2.1.15. *Para todo* $n \in \mathbb{N}$ *temos*

$$\sum_{d \mid n} \mu(d) = \begin{cases} 1, & se \quad n = 1, \\ 0, & se \quad n > 1. \end{cases}$$

Demonstração. Se $n = 1$ temos que $d = 1$, donde $\sum_{d|1} \mu(d) = \mu(1) = 1$, pela definição da função de Möbius. Pela Proposição 2.1.13 a função $\sum_{d|n} \mu(d)$ é multiplicativa, logo resta mostrar o caso $n = p^k$ com p primo e $k \geq 1$. Como $\mu(n) = 0$ *se* $a^2 \mid n$ *para algum* $a > 1$, segue que

$$\sum_{d|p^k} \mu(d) = \mu(1) + \mu(p) + \mu(p^2) + \ldots + \mu(p^k) = 1 + (-1) + 0 + \ldots + 0 = 0.$$

□

Teorema 2.1.16 (Fórmula de inversão de Möbius)**.** *Sejam f uma função multiplicativa e $F(n) = \sum_{d|n} f(d)$, então vale*

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

Demonstração.

$$\begin{aligned}\sum_{d|n} \mu(d) F\left(\frac{n}{d}\right) &= \sum_{d|n} \mu(d) \sum_{d_1|\frac{n}{d}} f(d_1) = \sum_{d|n} \sum_{d_1|\frac{n}{d}} \mu(d) f(d_1) \\ &= \sum_{d_1|n} \sum_{d|\frac{n}{d_1}} \mu(d) f(d_1) = \sum_{d_1|n} f(d_1) \sum_{d|\frac{n}{d_1}} \mu(d) = f(n)\mu(1) = f(n).\end{aligned}$$

□

Capítulo 3

Algumas estimativas sobre primos

3.1 Teorema de Chebyshev

Nesta seção vamos estudar o comportamento assintótico de algumas funções envolvendo números primos e obter estimativas sobre o crescimento das mesmas, com isso conseguiremos entender o comportamento das funções aritméticas da seção anterior.

Proposição 3.1.1 (Fatores do fatorial)**.** *Se p é um número primo e p^α é a maior potência de p que divide $n!$, então*

$$\alpha = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \dots$$

Demonstração. Observe que na expansão de $n!$, somente os números múltiplos de p adicionam um fator p. Existem $\left\lfloor \frac{n}{p} \right\rfloor$ múltiplos de p entre 1 e n. Sendo que os fatores múltiplos de p^2 adicionam um fator p a mais, temos mais $\left\lfloor \frac{n}{p^2} \right\rfloor$ potências, assim sucessivamente para $p^3, p^4, \dots$ Como resultado temos a fórmula de α. □

Exemplo 3.1.2. *Com quantos zeros termina o número* $2021!$*?*
Os zeros do número $2021!$ *são produzidos pelos fatores* $10 = 2 \cdot 5$*. Como temos mais fatores* 2 *do que fatores* 5 *entre* 1 *e* 2021*, basta saber quantos fatores* 5 *temos entre* 1 *e* $2021!$*. Utilizando a Proposição 3.1.1,temos que o número de fatores* 5 *em* $2021!$ *é*

$$\alpha = \left\lfloor \frac{2021}{5} \right\rfloor + \left\lfloor \frac{2021}{5^2} \right\rfloor + \left\lfloor \frac{2021}{5^3} \right\rfloor + \left\lfloor \frac{2021}{5^4} \right\rfloor + \left\lfloor \frac{2021}{5^5} \right\rfloor = 404 + 80 + 16 + 3 + 0 = 503.$$

Com isso o número de zeros à direita de $2021!$ *é* 503*.*

Lema 3.1.3. *Sejam $n \in \mathbb{N}$, p um número primo e θ_p o inteiro tal que $p^{\theta_p} \leq 2n < p^{\theta_p+1}$. Resulta que θ_p é o expoente da maior potência de p que divide $\binom{2n}{n}$. Em particular, se*

$p > \sqrt{2n}$ então o expoente da máxima potência de p é 0 ou 1. Também temos que se $\frac{2}{3}n < p < n$ então p não divide $\binom{2n}{n}$.

Demonstração. Sejam α e β os expoentes das maiores potências de p que dividem $(2n)!$ e $n!$ respectivamente. Como visto na proposição acima

$$\alpha = \left\lfloor \frac{2n}{p} \right\rfloor + \left\lfloor \frac{2n}{p^2} \right\rfloor + \dots \text{ e } \beta = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \dots$$

Dessa forma, temos que o expoente da máxima potência de p que divide $\binom{2n}{n} = \frac{(2n)!}{n!n!}$ é

$$\alpha - 2\beta = \sum_{i=1}^{\theta_p} \left\lfloor \frac{2n}{p^i} \right\rfloor - 2 \left\lfloor \frac{n}{p^i} \right\rfloor.$$

Observe que

$$\frac{2n}{p_i} \geq \left\lfloor \frac{2n}{p^i} \right\rfloor > \frac{2n}{p^i} - 1 \text{ e } -2\left(\frac{n}{p^i} - 1\right) > -2\left\lfloor \frac{n}{p^i} \right\rfloor \geq -2\frac{n}{p^i}.$$

Somando as inequações acima, temos

$$2 > \left\lfloor \frac{2n}{p^i} \right\rfloor - 2 \left\lfloor \frac{n}{p^i} \right\rfloor > -1.$$

Logo, o termo do meio da inequação pode admitir somente os valores 0 e 1. Consequentemente

$$\alpha - 2\beta \leq \sum_{i=1}^{\theta_p} 1 = \theta_p.$$

Ademais, se $\frac{2n}{3} < p < n$ então $\alpha = 2$ e $\beta = 1$, assim $\alpha - 2\beta = 0$. □

Exemplo 3.1.4. *Tome $n = 4$ e $p = 5$. Dessa forma $\theta_5 = 1$ e $\binom{8}{4} = \frac{8!}{4!(8-4)!} = 70$ que é divisível por 5^1. Para o caso $p > \sqrt{2n}$, tome $p = 7$ e $n = 4$, $\binom{8}{4} = \frac{8!}{4!(8-4)!} = 70$, o expoente da maior potência de 7 que divide 70 é $\theta_7 = 1$. Por fim, para o caso $\frac{2}{3}n < p < n$, tomamos $n = 9$ e $p = 7$ e vemos que 7 não divide $\binom{18}{9} = \frac{18!}{9!(18-9)!} = 48620$, pois deixa resto 5 na divisão por 7.*

Definição 3.1.5. *Seja $x \in \mathbb{R}$. Define-se $\pi(x)$ como a quantidade de números primos menores ou iguais a x.*

Podemos escrever $\pi(x) = \sum_{p \leq x} 1$.

Proposição 3.1.6 (Chebyshev)**.** *Existem $c, C \in \mathbb{R}_+$, com $c < C$ tais que*

$$c\frac{x}{\log x} < \pi(x) < C\frac{x}{\log x}$$

para todo $x \geq 2$.

Demonstração. Inicialmente temos que todo p satisfazendo a condição $n < p \leq 2n$ divide $\binom{2n}{n} = \frac{(2n)!}{n!n!}$. Pelo binômio de Newton, temos

$$\binom{2n}{n} < \sum_{k=0}^{2n} \binom{2n}{k} = (1+1)^{2n} = 2^{2n},$$

e isso acarreta que 2^{2n} é maior que o produto dos primos p com $n < p \leq 2n$. Existem $\pi(2n) - \pi(n)$ primos dessa forma, logo $n^{\pi(2n)-\pi(n)} < 2^{2n}$, daí $(\pi(2n) - \pi(n)) \log\ n < 2n\ \log 2$ e

$$\pi(2n) - \pi(n) < \frac{2n \log 2}{\log n}.$$

Temos que

$$\begin{aligned} \pi(4) - \pi(2) &< \frac{4 \log 2}{\log 2} \\ \pi(8) - \pi(4) &< \frac{8 \log 2}{\log 4} \\ &\vdots \\ \pi(2^{k+1}) - \pi(2^k) &< \frac{2^{k+1} \log 2}{\log 2^k} \end{aligned}$$

Somando-se todos os termos

$$\pi(2^{k+1}) < 1 + \sum_{j=1}^{k} \frac{2^{j+1}}{j}.$$

Vamos provar, por indução, a seguinte desigualdade

$$\pi(2^{k+1}) \leq \frac{5 \cdot 2^k}{k}.$$

Para valores de k até 6, temos

$$\begin{aligned} k = 1 &: \ \pi(2^2) = 2 < \frac{5 \cdot 2^1}{1} = 10 \\ k = 2 &: \ \pi(2^3) = 4 < \frac{5 \cdot 2^2}{2} = 10 \\ k = 3 &: \ \pi(2^4) = 6 < \frac{5 \cdot 2^3}{3} \simeq 13.3 \end{aligned}$$

$$k=4 \;:\; \pi(2^5)=11<\frac{5\cdot 2^4}{4}=20$$
$$k=5 \;:\; \pi(2^6)=18<\frac{5\cdot 2^5}{5}=32.$$

