UNIVERSIDADE FEDERAL DE SERGIPE
PRÓ-REITORIA DE PÓS-GRADUAÇÃO E PESQUISA
PROGRAMA DE MESTRADO PROFISSIONAL EM MATEMÁTICA

Márcia Oliveira Vieira

O Teorema dos Números Primos

SÃO CRISTÓVÃO - SE
2023

Márcia Oliveira Vieira

O Teorema dos Números Primos

Dissertação apresentada ao
Programa de Pós-Graduação em
Matemática, da Universidade
Federal de Sergipe, como
requisito parcial para obtenção do
título de Mestre em Matemática.

Orientador: Dr. Evilson da Silva Vieira

SÃO CRISTÓVÃO - SE
MAIO, 2023

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA CENTRAL
UNIVERSIDADE FEDERAL DE SERGIPE

Vieira, Márcia Oliveira.
V658t O teorema dos números primos / Márcia Oliveira Vieira ; orientador Evilson da Silva Vieira. – São Cristóvão, SE, 2023.
99 f. ; il.

Dissertação (mestrado Profissional em Matemática) – Universidade Federal de Sergipe, 2023.

1. Números primos. 2. Logarítmos. 3. Integrais (Matemática). 4. Análise matemática. I. Silva, Evilson da Silva, orient. II. Título.

CDU 511.14

Dissertação submetida à aprovação pelo Programa de Pós-Graduação em Matemática da Universidade Federal de Sergipe, como parte dos requisitos para obtenção do grau de Mestre em Matemática.

O Teorema dos Números Primos

por

Márcia Oliveira Vieira

Aprovada pela Banca Examinadora:

Prof. Dr. Evilson da Silva Vieira - UFS
Orientador

Prof. Dr. Disson Soares dos Prazeres - UFS
Primeiro Examinador

Prof. Dr. Cayo Rodrigo Felizardo Dória - UFS
Segundo Examinador

São Cristóvão, 19 de Junho de 2023.

Agradecimentos

Alguém pode pensar: “O que um servidor público com quase 20 anos de carreira e com estabilidade financeira faz voltando para a sala de aula?” Bom, talvez a realização de um sonho e a sensação de que o conforto e a comodidade estão a ponto de o sufocar. Após 17 anos, senti o desafio bater à minha porta. Havia chegado a hora de voltar a um plano traçado no último ano de graduação, abandonado pelo comodismo e falsa sensação de segurança. O pensamento de uma fase que escolhi não viver me perseguia, a cada dia, em pensamento. Hoje, posso dizer que mais um sonho se realizou, e quaisquer palavras que usar aqui não são suficientes para expressar tal sentimento.

Em primeiro lugar, e jamais poderia ser diferente, agradeço àquele que é o criador de todas as coisas, mantenedor da vida. Ouvi alguns dizerem que eu estava louca, ou que, se eu não conseguisse concluir meu curso, era a vontade de Deus. Mas, sei que, desde o momento em que escolhi me inscrever para a seleção, Deus estava ao meu lado verdadeiramente. Foi muito difícil, em certos momentos, ter a sensação de que estava só em minha jornada, até que ele me fazia lembrar que isto não era verdade. Por isso, eu agradeço a esse Deus maravilhoso. Ele realmente me inspirou em cada momento, em cada prova ou exercício, em cada linha deste trabalho. Este Deus é poderoso, e mostrou sua bondade todos os dias da minha vida. Em segundo lugar, quero agradecer ao meu amado marido, Thiago. Perdemos meu sogro faltando uma semana para a seleção do mestrado, e os meses seguintes foram tensos e extremamente desgastantes. Mas, Thiago esteve sempre me apoiando e ajudando. Se eu fui forte, ele foi mais ainda.

Quero agradecer também ao meu querido orientador, o professor Evilson. Quero agradecer pelos votos de confiança, desde o início do curso, acreditando que eu seria capaz de vencer essa jornada. Logo no início, tive uma dificuldade enorme em acompanhar suas ideias desafiadoras. Mas, o que seria da vida sem um desafio? Ao meu ponto de vista, sem graça. Foi uma grande honra trabalhar com alguém tão brilhante, responsável e comprometido com o trabalho. Tive grandes lições, tanto no âmbito acadêmico, quanto profissional e pessoal. Muito obrigada pela infindável paciência e disposição em sanar minhas dúvidas, mesmo que isto ocorresse em momentos inusitados do dia, mesmo que ocorressem em domingos ou feriados. Realmente, é impossível descrever meu nível de gratidão. Agadeço também a minha nova amiga, Ana Luíza, esposa do professor Evilson. Você nos acolheu, apoiou, aconselhou e suportou durante o último ano do meu mestrado. Obrigada por todo apoio e cada momento de escuta, por todo carinho e grande zelo. Você foi, realmente, mais um presente divino para nós.

Agradeço aos colegas de curso, Michel, Bruno, Erivaldo, Carlos, Renato, Walisson, Robson, Antônio e Rômulo. Todos foram maravilhos comigo, respeitaram minha fé, e aceitaram o desafio de ter aulas aos sábado a noite por um ano, a fim de que eu fizesse o curso sem precisar de reposições. Que Deus retribua a benção que me foi concedida, derramando outras mais na vida de cada um de vocês. Agradeço também aos demais professores que passaram pela grade do PROFMAT, cada um com valiosas lições.

Agradeço à minha família sanguínea e aos meus irmãos em fé, da Igreja Adventista do Sétimo Dia. Obrigada pelas orações, pelos momentos de escuta e pelo apoio.

Por fim, eu não poderia deixar de agradecer aos meus colegas de trabalho, os meus parceiros do C.E. Prof. Gonçalo Rollemberg Leite. Eles também tiveram um grande papel no desenrolar do meu curso. Foram apoiadores em todos os sentidos, e suportaram meus desabafos diários na sala dos professores e nos grupos de whatsapp. Amo todos vocês. Vocês são minha segunda família.

Não sei se esqueci de citar alguém, mas meu coração agradece, ainda assim, a todos que fizeram parte desta jornada. Recebam meu abraço. Deus abençoe a todos!

Graças ao grande amor do Senhor é que não somos consumidos, pois as suas misericórdias são inesgotáveis. Renovam-se cada manhã; grande é a sua fidelidade! Digo a mim mesmo: a minha porção é o Senhor, portanto, nele porei a minha esperança.

Lamentações $3 : 22 - 24$

Resumo

O objetivo deste trabalho é apresentar os números primos e mostrar uma relação entre a função de contagem de primos, $\pi(x)$, e a função logaritmo natural, $\log(x)$. Inicialmente, faremos um breve apanhado histórico. Em seguida, traremos alguns conceitos importantes acerca dos números primos e sobre alguns elementos da Análise Complexa. Por fim, estudaremos a função Zeta de Riemann e traremos a demonstração do Teorema dos Números Primos, traçando uma conexão entre a função Zeta de Riemann e a função $\pi(x)$.

Palavras chave: Teorema dos Números Primos; Distribuição dos números primos; Função Zeta de Riemann; Teoria dos Números.

Abstract

The objective of this work is to present prime numbers and show a relationship between the prime counting function, $\pi(x)$, and the natural logarithm function, $\log(x)$. Initially, we will make a brief historical overview. Next, we will bring some important concepts about prime numbers and about some elements of Complex Analysis. Finally, we will study the Riemann Zeta function and bring the demonstration of the Prime Number Theorem, tracing a connection between the Riemann Zeta function and the $\pi(x)$ function.

Keywords: Prime Number Theorem; Distribution of prime numbers; Riemann's Zeta function; Number Theory.

Sumário

Lista de Figuras

Lista de Tabelas

Capítulo 1

Introdução

Quando se ouve a expressão "um número x é primo", a maioria das pessoas lembra de algum processo que envolva divisão, como, por exemplo, fatoração de um número natural, o cálculo do máximo divisor comum entre dois números inteiros, ou alguns outros problemas específicos de Aritmética que envolvam a ideia da divisão. Dizer que a distribuição dos números primos ao longo da sequência dos números naturais tem alguma conexão com logaritmos ou números complexos talvez pareça soar estranho para algumas pessoas, mas, um jovem fanático por tábuas de logaritmo do século XVIII com apenas 15 anos de idade, Karl Friedrich Gauss, percebeu que a quantidade de números primos até um dado valor x real correspondia a um valor próximo do quociente $\frac{x}{\log x}$. Anos depois, um dos alunos de Gauss, o jovem Georg Friedrich Bernhard Riemann, percebeu que a distribuição dos números primos sobre a reta real tinha uma forte relação com a série

$$\frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \cdots + \frac{1}{n^s} + \cdots$$

aplicada a valores s complexos com parte real maior que 1.

Em séculos passados, acreditou-se que os números primos possuíam alguma propriedade mística, uma vez que dificilmente um matemático fazia descobertas nesta área da Teoria dos Números. Apesar dos primeiros teoremas envolvendo números primos terem sido enunciados e provados no século III a.C., as primeiras fórmulas que geravam alguns números primos surgiram apenas no século XVII. Neste mesmo sentido, o Teorema dos Números Primos, que mostra como ocorre a distribuição dos números primos dentro do conjunto dos números reais, só foi demonstrado em 1.896.

Hoje, há aplicações para o uso de números primos em diversas áreas de conhecimento, como em Física e em tecnologia da informação. Particularmente, grandes investimentos ocorrem na busca por novos números primos com grande quantidade de dígitos. Popularmente conhecida, a criptografia RSA é mais um exemplo de aplicação para números primos, uma vez que usa cálculos à base de números primos para promover a segurança no tráfego de dados entre dispositivos de comunicação.

Este trabalho tem por objetivo mostrar a associação da distribuição dos números primos com as funções holomorfas. No capítulo 1, traremos um breve apanhado sobre a história dos números primos, desde o primeiro registro histórico de contato humano com a ideia destes números, passando pelo ponto em que houve a primeira ideia acerca da distribuição dos números primos, até a tão buscada prova do Teorema dos Números Primos. No capítulo 2, apresentaremos a definição de um número primo, embasada nos conceitos relativos a divisibilidade. Mostraremos alguns tipos de números primos, apresentaremos

a função $\pi(x)$, conhecida como função de contagem de números primos, e traremos uma aplicação do Teorema dos Números Primos. No capítulo 3, apresentaremos o conjunto dos números complexos ($\mathbb{C}$) e um pouco de sua topologia. Trataremos sobre algumas funções em uma variável complexa, noções sobre sequências e séries de números complexos, dentre algumas importantes noções de cálculo complexo, como derivação, integração, representação em séries de potências e cálculo de resíduos. Por fim, no capítulo 4, apresentaremos a função Zeta de Riemann e as funções de Chebshevy. A partir daí, estabeleceremos uma ligação entre estas funções e a função $\pi(x)$, obtendo ferramentas suficientes para provar o Teorema dos Números Primos, ou seja, mostraremos a igualdade

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

Capítulo 2

Um breve apanhado histórico

Um dos grandes desafios da Matemática é entender padrões que expliquem a aleatoriedade do aparecimento de números primos na reta dos números reais. Considerados como *blocos de construção* dos números inteiros, durante séculos, matemáticos se debruçaram sobre a esperança de ter avanços nesta área da Teoria dos Números. Neste capítulo, veremos resumidamente como ocoreu a evolução das descobretas que marcaram a história da Matemática, no tocante aos números primos.

2.1 Os primeiros contatos com os números primos

A história sobre os números primos se inicia bem antes do que muitas pessoas imaginam. O artefato mais antigo que remete à ideia de números primos é o *osso de Ishango*. Registrado de 6.500 a.C, aproximadamente, este artefato foi encontrado na região da África Central Equatorial. Na imagem 2.1, temos uma foto deste artefato, exposto no Real Instituto Belga de Ciências Naturais, em Bruxelas, Bélgica.

Figura 2.1: *Osso d'Ishango.*

Neste osso, há marcações que aparentam ter cunho matemático. Em uma coluna específica, observam-se marcações que aparentam ser elementos de uma lista dos números primos pertencentes ao intervalo $[10, 20]$, ou seja, fazendo referência aos números 11, 13, 17 e 19, como pode ser conferido na imagem 2.2.

Apesar da existência deste artefato, acredita-se que a primeira cultura a tentar desvendar os mistérios acerca dos números primos tenha sido a dos chineses, por volta de 1.000 a.C.. Há registros de que características femininas eram atribuídas aos números pares, e as masculinas, aos ímpares. A ideia de números afeminados estava associada a números ímpares maiores que a unidade, e que não eram primos (um tipo de número composto). Nesta cultura, a ideia de números machões se relacionava, então, aos números primos. O termo *machões* foi usado pelo fato de não conseguirem distribuir grãos de

quantidades dadas por números primos em fileiras com um mesmo número de linhas. Como se este tipo de quantidade de grãos "resistisse" às tentativas de distribuição. Por exemplo, se houvesse uma pilha com 10 grãos, poderiam ser feitas distribuições dos grãos em 2 colunas, contendo 5 grãos em cada, ou 5 colunas contendo 2 grãos em cada. Poderia, ainda, formar uma única coluna, contendo todos os 10 grãos. Mas, a partir de uma pilha com 13 grãos, que se trata de uma quantidade com número primos de grãos, por exemplo, não seria possível formar mais de uma coluna com quantidade igual de grãos. Ou seja, todos os grãos deveriam vir em uma única coluna [14].

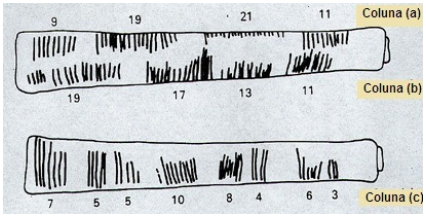

Figura 2.2: *Detalhes do conteúdo do osso d'Ishango.*

2.2 Os primos e os pitagóricos

Dentre todos os povos antigos, a história registra que os gregos foram os primeiros a associar a ideia de blocos de construção para os números a partir de números primos. Possivelmente, a noção de número primo tenha sido introduzida por Pitágoras, por volta de 530 a.C. Os gregos pitagóricos perceberam que havia números que não poderiam ser expressos como o produto de dois outros menores, diferentes da unidade. Então, começaram a estudar com mais interesse as propriedades de tais números. Eles perceberam que qualquer número diferente da unidade era originário de algum produto envolvendo números primos, como por exemplo, $2 = 1 \cdot 2$ e $10 = 2 \cdot 5$.

Dentro de sua base teórica, os gregos antigos associavam a ideia de uma grandeza ou de um número ao comprimento de um segmento de reta. A unidade era considerada como algo indivisível, servindo de parâmetro de contagem, mas não era considerada um número. Na verdade, a nomenclatura atribuída à unidade recebia o nome de *monad*. Já a coleção de unidades foi nomeada como *arithmói*. O próprio Pitágoras atribuiu o termo *protoi arithmói* a números que traduzimos como números primários, ou seja, números primos. Por sua vez, os números gerados a partir de primos eram denominados *deuterói arithmói*, cuja tradução corresponde a números secundários. Sendo assim, aplicavam conceitos relativos à Teoria dos Números a conceitos de Geometria.

Um dos primeiros matemáticos a estudar com vigor a Teoria dos Números foi Euclides de Alexandria (aprox. 323 - 283 a.C). Apesar de ser conhecido por grandes descobertas no campo da geometria, Euclides chegou a escrever três livros voltados para a teoria elementar dos números. O livro *Elementos VII*, por exemplo, inicia com um processo para calcular o máximo divisor de dois ou mais números, e que verificava se dois números inteiros são primos entre si. Neste mesmo livro, Euclides apresenta a noção de número e unidade. Abaixo, temos a tradução do trecho de seu livro em que há esta apresentação.

Definição VII.1 *A unidade é aquilo segundo o que cada uma das coisas existentes é dita 'uma'.*
Definição VII.2 *O número é uma multiplicidade composta de unidades.*
Definição VII.3 *Um número é uma parte de um número, o menor do maior, quando ele mede o maior.*

Tal definição acerca da unidade serviu de fundamento para o famoso *Algoritmo de Euclides*, que visa calcular a maior medida comum de dois números, o que chamamos, atualmente, de *máximo divisor comum* ou mdc [13]. A ideia geométrica para determinar o mdc consite em tomar dois números, x e y, e representá-los, respectivamente, por segmentos. Denotaremos estes segmentos respectivamente por AB e CD. Observa-se, então, qual destes é o de maior medida. Sem perda de generalidade, considere este sendo AB.

O procedimento consiste em verificar se CD mede AB. Ou seja, verifica-se a possibilidade de retirar continuamente do segmento AB pedaços de medida igual à de CD, observando se há alguma sobra.