Visto que para $k\leq 6$ o resultado é válido, veremos a indução para $k\geq 6$. Basta provar que $1+\sum_{j=1}^{k}\frac{2^{j+1}}{j}\leq\frac{5\cdot 2^k}{k}$. Supondo que essa última desigualdade vale para algum $k-1\geq 4$ e somando o último termo, teremos

$$1+\sum_{j=1}^{k+1}\frac{2^{j+1}}{j} < \frac{5\cdot 2^k}{k}+\frac{2^{k+2}}{k+1}=\frac{5\cdot 2^k}{k}+\frac{4\cdot 2^k}{k+1}\leq\frac{5\cdot 2^{k+1}}{k+1}\Leftrightarrow\frac{5}{k}+\frac{4}{k+1}<\frac{10}{k+1}$$
$$\Leftrightarrow \frac{5}{k-1}\leq\frac{6}{k}\Leftrightarrow 5(k+1)\leq 6k\Leftrightarrow 5\leq k.$$

Daí segue que se $2^k<x\leq 2^{k+1}$ então $\pi(x)\leq\pi(2^{k+1})\leq\frac{5\cdot 2^k}{k}<\frac{5\cdot x\log 2}{\log x}$, pois a função $\frac{5x\log 2}{\log x}$ é crescente para $x\geq 3$ uma vez que sua derivada $\frac{5\log 2(\log x-1)}{\log^2 x}$ é positiva
Para a segunda desigualdade, temos que, se a fatoração em primos de $\binom{2n}{n}=\prod_{p<2n}p^{\alpha_p}$ então pelo Lema 3.1.3 temos $p^{\alpha_p}\leq 2n$ se, e somente se, $\alpha_p\log p\leq\log 2n$, logo é válido

$$\log\binom{2n}{n}=\sum_{p<2n}\alpha_p\log p\leq\pi(2n)\log(2n),$$

daí

$$\pi(2n)\geq\frac{\log\binom{2n}{n}}{\log(2n)}\geq\frac{n\log 2}{\log(2n)}$$

pois

$$\binom{2n}{n}=\frac{2n}{n}\cdot\frac{2n-1}{n-1}\cdots\frac{n+1}{1}\geq 2^n.$$

Dessa forma,

$$\pi(x)\geq\frac{x\log 2}{2\log x}$$

para todo x inteiro par, logo é valido para todo x inteiro pois $\pi(2k-1)=\pi(2k)$. □

Exemplo 3.1.7.

x	$\pi(x)$	$x/\log x$	$\frac{\pi(x)}{x/\log x}$
10	4	4,3429	0,9210
100	25	21,7147	1,1512
1000	168	144,7648	1,1605
10000	1229	1085,7365	1,1319
100000	9592	8685,8896	1,1043

Corolário 3.1.8. *Seja p_n o n-ésimo primo. Então existem $c', C' \in \mathbb{R}_+^*$ tais que*

$$c' n \log n < p_n < C' n \log n$$

para todo $n \geq 2$.

Observemos numericamente que c' e C' do Corolário 3.1.8 estão se aproximando de 1. No Capítulo 4, vamos mostrar que realmente podemos toma-las tão próximas de 1 quanto quisermos.

Demonstração. Se $\limsup_{n\to\infty} \frac{p_n}{n \log n} > C'$ para todo $C' > 0$, então

$$\begin{aligned} \liminf_{n\to\infty} \frac{\pi(x)}{x/\log x} &\leq \liminf_{n\to\infty} \frac{\pi(p_n)}{p_n/\log p_n} \leq \liminf_{n\to\infty} \frac{n}{C' \log n/\log(C' \log n)} \\ &\leq \liminf_{n\to\infty} \frac{n(\log C' + \log n + \log\log n)}{C' n \log n} = \frac{1}{C'}, \end{aligned}$$

uma vez que para $x \geq 3$, $\frac{x}{\log x}$ é crescente. Como $\liminf_{n\to\infty} \frac{\pi(x)}{x/\log x} > 0$ e utilizando resultados da Proposição 3.1.6, temos que existe C' tal que $p_n < C' n \log n$ para todo $n \geq 2$. Caso análogo para a demostração da existência de c', basta trocar C' por c' e todas as desigualdades. □

Exemplo 3.1.9. *Uma prova da infinidade dos primos, atribuída a Paul Erdős é a seguinte: suponha por absurdo que a série dos inverso dos primos é convergente, logo existe uma constante positiva k tal que*

$$\sum_{i=k+1}^{\infty} \frac{1}{p_i} < \frac{1}{2}.$$

Defina o conjunto $S(x)$ como o conjunto dos números $n \in \mathbb{N}$ com $n \leq x$, tal que n é divisível apenas por alguns primos $2, 3, 5, \ldots, p_k$, isto é,

$$S(x) = \{n \in \mathbb{N} : n \leq x \wedge p_i \nmid n, \forall i > k\}.$$

Defina o conjunto $N(x)$ como o número de elementos do conjunto $S(x)$. Para provarmos o resultado vamos estabelecer valores máximos e mínimos para $N(x)$ e observar o que acontece para x grande. Primeiro provaremos que vale a seguinte cota superior para $N(x)$

$$N(x) \leq 2^k \sqrt{x}.$$

Segue do Teorema Fundamental da Aritmética que todo $r \in \mathbb{N}$ pode ser escrito como $r = sm^2$, onde s é um natural livre de quadrados. Os elementos r pertencentes ao conjunto

$S(x)$ só podem ter em sua decomposição os primos $p_1, p_2, \ldots, p_k$. Logo $s = p_1^{e_1} \cdot p_2^{e_2} \ldots p_k^{e_k}$, onde os expoentes e_i valem 0 ou 1. Dessa forma existem 2^k possibilidades para o valor de s. Como $1 \leq m^2 \leq x$, temos no máximo $\sqrt{x}$ possibilidades para o valor de m. Logo, temos $2^k\sqrt{x}$ possibilidades para $N(x)$. Agora, vamos provar a seguinte cota inferior:

$$N(x) > \frac{x}{2}$$

O complemento do conjunto $S(x)$ tem $x - N(x)$ elementos. Cada elemento nesse conjunto complementar a $N(x)$ deve ser divisível por algum primo p_i com $i > k$. No entanto, a quantidade de números naturais em tal conjunto complementar que são divisíveis por p_i é menor que $\frac{x}{p_i}$. Portanto

$$x - N(x) \leq \sum_{i=k+1}^{\infty} \frac{x}{p_i} = x \sum_{i=k+1}^{\infty} \frac{1}{p_i} < \frac{x}{2},$$

ou seja, $N(x) > \frac{x}{2}$.
Assim, vemos que para x grande as cotas superiores e inferiores se contradizem.

3.2 O Postulado de Bertrand

Dado $k > 1$ natural arbitrário, podemos construir uma sequência arbitrariamente longa formada apenas por números compostos. A sequência a seguir possui $k - 1$ termos, todos compostos:

$$k! + 2, k! + 3, k! + 4, \ldots, k! + k.$$

De fato para $2 \leq j \leq k$ temos que $k! + j$ é múltiplo de j, logo $k! + j$ não é primo. Na seção a seguir, veremos que os números primos não são tão esparsos, apesar da existência de sequências longas formadas apenas por números compostos. Vamos apresentar o "postulado"de Bertrand, também conhecido como Teorema de Chebyshev, por ter sido demonstrado por Pafnuti Chebyshev.

Lema 3.2.1. *Para todo $n \geq 2$, vale a desigualdade*

$$\prod_{\substack{p \leq n \\ p \text{ primo}}} p < 4^n.$$

Demonstração. Vamos provar por indução em $n \geq 2$. Para $n = 2$ temos $2 < 4^2$. Suponha que a desigualdade seja válida para algum $n \geq 2$. Dividiremos a demonstração do lema

em dois casos, caso n seja par e caso n seja ímpar. Se n for par então

$$\prod_{p\leq n} p = \prod_{p\leq n-1} p < 4^{n-1} < 4^n$$

Para n ímpar iremos tomar $n = 2m+1$. Para todo p primo vale que se $m+1 \leq p \leq 2m+1$ então p divide $(2m+1)!$ mas não divide $(m+1)!$ e $(m)!$, logo

$$\prod_{m+1<p\leq 2m+1} p \leq \binom{2m+1}{m+1} = \binom{2m}{m+1} + \binom{2m}{m} < (1+1)^{2m} = 4^m,$$

na igualdade foi utilizada a relação de Stifel. Por hipótese de indução, temos

$$\prod_{p\leq 2m+1} p = \prod_{p\leq m+1} p \prod_{m+1<p\leq 2m+1} p < 4^{m+1}4^m = 4^{2m+1} = 4^n.$$

Pelo Princípio de Indução, obtemos o resultado desejado. □

Teorema 3.2.2 (Postulado de Bertrand)**.** *Para todo n sempre haverá p primo tal que $n \leq p \leq 2n$.*

Demonstração. Faremos a prova por contradição: iremos supor que o resultado é falso para um n e veremos que n não pode ser muito grande.
Considere α_i a máxima potência do primo p_i tal que $p_i^{\alpha_i} \mid \binom{2n}{n}$. Pelo Lema 3.1.3 não há primo p entre $\frac{2n}{3}$ e n tal que p, nesse intervalo, divida $\binom{2n}{n}$. Outro resultado do Lema 3.1.3 é o seguinte: temos $p_i^{\alpha_i} \leq 2n$ e temos $\alpha_j \leq 1$ para $p_j > \sqrt{2n}$. Então

$$\binom{2n}{n} \leq \prod_{p_i\leq\sqrt{2n}} p_i^{\alpha_i} \prod_{\sqrt{2n}<p_j\leq 2n/3} p_j \leq \prod_{p_i\leq\sqrt{2n}} 2n \prod_{p_j\leq 2n/3} p_j \leq (2n)^{\pi(\sqrt{2n})} \cdot 4^{2n/3}.$$

Supondo que $n \geq 50$, temos $\pi(\sqrt{2n}) \leq \sqrt{2n}/2 - 1 = \sqrt{n/2} - 1$, podemos, uma vez que metade dos números entre 1 e $\sqrt{2n}$ é par. Dessa forma

$$\binom{2n}{n} < (2n)^{\sqrt{n/2}-1} 4^{2n/3}.$$

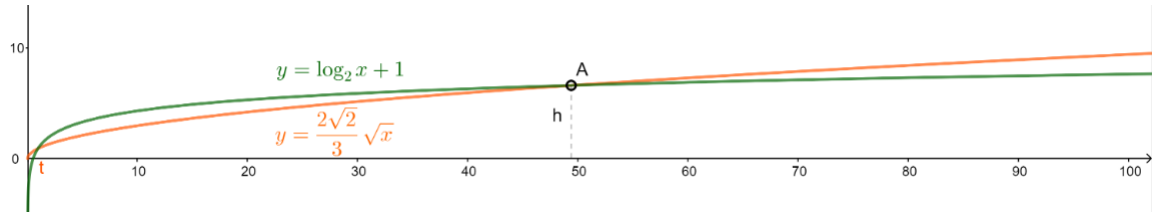
Por outro lado temos, pela relação de Stifel, que

$$\begin{aligned} n\binom{2n}{n} &= n\binom{2n-1}{n} + n\binom{2n-1}{n-1} \\ &> \binom{2n-1}{0} + \binom{2n-1}{1} + \cdots + \binom{2n-1}{n-1} + \binom{2n-1}{n} + \cdots + \binom{2n-1}{2n-1} \\ &> (1+1)^{2n-1} = 2^{2n-1}. \end{aligned}$$

Logo, pelas duas últimas desigualdade, temos

$$\frac{2^{2n-1}}{n} < \binom{2n}{n} < (2n)^{\sqrt{n/2}-1} \cdot 4^{2n/3} \Longrightarrow 2^{2n/3} < (2n)^{\sqrt{n/2}}.$$

Tomando o logaritmo na base 2 de ambos os lados da desigualdade anterior obtemos $\frac{2\sqrt{2}}{3}\sqrt{n} < \log_2 n + 1$. Tal desigualdade não é válida para $n > 50$, como exibido no gráfico a seguir



Logo, se o Postulado de Bertrand possui um contra-exemplo, este deve ser menor do que 100. Por fim vamos exibir primos que satisfaçam as condições do teorema até 100:

$$\begin{aligned}
p &= 2 \text{ para } 1 \leq n \leq 2,\\
p &= 5 \text{ para } 3 \leq n \leq 5,\\
p &= 11 \text{ para } 6 \leq n \leq 11,\\
p &= 23 \text{ para } 12 \leq n \leq 23,\\
p &= 47 \text{ para } 24 \leq n \leq 47,\\
p &= 79 \text{ para } 48 \leq n \leq 79,\\
p &= 101 \text{ para } 80 \leq n \leq 100.
\end{aligned}$$

□

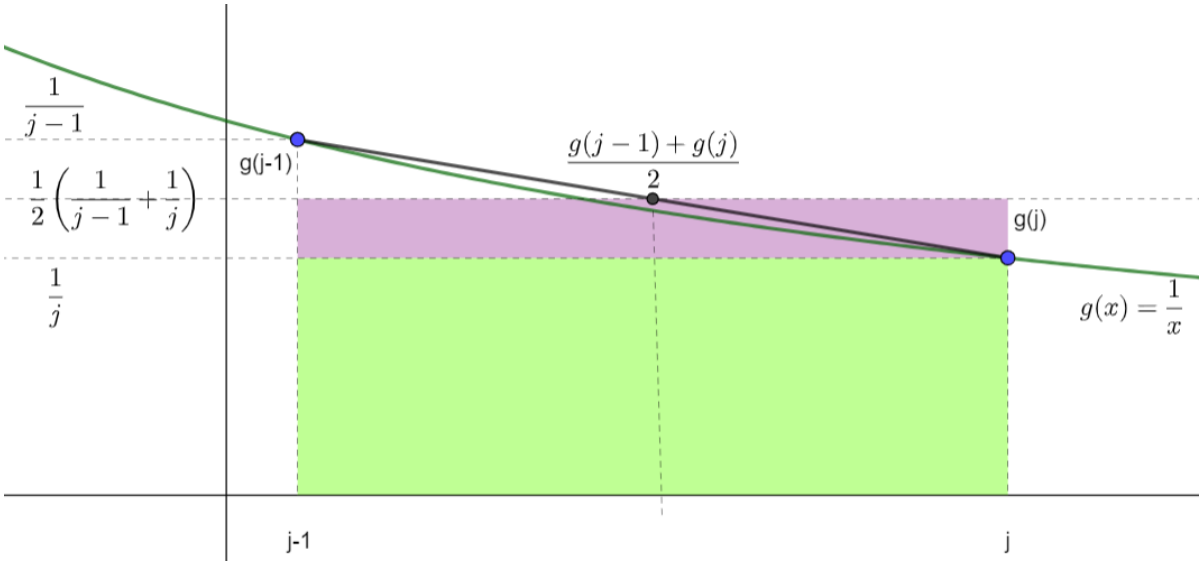
.

3.3 Fórmulas de Mertens

Nessa seção, vamos apresentar dois teoremas que são chamadas primeira e segunda Fórmulas de Mertens. Esses teoremas exibem o comportamento assintótico de somatórios envolvendo primos, mas antes vamos apresentar outras estimativas relacionadas a soma de inteiros. A heurística dos lemas a seguir segue do teste da integral para séries.

Lema 3.3.1. $\displaystyle\sum_{j=1}^{n} \frac{1}{j} = \log n + O(1)$

Demonstração. Observe que a função $g(x) = \frac{1}{x}$ é estritamente decrescente, pois $g'(x) = -\frac{1}{x^2} < 0$ para todo $x > 0$ e tem a concavidade voltada para cima, pois $g''(x) = \frac{2}{x^3} > 0$ para valores de $x > 0$. Considerando $j > 1$, a reta que passa pelos pontos $\left(j-1, \frac{1}{j-1}\right)$ e $\left(j, \frac{1}{j}\right)$ fica acima de $y = g(x) > 0$ que, por sua vez, fica acima da reta $y = \frac{1}{j}$.



Calculando as áreas das curvas citadas, temos

$$\frac{1}{j} < \int_{j-1}^{j} \frac{1}{x} dx < \frac{1}{2}\left(\frac{1}{j-1} + \frac{1}{j}\right).$$

Somando as desigualdades acima de $j = 2$ até n, temos

$$\begin{aligned}
\sum_{j=2}^{n} \frac{1}{j} &< \int_{1}^{n} \frac{1}{x} dx < \sum_{j=2}^{n} \frac{1}{2}\left(\frac{1}{j-1} + \frac{1}{j}\right) \\
&= \frac{1}{2}\left(\frac{1}{1} + \frac{1}{2}\right) + \frac{1}{2}\left(\frac{1}{2} + \frac{1}{3}\right) + \cdots + \frac{1}{2}\left(\frac{1}{n-2} + \frac{1}{n-1}\right) + \frac{1}{2}\left(\frac{1}{n-1} + \frac{1}{n}\right) \\
&= \frac{1}{2} \cdot 1 + \frac{1}{2}\sum_{j=2}^{n} \frac{2}{j} - \frac{1}{2n} = \frac{1}{2} - \frac{1}{2n} + \sum_{j=2}^{n} \frac{1}{j}.
\end{aligned}$$

Dessa forma,

$$\frac{1}{2} + \frac{1}{2n} + \log n < \sum_{j=1}^{n} \frac{1}{j} < 1 + \log n.$$

□

Lema 3.3.2. $\displaystyle\sum_{j=1}^{n} \log j = \left(n + \frac{1}{2}\right)\log n - n + O(1).$

Demonstração. Temos que a função $h(x) = \log x$ é estritamente crescente e tem concavidade para baixo. Assim como na estimativa anterior, observe que para j inteiro e maior que 1, a reta que contém o ponto $(j, \log j)$ no intervalo $[j-1, j]$ tem inclinação $m_j = h'(j) = \frac{1}{j}$. Logo, a reta que passa pelos pontos $(j-1, \log(j-1)), (j, \log j)$ fica abaixo do gráfico da função $y = h(x)$, que por sua vez fica abaixo da reta acima que tem inclinação $h'(x)$. Dessa forma

$$\log j - \frac{1}{2j} > \int_{j-1}^{j} \log x dx > \frac{1}{2}(\log(j-1) + \log j).$$

Somando para $j = 2$ até n, temos

$$\begin{aligned}
\sum_{j=2}^{n} \log j - \sum_{j=2}^{n} \frac{1}{2j} &> \int_1^n \log x \; dx \\
&> \sum_{j=2}^{n} \frac{1}{2}(\log(j-1) + \log j) = \frac{1}{2}(\log 1 + \log 2) + \frac{1}{2}(\log 2 + \log 3) + \\
&\quad \cdots + \frac{1}{2}(\log(n-2) + \log(n-1)) + \frac{1}{2}(\log(n-1) + \log n) \\
&= \sum_{j=2}^{n} \log j - \frac{1}{2}\log n.
\end{aligned}$$

Dessa forma

$$\left(n + \frac{1}{2}\right)\log n - n + 1 > \sum_{j=1}^{n} \log j > n \log n - n + \frac{1}{2} + \frac{1}{2}\sum_{j=1}^{n} \frac{1}{j}.$$

Como consequência, temos que

$$\left(n + \frac{1}{2}\right)\log n - n + 1 > \sum_{j=1}^{n} \log j > \left(n + \frac{1}{2}\right)\log n - n + \frac{1}{4n} + \frac{3}{4}.$$