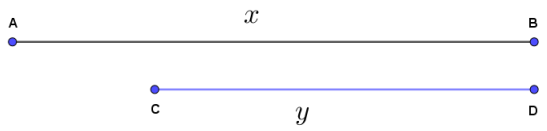

Figura 2.3: *Ilustração da comparação entre os segmentos de medidas x e y.*

Não havendo uma sobra, dize-se que CD mede AB. Consequentemente, x é múltiplo de y. Caso contrário, nomeando o segmento restante de AR_1, percebe-se que a medida de AR_1 correspondente ao resto da divisão de x por y. Digamos que a medida de AR_1 represente o número natural r_1. A título de ilustração, temos a figura 2.4 indicando esta ideia de sobra.

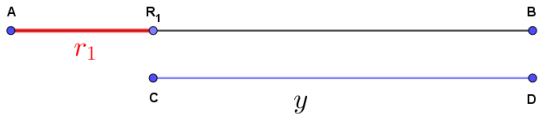

Figura 2.4: *Ilustração do processo de divisão.*

Analogamente, verificamos quantas vezes AR_1 cabe em CD, e se há um "resto" CR_2. Sendo possível prosseguir o processo, pode-se obter sobras AR_3, CR_4, sucessivamente. Se, em algum momento do processo de comparações e retiradas sucessivas, houver um segmento restante equivalente ao padrão da unidade, então x e y são ditos primos entre si, uma vez que os gregos não consideravam 1 como um número. No caso em que x e y não são primos entre si, em algum momento do processo haverá um segmento restante diferente da unidade, e que mede, exatamente, o precedente. Este "resto" representa o mdc entre x e y.

Uma das consequências destas comparações é que, caso um número natural não possa ser medido por nenhum outro número diferente dele mesmo, exceto pela unidade, tal número é entitulado número primo[14]. Vejamos a seguir um exemplo prático do processo de divisão euclidiana.

Exemplo 2.2.1. *Calcule o* mdc *de* 30 *e* 25.

Inicialmente, observamos que 30 é maior que 25. Então, podemos retirar 25 unidades, de uma única vez, de um segmento de 30 unidades de comprimento, restando um segmento de $r_1 = 5$ unidades. Em seguida, percebemos que pode-se retirar cinco segmentos de tamanho correspondente a 5 unidades do segmento de 25 unidades de comprimento, sem que haja sobra. Ou seja, 5 "cabe" uma quantidade exata de vezes dentro de 25. Desta maneira, chegamos à conclusão de que o mdc entre 30 e 25 é 5. O processo algébrico corresponde a:
a) $30 = 25 \cdot 1 + 5$,
b) $25 = 5 \cdot 5$

Usualmente, o dispositivo de Euclides para calcular o mdc entre os números naturais a e b é representado como na tabela 2.1. Sua ideia coincide com o processo geométrico descrito acima. Todos os números envolvidos são números naturais. Assim, as divisões sucessivas

$$\begin{aligned} a &= bq_1 + r_1 \\ b &= r_1q_2 + r_2 \\ r_1 &= r_2q_3 + r_3 \\ &\vdots \\ r_{n-1} &= r_nq_{n+1}, \end{aligned}$$

onde $\text{mdc}(a, b) = r_n \geq 0$, são representadas do seguinte modo: na primeira linha, a partir da segunda coluna, são colocados os quocientes de cada divisão sucessiva $q_1, q_2, q_3, ..., q_n$. Na segunda linha, a primeira coluna é preenchida pelo dividendo, e a partir da segunda coluna, pelos sucessivos divisores $b, r_1, r_2, ..., r_{n-1}, r_n$. Na terceira linha, logo a partir da primeira coluna, são inseridos os restos de cada divisão $r_1, r_2, ..., r_{n-1}, r_n$. Ou seja,

	q_1	q_2	q_3	...	q_{n-1}	q_n	q_{n+1}
a	b	r_1	r_2	...	r_{n-2}	r_{n-1}	r_n
r_1	r_2	r_3	r_4	...	r_n		

Tabela 2.1: Algoritmo de Euclides

Além do algoritmo que leva seu nome, Euclides também enunciou em seu livro *Elementos IX*, na proposição IX 14, o equivalente ao Teorema Fundamental da Aritmética. Este teorema mostra que todo número inteiro maior que um é primo ou se escreve de modo único como produto de, no mínimo, dois primos, salvo quanto à ordem de seus fatores. Neste mesmo livro, através da proposição IX 20, Euclides provou o teorema sobre a infinitude dos números primos. Esta demonstração é considerada universalmente como modelo de elegância matemática, devido à maestria na manipulação da hipótese [13].

2.3 O surgimento de um crivo

Registra-se que o primeiro matemático a escrever uma tabela de números primos foi o bibliotecário-chefe da universidade local de Alexandria, o grego Eratóstenes de Cirene (aprox. 276 – 194 a.C.). Ele criou um dispositivo muito útil para descobrir todos os números primos pertencentes ao intervalo $[1, N]$, onde N é um número natural. Este dispositivo recebeu o nome de *crivo de Eratóstenes*. Até o presente momento, o único método utilizado para verificar se dois números eram primos consistia na divisão euclidiana, verificando o resultado do mdc de dois números quaisquer. O método utilizado

por Eratóstenes consiste em eliminar gradativamente números compostos. Inicialmente, escreve-se uma tabela com os N primeiros números naturais, reservando o número 2 e riscando da lista todos os múltiplos de 2. Em seguida, repete-se o processo, reservando o próximo elemento da lista após o número 2 que não havia sido riscado, ou seja, o número 3, e riscando todos os seus múltiplos. Posteriormente, reserva-se o número 5, e assim por diante, até o maior inteiro cujo quadrado é menor ou igual a N. Ao final deste processo, todo número não riscado da lista é um primo [14].

Na tabela 2.2, temos um exemplo do crivo para descobrir os números primos entre 1 e 100. Automaticamente, o número 1 é o primeiro a ser eliminado. Em azul, foram destacados os múltiplos de 2, e em verde, os múltiplos de 3 que ainda não haviam ganhado destaque. De modo análogo, em vermelho, temos os múltiplos de 5 ainda não destacados anteriormente, e, em cinza, os múltiplos de 7. O próximo número primo usado para eliminar números compostos seria 11, mas o primeiro elemento da tabela que ele eliminaria seria $11^2 = 121$, que já não consta na tabela de 1 a 100. Deste modo, os números sem destaque na tabela são todos os números primos pertencentes a este intervalo.

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Tabela 2.2: Crivo de Eratóstenes

Esse método foi estudado e aprimorado por outros matemáticos posteriormente, como por Ernst Meissel em 1.870, por Bertelsen em 1.893, e por D.H. Lehmer, em 1.959. Apesar de ser um método simples, torna-se trabalhoso e lento para valores de N muito grandes. Atualmente, existem testes de primalidade mais rápidos e eficazes, desenvolvidos por outros matemáticos séculos mais tarde.

2.4 Um teste de primalidade e a busca por fórmulas

Apesar de sua ocupação principal ser de um advogado, e de ter recebido sua educação inicial em casa, o francês Pierre de Fermat (1.601 – 1.665) dedicava horas de lazer para o estudo da Matemática. Sua avidez trouxe contribuições altamente relevantes para vários campos de estudo, dentre eles, a Teoria dos Números. Em especial, enunciou teoremas voltados ao estudo dos números primos. Destacamos neste trabalho o *Pequeno Teorema de Fermat*, que fornece um importante teste de primalidade. Fermat apenas enunciou este teorema através de uma carta com data de 18 de outubro de 1.640, destinada a Frénicle de Bessy. A primeira demonstração do PTF, assim conhecido pelos matemáticos, data de 1.736, por Euler [3]. Falaremos mais sobre este teorema na Seção 3.3 deste trabalho.

Fermat também foi responsável por apresentar uma prova de que todo número primo ímpar pode ser expresso de modo único como a diferença entre dois quadrados. Exemplificando este fato, temos que $3 = 2^2 - 1^2$ e $17 = 9^2 - 8^2$. Para a demonstração

desta afirmativa, Fermat partiu da premissa de que, se p é um primo ímpar, então

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

Observe que, se $p = x^2 - y^2$, então $p = (x+y)(x-y)$. Como p é primo, então $x + y = p$ e $x - y = 1$, de onde se obtém o resultado.

Fermat chegou apenas a enunciar outros dois teoremas acerca dos números primos da forma $4n + 1$. Estes também foram provados posteriormente por outros matemáticos. Em 1.640, Fermat escreveu uma carta para um grande estudioso das ciências: o padre Marin Mersenne (1.588 – 1.648). Nesta carta, Fermat afirmou que possivelmente teria descoberto uma fórmula para calcular alguns números primos. Mas, em 1.732, Euler apresentou uma prova de que tal fórmula não era totalmente válida [3]. Detalharemos sobre esta fórmula proposta por Fermat na Seção 3.3 deste trabalho.

2.5 Euler e o início da análise complexa

Mesmo diante de sérios problemas na visão, o suiço Leonhard Euler (1.707 – 1.783), inspirado pelas ideias de Fermat, foi responsável por implementar importantes notações, tais como $f(x)$ para funções, e para a base de logaritmos naturais, Σ para somatórios e i para a unidade imaginária, onde $i^2 = -1$. Suas descobertas foram de grande maestria, sendo que chegou a publicar 530 trabalhos durante sua vida [3].

Euler também foi responsável por uma identidade bastante utilizada na Análise Complexa:

$$e^{ix} = \cos(x) + i\,\mathrm{sen}(x),$$

onde, para $x = \pi$, relaciona cinco dos mais importantes números da Matemática: 0, 1, π, e e i.

Euler se interessava por uma diversidade de assuntos da Matemática de sua época, mas tinha uma grande visão para resolução de problemas sobre hidráulica, construção de navios e balísticas. Uma de suas conquistas, foi dar uma solução plausível para o problema das pontes de Königsberg. Sua paixão por cálculos foi possivelmente estimulada pelo contato através de cartas com o matemático alemão Christian Goldbach. Em um de seus contatos, anunciou a conjectura de que todo número par poderia ser expresso como a soma de dois números primos. Seu amor pela Teoria dos Números se estendeu pelo interesse acerca do mistério dos números primos, levando-o a construir tabelas de primos para valores pouco superiores a 100.000. Euler escreveu uma fórmula para calcular uma lista de alguns números primos: $x^2 + x + 41$, válida para valores inteiros de x tais que $0 \leq x \leq 39$. Euler sabia que sua fórmula falharia em algum ponto, e desviou seu trabalho para a análise dos valores de q para os quais a fórmula $x^2 + x + q$ também geraria números primos.

Euler foi um dos primeiros matemáticos a estudar uma função que envolve séries infinitas que convergiam, denominada função zeta e representada pela letra grega ζ. Nesta representação para a função zeta, Euler utilizou valores de x reais maiores que 1.

$$\zeta(x) = \frac{1}{1^x} + \frac{1}{2^x} + \frac{1}{3^x} + \cdots + \frac{1}{n^x} + \cdots$$

Em particular, Euler analisou a soma dos inversos dos quadrados de números naturais, mostrando que

$$1 + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \cdots = \frac{\pi^2}{6}.$$

Atribui-se também a Euler a ideia de produto de séries de frações relacionadas a números primos, conhecido como *produto de Euler*, cuja igualdade é válida para $x \in \mathbb{C}$, com parte real de x maior que 1. Assim, relaciou o produto infinito de somas de Progressões Geométricas, cujas razões são da forma $\frac{1}{p}$, onde p é um número primo, à função zeta[14].

$$\zeta(x) = \frac{1}{1^x} + \frac{1}{2^x} + \frac{1}{3^x} + \cdots + \frac{1}{n^x} + \cdots$$

$$= \left(1 + \frac{1}{2^x} + \frac{1}{(2^2)^x} + \cdots\right) \cdot \left(1 + \frac{1}{3^x} + \frac{1}{(3^2)^x} + \cdots\right) \cdots \left(1 + \frac{1}{p^x} + \frac{1}{(p^2)^x} + \cdots\right) \cdots$$

2.6 A disputa entre Gauss e Legendre

Aos 15 anos de idade, Karl Friedrich Gauss (1.777 – 1.855) ficou intrigado com o fato de um livro sobre logaritmos conter uma tabela de números primos na sua contracapa. Em sua época, era muito comum trabalhar com logaritmos em vários ramos, como na navegação, contabilidades bancárias e com mercadores. Sua curiosidade o fez trabalhar em tabelas, e perceber que esses dois temas possuíam alguma conexão. Ao comparar a quantidade de números primos entre 1 e 10, 1 e 100, 1 e 1.000, ou 1 e qualquer outra potência de base 10, notava que precisava adicionar aproximadamente 2,3 ao quociente entre a quantidade x de números analisados e a quantidade de primos até o mesmo x. A relação entre multiplicação e adição dos valores encontrados está justamente relacionada às propriedades de logaritmo, tão conhecidas por Gauss. O detalhe sutil proposto por Gauss se referia ao logaritmo natural, ou seja, logaritmo cuja base seja o número e. Usando a simbologia $\pi(x)$ para expressar a quantidade de números primos existentes de 1 até o número x, Gauss estimou que $\pi(x)$ era, aproximadamente,

$$\frac{x}{\log(x)},$$

onde $\log(x)$ representa o logaritmo na base e. Seu objetivo não consistia em prever a posição do próximo número primo no conjunto dos números naturais, mas observar o padrão relativo à quantidade de primos até dado x. Apesar de sua grande descoberta, Gauss não a consideraria realmente valiosa se não pudesse escrever uma prova a esse respeito. Assim, resolveu deixar suas ideias iniciais em segredo, apenas como anotações. Na verdade, muitas de suas descobertas estavam em uma linguagem secreta própria. Certas anotações continuam sem uma "tradução" até a atualidade. Somente após sua morte, foi descoberta a época aproximada em que Gauss conjecturou estas ideias acerca da quantidade de números primos. Isto se deu através da abertura de algumas correspondências e artigos antigos.

Na mesma época que Gauss, Adrien-Marie Legendre (1.752 – 1.833) também estudava o mistério em torno dos números primos. Diferentemente de Gauss, Legendre não temia o anúncio de ideias sem o respaudo de uma prova. Assim, em 1.798, ousou anunciar uma relação entre os números primos e logaritmos próxima à ideia de Gauss: a quantidade de números primos existentes de 1 até o número x consistia em um valor próximo a

$$\frac{x}{\log(x) - 1{,}08366}.$$

Para valores baixos de x, a fórmula sugerida por Legendre era mais próxima do valor real de $\pi(x)$. Iniciou-se o que parecia uma disputa entre Gauss e Legendre, o que levou Gauss a continuar trabalhando em sua análise de anos antes. Inspirado na ideia de comparar a probabilidade de obter um número primo entre 1 e x à probabilidade de se obter "cara" em uma moeda viciada, chegou à função $\mathrm{Li}(x)$, que possui uma aproximação melhor a $\pi(x)$ do que a previsão de Legendre.

Baseado na sua ideia inicial de que probabilidade de um número N ser primo era $\frac{1}{\log N}$, a nova função de Gauss, $\mathrm{Li}(x)$, se baseava na variação da soma das probabilidades de obtermos primos entre 1 e x tomados aleatoriamente, expressa por uma integral.

$$\mathrm{Li}(x) = \int_2^x \frac{dx}{\log(x)}$$

Gaus chegou a listar números primos até 3.000.000. Apesar de próximos para esta faixa, o gráfico de $\pi(x)$ e $\mathrm{Li}(x)$ são distintos, uma vez que $\mathrm{Li}(x)$ possui uma curva suave e $\pi(x)$ possui formato de "escada" [14]. Na figura 2.5, temos um gráfico que mostra a aproximação entre as funções $\pi(x)$ e $\mathrm{Li}(x)$, para valores até 550. Em azul, está representada $\mathrm{Li}(x)$, em verde, $\pi(x)$, e em vermelho, $x/\log(x)$.

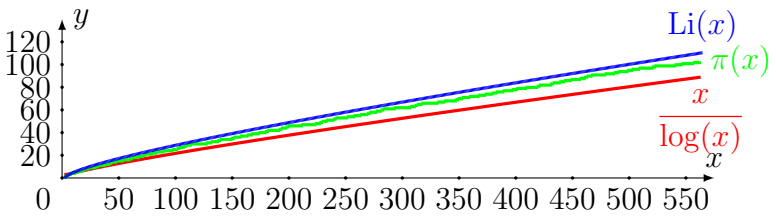

Figura 2.5: *Gráfico comparativo entre* $\pi(x)$ *e* $\mathrm{Li}(x)$.

2.7 Chebyshev e uma importante estimativa

As grandes contribuições que fundamentaram uma posterior demonstração para a conjectura de Gauss não se resumiram apenas a matemáticos europeus. Em meados do século XIX, o russo Pafnuti Lvovitch Chebyshev $(1.821 - 1.894)$ conseguiu mostrar que a razão entre $\pi(x)$ e $x/\log(x)$ estava sempre contida em um intervalo (C_1, C_2), onde C_1 e C_2 são números positivos, para todo valor $x \geq 2$. Esta se tornou a primeira contribuição concreta para a prova do teorema dos números primos. Dentre suas muitas descobertas, destacamos também a primeira e a segunda funções de Chebyshev, que relacionam os logaritmos dos números primos existentes no intervalo de 1 até n, como veremos na Seção 5.1. Chebyshev também conseguiu provar que, para todo inteiro $n \geq 2$, existe, ao menos, um número primo pertencente ao intervalo de n a $2n$. Este teorema foi intitulado *postulado de Bertrand* [14].

2.8 Riemann, os números primos e a música

Aluno de Gauss e do matemático Dirichlet, o alemão Georg Friedrich Bernhard Riemann (1.826 - 1.866) foi responsável por relacionar uma função antiga grega, a função zeta $\zeta(x)$, à Análise Complexa e à Teoria dos Números primos. Em 1.748, Euler percebeu

que ao inserir números complexos na função 2^x, seu gráfico possuia ondulações semelhantes às de ondas sonoras, e acreditava que os números primos tinham algo em relação a "combinações de notas musicais", segundo [14]. Como um grande mentor, Dirichlet influenciou fortemente Riemann a estudar a função zeta, e tomar como base as análises feitas por Euler um século antes. Através de tal função aplicada a números complexos com parte real maior que 1, Riemann percebeu que a afirmação acerca dos logaritmos feita por Gauss era cada vez mais próxima da veracidade para valores muito altos de x.

As ideias de Riemann sobre os números primos foram revolucionárias, pois indicavam que existe alguma ordem em meio à aleatoriedade do surgimento de números primos à medida que caminhamos na reta dos números naturais. Ele afirmou que a distribuição dos números primos estava diretamente relacionada à função zeta, mas não conseguiu mostrar tal fato. Riemann afirmou que a função zeta poderia ser estendida para todo o plano complexo, percebendo que tal função se anulava para -2, -4, -6,.... Além disso, Riemann fez uma forte afirmação, chamada *hipótese de Riemann*. Nenhum matemático conseguiu realizar a prova desta hipótese até o momento da escrita deste trabalho, em maio de 2.023. Em sua afirmação, todos os demais zeros da função zeta, denominados zeros não triviais da função zeta, são números complexos cuja parte real é igual a $\frac{1}{2}$. A repercusão da hipótese de Riemann gerou uma corrida entre os matemáticos em busca de novas descobertas, e ganhou destaque no Congresso Internacional de Matemática realizado no ano de 1.900, na Universidade de Göttingen, Alemanha. Tal problema entrou para a lista dos 23 problemas do século em questão, propostos pelo professor David Hilbert durante sua palestra realizada neste mesmo congresso.

Em 24 de maio de 2.000, uma reunião no Collège de France marcou o 100º aniversário do problema proposto por Hilbert. Seriam lançados novos desafios para o novo milênio que iniciara. Dentre os sete problemas propostos nesta reunião, a hipótese de Riemann ainda permanecia ilesa. Entretanto, agora há uma recompensa de um milhão de dólares para aquele que apresentar soluções devidamente fundamentadas para a hipótese. A prova desta afirmativa é de serventia essencial para o estudo da distribuição dos números primos, uma vez que muitas outras afirmativas da área da Teoria dos Números se baseiam na veracidade desta hipótese [14].

2.9 Hadamard, Poussin e uma demonstração

Após séculos de hipóteses e descobertas, finalmente, no final do século XIX, Jacques Hadamard (1.865 - 1.963) e Charles Jean de la Vallée-Poussin (1.866 - 1.962) conseguiram demonstrar o Teorema dos Números Primos usando as análises de Riemann, de forma independente e no mesmo ano. A prova deste teorema corresponde à prova da conjectura proposta por Gauss de que, para um x suficientemente grande, $\pi(x)$ era aproximadamente

$$\frac{x}{\log(x)}$$

Vários matemáticos após Hadamard e Vallé-Poussin trabalharam para obter outras demonstações mais elementares ou simples para o mesmo teorema, como Atle Selberg e Paul Erdös em 1.949, e Donald J. Newman em 1.980 [14]. A demonstração do Teorema dos Números Primos envolve técnicas de Análise Complexa, as quais detalharemos no Capítulo 4.

Apesar desta grande conquista, muitas outras questões ainda necessitam de respostas comprovadas, como por exemplo:

- Há uma quantidade limitada de números primos na seqüência de Fibonacci?
- Até qual valor de n natural há um número primo entre n^2 e $(n+1)^2$?
- Há quantos primos da forma $n^2 + 1$?
- Há mais que quatro números primos de Fermat?

Capítulo 3

Espaçamentos entre primos

A essência da Matemática consiste na busca por padrões, algo que tem desafiado os adeptos da Teoria dos Números através dos números primos. Encontramos referência aos números primos na natureza, como no ciclo das cigarras, que saem da toca apenas a cada 7, 13 ou 17 anos, em romances, como no livro *Contato* de Carl Sagan, que trata de contatos extraterrestres através de códigos fundamentados em sequências de primos, e até mesmo em filmes, como *Número 23*, onde o personagem principal do filme se sente perseguido pelo número 23 [14]. Este capítulo visa trazer algumas definições, teoremas e proposições acerca do conceito de divisibilidade. De posse destas informações, traremos o conceito de número primo, bem como a classificação para alguns destes. Por fim, apresentaremos o conceito de lacunas entre primos e uma aplicação direta do Teorema dos Números Primos.

3.1 Conceitos básicos

Para entender o que é um número primo, faz-se necessário conhecer alguns conceitos importantes acerca da ideia de divisibilidade. Comecemos com a definição de divisor.

Definição 3.1.1. *Dados dois números $n, m \in \mathbb{Z}$, se existe um $k \in \mathbb{Z}$ tal que $n = m \cdot k$, então m é dito divisor ou fator de n.*

Uma consequência imediata desta definição é que, para qualquer que seja n natural, $n = 1 \cdot n$, ou seja 1 e n são divisores de n. Então todo número natural maior que 1 possui, no mínimo, dois divisores distintos positivos. Usaremos a notação $m \mid n$ para dizer que m é um divisor de n.

Proposição 3.1.2. *Sejam $a, b, c \in \mathbb{Z}$ tais que $a \mid b$ e $b \mid c$, então $a \mid c$.*

Demonstração. Como $a \mid b$ e $b \mid c$, então existem $m, n \in \mathbb{Z}$ tais que $b = na$ e $c = mb$. Logo, $c = mna$ e, por consequência, $a \mid c$. □

Esta propriedade transitiva nos garante que todos os divisores do número inteiro k também são divisores de nk, onde n também é inteiro. Esta propriedade será essencial para entender o conceito de mdc.

Exemplo 3.1.3. *Como $5 \mid 15$ e $15 \mid 30$, então $5 \mid 30$.*

Proposição 3.1.4. *Se $a, b, c, m, n \in \mathbb{Z}$, $c \mid a$ e $c \mid b$ então $c \mid (ma + nb)$.*

Demonstração. Suponha que $a, b, c \in \mathbb{Z}$. Como $c \mid a$, existe $k_1 \in \mathbb{Z}$ tal que $a = k_1 \cdot c$.

Tomando $m \in \mathbb{Z}$, podemos escrever

$$m \cdot a = m \cdot k_1 c \tag{3.1}$$

Analogamente, como $c \mid b$, existe $k_2 \in \mathbb{Z}$ tal que $b = k_2 \cdot c$. Tomando $n \in \mathbb{Z}$, escrevemos

$$n \cdot b = n \cdot k_2 c \tag{3.2}$$

Somando 3.1 e 3.2 membro a membro, temos

$$\begin{aligned} ma + nb &= mk_1 c + nk_2 c \\ &= (mk_1 + nk_2) \cdot c \end{aligned}$$

Logo, $c \mid (ma + nb)$. □

Exemplo 3.1.5. *Como* $3 \mid 12$ *e* $3 \mid 9$*, então* $3 \mid (4 \cdot 12 - 2 \cdot 9) = 30$.

Antes de trabalhar essencialmente com números primos, vejamos a ideia fundamental de Euclides sobre a conhecida operação da divisão entre números inteiros. Este algoritmo aparece no livro VII dos "Elementos" de Euclides, escrito por volta do ano 300 a.C, e tem por base o uso da Proposição 3.1.4.

Teorema 3.1.6. *(Divisão Euclidiana) Sejam* $a, b \in \mathbb{Z}$*, onde* $|b| \neq 0$*. Então existem dois únicos inteiros* q *e* r *tais que* $a = q \cdot b + r$*, onde* $0 \leq r < |b|$*. O número* q *é chamado quociente da divisão de* a *por* b*, e o número* r *é chamado resto da divisão.*

Demonstração. Inicialmente, verifiquemos a existência dos números inteiros q e r. Sem perda de generalidade, tomemos b positivo. Pelo Teorema de Eudoxius (chamado Princípio Arquimediano), como $b > 0$, existe $q \in \mathbb{Z}$ tal que

$$qb \leq a < (q+1)b$$

Somando $-qb$ a cada membro da desigualdade, obtemos

$$0 \leq a - qb < b$$

Assim, tomando $r = a - q \cdot b$, temos que, de fato, existem r e q que satisfaçam a condição do teorema, ou seja, $a = q \cdot b + r$, onde $0 \leq r < b$.

Para a unicidade, suponha que exista outro par de números, r_1 e q_1 inteiros, $0 \leq r_1 < |b|$, tais que

$$a = q_1 \cdot b + r_1$$

Como $a - a = 0$, então

$$(q \cdot b + r) - (q_1 \cdot b + r_1) = 0$$

Consequentemente

$$(q - q_1) \cdot b = r - r_1$$

Note que, como $r_1 < |b|$ e $r < |b|$, então $|r_1 - r| < |b|$.

Este fato implica dizer que se $b \mid (r_1 - r)$, então $r_1 - r = 0$. Ou seja, $r = r_1$.

Consequentemente,

$$q_1 b = qb$$

e, uma vez que $b \neq 0$,

$$q_1 = q$$

□

Observe que se $r = 0$, então $a = q \cdot b$, mostrando que b e q são divisores de a.
Vejamos agora a ideia de divisor comum e de máximo divisor comum.

Definição 3.1.7. *Sejam $a, b \in \mathbb{Z}$. Se $d \mid a$ e $d \mid b$, onde $d \in \mathbb{Z}$. Então d será dito um divisor comum de a e b.*

Definição 3.1.8. *Um número inteiro d é dito o máximo divisor comum entre dois números inteiros a e b, se atender às seguintes condições:*
i) d é um divisor comum de a e b.
ii) Se existe $c \in \mathbb{N}$ tal que $c \mid a$ e $c \mid b$, então $c \mid d$.

Denotaremos o máximo divisor comum entre a e b por $\text{mdc}(a, b)$. Intuitivamente, podemos perceber que o conjunto dos divisores de dado inteiro n é limitado. Percebemos também que qualquer número inteiro é divisível pelo número 1. Ou seja, o conjunto dos divisores comuns de dois números inteiros a e b possui, pelo menos, um elemento. Então podemos dizer que sempre existirá o número $d = \text{mdc}(a, b)$, e que $d > 0$. Para uma demonstração rigorosa deste fato, recomendamos a leitura de [5].

Exemplo 3.1.9. $\text{mdc}(12, 3) = 3$*, uma vez que os divisores positivos de 12 são* 1, 2, 3, 4, 6 *e* 12*, e os divisores positivos de* 3 *são* 1 *e* 3*.*

Proposição 3.1.10. *Sejam a, b e n números inteiros. Se existe um $d \in \mathbb{N}$ tal que $d = \text{mdc}(a, b - na)$, então $d = \text{mdc}(a, b)$.*

Demonstração. Note que se existe $d \in \mathbb{N}$ tal que

$$d = \text{mdc}(a, b - na)$$

então $d \mid a$ e $d \mid (b - na)$ e, pela Proposição 3.1.4, $d \mid b$. Assim, d é um divisor comum de a e b.

Agora, suponha que $c \in \mathbb{Z}$ seja um divisor comum de a e b. Então ainda pela Proposição 3.1.4, sendo n inteiro,

$$c \mid (b - na)$$

Assim, c é um divisor comum de a e $b - na$. Logo, pela nossa hipótese, $c \mid d$, mostrando que $d = \text{mdc}(a, b)$. □

Corolário 3.1.11. *Sejam $a, b \in \mathbb{Z}$. Se existem $q, r \in \mathbb{Z}$, com $r \neq 0$ e r positivo, tais que $a = b \cdot q + r$, então* $\text{mdc}(a, b) = \text{mdc}(b, r)$*.*

Demonstração. Segue da Proposição 3.1.6 e da proposição anterior. □

Note que este colorário descreve e justifica as divisões sucessivas ocorridas no algoritmo de Euclides, citados no capítulo 2, seção 2.2.

Teorema 3.1.12. *Sejam $a, b \in \mathbb{Z}$, b não nulo, tais que $d = \text{mdc}(a, b)$. Então existem m e n inteiros tais que*

$$d = ma + nb$$

Demonstração. Considere o seguinte conjunto $I(a, b)$ de combinações lineares entre a e b dado por

$$I(a, b) = \{xa + yb\,;\, x, y \in \mathbb{Z}\}.$$

Pelo Princípio da Boa Ordem, $I(a,b)$ possui um menor elemento positivo, digamos c. Então temos inteiros m, n tais que $c = ma + nb$.

Por outro lado, pela Proposição 3.1.6, existem q e r tais que $a = qc + r$, com $0 \leq r < c$. Daí, temos

$$\begin{aligned} r &= a - qc \\ &= a - q(ma + nb) \\ &= (1 - qm)a + (-qn)b \end{aligned}$$

Como $1 - qm$ e $-qn$ são inteiros, $r \in I(a,b)$. Mas, por hipótese, c é o menor elemento positivo de I. Logo, $r = 0$ e $c \mid a$. De maneira análoga, prova-se que $c \mid b$.

Agora, suponha que $d = \text{mdc}(a,b)$. Então $d \mid a$ e $d \mid b$. Logo, existem $k_1, k_2 \in \mathbb{Z}$ tais que $a = k_1 d$ e $b = k_2 d$. Daí, temos

$$\begin{aligned} c &= ma + nb \\ &= mk_1 d + nk_2 d \\ &= d(mk_1 + nk_2) \end{aligned}$$

Ou seja, $d \mid c$. Mas, como $c \mid a$, $c \mid b$ e $d = \text{mdc}(a,b)$, então $d = c$, de onde segue o resultado. □

Para encerrar esta seção, vejamos um teorema que nos trará uma importante ferramenta para escrever os fatores de dado número inteiro.

Teorema 3.1.13. *Sendo a, b e c inteiros não nulos, onde $a \mid bc$ e $\text{mdc}(a,b) = 1$, então $a \mid c$.*

Demonstração. Pelo Teorema 3.1.12, existem m e n inteiros tais que

$$am + bn = 1.$$

Multiplicando ambos os membros por c, temos que

$$amc + bcn = c.$$

Uma vez que $a \mid bc$ por hipótese, podemos escrever, para dado k inteiro

$$\begin{aligned} c &= a(mc) + (ak)n \\ &= a(mc + kn). \end{aligned}$$

Logo, $a \mid c$. □

3.2 Os números primos

Diante de todos os resultados postos até aqui acerca da divisibilidade, podemos definir o conceito de número primo.

Definição 3.2.1. *Um número inteiro p, onde $p > 1$, é dito primo se possuir exatamente dois divisores distintos positivos, a saber, 1 e p.*

Note que se um número natural n não é primo, então $n = rs$, onde $1 < r, s < n$ e $r, s \in \mathbb{N}$. Assim, todo número natural que possuir mais de dois divisores positivos distintos será chamado *composto*.

Definição 3.2.2. *Sejam $a, b \in \mathbb{Z}$. Então a e b serão ditos primos entre si, ou coprimos, se* $\text{mdc}(a, b) = 1$.