□

Lema 3.3.3. $\displaystyle\sum_{j=2}^{n} \frac{1}{j \log j} = \log\log n + O(1).$

Demonstração. Observemos que a função $f(x) = \frac{1}{x \log x}$ é estritamente decrescente, pois $f'(x) = \frac{\log x + 1}{(x \log x)^2} < 0$ para valores de $x > 0$ e a função tem concavidade voltada para cima, pois $f''(x) = \frac{2\log^2 x + 3\log(x) + 2}{(x \log x)^3} > 0$, para todo $x > 1$. Como nas estimativas anteriores, temos que a reta que passa pelos pontos $(f(j-1), f(j))$, fica acima de $y = f(x)$, que por sua vez fica acima da reta que passa pelos pontos $\left((j-1), \frac{1}{(j-1)\log(j-1)}\right)$. Calculando as

áreas sob as curvas temos que

$$\frac{1}{j\log j} < \int_{j-1}^{j} \frac{1}{x\log x}dx < \frac{1}{2}\left(\frac{1}{(j-1)\log(j-1)} + \frac{1}{j\log j}\right).$$

Somando de $j = 3$ até n, obtemos

$$\begin{aligned}\sum_{j=3}^{n}\frac{1}{j\log j} &< \int_{2}^{n}\frac{1}{x\log x}dx = \log\log x - \log\log 2 < \sum_{j=3}^{n}\frac{1}{2}\left(\frac{1}{(j-1)\log(j-1)} + \frac{1}{j\log j}\right)\\ &= \frac{1}{2}\left(\frac{1}{2\log 2} + \frac{1}{3\log 3}\right) + \frac{1}{2}\left(\frac{1}{3\log 3} + \frac{1}{4\log 4}\right) +\\ &\cdots + \frac{1}{2}\left(\frac{1}{(n-2)\log(n-2)} + \frac{1}{(n-1)\log(n-1)}\right) + \frac{1}{2}\left(\frac{1}{(n-1)\log(n-1)} + \frac{1}{n\log n}\right)\\ &= \sum_{n=3}^{n}\frac{1}{j\log j} - \frac{1}{2\cdot 2\log 2} - \frac{1}{2\cdot n\log n}.\end{aligned}$$

Logo

$$\sum_{j=2}^{n}\frac{1}{j\log j} < \log\log n + \frac{1}{2\log 2} - \log\log 2 = \log\log n + O(1)$$

e

$$\sum_{j=2}^{n}\frac{1}{j\log j} > \log\log n - \log\log 2 + \frac{1}{4\log 2} + \frac{1}{2n\log n} = \log\log n + O(1).$$

□

Teorema 3.3.4 (Primeira Fórmula de Mertens)**.** $\displaystyle\sum_{p\leq n}\frac{\log p}{p} = \log n + O(1)$

Demonstração. Como visto na Proposição 3.1.1,

$$n! = \prod_{p\leq n} p^{\upsilon_p} \text{ onde } \upsilon_p = \sum_{k=1}^{\infty}\left\lfloor\frac{n}{p^k}\right\rfloor.$$

Aplicando o logaritmo, temos $\sum_{k=1}^{n}\log k = \sum_{\substack{p \text{ primo}\\ p\leq n}}\upsilon_p\log p$ e temos a desigualdade $\frac{n}{p} - 1 < \left\lfloor\frac{n}{p}\right\rfloor \leq \upsilon_p < \sum_{k=1}^{\infty}\frac{n}{p^k} = \frac{n}{p-1}$, onde na última igualdade usamos a soma de progressão geométrica infinita. Logo,

$$\sum_{p\leq n}\left(\frac{n}{p} - 1\right)\log p \leq \sum_{k=1}^{n}\log k \leq \sum_{\substack{p \text{ primo}\\ p\leq n}}\frac{n}{p-1}\log p,$$

dividindo tudo por n e subtraindo $\sum \frac{\log p}{p}$, obtemos

$$\begin{aligned} -\frac{1}{n}\sum_{p\leq n}\log p &\leq \frac{1}{n}\sum_{k=1}^{n}\log k - \sum_{p\leq n}\frac{\log p}{p} \leq \sum_{p\leq n}\frac{\log p}{(p-1)} - \sum_{p\leq n}\frac{\log p}{p} \\ &= \sum_{p\leq n}\log p\left(\frac{1}{p-1}-\frac{1}{p}\right) = \sum_{p\leq n}\log p\left(\frac{1}{[p(p-1)]}\right). \end{aligned}$$

Observe que $\sum_p \frac{\log p}{p(p-1)} < \sum_{n\geq 2}\frac{\log n}{n(n-1)} < \sum_{n\geq 1}\frac{1}{n^{3/2}} = O(1)$. Por outro lado, pelo Teorema 3.1.6, temos $\sum_{p\leq n}\log p \leq \sum_{p\leq n}\log n = \pi(n)\log n = O(n)$. □

Teorema 3.3.5 (Segunda Fórmula de Mertens)**.** $\displaystyle\sum_{p\leq n}\frac{1}{p} = \log\log n + O(1)$.

Demonstração. Defina as funções a_k e S_n da seguinte forma

$$a_k = \begin{cases} \frac{\log k}{k} & \text{se } k \text{ é primo} \\ 0 & \text{caso contrário} \end{cases} \quad \text{e} \quad S_n = \sum_{k=1}^{n} a_k.$$

Pelo Teorema, 3.3.4 vale a igualdade $S_k = \sum_{\substack{p \ primo \\ p\leq k}} \frac{\log p}{p} = \log k + O(1)$. Assim temos

$$\begin{aligned} \sum_{p\leq n}\frac{1}{p} &= \sum_{k=2}^{n}\frac{a_k}{\log k} = \sum_{k=2}^{n}\frac{S_k - S_{k-1}}{\log k} \\ &= \sum_{k=2}^{n} S_k\left(\frac{1}{\log k} - \frac{1}{\log(k+1)}\right) + \frac{S_n}{\log(n+1)} \\ &= \sum_{k=2}^{n}\log k\left(\frac{1}{\log k} - \frac{1}{\log(k+1)}\right) + O\left(\sum_{k=2}^{n}\left[\frac{1}{\log k} - \frac{1}{\log(k+1)}\right]\right) + \frac{S_n}{\log(n+1)} \\ &= \sum_{k=2}^{n}\log k\left[\frac{1}{\log k} - \frac{1}{\log(k+1)}\right] + O(1) \\ &= \sum_{k=2}^{n}\frac{\log(k+1)-\log k}{\log(k+1)} + O(1) \\ &= \sum_{k=2}^{n}\frac{1}{(k+1)\log(k+1)} + O(1) \\ &= \log\log n + O(1), \end{aligned}$$

onde na penúltima igualdade usamos que

$$\frac{1}{k+1} \leq \int_k^{k+1}\frac{dx}{x} \leq \frac{1}{k} \Longrightarrow \frac{1}{(k+1)\log\,(k+1)} \leq \frac{\log(k+1)-\log k}{\log(k+1)} \leq \frac{1}{k\log(k+1)}$$

e

$$\left|\sum_{k=2}^{n}\frac{1}{k\log(k+1)}-\sum_{k=2}^{n}\frac{1}{(k+1)\log(k+1)}\right|\leq\sum_{k=2}^{n}\left(\frac{1}{k}-\frac{1}{k+1}\right)=O(1).$$

□

Observação 3.3.6. *A Terceira Fórmula de Mertens, que não vai ser provada nem usada nesse texto, afirma que*

$$\lim_{x\to\infty}\log x\cdot\prod_{p\leq x}(1-1/p)=e^{-\gamma},$$

onde γ é chamada a constante de Euler-Mascheroni, que é definida, (ver Lema 3.3.1), como

$$\gamma=\left(\sum_{j=1}^{n}\frac{1}{j}\right)-\log n=0,57721\cdots$$

Capítulo 4

Teorema dos Números Primos

Nesse capítulo, vamos finalmente obter o comportamento assintótico da função $\pi(x)$ que conta o número de primos menores ou iguais a x. Para isso, vamos relacionar os primos à função Zeta de Riemann. Em particular, vamos provar o seguinte:

Teorema 4.0.1 (Teorema dos Números Primos)**.** *Seja $x \in \mathbb{R}$, vale que*

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

Para estimativas mais apuradas, indicamos o livro [2, Teorema 7.1], que exibe a função $Li(x) = \int_0^x \frac{1}{\log t} dt$ como uma melhor aproximação de $\pi(x)$ que $x/\log x$ (além do termo de erro da aproximação), embora sua demonstração seja muito mais rebuscada pois envolve a região sem zeros da função Zeta na faixa crítica. Podemos verificar usando integração por partes que $\lim_{x\to\infty} \frac{Li(x)}{x/\log x} = 1$.

4.1 Função Zeta de Riemann

Nessa seção, vamos definir a função Zeta e citar suas principais propriedades, como o produto de Euler. Para isso, vamos usar algumas propriedades de funções complexas, que podem ser encontradas em [7, Capítulos 2 e 4]. Em particular, vamos lembrar que uma função $f : \Omega \to \mathbb{C}$, onde Ω é um subconjunto aberto de $\mathbb{C}$, é *analítica em um ponto* $x_0 \in \Omega$ se existir uma série de potências de f em torno de x_0 com raio de convergência positivo. Dizemos também que f é *analítica* se f é analítica em x_0 para todo $x_0 \in \Omega$. Além disso, f é dita *holomorfa em* x_0 se existir a derivada $f'(x_0)$, e f é dita *holomorfa* se for holomorfa para todo $x_0 \in \Omega$. É possível mostrar que f é analítica se, e somente se, f é holomorfa (ver [7, Seção 2.2]). Vamos precisar também das propriedades dos resíduos, que podem ser encontradas em [7, Seção 4.4].