Exemplo 3.2.3. $(4, 15)$, $(9, 14)$, $(21, 25)$ *são pares de coprimos.*

Proposição 3.2.4 (Lema de Euclides)**.** *Sejam $a, b \in \mathbb{Z}$ e p primo, se $p \mid ab$, então $p \mid a$ ou $p \mid b$.*

Demonstração. Se p não é divisor de a, então, pela Definição 3.2.2, $\text{mdc}(a, p) = 1$. Assim, pelo Teorema 3.1.13, $p \mid b$. □

Note que esta proposição reflete uma propriedade dos números primos que os caracterizam. Ela será essencial para a demonstração do Teorema Fundamental da Aritmética, enunciado por Euclides há, aproximadamente, 2.300 anos. Este teorema aponta para a ideia de que os números primos são "blocos de construção" para os números inteiros não nulos.

Teorema 3.2.5 (Teorema Fundamental da Aritmética)**.** *Dado um número natural n, diferente da unidade, então n é primo ou se escreve de modo único como produto de primos, a menos da ordem de seus fatores.*

Demonstração. Primeiramente, vamos mostrar a validade da decomposição em fatores primos usando o Princípio da Indução.

Observe que a afirmativa é válida trivialmente para o caso $n = 2$, uma vez que o número 2 é primo.

Suponha, então, que a afirmação seja verdadeira para qualquer número natural menor do que n, $n \neq 1$ e $n \geq 2$. Se n for primo, não há o que demonstrar. Se n não for primo, então existem $a, b \in \mathbb{N}$, com $1 < a, b < n$, tais que $n = a \cdot b$. Pela hipótese de Indução, a e b são números primos ou podem ser escritos como produto entre primos. Ou seja

$$a = p_1 \cdot p_2 \cdots p_r \quad \text{e} \quad b = q_1 \cdot q_2 \cdots q_s$$

onde $p_1, ..., p_r, q_1, ..., q_s$ são primos. Então

$$n = p_1 \cdot p_2 \cdots p_r \cdot q_1 \cdot q_2 \cdots q_s,$$

ou seja, a afirmação vale para n. Logo, vale para todo n natural

Para provar a unicidade, usaremos novamente o Princípio da Indução sobre a quantidade r de fatores primos de n.

Suponhamos que $n = p_1$, onde p_1 é primo. Logo, n também é primo e só admite uma única representação na forma fatorada.

Agora, suponhamos que a afirmação seja verdadeira para todo número natural cuja fatoração é composta por até r fatores primos.

Seja $n \in \mathbb{N}$ um número que admite fatoração com $r + 1$ fatores primos.

$$n = p_1 \cdot p_2 \cdots p_{r+1} \tag{3.3}$$

onde $p_1 \leq p_2 \leq \cdots \leq p_{r+1}$.

Suponha que n admita uma segunda forma fatorada

$$n = q_1 \cdot q_2 \cdots q_s \tag{3.4}$$

Note que $s \geq r+1$. De fato, se $s \leq r$, então, pela hipótese de indução, $q_1 \cdot q_2 \cdots q_s$ é a única forma fatorada para n. Isso contraria a hipótese de n possuir $r+1$ fatores primos em sua fatoração.

Sendo assim, temos que p_1 divide $q_1 \cdot q_2 \cdots q_s$ e, considerando a Proposição 3.2.4, podemos admitir sem perda de generalidade que p_1 divide q_1. Daí, pela natureza dos números primos, $p_1 = q_1$. Assim, temos que

$$p_2 \cdot p_3 \cdots p_{r+1} = q_2 \cdot q_3 \cdots q_s,$$

onde $p_2 \cdot p_3 \cdots p_{r+1}$ possui r fatores. Pela hipótese de indução, esta decomposição é única, o que implica dizer que $r+1 = s$. Como $p_1 = q_1$, a expressão contida no segundo membro da igualdade 3.2 coincide com a expressão do segundo membro da igualdade 3.2, a menos da ordem de seus fatores. Isto valida a afirmação para o caso de $r+1$ fatores. Logo, pelo Princípio da Indução, a afirmação é válida para todo r natural.

□

O maior número primo descoberto até maio de 2.023 possui 24.862.048 dígitos, e pode ser expresso como $2^{82.589.933} - 1$. Esta descoberta foi feita através do computador de um colaborador do Great Internet Mersenne Prime Search (GIMPS), Patrick Laroche, morador de Ocala (Flórida, EUA), em dezembro de 2.018 [MO]. Um dos grandes desafios no estudo dos números primos se refere a encontrar novos números primos, e com uma quantidade cada vez maior de dígitos. Vejamos uma demosntração semelhante à realizada por Euclides de que há infinitos números primos.

Teorema 3.2.6. *Existem infinitos números primos.*

Demonstração. Suponha que exista uma quantidade k de números primos $p_1, p_2, ..., p_k$. Sem perda de generalidade, suponha p_k o maior destes. Agora, tome o número

$$a = p_1 \cdot p_2 \cdots p_k + 1.$$

Por hipótese, a é um número composto. Sendo assim, algum $p_i = p$ é fator de a, onde $1 \leq i \leq k$. Uma vez que

$$p \mid p_1 \cdot p_2 \cdots p_k,$$

pela Proposição 3.1.4,

$$p \mid a - p_1 \cdot p_2 \cdots p_k,$$

ou seja $p \mid 1$, o que é um absurdo. Logo, há infinitos números primos. □

3.3 Alguns tipos de números primos

Mesmo após séculos de estudos acerca dos números primos, poucas foram as descobertas acerca destes números. Apesar de não existir uma fórmula que expresse o n-ésimo número primo, a história da Matemática mostra que alguns estudiosos tiveram sucesso ao encontrar fórmulas que gerassem alguns primos. Todas as informações que apresentaremos nesta seção foram coletadas em maio de 2.023.

O primeiro matemático que destacamos, já foi citado neste trabalho. Fermat estudou uma sequência de números na forma $F_n = 2^{2^n} + 1$, onde n é um número inteiro não negativo. Tais números receberam o nome de *números de Fermat*.

Definição 3.3.1. *Um número F_n, onde $n \in \mathbb{N} \cup \{0\}$, é dito primo de Fermat, se houver um n inteiro não negativo tal que*

$$F_n = 2^{2^n} + 1$$

Em sua conjectura, Fermat acreditou que sua fórmula valia para qualquer valor natural de n. Para $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ e $F_4 = 65.537$, temos que tais números são de fato primos. Um resultado interessante se relaciona diretamente com a escolha de Fermat por esta fórmula. Para tanto, precisaremos do seguinte lema.

Lema 3.3.2. *Sejam $a, b \in \mathbb{Z}$, $a \neq b$ e $n \in \mathbb{N} \cup \{0\}$. Então $a - b \mid a^n - b^n$.*

Em particular, para $b = -c$, onde $c \in \mathbb{N}$, se n for par, então $a + c \mid a^n - c^n$. Se n for ímpar, então $a + c \mid a^n + c^n$.

Demonstração. Usemos o princípio da indução para esta prova.

Para $n = 1$, temos que $a - b$ divide $a^1 - b^1 = a - b$.

Agora, suponha que $a - b \mid a^n - b^n$, para algun n natural. Temos que

$$\begin{aligned} a^{n+1} - b^{n+1} &= aa^n - ba^n + ba^n - bb^n \\ &= (a-b)a^n + b(a^n - b^n) \end{aligned}$$

Como $a - b \mid a^n - b^n$, por hipótese, então conclui se que $a - b \mid a^{n+1} - b^{n+1}$ pela Proposição 3.1.4. Logo, $a - b \mid a^n - b^n$ para todo n natural.

Para o caso particular $b = -c$, onde $c \in \mathbb{N}$, se n for um número par, temos que $a^n - (-c)^n = a^n - c^n$. Logo, $a + c \mid a^n - c^n$. Se n for um número ímpar, temos que $a^n - (-c)^n = a^n + c^n$. Logo, $a + c \mid a^n + c^n$.

□

Proposição 3.3.3. *Sejam $a, n \in \mathbb{N}$, ambos diferentes da unidade. Se $a^n + 1$ é primo, então a é par e, para algum $m \in \mathbb{N}$,*

$$n = 2^m.$$

Demonstração. Suponha que $a^n + 1$ seja primo, com $a > 1$ e $n > 1$. Suponha também que a seja ímpar. Então, a^n é ímpar, e, consequentemente, $a^n + 1$ é par e maior que 2. Logo, $a^n + 1$ é composto, o que é um absurdo.

Agora, suponha que exista um primo $p \neq 2$ tal que $p \mid n$. Então, existe um k natural tal que $n = kp$. Como

$$a^n + 1 = (a^k)^p + 1,$$

então, pelo Lema 3.3.2,

$$a^k + 1 \mid a^n + 1,$$

o que é uma contradição. Logo, n é da forma 2^m. □

Observe que esta proposição não garante que a fórmula proposta por Fermat é válida para todo valor de n. Na realidade, os fatores primos de um número de Fermat seguem um padrão, o qual demonstraremos neste trabalho. Para tanto, apresentamos o Pequeno Teorema de Fermat e um lema, usando as seguintes notações:

- sendo $a, b, p \in \mathbb{Z}$ e $p > 1$, se $p \mid a - b$, então $a \equiv b \pmod{p}$,
- $\text{ord}_p(a)$ é o menor número inteiro positivo x tal que $a^x \equiv 1 \pmod{p}$, onde $a \in \mathbb{N}$ e p não é fator de a .

Teorema 3.3.4 (Pequeno Teorema de Fermat)**.** *Se p é um número primo e $a \in \mathbb{Z}$, onde* $\text{mdc}(a,p) = 1$*, então*

$$a^{p-1} \equiv 1 \pmod{p}$$

Demonstração. Uma demonstração deste teorema é encontrada em [5]. □

O lema a seguir é um corolário do Teorema de Lagrange. Para mais detalhes acerca do Teorema de Lagrange, recomendamos a leitura de [4].

Lema 3.3.5. *Sejam $a, m \in \mathbb{Z}$, onde* $\text{mdc}(a,m) = 1$*. Então, $a^n \equiv 1 \pmod{m}$ se, e somente se,* $\text{ord}_m(a) \mid n$*.*

Demonstração. Uma demonstração deste lema é encontrada em [5]. □

Proposição 3.3.6. *Seja F_n um número de Fermat. Seja também o número primo p tal que $p \mid F_n$. Então, existe um $c \in \mathbb{N}$ tal que*

$$p = c \cdot 2^{n+2} + 1.$$

Demonstração. Para $n \geq 2$, tome $\alpha_n = (2^{2^{n-2}} - 1) \cdot 2^{3 \cdot 2^{n-2}} + 2^{2^{n-2}} + 1$. Então:

$$\begin{aligned}
\alpha_n^2 &\equiv \left((2^{2^{n-2}} - 1) \cdot 2^{3 \cdot 2^{n-2}} + 2^{2^{n-2}} + 1\right)^2 && \pmod{2^{2^n} + 1} \\
&\equiv \left(2^{4 \cdot 2^{n-2}} - 2^{3 \cdot 2^{n-2}} + 2^{2^{n-2}} + 1\right)^2 && \pmod{2^{2^n} + 1} \\
&\equiv \left(\cancel{2^{2^n}} - 2^{3 \cdot 2^{n-2}} + 2^{2^{n-2}} + \cancel{1}\right)^2 && \pmod{2^{2^n} + 1} \\
&\equiv \left(-2^{3 \cdot 2^{n-2}} + 2^{2^{n-2}}\right)^2 && \pmod{2^{2^n} + 1} \\
&\equiv 2^{3 \cdot 2^{n-1}} - 2 \cdot 2^{4 \cdot 2^{n-2}} + 2^{2^{n-1}} && \pmod{2^{2^n} + 1} \\
&\equiv 2^{2^{n-1}} \cdot \left(2^{2 \cdot 2^{n-1}} + 1\right) - 2 \cdot 2^{4 \cdot 2^{n-2}} && \pmod{2^{2^n} + 1} \\
&\equiv 2^{2^{n-1}} \cdot \left(\underbrace{2^{2^n} + 1}_{0}\right) - 2 \cdot \underbrace{2^{2^n}}_{-1} && \pmod{2^{2^n} + 1} \\
&\equiv 2 && \pmod{2^{2^n} + 1}
\end{aligned}$$

Ou seja, $\alpha_n^2 \equiv 2 \pmod{F_n}$. Visto que $2^{2^n} \equiv -1 \pmod{F_n}$, então

$$\begin{aligned}
\left(\alpha_n^2\right)^{2^n} &\equiv -1 && \pmod{F_n} \\
\alpha_n^{2^{n+1}} &\equiv -1 && \pmod{F_n}
\end{aligned}$$

Se $p \mid F_n$, então

$$\begin{aligned}
\alpha_n^{2^{n+1}} &\equiv -1 && \pmod{p} \\
\left(\alpha_n^{2^{n+1}}\right)^2 &\equiv (-1)^2 && \pmod{p} \\
\alpha_n^{2^{n+2}} &\equiv 1 && \pmod{p}.
\end{aligned}$$

Daí, como $\alpha_n^{2^{n+1}} \equiv -1 \pmod{p}$, temos que $\text{ord}_p(\alpha_n) = 2^{n+2}$. Então, pelo Teorema 3.3.4 e pelo Lema 3.3.5,

$$2^{n+2} \mid p - 1.$$

Ou seja, existe um $c \in \mathbb{N}$ tal que

$$p = c \cdot 2^{n+2} + 1.$$

Note que os cálculos desenvolvidos acima foram feitos para apenas $n \geq 2$, o que é suficiente, visto que só precisamos encontrar um fator primo de F_n para $n \geq 5$. □

Exemplo 3.3.7. *Os fatores primos de F_5 são:*

- $641 = 20 \cdot 2^7 + 1$ *e*
- $6.700.417 = 209.388 \cdot 2^7 + 1$.

Em três séculos de análises, já foram encontrados mais de 200 divisores de alguns números de Fermat. Ainda assim, há muita dificuldade em realizar tais cálculos, uma vez que, a medida que n aumenta, o número de dígitos de F_n cresce exponencialmente. Até o momento, apenas os números de Fermat para valores de n pertencentes ao intervalo $[5, 11]$ foram completamente fatorados. Até esta mesma data, foi provado que F_{20} e F_{24} são compostos, mas seus fatores ainda permaneciam desconhecidos. Em 9 de fevereiro de 2.023, foi descoberto o fator $623.619.365.837 \cdot 2^{1.495} + 1$, pertencente a F_{1493}, realizada por Gary Gostin. Até esta mesma data, ainda não haviam encontrado números de Fermat primos para $n > 4$ [FS].

Inspirado pela determinação de Fermat, outro matemático do século XVII aceitou o desafio desta grande busca por fórmulas. O padre e matemático Marin Mersenne estudou amplamente uma sequência de números que recebeu seu nome. A sequência $(2^n - 1)_{n \in \mathbb{N}}$ havia sido analisada anteriormente por Euclides, em torno do século III *a.C.*, e tinha conexão com os números perfeitos. Mersenne descobriu uma particularidade para quando n fosse primo, e se dedicou a esse caso.

Definição 3.3.8. *Um número primo é dito de Mersenne se ele for da forma*

$$M_p = 2^p - 1,$$

onde p é um número primo.

De maneira análoga aos primos de Fermat, a condição de que p seja primo em M_p também pode ser justificada, como veremos na proposição a seguir.

Proposição 3.3.9. *Se $a^n - 1$ é primo, onde $a, n \in \mathbb{N}$ e $a, n \neq 1$, então $a = 2$ e n é primo.*

Demonstração. Suponha que para a e n naturais e diferentes da unidade. Se $a > 2$, temos que $a - 1 > 1$. Então, pelo Lema 3.3.2, $a - 1 \mid a^n - 1$ e $a^n - 1$ é composto. Logo, $a = 2$.

Por outro lado, suponha que n não seja primo. Então, existem $r, s \in \mathbb{N}$ tais que $n = rs$, onde r e s são diferentes da unidade. Observe que, como

$$a^n - 1 = (a^r)^s - 1,$$

então, do Lema 3.3.2,

$$a^r - 1 \mid a^n - 1,$$

o que é uma contradição por hipótese. Logo, n é primo. □

Algo importante a se destacar é que nem todo número de Mersenne é primo. Um exemplo ocorre para o caso $n = 11$. Temos que $M_{11} = 2047 = 23 \cdot 89$, não correspondendo a um número primo. Mersenne afirmou que sua fórmula calculava números primos para os valores de n correspondentes a $2, 3, 5, 7, 13, 17, 19, 31, 67, 127$ e 257. O maior número de Mersenne descoberto, até o momento, é

$$M_{2^{51}-1} = 2^{82.589.933} - 1$$

e coincide com o maior número primo conhecido. Foram necessárias duas semanas para confirmar que este número era realmente primo, e a recompensa para a descoberta correspondeu ao valor de 3.000 dólares [MO].

Assim como os números de Fermat, há como verificar uma padrão para os divisores de dado M_n.

Proposição 3.3.10. *Seja o número de Mersenne M_p composto. Se $q \mid M_p$, onde q é primo, então, q é da forma*

$$2ap + 1.$$

Demonstração. Se $q \mid 2^p - 1$, então

$$2^p \equiv 1 \pmod{q}.$$

Por outro lado, observe que

$$2^{\mathrm{ord}_q(2)} \equiv 1 \pmod{q}.$$

Então, pelo Lema 3.3.5, $\mathrm{ord}_q(2) \mid p$. Uma vez que p é primo, $\mathrm{ord}_q(2) = p$. Daí, novamente pelo pelo Lema 3.3.5 e pelo Teorema 3.3.4, temos que $p \mid q - 1$. Ou seja, existe c inteiro tal que

$$q - 1 = cp.$$

Observe ainda que $q - 1$ é um número par. Então, para algum a inteiro,

$$q = 2ap + 1.$$

□

Alguns testes de primalidade são mais eficazes para primos de Mersenne, em comparação a outros tipos de números primos. Como resultado deste fato, a lista com os 8 maiores primos conhecidos até o momento é composta apenas de primos de Mersenne [GIMPS]. Um grande destaque se dá para o teste de Lucas–Lehmer, baseado no teorema a seguir.

Teorema 3.3.11. *Se p é ímpar, o número de Mersenne $2^p - 1$ é primo se, e somente se, $2^{p-1} \mid S_{p-1}$, onde S_n é uma sequência tal que $S_{n+1} = S_n^2 - 2$ e $S_1 = 4$.*

Demonstração. A demonstração deste teorema se encontra em [7]. □

O próximo tipo de número primo que destacamos foi descoberto pela francesa Sophie Germain no século XVII.

Definição 3.3.12. *Um primo p é dito de Sophie Germain, se $2p + 1$ também é primo.*

Usando um pseudômino em seus trabalhos e comunicações, Sophie estudou e se comunicou com vários matemáticos, inclusive com Gauss e Legendre, se passando por homem. Além de descobrir uma fórmula que gerasse alguns números primos, ela também mostrou que se p e $2p+1$ são números primos, onde $p \neq 2$, então a equação

$$x^p + y^p = z^p$$

não possui solução para x, y e z naturais. Tal demonstração contempla parte do Último Teorema de Fermat, que possui a mesma afirmativa de ausência de solução para $n > 2$ na equação

$$x^n + y^n = z^n$$

com x, y e z naturais.

Ainda não foi provado se existem infinitos primos de Sophie Germain, sendo que já foi descoberta uma quantidade próxima a 200 destes até esta data. Os primeiros primos deste tipo ocorrem para os seguintes valores de p: 2, 3, 5, 11, 23 e 29, sendo que o maior primo de Sophie Germain foi descoberto em março de 2.016, e corresponde a $2.618.163.402.417 \cdot 2^{1.290.000} - 1$. Tal número primo possui 388.342 dígitos [PP].

O último destaque que damos se refere a números primos cuja quantidade de dígitos também aumenta absurdamente à medida que n cresce. Para tanto, consideraremos o fatorial de um real x, denotado por $x!$. Este número será correspondente ao produto de todos os números naturais menores ou iguais a x.

Definição 3.3.13. *Um número primo p é chamado primo fatorial, se puder ser escrito na forma*

$$p = n! \pm 1,$$

onde, $n \in \mathbb{N}$.

O maior primo fatorial até o momento foi descoberto em fevereiro de 2.022, e corresponde a $422.429! + 1$. Este número primo possui 2.193.027 dígitos [PP]. Os cinco primeiros números primos fatoriais ocorrem para

- $n = 1$, onde $p = 2$,
- $n = 2$, onde $p = 3$,
- $n = 3$, onde $p = 5$,
- novamente $n = 3$, onde $p = 7$,
- $n = 4$, onde $p = 23$.

3.4 Lacunas entre primos

O uso de números primos na atualidade ocorre em diversas áreas, como em ramos da Física e da Engenharia. Um exemplo específico é o uso de números primos como base para criptografia de dados de vários algorítmos de segurança. Sabemos que existem infinitos números primos e que não há como prever o surgimento de um número primo à medida que observamos a evolução da sequência dos números naturais em direção ao infinito. Mas, mesmo diante de tantas questões acerca dos números primos, há como prever alguns intervalos onde há uma série de números compostos consecutivos. Estes intervalos são chamados lacunas ou, usando a expressão correspondente em inglês, os *gaps*.

Definição 3.4.1. *Sejam p_{n+1} e p_n os $(n+1)$-ésimo e o n-ésimo primos consecutivos, respectivamente. Então, $p_{n+1} - p_n$ será a n-ésima lacuna entre primos, denotado por d_n.*

Observe que o único número primo par é o número 2. Assim, todos os demais números primos serão ímpares. Este fato irá influenciar diretamente a sequência (d_n).

Proposição 3.4.2. *O único par de primos consecutivos cujo intervalo é de apenas 1 unidade é $(2, 3)$.*

Demonstração. Todo número natural maior que a unidade é da forma $2k$ ou $2k+1$, onde $k \in \mathbb{Z}$. Note que, se $2k$ é primo, então seus únicos divisores são 1 e 2. Logo, $k = 1$ obrigatoriamente, $2k = 2 \cdot 1 = 2$ e $2k + 1 = 2 \cdot 1 + 1 = 3$. □

Como consequência desta proposição, vemos que $d_1 = 1$. Observando os cinco primeiros números primos, 2, 3, 5, 7 e 11, percebemos que

$$\begin{aligned} d_2 &= 2 \\ d_3 &= 2 \\ d_4 &= 4 \end{aligned}$$

Ou seja, a partir do 2º intervalo entre primos consecutivos, ainda podemos perceber outra importante relação entre os termos de (d_n), demonstrada na proposição a seguir.

Proposição 3.4.3. *Sejam dois números primos consecutivos p e q, $p, q > 2$. Então, a distância entre p e q é um número par.*

Demonstração. Sem perda de generalidade, suponha $p > q$. Vamos denotar $p = 2k_1 + 1$ e $q = 2k_2 + 1$, com k_1 e k_2 naturais e distintos. Temos que

$$\begin{aligned} p - q &= 2k_1 + 1 - (2k_2 + 1) \\ &= 2k_1 - 2k_2 \\ &= 2(k_1 - k_2) \end{aligned}$$

□

Note que o significado desta proposição é de extrema importância. A única distância entre primos consecutivos de valor ímpar é de 1 unidade, e ocorre entre os números primos 2 e 3. Como todo número primo maior que 2 é ímpar, qualquer distância entre primos consecutivos a partir deste ponto sempre será um número par.

Vejamos algumas classificações para números primos baseadas nas informações sobre as lacunas entre primos.

Definição 3.4.4. *Dois números primos consecutivos p_1 e p_2 são ditos gêmeos se $p_2 = p_1 + 2$.*

Os primeiros pares de primos gêmeos são $(3, 5)$, $(5, 7)$, $(11, 13)$, e o maior par de primos gêmeos descobertos até maio de 2.023 é

$$(2.996.863.034.895 \cdot \ 2^{1.290.000} - 1, 2.996.863.034.895 \cdot \ 2^{1.290.000} + 1),$$

contendo 388.342 dígitos. A descoberta foi feita em setembro de 2.016 [PP].

A título de curiosidade, existe um padrão a partir do segundo par de primos gêmeos que se refere ao resto da divisão de cada um deles por 6.

Proposição 3.4.5. *À exceção do par* $(3, 5)$*, todo par de primos gêmeos é da forma*

$$(6k - 1, 6k + 1)$$

onde $k \in \mathbb{N}$.

Demonstração. Como o único número primo par é 2, então os demais primos maiores que 3 só podem ser da forma $6k - 1$, $6k + 1$ ou $6k + 3$, onde k é natural. Observe então que

$$6k + 3 = 3 \cdot (2k + 1),$$

logo, como k é natural, todo número desta forma será composto.

Sabendo que

$$6k + 1 - (6k - 1) = 2,$$

então o único tipo de par de primos gêmeos ímpares é da forma

$$(6k - 1, 6k + 1).$$

□

Definição 3.4.6. *Três números primos consecutivos* p_1*,* p_2 *e* p_3 *são ditos trigêmeos se*

$$p_3 = p_2 + 2 = p_1 + 4.$$

Diferentemente dos primos gêmeos, há uma prova sobre a quantidade de primos trigêmeos.

Proposição 3.4.7. *A única terna de primos gêmeos consecutivos é* $(3, 5, 7)$.

Demonstração. Sejam a, b e c primos trigêmeos. Note que em uma Progressão Aritmética de razão 2, tomando 3 termos consecutivos, um destes será garantidamente múltiplo de 3.

De fato. Pela Proposição 3.4.5, se $a = 6k-1$, onde $k \in \mathbb{N}$, então $c = a+4 = 6k+3$ e c não é primo. Ainda pela Proposição 3.4.5, se $b = 6k - 1$, então $a = b - 2 = 6k - 3$ e $a = 3$. Analogamente, se $c = 6k - 1$, $b = 3$ e $a = 1$, ou seja, a não é primo. Logo concluímos que $a = 3$, $b = 5$ e $c = 7$.

□

Em 1.949, P.A. Clement anunciou e provou o seguinte teorema: *"dois primos consecutivos são gêmeos se, e somente se,* $p \cdot (p + 2)$ *for um divisor de* $4 \cdot (p - 1)! + (p + 4)$*."* [2]. Euclides já havia afirmado sobre a existência de infinitos pares de primos gêmeos, mas até o momento não se conseguiu provar a validade desta conjectura. Godfrey Hardy (1.877 – 1.947) e John Littlewood (1.885 – 1.977) fizeram uma fórmula para calcular tais pares de primos. Tal fórmula obteve sucesso para todos os pares de gêmeos testados até o momento, mas também não há prova desta conjectura. Em 1.915, Viggo Brun provou um teorema sobre a soma dos inversos dos primos gêmeos, mostrando que tal soma é convergente.

Na contramão destes fatos, há uma descoberta recente acerca da questão das lacunas entre primos. O responsável por tal descoberta foi o matemático chinês Yitang Zhang, anunciada em Abril de 2.013. Zhang, ex-funcionário de uma franquia internacional muito conhecida de lanchonetes, provou que existem infinitos pares de primos cuja distância é N, para algum $N \in \mathbb{N}$ menor que 70.000.000. Para os primos gêmeos, faz-se necessário

provar o caso específico do teorema de Zhang para $N = 2$. Vários matemáticos têm trabalhado desde então para diminuir a cota de Zhang. Através do projeto Polymath8, um grupo de colaboradores matemáticos alcançou uma cota em 2.014 de apenas 246 para N [NPG].

Além destas classificações para pares de primos baseadas na distância entre eles, temos ainda notações para primos cujas lacunas são de 4 unidades. O termo designado em inglês é *cousin primes*. Para primos cuja lacuna seja de 6 unidades, a nomenclatura designada é *sexy primes*.

Mesmo que não haja uma regra para determinar a posição exata de todos os números primos dentro da sequência dos números naturais, podemos fazer manipulações algébricas a fim de encontrar, ao menos, pedaços de lacunas de números primos.

Definição 3.4.8. *O primorial de um número real x é dado pelo produtório de todos os números primos menores ou iguais a x, e é denotado por $x\#$.*

$$n\# = \prod_{p \leq x} p,$$

onde p é um número primo.

Exemplo 3.4.9. *Vejamos que*

a) $10\# = 2 \cdot 3 \cdot 5 \cdot 7 = 210$.

b) $7\# = 2 \cdot 3 \cdot 5 \cdot 7 = 210$.

c) $12\# = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 = 2.310$.

Note que o primorial de um número n composto será igual ao primorial do maior número primo menor que n. Além disso, $x\# < x!$ para $x > 3$.

Proposição 3.4.10. *Dado qualquer número n natural, existem lacunas com, pelo menos, n números naturais compostos consecutivos.*

Demonstração. Pelo Teorema Fundamental da Aritmética, todo número natural i maior que a unidade, ou é primo, ou pode ser escrito como o produto de, no mínimo, dois números primos. Temos que qualquer fator primo do número natural i, onde $1 < i \leq n+1$, também é fator de $(n+1)\#$. Logo, cada elemento da lista

$$\begin{gathered} (n+1)\# + 2 \\ (n+1)\# + 3 \\ \vdots \\ (n+1)\# + (n+1) \end{gathered}$$

é um número composto. □

Um ponto importante a destacar na Proposição 3.4.10 é a ausência de garantia que o termo $(n+1)\# + 1$ represente, de fato, um número primo. Do mesmo modo, se $n+2$ não é um número primo, então $(n+1)\# + (n+2)$ é composto. Assim, há possibilidade do intervalo $[(n+1)\# + 2, (n+1)\# + (n+1)]$ representar apenas um trecho de uma lacuna entre primos.

Vejamos um exemplo prático da Proposição 3.4.10.

Exemplo 3.4.11. *Como escrever uma lista com* 100 *números naturais consecutivos, todos compostos?*

Como 101 é um número primo, então podemos tomar a seguinte lista

$$\begin{gathered} 101\# + 2 \\ 101\# + 3 \\ \vdots \\ 101\# + 101 \end{gathered}$$

Note que esta lista é apenas uma possibilidade. Um exemplo a ser considerado, consiste na primeira lacuna de primos de 14 unidades, que ocorre entre os primos consecutivos 113 e 127. Pela Proposição 3.4.10, obteríamos nosso intervalo começando pelo número $15\# + 2 = 30.032$. Podemos obter lacunas usando fatorial ao invés de primorial, mas o primeiro elemento do intervalo fica bem maior que o primeiro elemento obtido usando primorial, por exemplo

$$\begin{gathered} 101! + 2 \\ 101! + 3 \\ \vdots \\ 101! + 101 \end{gathered}$$

cujos elementos possuem 160 dígitos cada, escritos na base 10.

A proposição a seguir reflete como as lacunas se tornam cada vez maiores e mais frequentes à medida que obtemos novos números primos. Para tanto, usaremos o Teorema Chinês dos Restos [5].

Proposição 3.4.12. *Para todo $n \in \mathbb{N}$, existe uma lista com n números consecutivos compostos que possuem algum fator com potência maior do que um.*

Demonstração. Tome um x natural tal que

$$\begin{cases} x & \equiv 0 & (\text{mod } 2^2) \\ x+1 & \equiv 0 & (\text{mod } 3^2) \\ & \vdots & \\ x+(n-1) & \equiv 0 & (\text{mod } p_n^2), \end{cases}$$

onde p_n é o n-ésimo número primo.

O Teorema Chinês dos Restos garante que o sistema admita solução módulo $2^2 \cdot 3^2 \cdot 5^2 \cdots p_n^2$, uma vez que cada p_i é coprimo com cada p_j, para $i, j \in \mathbb{N}$ e $i \neq j$. Ou seja, existe uma solução módulo $(p_n\#)^2$ para o sistema. □

Perceba que estes intervalos gerados possuem números relativamente altos, em comparação com a evolução da quantidade n de elementos da lista. Ilustrando este fato, temos que a solução, para $n = 2$, seria uma lista com números da forma

$$\begin{gathered} 36k + 8 \\ 36k + 9 \end{gathered}$$

onde k é um número inteiro não negativo. Já para $n = 3$, a solução seria uma lista com números da forma

$$\begin{gathered} 900k + 548 \\ 900k + 549 \\ 900k + 550 \end{gathered}$$

Outra possibilidade de solução se dá escolhendo primos aleatoriamente para o módulo das congruências. Observe que para o caso $n = 2$, tomando as congruências a partir dos primos 43 e 71, por exemplo, teremos como solução uma lista com números da forma

$$3.053k + 1.419$$
$$3.053k + 1.420$$

3.5 As lacunas e o Teorema dos Números Primos

Ao pensar em sua conjectura, Gauss comparou a probabilidade de obter um número primo, ao sortear um número natural qualquer, com os resultados obtidos no lançamento de uma moeda viciada. Em sua hipótese, a probabilidade de obtermos um número primo dentro de um conjunto com os n primeiros números naturais seria $1/\log(n)$.