Definição 4.1.1 (Função Meromorfa)**.** *Seja $\Omega \subset \mathbb{C}$ aberto. Uma função $f : \Omega \to \mathbb{C}$ é* meromorfa *se for holomorfa a menos de pontos isolados, que são polos de f.*

Proposição 4.1.2. *Seja $f : \mathbb{N} \to \mathbb{C}$ limitada e multiplicativa. Então*

$$\sum_{n\geq 1} \frac{f(n)}{n^s} = \prod_p \left(\sum_{m\geq 0} \frac{f(p^m)}{p^{ms}} \right)$$

em $\Re(s) > 1$. No caso estritamente multiplicativa temos

$$\sum_{n\geq 1} \frac{f(n)}{n^s} = \prod_p \left(1 - \frac{f(p)}{p^s} \right)^{-1}$$

no mesmo domínio.

Demonstração. Temos que f é limitada, logo a série $\sum_{n\geq 1} \frac{f(n)}{n^s}$ converge uniformemente em $\Re(s) > \delta$, para todo $\delta > 1$, pois se $|f(n)| \leq L$ então

$$|\sum_{n\geq 1} f(n)/n^s| \leq \sum_{n\geq 1} |f(n)/n^s| \leq L \sum_{n\geq 1} |1/n^s| = L \sum_{n\geq 1} 1/n^{\Re(s)} \leq L \sum_{n\geq 1} 1/n^{\delta}.$$

Tome $S = \sum_{n\geq 1} \frac{f(n)}{n^s}$ e $P(x) = \prod_{p\leq x}(1 + f(p)/p^s + f(p^2)/p^{2s} + \cdots)$, s fixo com $\Re(s) > 1$. Como $\sum_{n\geq 1} f(n)/n^s$ converge uniformemente em $\Re(s) \geq \delta > 1$, se $\varepsilon > 0$ temos

$$|S - P| \leq \sum_{\substack{n\geq 1 \\ \exists p>x; p|n}} |f(n)/n^s| \leq \sum_{n>x} |f(n)/n^s| < \varepsilon$$

para todo x grande. Logo, $\lim_{x\to\infty} P(x) = S$.

Caso f seja estritamente multiplicativa, vale que $f(p^m) = f(p)^m$, dessa forma

$$\sum_{m\geq 0} f(p^m)p^{-ms} = \sum_{m\geq 0} (f(p)p^{-s})^m = 1 + \frac{f(p)}{p^s} + \left(\frac{f(p)}{p^s}\right)^2 + \cdots = \frac{1}{1 - f(p)p^{-s}}.$$

□

Definição 4.1.3. *Definimos a função $\zeta : \mathbb{C} \to \mathbb{C}$ como a única extensão meromorfa de $\sum_{n\geq 1} \frac{1}{n^s}$, que é uma soma convergente se $\Re(s) > 1$. Tal função é chamada função Zeta de Riemann.*

Como consequência da Proposição 4.1.2, tomando $f(n) = 1$ para todo n, segue o seguinte resultado.

Corolário 4.1.4 (Euler)**.** *Seja $s \in \mathbb{C}$, com $\Re(s) > 1$, vale a seguinte igualdade:*

$$\zeta(s) = \sum_{n\geq 1} \frac{1}{n^s} = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}$$

A seguir, vamos usar a função Zeta para dar uma prova alternativa para o Teorema de Euclides (exibido na Introdução), que afirma que existem infinitos primos. Apesar da demonstração a seguir ser menos elementar, ela traz mais frutos que a demonstração mais simples dada na Introdução.

Teorema 4.1.5. *A série dos inversos dos primos diverge. Em particular, existem infinitos números primos.*

Demonstração. Partindo da igualdade do Corolário 4.1.4

$$\sum_{n\geq 1} \frac{1}{n^s} = \prod_p \left(1 - \frac{1}{p^{-s}}\right)^{-1},$$

aplicamos o logaritmo em ambos os membros da equação, obtemos

$$\log\left(\sum_{n\geq 1} \frac{1}{n^s}\right) = -\log[(1-2^{-s})\cdot(1-3^{-s})\cdot(1-5^{-s})\cdots] = -\sum_p \log\left(1 - \frac{1}{p^{-s}}\right).$$

Utilizando a expansão do logaritmo em série de potências, obtemos o seguinte resultado

$$\log\left(\sum_{n\geq 1} \frac{1}{n^s}\right) = \sum_p \sum_{m\geq 1} \frac{1}{mp^{ms}} = \sum_p \frac{1}{p^s} + \sum_p \sum_{m\geq 2} \frac{1}{mp^{ms}}.$$

Entretanto

$$\sum_p \sum_{m\geq 2} \frac{1}{mp^{ms}} < \sum_p \sum_{m\geq 2} \frac{1}{p^m} = \sum_p \frac{1}{p(p-1)} < \sum_{n\geq 2} \frac{1}{n(n-1)} = \sum_{n\geq 2} \left(\frac{1}{n-1} - \frac{1}{n}\right) = 1.$$

Fazendo $s \to 1^+$ encontramos a série harmônica, que diverge, logo $\sum_p \frac{1}{p}$ diverge e portanto existem infinitos primos. □

4.2 Extensões de Zeta

Essa seção vai estender a função Zeta para domínios mais amplos que $\Re(s) > 1$, a saber, $\Re(s) \geq 1$. Vamos precisar do seguinte Lema:

Lema 4.2.1 (Lema da representação integral)**.** *Seja $f(s)$ uma função meromorfa e $(a_n)_{n\in\mathbb{N}}$ uma sequência de números complexos tal que $f(s) = \sum_{n\geq 1} \frac{a_n}{n^s}$ em $\Re(s) > a$. Sendo $P(x) = \sum_{n\geq x} a_n$, suponha que $\sum_{n\geq 1} \frac{P(n)}{n^s}$ e $\sum_{n\geq 1} \frac{P(n-1)}{n^s}$ convergem em $\Re(s) > b$, e que $\int_1^\infty P(x)x^{-1-s}dx$ representa uma função analítica em $\Re(s) > c$. Então*

$$f(s) = s\int_1^\infty P(x)x^{-1-s}dx$$

em $\Re(s) > c$.

Demonstração.

$$\begin{aligned} f(s) &= \sum_{n\geq 1}\frac{a_n}{n^s} = \sum_{n\geq 1}\frac{P(n)-P(n-1)}{n^s} \\ &= \sum_{n\geq 1}\frac{P(n)}{n^s} - \sum_{n\geq 1}\frac{P(n-1)}{n^s} = \sum_{n\geq 1}\frac{P(n)}{n^s} - \sum_{n\geq 1}\frac{P(n)}{(n+1)^s} \\ &= \sum_{n\geq 1} P(n)\left(\frac{1}{n^s} - \frac{1}{(n+1)^s}\right) = \sum_{n\geq 1} sP(n)\int_n^{n+1} x^{-1-s}dx \\ &= s\sum_{n\geq 1}\int_n^{n+1} P(x)x^{-1-s}dx = s\int_1^\infty P(x)x^{-1-s}dx \end{aligned}$$

Segue-se o resultado em $\Re(s) > c$ por continuação analítica. □

Para estender a função zeta para $\Re(s) \geq 1$, precisamos localizar os zeros e os polos de zeta nessa região. É isso que faremos nos próximos resultados.

Proposição 4.2.2. *A função ζ possui um único polo em $\Re(s) > 0$; este polo é simples, de resíduo 1 e localizado em $s = 1$.*

Demonstração. Com $P(x) = \lfloor x \rfloor$, temos que em $\Re(s) > 2$, $\sum_{n\geq 1} \frac{P(n)}{n^s}$ e $\sum_{n\geq 1} \frac{P(n-1)}{n^s}$ convergem, e $\int_1^\infty P(x)x^{-1-s}dx$ representa uma função analítica em $\Re(s) > 1$, dessa forma

$$\zeta(s) = s\int_1^\infty \lfloor x \rfloor\ x^{-1-s}dx \text{ em } \Re(s) > 1.$$

Observe que $\lfloor x \rfloor = x - \{x\}$, com isso

$$\zeta(s) = s\int_1^\infty \frac{\lfloor x \rfloor}{x^{1+s}}dx = s\int_1^\infty \frac{x-\{x\}}{x^{1+s}}dx$$

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

com a última integral convergente em $\Re(s) > 1$, ou seja, analítica neste domínio. □

Corolário 4.2.3. *$\zeta(s) \neq 0$ em $\Re(s) > 1$.*

Demonstração. Pelo Corolário 4.1.4, temos em $\Re(s) > \sigma > 1$

$$\frac{1}{|\zeta(s)|} = \prod_p |1 - p^{-s}| \leq \prod_p \left(1 + \frac{1}{|p^s|}\right) \leq \prod_p \left(1 + \frac{1}{p^\sigma}\right).$$