Nessa seção, veremos uma importante aplicação do Teorema dos Números Primos em relação às lacunas de primos. Esta aplicação reflete a ideia de logaritmo proposta por Gauss. Para tanto, precisamos definir uma função que expresse a quantidade de números primos em função de dado número x real não negativo.

Definição 3.5.1. *Seja x um número real, $x \geq 0$, então $\pi(x)$ representa a quantidade de números primos existentes no intervalo $[0, x]$. Assim, podemos escrever*

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

onde p é um número primo.

Exemplo 3.5.2. *Temos que*

a) $\pi(1) = 0$.

b) $\pi(7) = \pi(10) = 4$.

c) $\pi(100) = 25$.

d) $\pi(1000) = 168$.

A função $\pi(x)$ é de extrema importância para o estudo da distribuição dos números primos. Pela definição, notamos que $\pi(x)$ é não-decrescente. A análise desta função está associada à demonstração do Teorema dos Números Primos, cuja prova veremos na Seção 5.4.

Teorema 3.5.3 (Teorema dos Números Primos)**.**

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

Por este teorema, a quantidade de números primos menores ou iguais a x corresponde a, aproximadamente, $x/\log(x)$. Por outro lado, há uma importante consequência para o Teorema dos Números Primos em relação ao espaçamento médio entre números primos na reta real. Na tabela 3.1, temos um comparativo entre o crescimento das funções $\log(x)$, $\pi(x)$ e da distância média entre primos para valores até 10^{15}.

x	$\pi(x)$	$x/\pi(x)$	$\log(x)$
10	4	2,500	2,302
10^2	25	4,000	4,605
10^3	168	5,592	6,907
10^4	1.229	8,137	9,2103
10^5	9.592	10,425	11,512
10^6	78.498	12,740	13,815
10^7	664.579	15,047	16,118
10^8	5.761.455	17,357	18,420
10^9	50.847.534	19,666	20,723
10^{10}	455.052.511	21,975	23,025
10^{11}	4.118.054.813	24,283	25,328
10^{12}	37.607.912.018	26,590	27,631
10^{13}	346.065.536.839	28,896	29,933
10^{14}	3.204.941.750.802	31,202	32,236
10^{15}	29.844.570.422.669	33,507	34,538

Tabela 3.1: Distância média entre primos até 10^{15}

Observe que o espaçamento médio entre números primos no intervalo $[0, x]$ é $\dfrac{x}{\pi(x)}$. Uma vez que pelo Teorema dos Números Primos

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

esse espaçamento médio se aproxima cada vez mais de $\log x$ à medida que x cresce.

Capítulo 4

Um pouco sobre análise complexa

Apesar do conjunto dos números reais ser um corpo completo, Riemann associou diretamente a ideia do conjunto dos números primos a um corpo que engloba o conjunto dos números reais: o conjunto dos números complexos. Riemann analisou e fez conjecturas envolvendo a função

$$\zeta(x) = \frac{1}{1^x} + \frac{1}{2^x} + \frac{1}{3^x} + \cdots + \frac{1}{n^x} + \cdots$$

quando x for um número complexo com parte real maior do que 1. Este pensamento revolucionou o estudo da Teoria dos Números e trouxe grandes desafios para os matemáticos desde a exposição de sua conjectura.

Neste capítulo, trataremos sobre ferramentas da Análise Complexa necessárias para a demonstração do Teorema dos Números Primos. Falaremos um pouco sobre o corpo $\mathbb{C}$, apresentaremos algumas funções, sequências e séries de variáveis complexas, além de noções a respeito das funções analíticas.

4.1 O corpo dos números complexos

A notação i para a unidade imaginária foi adotada pela primeira vez apenas no século XVII, por Leonard Euler. Mas, o problema para a solução da equação $x^2 + 1 = 0$ data um período bem anterior, na época do século XVI, com Niccolò Fontana, conhecido como Tartaglia. Ainda assim, a expressão *número complexo* só foi usada pela primeira vez apenas em 1.832, por Gauss. Esta seção trará um breve apanhado acerca do corpo $\mathbb{C}$.

O conjunto dos números complexos é o conjunto

$$\mathbb{C} = \{x + yi \,;\, x, y \in \mathbb{R}\},$$

onde i é a unidade imaginária que satisfaz a igualdade $i^2 = -1$. Para o número complexo $z = x + yi$, dizemos que x é a parte real de z e y a parte imaginária.

Definição 4.1.1. *Sendo $z_1 = x_1 + y_1 i$ e $z_2 = x_2 + y i_2$ números complexos, as operações soma e produto estão definidas por*

i) $z_1 + z_2 = (x_1 + y_1 i) + (x_2 + y_2 i) = (x_1 + y_1) + (x_2 + y_2)i.$

ii) $z_1 z_2 = (x_1 + y_1 i)(x_2 + y_2 i) = (x_1 x_2 - y_1 y_2) + (x_1 y_2 + y_1 x_2)i.$

Estas operações gozam das seguintes propriedades:

I) comutatividade em relação à soma: $z_1 + z_2 = z_2 + z_1$.

II) comutatividade em relação ao produto: $z_1 z_2 = z_2 z_1$.
III) 0 é o elemento neutro aditivo: $z + 0 = z$, $\forall z \in \mathbb{C}$.
IV) 1 é a identidade multiplicativa: $z \cdot 1 = z$, $\forall z \in \mathbb{C}$.
V) $-z = -x - yi$ é o simétrico aditivo do número $z = x + yi$, $\forall z \in \mathbb{C}$. Ou seja,

$$(x + yi) + (-x - yi) = 0.$$

VI) o inverso multiplicativo do número $z = x + iy \neq 0$ é o número

$$z^{-1} = \frac{x}{x^2 + y^2} - \frac{y}{x^2 + y^2} i$$

$\forall z \in \mathbb{C}$. Ou seja,

$$(x + iy) \cdot \left(\frac{x}{x^2 + y^2} - \frac{y}{x^2 + y^2} i \right) = 1.$$

VII) distributividade do produto em relação à soma: $z_1(z_2 + z_3) = z_1 z_2 + z_1 z_3$.

As propriedades relativas à soma e ao produto decorrem da própria definição, e do fato de serem válidas para a soma e o produto de números reais.

O número complexo $z = x + yi$ também pode ser denotado pelo par ordenado (x, y) representado no plano $\mathbb{R}^2$. Tal plano é chamado *plano complexo*. Sendo assim, o número complexo $(x, 0)$ representa o número real x. Deste modo, podemos identificar que o conjunto dos números reais é um subconjunto dos complexos. O número complexo $(0, 1)$ representa, por sua vez, a unidade imaginária i.

Uma vez que todo número complexo está associado a uma representação através de coordenadas no plano complexo, outra forma de representar um número $z = (x, y)$ se dá através de coordenadas polares, conhecida como *forma trigonométrica*.

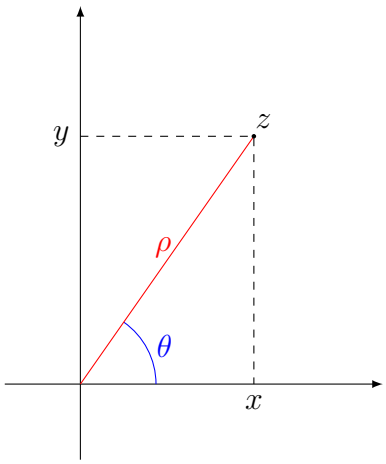

Figura 4.1: *Representação geométrica do número complexo z no plano*

Na figura 4.1, temos uma ilustração da representação do número complexo $z = (x, y)$ no plano complexo. As coordenadas polares (ρ, θ) são tais que

$$z = \rho \cdot (\cos(\theta) + i \operatorname{sen}(\theta)),$$

onde $\rho = \sqrt{x^2 + y^2}$, $x = \rho \cos(\theta)$ e $y = \rho \operatorname{sen}(\theta)$. Considerando $0 \leq \theta < 2\pi$, então o ângulo de medida θ corresponde ao ângulo entre o vetor (x, y) e o semi eixo horizontal positivo do plano complexo. Por sua vez, ρ representa a medida da distância do ponto $z = (x, y)$ à origem $(0, 0)$.

Chamaremos o número real $|z| = \rho$ de *norma* ou *módulo* de $z = (x, y)$. O valor θ recebe o nome de *argumento* de z, cuja notação utilizada neste trabalho será $\theta = \arg(z)$.

Exemplo 4.1.2. *Vamos escrever o número complexo* $z = 1 + \sqrt{3}i$ *na forma trigonométrica.*

Temos que $x = 1$, $y = \sqrt{3}$ *e* $|z| = \sqrt{1^2 + \left(\sqrt{3}\right)^2} = 2$. *Logo,*

$$z = 2 \cdot \left(\frac{1}{2} + \frac{\sqrt{3}}{2}i\right).$$

Como $\cos\frac{\pi}{3} = \frac{1}{2}$ *e* $\operatorname{sen}\frac{\pi}{3} = \frac{\sqrt{3}}{2}$, *então*

$$z = 2 \cdot \left(\cos\left(\frac{\pi}{3}\right) + i\operatorname{sen}\left(\frac{\pi}{3}\right)\right).$$

São verificadas as seguintes propriedades a respeito do módulo de números complexos:

I) $|z| \geq 0$.
II) $|z| = 0 \Leftrightarrow z = 0$.
III) $|z| = |-z|$.
IV) $|\operatorname{Re} z| \leq |z|$ e $|\operatorname{Im} z| \leq |z|$.
V) $|z_1 z_2| = |z_1||z_2|$.
VI) $|z_1 + z_2| \leq |z_1| + |z_2|$. Esta desigualdade é chamada *desigualdade triangular.*

Recomendamos a leitura de [1] para a análise da demonstração de cada propriedade do módulo de números complexos.

Para a ideia de potenciação inteira de um complexo z, partiremos da definição do produto entre números complexos, juntamente com a análise do número z em sua forma trigonométrica.

Proposição 4.1.3. *Seja o número complexo* z, *tal que* $z = \rho(\cos(\theta) + i\operatorname{sen}(\theta))$, *então, para* $n \in \mathbb{N}$

$$z^n = \rho^n(\cos(n\theta) + i\operatorname{sen}(n\theta)).$$

Demonstração. Faremos a prova por indução sobre n.

Para o caso $n = 1$, o caso é trivial.

Para o caso $n = 2$, usaremos a definição de produto. Para tanto, considere $z_1 = \rho_1(\cos(\theta_1) + i\operatorname{sen}(\theta_1))$ e $z_2 = \rho_2(\cos(\theta_2) + i\operatorname{sen}(\theta_2))$. Daí, temos que

$$\begin{aligned} z_1 z_2 &= \rho_1(\cos(\theta_1) + i\operatorname{sen}(\theta_1)) \cdot \rho_2(\cos(\theta_2) + i\operatorname{sen}(\theta_2)) \\ &= \rho_1\rho_2[\cos(\theta_1)\cos(\theta_2) - \operatorname{sen}(\theta_1)\operatorname{sen}(\theta_2) + i(\cos(\theta_1)\operatorname{sen}(\theta_2) + \cos(\theta_2)\operatorname{sen}(\theta_1))] \\ &= \rho_1\rho_2[\cos(\theta_1 + \theta_2) + i\operatorname{sen}(\theta_1 + \theta_2)] \end{aligned}$$

Então, fazendo $z_1 = z_2 = z$, onde $z = \rho(\cos(\theta) + i\operatorname{sen}(\theta))$, temos que

$$z^2 = \rho^2(\cos(2\theta) + i\operatorname{sen}(2\theta))$$

Suponha que a afirmação seja válida para um dado n natural. Então, para o caso $n + 1$, temos

$$\begin{aligned} z^{n+1} = z^n \cdot z &= \rho^n(\cos(n\theta) + i\operatorname{sen}(n\theta)) \cdot \rho(\cos(\theta) + i\operatorname{sen}(\theta)) \\ &= \rho^n \cdot \rho[\cos(n\theta + \theta) + i\operatorname{sen}(n\theta + \theta)] \\ &= \rho^{n+1}[\cos((n+1)\theta) + i\operatorname{sen}((n+1)\theta)] \end{aligned}$$

Como a proposição é válida para $n + 1$, então, pelo Princípio da Indução, é válida todo n natural. □

A igualdade envolvida na Proposição 4.1.3 é conhecida como *fórmula de Moivre*. Esta fórmula é grande valia, uma vez que dá alternativa para calcular $(x+yi)^n$ sem o uso de binômios de Newton. Vejamos um exemplo.

Exemplo 4.1.4. *Considerando $z = 1 - i$, vamos calcular z^{10}.*

Escrevendo o número z na forma trigonométrica, temos que

$$z = \sqrt{2}\left(\cos\frac{7\pi}{4} + i\,\mathrm{sen}\,\frac{7\pi}{4}\right).$$

Então,

$$\begin{aligned} z^{10} &= (\sqrt{2})^{10}\left[\cos\left(10\cdot\frac{7\pi}{4}\right) + i\,\mathrm{sen}\left(10\cdot\frac{7\pi}{4}\right)\right] \\ &= 32\left(\cos\frac{35\pi}{2} + i\,\mathrm{sen}\,\frac{35\pi}{2}\right) \\ &= 32\left(\cos\frac{3\pi}{2} + i\,\mathrm{sen}\,\frac{3\pi}{2}\right) \\ &= 32(0 - i) \\ &= -32i \end{aligned}$$

A proposição a seguir mostra como calcular o inverso multiplicativo do número complexo z em função da representação na forma trigonométrica.

Proposição 4.1.5. *Seja o número complexo $z = \rho(\cos(\theta) + i\,\mathrm{sen}(\theta))$, onde $z \neq (0,0)$. O número complexo denotado por z^{-1} tal que $z \cdot z^{-1}$ é dado por*

$$z^{-1} = \rho^{-1}(\cos(\theta) - i\,\mathrm{sen}(\theta)).$$

Demonstração. Sejam $z = \rho_1(\cos(\theta_1) + i\,\mathrm{sen}(\theta_1))$ e $w = \rho_2(\cos(\theta_2) + i\,\mathrm{sen}(\theta_2))$. Temos que

$$z \cdot w = \rho_1\rho_2[(\cos(\theta_1 + \theta_2) + i\,\mathrm{sen}(\theta_1 + \theta_2)].$$

Daí, se $z \cdot w = 1$, então $\rho_1\rho_2 = 1$ e $\theta_1 + \theta = 0$. Logo, $w = z^{-1}$ e

$$\begin{aligned} z^{-1} &= \rho^{-1}(\cos(-\theta) + i\,\mathrm{sen}(-\theta)) \\ &= \rho^{-1}(\cos(\theta) - i\,\mathrm{sen}(\theta)). \end{aligned}$$

□

4.2 Funções Complexas

A ideia de funções complexas está intimamente ligada à noção de funções reais, uma vez que associamos um par ordenado $z = (x, y) \in \mathbb{R}^2$ a um par $w = (u(x, y), v(x, y)) \in \mathbb{R}^2$. Vejamos a definição de algumas funções complexas pertinentes ao nosso trabalho.

Definição 4.2.1. *Seja o número complexo $z = x + iy$, então definimos as seguintes funções*

$$\begin{cases} \mathrm{Re}(z) &= x \\ \mathrm{Im}(z) &= y. \end{cases}$$

Note que as duas funções retornam um número real a cada uma delas: $\mathrm{Re}(z)$ à parte real de z e $\mathrm{Im}(z)$ à parte imaginária.

Exemplo 4.2.2. *Para o número complexo $z = 5 - 4i$, temos que*

- $\mathrm{Re}(z) = 5$
- $\mathrm{Im}(z) = -4$.

Observe que, para qualquer número complexo z,

$$z = \mathrm{Re}(z) + \mathrm{Im}(z)i.$$

Vejamos uma função que será tomada como base para o estudo das funções polinomiais complexas.

Definição 4.2.3. *Dado um $n \in \mathbb{N}$ fixo, definimos $f : \mathbb{C} \to \mathbb{C}$ função de potência inteira*

$$f(z) = z^n$$

Podemos estender esta definição para $n \in \mathbb{Z}$. Assim, definimos $f : \mathbb{C} - \{0\} \to \mathbb{C}$, onde

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

se $n < 0$ e, para $n = 0$,

$$f(z) = z^0$$

Vamos analisar o número complexo $w = \alpha(\cos(\beta) + i\,\mathrm{sen}(\beta))$, tal que $z^n = w$, onde $n > 0$. Sendo $z = \rho(\cos(\theta) + i\,\mathrm{sen}(\theta))$, então busquemos ρ e θ tais que

$$[\rho(\cos(\theta) + i\,\mathrm{sen}(\theta))]^n = \alpha(\cos(\beta) + i\,\mathrm{sen}(\beta)).$$

Se $\alpha \neq 0$, então $\rho = \sqrt[n]{\alpha}$ e

$$\begin{cases} \cos(n\theta) &= \cos(\beta) \\ \mathrm{sen}(n\theta) &= \mathrm{sen}(\beta) \end{cases}$$

Assim, $\theta = \dfrac{\beta}{n} + \dfrac{2\pi}{n} \cdot (n - j)$, onde $1 \leq j \leq n$. Como o sistema possui n soluções, isto mostra que a função de potência inteira não é injetiva.

Exemplo 4.2.4. *Considere a função $f(z) = z^3$, os valores de z tais que $f(z) = i$ são*

- $z_1 = \dfrac{\sqrt{3}}{2} + \dfrac{i}{2}$,
- $z_2 = \dfrac{-\sqrt{3}}{2} + \dfrac{i}{2}$,
- $z_3 = -i$.

Definição 4.2.5. *Um função complexa é dita polinomial de grau n, para n um inteiro não negativo, se for da forma*

$$f(z) = a_n z^n + a_{n-1} z^{n-1} + ... + a_2 z^2 + a_1 z + a_0$$

onde $a_n, a_{n-1}, ..., a_2, a_1, a_0 \in \mathbb{C}$, com $a_n \neq 0$.

Assim como no corpo $\mathbb{R}$, se $n = 0$, então a função polinomial é dita *constante*, e para $n = 1$ a função é dita $afim$.

Vejamos uma das funções mais notáveis deste capítulo.

Definição 4.2.6. *A função exponencial complexa* $\exp: \mathbb{C} \to \mathbb{C}$ *é definida por*

$$e^z = \exp(x + iy) = e^x(\cos(y) + i\,\mathrm{sen}(y)),$$

onde $x, y \in \mathbb{R}$.

O uso da notação $\exp(i\theta) = e^{i\theta}$, onde $z = \rho(\cos\theta + i\,\mathrm{sen}\,\theta)$, deve-se às observações realizadas por Euler ao estudar os números complexos.

Algo importante a se destacar, consiste no caso de tomarmos $z = x + 0i$. Com esta restrição, a exponencial complexa coincide com a exponencial real.

Algumas propriedades relacionadas à potenciação de números reais coincidem com as propriedades relacionadas à exponencial complexa. Em particular, uma vez que $z, w \in \mathbb{C}$, então

$$e^{z+w} = e^z \cdot e^w \qquad \text{e} \qquad (e^z)^w = e^{z \cdot w}.$$

Exemplo 4.2.7. *Vamos calcular* $\exp(1 + \pi i)$.

Pela definição da exponencial complexa, temos

$$e^{1+\pi i} = e(\cos(\pi) + i\,\mathrm{sen}(\pi)) = e(-1 + i \cdot 0) = -e.$$

Em particular, $e^{\pi i} = -1$.

A proposição a seguir trata sobre uma importante propriedade a respeito do módulo de uma exponencial complexa, mostrando a influência da parte real e da parte imaginária do número complexo z sobre $|e^z|$.

Proposição 4.2.8. *Seja o número complexo* $z = x + iy$, *então* $|e^z| = e^x$.

Demonstração. Considerando a definição da exponencial complexa, temos que

$$\begin{aligned} |e^{x+iy}| &= |e^x\cos(y) + ie^x\,\mathrm{sen}(y))| \\ &= \sqrt{e^{2x}\,(\cos(y)^2 + \mathrm{sen}(y)^2)} \\ &= \sqrt{e^{2x}} \\ &= e^x. \end{aligned}$$

Em particular, se tomarmos $z = yi$, onde $y \in \mathbb{R}$, então $|e^z| = 1$. □

A função exponencial complexa possui uma particularidade em relação à exponencial real, e que também traz reflexos sobre a injetividade. Note que, sendo $z = x + yi$,

$$\begin{aligned} \exp(z + 2\pi i) &= e^x \cdot e^{(y+2\pi)i} \\ &= e^x(\cos(y + 2\pi) + i\,\mathrm{sen}(y + 2\pi)) \\ &= e^x(\cos(y) + i\,\mathrm{sen}(y)) \\ &= \exp(z). \end{aligned}$$

Assim, ao definir um logaritmo complexo, é preciso notar que a exponencial complexa é *periódica*. Então, para considerar uma função inversa da exponencial complexa, faz-se necessário tomar um *ramo de logaritmo complexo*.

Definição 4.2.9. *Seja* $B = \{\rho e^{i\theta} \ ; \ \rho > 0 \ e \ \theta \in (-\pi, \pi)\}$. *Defininimos o Ramo Principal do Logaritmo complexo*

$$\begin{array}{rccl} \log\colon & B & \to & \mathbb{C} \\ & \rho e^{i\theta} & \mapsto & \log(\rho) + i\theta. \end{array}$$

Exemplo 4.2.10. *Considerando o Ramo Principal do Logaritmo complexo,*

$$\log(1 + \sqrt{3}i) \ = \ \log 2 + i \cdot \frac{\pi}{3}$$

A partir deste ponto, todas as vezes que nos referírmos ao logaritmo complexo, considere o Ramo Principal do Logaritmo.

4.3 Alguns subconjuntos de $\mathbb{C}$

Uma vez que podemos decompor a função complexa $f(z) = u(x, y)+iv(x, y)$, então, diz-se que a essência do cálculo diferencial e integral de funções de variável real se estende às funções de variável complexa. Dado que no corpo $\mathbb{C}$ não trabalhamos exclusivamente com pontos sobre uma reta numérica, o detalhe sutil se encontra na análise de uma vizinhança em torno do número complexo z. Chamaremos esta vizinhança em torno de z de *disco*.

Definição 4.3.1. *Seja* $z \in \mathbb{C}$ *e* $r \in \mathbb{R}^*_+$. *Assim,* $\mathbb{D}(z, r)$ *será chamado disco aberto centrado em* z *de raio* r, *definido por*

$$\mathbb{D}(z, r) = \{w \in \mathbb{C} \ ; \ |w - z| < r\}.$$

Exemplo 4.3.2. *Se o número complexo* z *pertence ao disco* $\mathbb{D}(i, 1)$, *então a distância entre o número* z *e o número* i *no plano complexo é menor que* 1 *unidade.*

Com base no conceito de disco, vejamos alguns tipos importantes de subconjuntos de $\mathbb{C}$.

Definição 4.3.3. *Seja o conjunto* $A \subset \mathbb{C}$, *o número* $z \in A$ *e os números* $r, R \in \mathbb{R}^*_+$. *Então,*
a) se, para todo z, *existir um* r *tal que* $\mathbb{D}(z, r) \subset A$, *então o conjunto* A *é dito aberto.*
b) se o conjunto $\mathbb{C} - A$ *é aberto, então* A *é dito fechado.*
c) se existir R, *tal que* $A \subset \mathbb{D}(z, R)$, *então* A *é dito limitado.*
d) se A *não for um conjunto limitado, será dito ilimitado.*
e) se A *é fechado e limitado,* A *é dito compacto.*

Note que o próprio conjunto $\mathbb{C}$, bem como o conjunto

$$A = \{z \in \mathbb{C}; \mathrm{Re}(z) > 1\},$$

são abertos. O conjunto $B = \{z_0\}$, onde z_0 é um complexo qualquer, é um exemplo de conjunto fechado. Como veremos mais a frente, dizer que um conjunto A não é aberto, não implica em dizer que A é fechado. De igual modo, dizer que A não é fechado, também não implica em dizer que A é aberto.

Definição 4.3.4. *Sejam o conjunto* $A \subset \mathbb{C}$ *e o número* $z \in A$. *Se existe* r *real,* $r > 0$, *tal que* $\mathbb{D}(z, r) \subset A$, *então* z *é um ponto interior de* A. *O conjunto de todos os pontos interiores de* A *é chamado interior de* A, *denotado por* $\mathrm{int}(A)$.

Definição 4.3.5. *Sejam os números $z \in \mathbb{C}$ e $r \in \mathbb{R}_+^*$. Então $\mathbb{D}^*(z,r)$ será chamado disco furado centrado em z de raio r, ou seja,*

$$\mathbb{D}^*(z,r) = \{w \in \mathbb{C}\,;\, 0 < |w - z| < r\}.$$

Perceba que a diferença entre os discos $\mathbb{D}(z,r)$ e $\mathbb{D}^*(z,r)$ consiste em um único detalhe: o fato do centro do disco pertencer ou não a cada um destes conjuntos.

A seguir, veremos uma importante definição, que fundamenta a teoria a respeito de limites e de convergência de sequências.

Definição 4.3.6. *Sejam $A \subset \mathbb{C}$, $z \in \mathbb{C}$ e $r \in \mathbb{R}_+^*$. Se, para todo r,*

$$\mathbb{D}^*(z,r) \cap A \neq \varnothing,$$

então z é um ponto de acumulação de A.

Como consequência desta definição, temos que se $B \subset \mathbb{C}$, e B possui algum ponto de acumulação, então podemos tomar dois pontos $z, w \in B$ tão próximos quanto queiramos. Ou seja, para todo real $\varepsilon > 0$, existem $z, w \in B$ tais que $0 < |z - w| < \varepsilon$.

Definição 4.3.7. *Sejam $A, B \subset \mathbb{C}$, onde B é composto por todos os pontos de acumulação de A. Definimos o conjunto $\overline{A}$, denomidado fecho de A, por*

$$\overline{A} = A \cup B.$$

Definição 4.3.8. *Seja $A \subset \mathbb{C}$. Definimos bordo ou fronteira de A, o conjunto ∂A, onde*

$$\partial A = \overline{A} - \mathrm{int}(A).$$

Exemplo 4.3.9. *A fronteira do conjunto dado pelo semiplano complexo*

$$A = \{z \in \mathbb{C}; \mathrm{Re}(z) > 1\},$$

consiste na reta dada pelo conjunto

$$\partial A = \{z \in \mathbb{C}; \mathrm{Re}(z) = 1\}.$$

Observe que um ponto $P \in \mathbb{C}$ é dito *ponto de fronteira* se, para qualquer valor real $r > 0$, $\mathbb{D}(P,r) \cap A \neq \varnothing$, e $\mathbb{D}(P,r) \cap (\mathbb{C} - A) \neq \varnothing$.

Exemplo 4.3.10. *Considere o conjunto $A = \{z \in \mathbb{C}\,;\, 1 \leq |z| < 2\}$.*

Perceba que

$$\mathrm{int}(A) = \{z \in \mathbb{C}\,;\, 1 < |z| < 2\},$$

e

$$\overline{A} = \{z \in \mathbb{C}\,;\, 1 \leq |z| \leq 2\}.$$

Logo, o conjunto A não é aberto, nem fechado. Além disso,

$$\partial A = \{z \in \mathbb{C}\,;\, |z| = 1\} \cup \{z \in \mathbb{C}\,;\, |z| = 2\}.$$

Definição 4.3.11. *Seja $A \subset \mathbb{C}$. Se existem $X, Y \subset \mathbb{C}$ disjuntos e abertos tais que $A \subset X \cup Y$, $A \cap X \neq \varnothing$ e $A \cap Y \neq \varnothing$, então, A é dito desconexo. Caso contrário, A é dito conexo. Se A for aberto e conexo, então será dito região ou domínio.*

No caso em que $A = X \cup Y$, onde X e Y são abertos e disjuntos e X é conexo, X é dito uma componente conexa de A.

Dizemos que um conjunto A é simplesmente conexo, se A não tiver "buracos". Ou seja, para todo $P \in A$, qualquer caminho fechado contido em A passando por P pode ser contraído para P. Para uma definição formal e detalhes sobre estes conceitos, indicamos a leitura de [1].

Exemplo 4.3.12. *O conjunto dos números naturais $\mathbb{N} \subset \mathbb{C}$ é desconexo.*

De fato, basta considerar os conjuntos

$$X = \left\{ x \in \mathbb{C} \,;\, |x| > \frac{17}{2} \right\} \quad e \quad Y = \left\{ x \in \mathbb{C} \,;\, |x| < \frac{17}{2} \right\}.$$

Definição 4.3.13. *Seja $A \subset \mathbb{C}$ e dois pontos quaisquer z e w de A. Se o segmento de reta que liga z a w está contido em A, então A é dito convexo.*

4.4 Noções sobre sequências de números complexos

A ideia de sequências de números complexos também está intimamente ligada à ideia de sequências de números reais, com a ressalva de alguns detalhes importantes. Inicialmente, vejamos a definição formal de uma sequência de números complexos.

Definição 4.4.1. *Uma sequência de números complexos é uma função*

$$f : \mathbb{N} \to \mathbb{C},$$

onde o número complexo $f(n)$ é chamado n-ésimo termo da sequência, também denotado por z_n. Representamos essa sequência por (z_n).

Exemplo 4.4.2. *$(1 + 5in)$ é a sequência $(1 + 5i, 1 + 10i, 1 + 15i, ...)$.*

Assim como na sequência de números reais, a ideia da convergência de uma sequência de números complexos está ligada à ideia de limite.

Definição 4.4.3. *Dizemos que um número complexo L é o limite de uma sequência (z_n), ou que (z_n) converge para L, se, para todo número real $\varepsilon > 0$, tomado arbitrariamente, existe um $N \in \mathbb{N}$ tal que $|z_n - L| < \varepsilon$ sempre que $n > N$. Ou seja, qualquer que seja o termo z_n na sequência, tomado após o termo z_N, está no disco $\mathbb{D}(L, \varepsilon)$. Podemos expressar essa mesma definição do seguinte modo: a sequência (z_n) converge, se*

$$\exists L \in \mathbb{C};\ \forall \varepsilon > 0, \exists N \in \mathbb{N} \ : |z_n - L| < \varepsilon,\ \forall n > N.$$

Denotamos,

$$\lim z_n = L \quad ou \quad z_n \to L.$$

Vamos tornar mais clara a linguagem desta definição. Se uma sequência (z_n) de números complexos é convergente, para qualquer valor positivo ε, por menor que seja, seus pontos estão a uma distância menor do que ε de L no plano, para todo $n > N$, para certo N natural. Assim, esceto a uma quantidade finita de pontos, podemos sempre tomar um z_n tão próximo quanto queiramos de L. Vejamos um exemplo de sequência convergente.

Exemplo 4.4.4. *A sequência* $\left(\frac{i^n}{n}\right)$ *converge para* 0.

De fato. Tome um $\varepsilon > 0$ *real qualquer. Assim, sendo* $N \in \mathbb{N}$*, onde* $N \geq \frac{1}{\varepsilon}$*, sempre que* $n > N$*, teremos:*

$$\left|\frac{i^n}{n} - 0\right| = \left|\frac{i^n}{n}\right| = \frac{1}{n} < \frac{1}{N} \leq \frac{1}{\left(\frac{1}{\varepsilon}\right)} = \varepsilon,$$

ou seja, $\left|\frac{i^n}{n} - 0\right| < \varepsilon$*. Em outras palavras, para* $n > N$*, o número* $\frac{i^n}{n}$ *sempre estará contido no disco* $\mathbb{D}(0, \varepsilon)$*. Assim, a medida que* n *cresce,* $\left(\frac{i^n}{n}\right)$ *se aproxima cada vez mais de* 0*.*

Na figura 4.2, temos uma ilustração dos primeiros 50 pontos da sequência $\left(\frac{i^n}{n}\right)$, ligados por segmentos de reta. Note que, a partir de $n = 1$, a medida que n cresce, z_n se torna cada vez mais próximo de 0.