Vamos provar que o produto anterior é finito. De fato, temos

$$\begin{aligned} \prod_p \left(1 + \frac{1}{p^\sigma}\right) = \beta \quad &\Leftrightarrow \quad \log\beta = \log\prod_p \left(1 + \frac{1}{p^\sigma}\right) = \sum_p \log\left(1 + \frac{1}{p^\sigma}\right) \\ &= \sum_p \left(\frac{1}{p^\sigma} - \frac{1}{2p^{2\sigma}} + \frac{1}{3p^{3\sigma}} - \frac{1}{4p^{4\sigma}} + \cdots\right) \\ &\leq \sum_p \left(\frac{1}{p^\sigma} + \frac{1}{2p^{2\sigma}} + \frac{1}{3p^{3\sigma}} + \frac{1}{4p^{4\sigma}} + \cdots\right) \\ &\leq \sum_p \left(\frac{1}{p^\sigma} + \frac{1}{p^{2\sigma}} + \frac{1}{p^{3\sigma}} + \ldots\right) = \sum_p \left(\frac{1/p^\sigma}{1 - 1/p^\sigma}\right) \\ &= \sum_p \left(\frac{1}{p^\sigma - 1}\right) \leq \sum_p \frac{2}{p^\sigma} = 2\sum_p \frac{1}{p^\sigma} < \infty \\ &\Rightarrow \quad \log\beta < \infty \Rightarrow \beta < \infty, \end{aligned}$$

onde na segunda linha da passagem anterior foi usado a série de potências de $\log(1 + p^\sigma)$ e na terceira linha a soma de série geometrica. Logo

$$|\zeta(s)| \cdot \prod_p \left(1 + \frac{1}{p^\sigma}\right) \geq 1,$$

o que implica $\zeta(s) \neq 0$. □

Proposição 4.2.4. *Em $\Re(s) = 1$ temos $\zeta(s) \neq 0$.*

Demonstração. Observe que

$$\begin{aligned} 3+4\cos\theta+\cos 2\theta &= 3+4\cdot\cos\theta+\cos^2\theta-\sin^2\theta \\ &= 3+4\cdot\cos\theta+\cos^2\theta-(1-\cos^2\theta) \\ &= 3+4\cdot\cos\theta+\cos^2\theta-1+\cos^2\theta \\ &= 2+4\cdot\cos\theta+2\cdot\cos^2\theta \\ &= 2\cdot(1+2\cdot\cos\theta+\cos^2\theta) \\ &= 2\cdot(1+cos\theta)^2\geq 0. \end{aligned}$$

Defina $\varphi(s)=\zeta^3(s)\zeta^4(s+ib)\zeta(s+2ib)$, e suponha que $\zeta(1+ib)=0$ para algum $b\in\mathbb{R}$. Temos que $b\neq 0$ pois 1 é um polo de ζ. Assim φ se anula em $s=1$, pois o polo simples de ζ (polo triplo de $\zeta^3(1)$ não cancela o zero de ordem pelo menos 4 de $\zeta^4(1+ib)$. Logo

$$\lim_{s\to 1}\log|\varphi(s)|=-\infty$$

Como $z=|z|\cdot e^{i\theta}$ para todo $z\in\mathbb{C}^*$, onde θ é o argumento de z, temos $\log z=\log|z|+i\theta$, Portanto para $s\in\mathbb{R}, s>1$, vale que

$$\begin{aligned} \log|\zeta(s+it)| &= \Re\log\zeta(s+it)=\Re\log\prod_p(1-p^{-s-it})^{-1} \\ &= -\Re\sum_p\log(1-p^{-s-it})=\Re\sum_p\sum_{n=0}^{\infty}\frac{(-1)^n\cdot(-p^{-s-it})^{n+1}}{n+1} \\ &= \Re\sum_p\left(p^{-s-it}+\frac{1}{2}(p^2)^{-s-it}+\frac{1}{3}(p^3)^{-s-it}+\cdots\right). \end{aligned}$$

Logo, podemos escrever o último somatório como

$$\log|\zeta(s+it)|=\Re\sum_{n\geq 1}a_n n^{-s-it},$$

com $a_n\geq 0$. Dessa forma, obtemos

$$\begin{aligned} \log|\varphi(s)| &= \log|\zeta^3(s)\zeta^4(s+ib)\zeta(s+2ib)| \\ &= \log|\zeta(s)|^3+\log|\zeta(s+ib)|^4+\log|\zeta(s+2ib)| \\ &= 3\log|\zeta(s)|+4\log|\zeta(s+ib)|+\log|\zeta(s+2ib)| \\ &= 3\Re(\log(\zeta(s))+4\Re(\log(\zeta(s+ib))+\Re(\log(\zeta(s+2ib)) \\ &= \Re(3\log\zeta(s)+4\log\zeta(s+ib)+\log\zeta(s+2ib)) \end{aligned}$$

$$\begin{aligned} &= \Re\left(3\sum_{n\geq 1} a_n n^{-s} + 4\sum_{n\geq 1} a_n n^{-s-ib} + \sum_{n\geq 1} a_n n^{-s-2ib}\right) \\ &= \Re\left(3a_n \sum_{n\leq 1} e^{-s\cdot\log n} + 4a_n \sum_{n\geq 1} e^{(-s-ib)\cdot\log n} + a_n \sum_{n\geq 1} e^{(-s-2ib)\cdot\log n}\right) \\ &= \sum_{n\geq 1} a_n n^{-s}[3 + 4\cos(b\log n) + \cos(2b\log n)] \geq 0, \end{aligned}$$

absurdo pois

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

□

Em termos informais, provamos que zeta não possui zeros com parte real maior ou igual a 1. Isso implicará a existência do limite do Teorema dos Números Primos. Caso consigamos melhorar essa região sem zeros, conseguiremos calcular também o termo de erro nesse limite.

Proposição 4.2.5. *A função* $-\frac{\zeta'(s)}{\zeta(s)} - \frac{1}{s-1}$ *possui continuação analítica sobre a reta* $\Re(s) > 1$.

Demonstração. Na Proposição 4.2.2 foi visto que

$$\zeta(s) = 1 + \frac{1}{s-1} + s\int_1^\infty (\lfloor x\rfloor - x)x^{-1-s}dx.$$

Multiplicando por $s-1$ obtemos

$$(s-1)\zeta(s) = (s-1) + 1 + s(s-1)\int_1^\infty (\lfloor x\rfloor - x)^{-1-s}dx.$$

Tomando o logaritmo, temos

$$\log(s-1) + \log\zeta(s) = \log\left[(s-1) + 1 + s(s-1)\int_1^\infty (\lfloor x\rfloor - x)^{-1-s}dx\right].$$

Derivando, obtemos que $\frac{1}{(s-1)} + \frac{\zeta'(s)}{\zeta(s)}$ é analítica. Dessa forma, $-\frac{\zeta'(s)}{\zeta(s)}$ possui um polo simples em $s = 1$ de resíduo 1. □

4.3 A Função $\psi(x)$

Definição 4.3.1. *A função $\psi : \mathbb{R}^+ \to \mathbb{R}$ é definida por*

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

onde

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

A função ψ é chamada função de Chebyshev *e Λ* função de von Mangoldt*.*

A função ψ também pode ser escrita da seguinte forma

$$\psi(x) = \sum_{p^n \leq x} \log p = \sum_{p \leq x} \left\lfloor \frac{\log x}{\log p} \right\rfloor \log p,$$

uma vez que $p^n \leq x$ equivale a $n \leq \lfloor \log x / \log p \rfloor$.

Exemplo 4.3.2. *$\Lambda(8) = \log 2$ pois $8 = 2^3$ e $\Lambda(10) = 0$ pois 10 não é potência de primo.*

Uma propriedade importante da função ψ é que $\psi(x) = \log mmc(1, 2, 3, \ldots, \lfloor x \rfloor)$, mas não vamos usar isso em nenhum momento desse texto.

Proposição 4.3.3. *Seja $g(s) = s \int_1^\infty \psi(x) x^{-1-s} dx$. Temos que g é analítica em $\Re(s) > 1$ e vale $g(s) = -\frac{\zeta'(s)}{\zeta(s)}$.*

Demonstração. Observe que $\psi(x) = \sum_{p^n \leq x} \log p \leq \log x \sum_{p^n \leq x} 1 \leq x \log x$, logo

$$|g(s)| \leq |s| \cdot \int_1^\infty |\psi(x) x^{-1-s}| dx \leq |s| \cdot \int_1^\infty \frac{\log x}{|x^s|} dx = |s| \cdot \int_1^\infty \frac{\log x}{x^{\Re(s)}} dx < \infty$$

logo vale a primeira afirmação. Para a segunda afirmação temos

$$\log \zeta(s) = -\sum_p \log(1 - p^{-s}) = \sum_p \sum_{m \geq 1} \frac{1}{m p^{ms}}, \tag{4.1}$$

onde a última série converge uniformemente em $\Re(s) \geq \delta > 1$, pois

$$\left| \sum_{m \geq 1} \frac{1}{m p^{ms}} \right| \leq \sum_{m \geq 1} \left| \frac{1}{m p^{ms}} \right| < \sum_p \frac{1}{p^\delta}.$$

Dessa forma, podemos derivar dentro do segundo termo da Equação 4.1 , logo obtemos

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_p \frac{p^{-s}}{1-p^{-s}} \log p = \sum_p (p^{-s} + p^{-2s} + \cdots) \log p = \sum_{n\geq 1} \Lambda(n) n^{-s}.$$

Agora basta utilizar o Lema 4.2.1 com $b = 3$ para terminar a demonstração. De fato,

$$\left| \sum_{n=1}^{\infty} \frac{\psi(n-1)}{n^s} \right| \leq \left| \sum_{n=1}^{\infty} \frac{\psi(n)}{n^s} \right| \leq \sum_{n=1}^{\infty} \frac{n^2}{|n^s|} \leq \sum_{n=1}^{\infty} \frac{1}{n^{\Re(s)-2}}.$$

□

Proposição 4.3.4. *É válida a seguinte equivalência:*

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

Demonstração. Observe que

$$\psi(x) = \sum_{p\leq x} \left\lfloor \frac{\log x}{\log p} \right\rfloor \log p \leq \log x \sum_{p\leq x} 1 = \pi(x) \cdot \log x.$$

Logo

$$\frac{\psi(x)}{x} \leq \frac{\pi(x)}{x/\log x}.$$

Também temos que, se $1 < y < x$, vale que

$$\pi(x) = \pi(y) + \sum_{y<p\leq x} 1 \leq \pi(y) + \sum_{y<p\leq x} \frac{\log p}{\log y} < y + \frac{1}{\log y} \sum_{p\leq x} \left\lfloor \frac{\log x}{\log p} \right\rfloor \log p = y + \frac{\psi(x)}{\log y}.$$

Para valores de x muito grandes temos $1 < \frac{x}{\log^2 x} < x$, assim tomando $y = x/\log^2 x$, temos

$$\pi(x) < \frac{x}{\log^2 x} + \frac{\psi(x)}{\log\left(\frac{x}{\log^2 x}\right)} = \frac{x}{\log^2 x} + \frac{\psi(x)}{\log x - 2\log\log x}.$$

Multiplicando por $\log x$ e $\frac{1}{x}$ obtemos

$$\frac{\pi(x)\log x}{x} < \frac{1}{\log x} + \frac{\psi(x)}{x} \frac{\log x}{\log x - 2\log\log x}.$$

Como $\lim_{x\to\infty} \frac{\log x}{\log x - 2\log\log x} = 1$, logo obtemos o resultado desejado.

□

Proposição 4.3.5. *Temos que $\psi(x) = O(x)$.*

Demonstração. O número $\binom{2n}{n} = \frac{(2n)!}{n!n!}$ é divisível por todos os primos no intervalo $(n, 2n]$. Dessa forma

$$\prod_{n<p\leq 2n} p < \binom{2n}{n} < \sum_{i=0}^{2n} \binom{2n}{i} = \binom{2n}{0} + \binom{2n}{1} \cdots + \binom{2n}{n} \cdots + \binom{2n}{2n} = 2^{2n}.$$

Aplicando o logaritmo,

$$\sum_{n<p\leq 2n} \log p < 2n \log 2.$$

Como consequência da desigualdade acima, temos

$$\sum_{2^{k-1}<p\leq 2^k} \log p < 2^k \log, 2$$

logo

$$\sum_{p\leq k} \log p < \sum_{i=0}^{k} 2^i \cdot \log 2 < 2^{k+1} \cdot \log 2.$$

Seja k um número inteiro tal que $2^{k-1} < x \leq 2^k$. Assim

$$\sum_{p\leq x} \log p \leq \sum_{p\leq 2^k} \log p < 2^{k+1} \cdot \log 2 = (4 \log 2) \cdot 2^{k-1} < 4x \log 2.$$

Para $m \geq 2$ inteiro e fixo, temos

$$\sum_{p^m\leq x} \log p = \sum_{p\leq x^{1/m}} \log p < 4 \cdot \log 2 \cdot x^{1/m} \leq 4 \log 2\sqrt{x}.$$

Além disso, $2^m \leq p^m \leq x$ implica $m \leq \log x / \log 2$. Somando a desigualdade acima para todos os valores possíveis de m temos:

$$\begin{aligned}
\psi(x) = \sum_{p\leq x} \log p + \sum_{2\leq m\leq \frac{\log x}{\log 2}} \sum_{p^m\leq x} \log p &= \sum_{p\leq x} \log p + \sum_{2\leq m\leq \log x/\log 2} 4 \cdot \log 2 \cdot \sqrt{x} \\
&\leq 4x \log 2 + 4 \cdot \log 2 \cdot \sqrt{x} \cdot \frac{\log x}{\log 2} \\
&= 4x \log 2 + 4\sqrt{x} \log x = O(x)
\end{aligned}$$

□

4.4 Teoremas Tauberianos

Na Proposição 4.2.5, demonstramos que $-\frac{\zeta'(s)}{\zeta(s)} - \frac{1}{(s-1)}$ possui extensão analítica sobre $\Re(s) = 1$. Além disso, em $\Re(s) > 1$ vale

$$-\frac{\zeta'(s)}{\zeta(s)} - \frac{1}{(s-1)} = 1 + s\int_1^\infty (\psi(x) - x) \cdot x^{-1-s} dx.$$

Contudo, não temos garantias que a integral acima convirja em $\Re(s) = 1$. Caso isso ocorra, fazendo $s = 1$ teremos que a integral $s\int_1^\infty (\psi(x) - x) \cdot x^{-1-s}$ converge. Isso implica que a função $\frac{\psi(x)-x}{x}$ tende a 0. Não vamos mostrar com todos os detalhes que isso de fato é verdade pois foge do escopo do texto, mas sendo verdade teremos que $\psi(x)/x$ tende a 1. Pela Proposição 4.3.4, segue que $\frac{\pi(x)}{x/\log x}$ tende a 1, logo obtemos o Teorema dos Números Primos (Teorema 4.0.1). A seguir, vamos apenas ilustrar as principais ideias para mostrar que $\lim_{x\to\infty}(\psi(x) - x)/x = 0$. Os detalhes nas demonstrações podem ser consultados em [2, Apêndice A.2]. Precisamos da Transformada de Laplace e da Transformada de Mellin.

Definição 4.4.1 (Transformada de Laplace)**.** *Seja $F : (0, \infty) \to \mathbb{R}$ limitada e integrável em qualquer subintervalo finito. Definimos a transformada de Laplace de F como*

$$G(z) = \int_0^\infty F(t)e^{-zt} dt.$$

Lema 4.4.2. *A transformada de Laplace de F está bem definida para $F : (0, \infty) \to \mathbb{R}$, limitada e integrável em qualquer subintervalo finito.*

Definição 4.4.3 (Transformada de Mellin)**.** *Seja $f : [1, \infty) \to \mathbb{R}$ integrável em qualquer subintervalo finito, não negativa, não decrescente, e $O(x)$. Definimos a* transformada de Mellin *como*

$$g(s) = s\int_1^\infty f(x)x^{-1-s} dx.$$

Lema 4.4.4. *A transformada de Mellin de f está bem definida para $f : [1, \infty) \to \mathbb{R}$, limitada, integrável em qualquer subintervalo finito e $O(x)$. Além disso, tal transformada é analítica em $\Re(s) > 1$.*

Teorema 4.4.5. *Sejam $F : (0, \infty) \to \mathbb{R}$ como no Lema 4.4.2 e G sua transformada de Laplace. Se G possui continuação analítica sobre a reta $\Re(z) = 0$, então sua integral imprópria $\int_0^\infty F(t)dt$ converge e*

$$G(0) = \int_0^\infty F(t)dt.$$

Teorema 4.4.6. *Seja $f : [1, \infty) \to \mathbb{R}$ como no Lema 4.4.4 e seja $g(s)$ a sua transformada de Mellin. Suponha que existe $c \in \mathbb{R}$ tal que*

$$g(s) - \frac{c}{s-1}$$

possui continuação analítica sobre a reta $\Re(s) = 1$. Então

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

Demonstração. Seja $t \geq 0$. Defina $F(t) = e^{-t}f(e^t) - c$. Como f é $O(x)$ integrável em intervalos finitos, temos que F é limitada em $(0, \infty)$ e também integrável em intervalos finitos. Assim, a transformada de Laplace de G de F é dada por

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

Trocando e^t por x temos

$$\begin{aligned} G(z) &= \int_1^\infty f(x)x^{-2-z}dx - \frac{c}{z} = \frac{g(z+1)}{z+1} - \frac{c}{z} \\ &= \frac{1}{z+1}\left(g(z+1) - \frac{c}{z} - c\right). \end{aligned}$$

Por hipótese, $g(z+1) - \frac{c}{z}$ possui extensão analítica sobre $\Re(z+1) = 1$, isto é, G pode ser estendida analiticamente sobre a reta $\Re(z) = 0$. Pelo Teorema 4.4.5 chegamos ao seguinte resultado

$$G(0) = \int_0^\infty (e^{-t}f(e^t) - c)dt = \int_1^\infty \frac{f(x) - cx}{x^2}dx.$$

Basta verificar que a convergência da última integral anterior implica $\lim\limits_{x\to\infty} \dfrac{f(x)}{x} = c$. Vamos supor que $\limsup \frac{f(x)}{x} > c$, logo existe $\delta > 0$ tal que

$$0 < 2\delta < \limsup \frac{f(x)}{x} - c.$$

Defina $\rho = \frac{c+2\delta}{c+\delta} > 1$. Note que a constante c deve ser não negativa, caso fosse negativa teríamos

$$\int_1^\infty \frac{f(x) - cx}{x^2}dx \geq \int_1^\infty \frac{-cx}{x^2}dx = \lim_{a\to\infty} \log(a^{-c}) = +\infty.$$

Como $\limsup \frac{f(x)}{x} > c$, tomamos que existe uma sequência $(y_n)_{n\in\mathbb{N}}$ com $y_n \to \infty$ tal que

$$\frac{f(y_n)}{y_n} > c + 2\delta$$

para todo $n \in \mathbb{N}$.

Como f é não decrescente, se $y_n < x < \rho y_n$ então

$$f(x) \geq f(y_n) > (c+2\delta)y_n = \rho(c+\delta)y_n > (c+\delta)x$$

Assim

$$\frac{f(x)-cx}{x} > \rho.$$

Multiplicando a integral anterior por $\frac{1}{x}$ e integrando de y_n até ρy_n, temos

$$\int_{y_n}^{\rho y_n} \frac{f(x)-cx}{x^2}dx \geq \int_{y_n}^{\rho y_n} \frac{\rho}{x}dx = \delta \log \rho > 0$$

Pelo Teorema 4.4.5, temos $G(0) = \int_1^\infty \frac{f(x)-cx}{x^2}dx$. Assim, dado $\varepsilon > 0$ existe $M > 1$ tal que se $a \geq M$ então

$$\left| \int_a^\infty \frac{f(x)-cx}{x^2}dx \right| < \varepsilon.$$

Tome $0 < \varepsilon < \frac{\delta}{2}\log\rho$. Como $y_n \to \infty$, existe $n_0 \in \mathbb{N}$ tal que se $a \geq y_{n_0}$, então

$$\left| \int_a^\infty \frac{f(x)-cx}{x^2}dx \right| < \varepsilon.$$

Porém

$$\begin{aligned} \delta \log \rho &< \left| \int_{y_{n_0}}^{\rho y_{n_0}} \frac{f(x)-cx}{x^2}dx \right| \\ &\leq \left| \int_{y_{n_0}}^\infty \frac{f(x)-cx}{x^2}dx \right| + \left| \int_{\rho y_{n_0}}^\infty \frac{f(x)-cx}{x^2}dx \right| < 2\varepsilon < \delta \log \rho. \end{aligned}$$

Esse absurdo nos leva a $\limsup \frac{f(x)}{x} \leq c$. Para o $\liminf \frac{f(x)}{x} < c$, basta tomar $0 < 2\delta < c - \liminf \frac{f(x)}{x}$. Os demais passos são completamente análogos.

□

4.5 O Teorema dos Números Primos

Nessa seção, vamos juntar as peças e terminar a demonstração do Teorema dos Números Primos.

Na Proposição 4.3.4 vimos que é válida a seguinte equivalência

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

Pela Proposição 4.3.5, temos que a função ψ é não negativa, não decrescente, integrável em intervalos finitos e $O(x)$, com sua transformada de Mellin sendo

$$g(s) = s\int_1^\infty \psi(x)x^{-1-s}dx = -\frac{\zeta'(s)}{\zeta(s)}.$$

Também é válido pela Proposição 4.2.5 que $g(s) - \frac{1}{s-1}$ possui continuação analítica sobre $\Re(s) > 1$. Como consequência do Teorema 4.4.6, temos que $\lim_{x\to\infty} \frac{\psi(x)}{x} = 1$, o que prova o Teorema dos Números Primos.

Exemplo 4.5.1. *Dado um intervalo pertencente aos números naturais veremos como os números primos se comportam em tal intervalo, faremos da seguinte forma: tome o intervalo* $(10^{100}, 10^{101})$ *e b um número natural ímpar. Verificaremos se b é um número primo. Se não for, tomaremos* $b+2$ *e faremos a mesma análise até encontrarmos um número primo. Uma pergunta natural é quantas vezes em média precisaremos somar* 2 *a b até encontrarmos um número primo? A quantidade de números primos nesse intervalo é* $\pi(10^{101}) - \pi(10^{100})$*, que, pelo Teorema dos Números Primos, vale aproximadamente*

$$\frac{10^{101}}{101\log 10} - \frac{10^{100}}{100\log 10} = \frac{10^{98}}{\log 10}\frac{899}{101}.$$

A quantidade de números ímpares nesse intervalo é $\frac{10^{101}-10^{100}}{2} = 45\cdot 10^{99}$*. Logo, supondo que os números primos fossem ímpares aleatórios nesse intervalo, segue que a probabilidade de um número ímpar nesse intervalo ser primo é aproximadamente*

$$\frac{899\cdot 10^{98}/101\log 10}{45\cdot 10^{99}} = 0,0086\ldots$$

Com isso, em média, teremos que testar $\frac{1}{0,0086\ldots} = 116,\ldots$ *valores de b até encontrar um número primo.*

4.6 Consequências

O seguinte corolário melhora a cota 4^x do Lema 3.2.1. Vale ressaltar que a base 4 vale para todo $x > 0$, já a base $e^{(1+\varepsilon)}$ vale apenas para x grande. Em [5] está provado que a base 3 também vale para todo $x > 0$.

Corolário 4.6.1. *Para todo* $\varepsilon > 0$*, existe* $x_0 > 0$ *tal que se* $x > x_0$*, então* $\prod_{p\le x} p \le e^{(1+\varepsilon)x}$.

Demonstração. Dado $\varepsilon > 0$, existe x_0 tal que se $x > x_0$ então $\pi(x) < (1+\varepsilon)x/\log x$. Logo,

$$\prod_{p\le x} p \le \prod_{p\le x} x \le x^{\pi(x)} \le e^{\pi(x)\log x} \le e^{(1+\varepsilon)x}.$$

□

Podemos também melhorar o Corolário 3.1.8 tomando as constantes $0 < c < 1$ e $C > 1$ tão próximas de 1 quanto quisermos. Em particular, segue que:

Corolário 4.6.2. *Dado $\varepsilon > 0$, existe n_0 natural tal que se $n \geq n_0$ então o p_n, o n enésimo número primo, satisfaz*

$$(1-\varepsilon)n \cdot \log n < p_n < (1+\varepsilon)n \cdot \log n.$$

Uma consequência da função Zeta é que a inversa de Zeta pode ser vista como a série da função de Möbius. De fato, temos:

Teorema 4.6.3. *Se $\Re(s) > 1$, então*

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

Demonstração. Pelo Corolário 4.1.4, temos

$$\frac{1}{\zeta(s)} = \prod_p (1-p^{-s}) = \sum_{n\geq 1} \frac{\mu(n)}{n^s}.$$

□

4.7 Primos em Progressão Aritmética

Seja $q \geq 3$ um inteiro e seja $0 < a < q$ um número primo com q. Há várias generalizações dos resultados anteriores. Primeiramente, notemos que se a e q não são primos entre si então $a + kq$ é múltiplo de $mdc(a, q)$, logo não pode ser primo (pelo menos não mais que para um valor de k). É importante ressaltar também que existem $\varphi(q)$ inteiros entre 1 e q que são primos com q. Vamos citar sem demonstrar algumas dessas generalizações, e com isso veremos que os primos estão aproximadamente equidistribuídos sobre os possíveis valores de a. As ideias para as demonstrações dos resultados a seguir são as mesmas por trás dos teoremas já vistos, mas ao invés de usar a função Zeta, usamos a chamada *L-série de Dirichlet*, que é uma série envolvendo caracteres de Dirichlet módulo q. Para mais detalhes, veja [4].

Teorema 4.7.1 (Fórmulas de Mertens em Progressão Aritmética)**.** *Seja $q \geq 3$ um inteiro e seja a coprimo com q. Então valem:*

$$\sum_{\substack{p\leq n\\ p\equiv a \pmod q}} \frac{\log p}{p} = \frac{\log n}{\varphi(q)} \quad e \quad \sum_{\substack{p\leq n\\ p\equiv a \pmod q}} \frac{1}{p} = \frac{\log\log n}{\varphi(q)}.$$

Definição 4.7.2. *Seja* $\pi(x;q,a) = \#\{p \leq x;\ p \text{ primo e } p \equiv a \pmod q\}$ *a função que conta os primos menores ou iguais a* x *que são da forma* $p = a + kq$ *para algum* k *inteiro.*

Teorema 4.7.3 (Teorema dos Números Primos em Progressão Aritmética)**.** *Seja* $q \geq 3$ *um inteiro e seja* a *coprimo com* q*. Então:*

$$\lim_{x\to\infty} \frac{\pi(x;q,a)}{x/\log x} = \frac{1}{\varphi(q)}.$$

Exemplo 4.7.4. *Seja* $q = 4$*. Os restos possíveis na divisão por 4 são 0, 1, 2 e 3. Os números que deixam resto 0 são múltiplos de 4, logo não são primos. Os números que deixam resto* 2 *são pares, logo o único primo nessa progressão aritmética é o 2. Observe que* 1 *e* 3 *são os únicos restos possíveis que são primos com* 4*. Temos* $\varphi(4) = 2$ *e*

$$\lim_{x\to\infty} \frac{\pi(x;4,1)}{x/\log x} = \frac{1}{2} = \lim_{x\to\infty} \frac{\pi(x;4,3)}{x/\log x}$$

ou seja, aproximadamente metade dos primos até x *são da forma* $4k+1$ *e metade da forma* $4k+3$*.*

Referências Bibliográficas

[1] ALFORD, W.R, GRANVILLE, A., POMERANCE, C.; *There are infinitely many Carmichael nunbers*. Ann. of Math. 140, 1994, 703-722.

[2] BROCHERO MARTINEZ, F.E., et al; *Teoria dos Números: um passeio com primos e outros números familiares pelo mundo inteiro*. 5ª edição. Rio de Janeiro: IMPA, 2018.

[3] COUTINHO, S.C.; *Números Inteiros e Criptografia RSA*. 2^a edição. Rio de Janeiro: IMPA, 2014.

[4] DAVENPORT, H.; *Multiplicative number theory*. 3 edição. Springer-Verlag, 2000.

[5] HANSOM, D.; *On the product of the primes*. Canad. Math. Bull. 15(1), 1972, 33-37.

[6] HEFEZ, A., VILLELA, M.L.T.; *Códigos Corretores de Erros*. 2^a edição. Rio de Janeiro: IMPA, 2017.

[7] LINS NETO,A.; *Funções de uma variável complexa*. 3^a edição. Rio de Janeiro: IMPA, 2016.