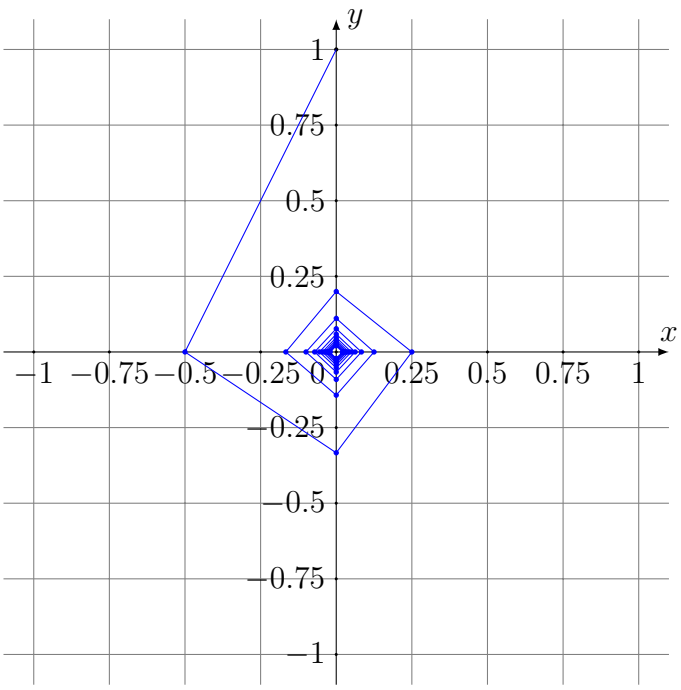

Figura 4.2: *Pontos ordenados da sequência*

Algumas funções têm limite em dado ponto z_0, mesmo que estas funções não estejam definidas em z_0. Com base nessa análise, trazemos a definição a seguir.

Para cada n da sequência (z_n), tem-se que $z_n = x_n + iy_n$, onde (x_n) e (y_n) são sequências de números reais. Assim, em vários casos, seus limites podem ser encontrados usando as mesmas técnicas usadas tradicionalmente no cálculo para variáveis reais.

Definição 4.4.5. *Uma sequência* (z_n) *é de Cauchy se, para todo* $\varepsilon > 0$*, existir* $N \in \mathbb{N}$ *tal que* $|z_m - z_n| < \varepsilon$*,* $\forall m, n > N$*.*

Perceba que, se uma sequência é de Cauchy, sempre haverá dois termos tão próximos quanto queiramos.

Proposição 4.4.6. *O conjunto dos pontos de uma sequência de Cauchy é um conjunto limitado.*

Demonstração. Se (z_n) é uma sequência de Cauchy, então, $\exists N \in \mathbb{N}$ tal que, se $n, m > N$, então $|z_m - z_n| < 1$. Daí, $z_n \in \mathbb{D}(z_{N+1}, 1)$, sempre que $n > N$.

Agora, tome $A = \max(|z_1|, |z_2|, ..., |z_N|, |z_{N+1}| + 1)$. Então, $\{z_n \,|\, n \in \mathbb{N}\} \subset \mathbb{D}(0, A)$. □

Uma vez que uma sequência de Cauchy é limitada, chegamos à última proposição desta seção, que mostra o porquê desse princípio, conhecido como *Princípio de Cauchy*, ser tão essencial para a Análise Complexa.

Proposição 4.4.7. *Uma sequência (z_n) converge se, e somente se, é de Cauchy.*

Demonstração. Para a primeira parte da afirmativa, suponha que exista $L \in \mathbb{C}$ tal que $z_n \to L$. Seja $\varepsilon > 0$, então existe $N \in \mathbb{N}$ tal que $z_n \in \mathbb{D}\left(L, \frac{\varepsilon}{2}\right), \forall n > N$. Logo, se $m, n > N$, então

$$\begin{aligned} |z_n - z_m| &= |z_n - L + L - z_m| \\ &\leq |z_n - L| + |z_m - L| \\ &< \frac{\varepsilon}{2} + \frac{\varepsilon}{2} \\ &= \varepsilon \end{aligned}$$

ou seja, (z_n) é de Cauchy.

Reciprocamente, suponha que (z_n) seja uma sequência de Cauchy.

Seja $\varepsilon > 0$. Então, existe $N_0 \in \mathbb{N}$ tal que $|z_m - z_n| < \frac{\varepsilon}{2}$, $\forall m, n > N_0$. Pela Proposição 4.4.6, o conjunto dos pontos dessa sequência é limitado. Por outro, este conjunto tem um ponto de acumulação, digamos, $L \in \mathbb{C}$ (este resultado é garantido pelo Teorema de Weierstrass, que pode ser encontrado em [1].) Logo, existe $N > N_0$ tal que $z_N \in \mathbb{D}\left(L, \frac{\varepsilon}{2}\right)$. Daí, temos que $\forall n > N$

$$\begin{aligned} |z_n - L| &= |z_n - z_N + z_N - L| \\ &\leq |z_n - z_N| + |z_N - L| \\ &< \frac{\varepsilon}{2} + \frac{\varepsilon}{2} \\ &= \varepsilon \end{aligned}$$

Ou seja, $z_n \in \mathbb{D}(L, \varepsilon)$. Assim, concluímos que $z_n \to L$. □

As propriedades relativas a operações entre limites para as sequências e funções de variável real se estendem às propriedades para limites de variáveis complexas [15].

4.5 Séries de potência e funções analíticas

Para falarmos na representação analítica de uma função, precisamos de algumas noções acerca de séries de potência e convergência de séries. Embasados nos resultados postos até aqui, apresentamos alguma breves noções.

Definição 4.5.1. *Uma série de números complexos é a sequência (s_n) gerada por uma sequência (z_n) de números complexos dada por*

$$s_n = \sum_{i=0}^{n} z_i.$$

Se (s_n) converge, dizemos que a série converge. Caso contrário, dizemos que a série diverge. Denotamos $\sum_{n=0}^{\infty} z_n$ a série gerada por (z_n).

Escrevendo $z_n = x_n + iy_n$, temos que $\sum_{n=0}^{\infty} z_n = \sum_{n=0}^{\infty}(x_n + iy_n)$ converge se, e somente se, as séries de números reais $\sum_{n=0}^{\infty} x_n$ e $\sum_{n=0}^{\infty} y_n$ convergem. Sendo assim, alguns testes de convergência para séries reais podem ser aplicados a séries de números complexos [15]. Vejamos um exemplo para a análise da conhecida *série geométrica.*

Exemplo 4.5.2. *Seja $r \in \mathbb{C}^*$. Para a série $\sum_{n=0}^{\infty} r^n$, considere (s_n) a sequência das somas parciais*

$$s_n = 1 + r + r^2 + \cdots + r^n = \frac{1 - r^{n+1}}{1 - r}.$$

Se $|r| < 1$, então $\lim_{n\to+\infty} |r^n| = 0$. Consequentemente, $\lim_{n\to+\infty} r^n = 0$. Logo, $\lim_{n\to+\infty} s_n = \frac{1}{1-r}$, e a série converge.

Por outro lado, se $|r| > 1$, então $\lim_{n\to+\infty} |r^n| = +\infty$, e a série diverge. Se $|r| = 1$, a série também diverge.

Dentre os testes de convergência existentes para séries de números complexos, destacamos o teste da convergência absoluta, que fundamentará o estudo das séries de potência.

Definição 4.5.3. *Uma série complexa $\sum_{n=0}^{\infty} z_n$ converge absolutamente se a série de números reais positivos $\sum_{n=0}^{\infty} |z_n|$ converge.*

Note que a análise da convergência absoluta de uma série de números complexos se assemelha à análise de convergência de uma série de números reais, uma vez que $\sum_{n=0}^{\infty} |z_n|$ corresponde a série das normas de cada z_n. Assim, como já destacamos anteriormente, para verificar a convergência deste tipo de série, basta aplicar os mesmos testes de convergência para séries de números reais. Os principais testes de convergência para séries de números reais podem ser conferidos em [9].

Proposição 4.5.4. *Se a série $\sum_{n=0}^{\infty} z_n$ converge absolutamente, então $\sum_{n=0}^{\infty} z_n$ converge.*

Demonstração. Seja $s_n = \sum_{i=0}^{n} z_i$ a n-ésima soma parcial da sequência (s_n). Por hipótese, como $\sum_{i=0}^{\infty} z_n$ converge absolutamente, para todo $\varepsilon > 0$, $\exists N \in \mathbb{N}$ tal que

$$\sum_{n=N+1}^{\infty} |z_n| < \varepsilon.$$

Então, para m, n naturais, com $n > m > N$, temos

$$|s_n - s_m| = \left| \sum_{i=m+1}^{n} z_i \right|.$$

Pela desigualdade triangular,

$$\left| \sum_{i=m+1}^{n} z_i \right| \leq \sum_{i=m+1}^{n} |z_i|,$$

e, como $\sum_{i=m+1}^{n} |z_i|$ tem um número finito de parcelas,

$$\sum_{i=m+1}^{n} |z_i| \leq \sum_{n=N+1}^{\infty} |z_n|.$$

Isso implica dizer que

$$|s_n - s_m| \leq \sum_{n=N+1}^{\infty} |z_n| < \varepsilon.$$

Logo, pelo critério de Cauchy, (s_n) converge. □

Proposição 4.5.5. *Seja $s \in \mathbb{C}$. A série $\sum_{n=1}^{\infty} n^{-s}$ converge para $\mathrm{Re}(s) > 1$ e diverge para $\mathrm{Re}(s) = 1$.*

Demonstração. De fato, considere $s = a + bi$, onde $a, b \in \mathbb{R}$. Então

$$\begin{aligned} |n^{-s}| &= |n^{-a-bi}| \\ &= |n^{-a} \cdot n^{-bi}| \\ &= n^{-a} \cdot |n^{-bi}| \\ &= n^{-a} \cdot \left|e^{i(b \log n)}\right|. \end{aligned}$$

Usando a Proposição 4.2.8, temos que

$$|n^{-s}| = n^{-a}.$$

Logo,

$$\sum_{n=1}^{\infty} |n^{-s}| = \sum_{n=1}^{\infty} n^{-a}.$$

Aplicando o teste da integral para a série de números reais, temos que

$$\int_1^{+\infty} x^{-a}dx = \lim_{t\to+\infty}\int_1^t x^{-a}dx$$

Se $\mathrm{Re}(s) > 1$, então

$$\begin{aligned}\lim_{t\to+\infty}\int_1^t x^{-a}dx &= \lim_{t\to+\infty}\left(\frac{t^{1-a}}{1-a} - \frac{1}{1-a}\right)\\ &= \frac{1}{a-1}.\end{aligned}$$

Logo, $\sum_{n=1}^{\infty} n^{-s}$ converge absolutamente para $\mathrm{Re}(s) > 1$. Consequentemente, $\sum_{n=1}^{\infty} n^{-s}$ converge para $\mathrm{Re}(s) > 1$.

Se $\mathrm{Re}(s) = 1$, então

$$\lim_{t\to+\infty}\int_1^t x^{-1}dx = \lim_{t\to+\infty}\log x\Big|_1^t = +\infty$$

Logo, $\sum_{n=1}^{\infty} n^{-s}$ não converge absolutamente para $\mathrm{Re}(s) = 1$.

Em particular, se $s = 1$,

$$\sum_{n=1}^{\infty} n^{-s} = \sum_{n=1}^{\infty}\frac{1}{n} = +\infty$$

□

Antes de apresentarmos as funções analíticas, precisamos de mais alguns conceitos importantes, e que dizem a respeito do conceito de derivada e de série de potências. As condições de diferenciabilidade são muito mais fortes no campo complexo, em comparação ao corpo dos números reais. O fato de uma função ser infinitamente derivável irá interferir na sua representação em forma de séries.

Definição 4.5.6. *Seja $\Omega \subset \mathbb{C}$ uma região, $f : \Omega \to \mathbb{C}$ e $z_0 \in \Omega$. Então f é uma função contínua se*

$$\lim_{z\to z_0} f(z) = f(z_0)$$

Note que esta definição é semelhante ao conceito de continuidade para funções de variável real.

Exemplo 4.5.7. *A função $f(z) = \dfrac{1}{z}$ é contínua em $\mathbb{C}^*$.*

Assim como o conceito de continuidade, o conceito de derivada de um função de variável complexa se assemelha ao caso real.

Definição 4.5.8. *Seja $\Omega \subset \mathbb{C}$ uma região, $f : \Omega \to \mathbb{C}$ e $z_0 \in \Omega$. Então f tem derivada complexa em z_0 se existir o limite*

$$\lim_{z\to z_0}\frac{f(z) - f(z_0)}{z - z_0}.$$

Chamaremos tal limite de derivada de f em z_0, $f'(z_0)$.

Proposição 4.5.9. *Se $f : \Omega \to \mathbb{C}$ tem derivada complexa em um ponto $z_0 \in \Omega$, então f é contínua em z_0.*

Demonstração. Basta provarmos que $\lim_{z\to z_0} |f(z) - f(z_0)| = 0$, a proposição será validada automaticamente. Observe que

$$\begin{aligned}
\lim_{z\to z_0} |f(z) - f(z_0)| &= \lim_{z\to z_0} \frac{|f(z) - f(z_0)|}{|z - z_0|} \cdot |z - z_0| \\
&= \lim_{z\to z_0} \left| \frac{f(z) - f(z_0)}{z - z_0} \right| \cdot |z - z_0| \\
&= \lim_{z\to z_0} \left| \frac{f(z) - f(z_0)}{z - z_0} \right| \cdot \lim_{z\to z_0} |z - z_0| \\
&= \left| \lim_{z\to z_0} \frac{f(z) - f(z_0)}{z - z_0} \right| \cdot \left| \lim_{z\to z_0} (z - z_0) \right| \\
&= |f'(z_0)| \cdot 0 \\
&= 0
\end{aligned}$$

□

Se a função $f(z) = u(z) + iv(z)$ é derivável num ponto $z = x + yi$, então

$$\lim_{z\to z_0} \frac{f(z) - f(z_0)}{z - z_0}$$

existe, independentemente do modo como $z \to z_0$. Por tal motivo, a condição de derivabilidade de uma função está atrelada às Condições de Cauchy-Riemann, apresentadas a seguir.

Teorema 4.5.10 (Condições de Cauchy-Riemann). *Seja $\Omega \subset \mathbb{C}$ um aberto e $z_0 = x_0 + iy_0$ um ponto de Ω. Seja $f : \Omega \to \mathbb{C}$ uma função tal que*

$$f(x + iy) = u(x + iy) + iv(x + iy).$$

Dizemos que f possui derivada complexa em z_0 se, e somente se, as derivadas parciais $\frac{\partial u}{\partial x}, \frac{\partial u}{\partial y}, \frac{\partial v}{\partial x}$ e $\frac{\partial v}{\partial y}$ existem e são contínuas em $z_0 = x_0 + iy_0$, satisfazendo às condições

$$\frac{\partial u}{\partial x}(z_0) = \frac{\partial v}{\partial y}(z_0) \quad e \quad \frac{\partial u}{\partial y}(z_0) = -\frac{\partial v}{\partial x}(z_0)$$

chamadas equações de Cauchy Riemann.

Demonstração. Uma prova deste teorema é encontrada em [1]. □

Observe que a condição de derivabilidade em um ponto z_0 não depende só da continuidade no ponto, nem apenas da comparação das derivadas parciais das funções $u(x, y)$ e $v(x, y)$.

Exemplo 4.5.11. *Vamos analisar em quais pontos do plano complexo a função $f(z) = \frac{1}{z}$ atende as condições de Cauchy-Riemann.*

Observe que, como $z = x + yi$, *então*

$$f(z) = \frac{x}{x^2+y^2} - \frac{y}{x^2+y^2}i.$$

Logo,

$$\begin{array}{lll} \dfrac{\partial u}{\partial x} = \dfrac{y^2-x^2}{(x^2+y^2)^2} & , & \dfrac{\partial v}{\partial y} = \dfrac{y^2-x^2}{(x^2+y^2)^2}, \\ \dfrac{\partial u}{\partial y} = \dfrac{-2xy}{(x^2+y^2)^2} & e & \dfrac{\partial v}{\partial x} = \dfrac{2xy}{(x^2+y^2)^2}. \end{array}$$

As derivadas parciais de $u(x,y)$ *e* $v(x,y)$ *não são contínuas em* $(x,y) = (0,0)$. *Logo, a função* $f(z)$ *não é derivável em* $z = 0$. *Em contrapartida, as equações de Cauchy-Riemann são satisfeitas em todo o restante do plano complexo, e as derivadas parciais de* $u(x,y)$ *e* $v(x,y)$ *são contínuas para* $z \neq 0$. *Logo,* $f(z) = \dfrac{1}{z}$ *é derivável em* $\mathbb{C} - \{0\}$. *A saber,* $f'(z) = \dfrac{1}{z^2}$.

De posse de todos os resultados postos aqui envolvendo a derivada complexa, podemos definir o conceito de função holomorfa.

Definição 4.5.12. *Seja* $\Omega \subset \mathbb{C}$ *uma região. A função* $f : \Omega \to \mathbb{C}$ *é dita holomorfa em* Ω *se* f *tem derivada complexa em todos os pontos de* Ω. *Denotaremos por* f' *a função derivada de* f, *onde* $f'(z)$ *é a derivada de* f *em* $z \in \Omega$.

Se $f : \mathbb{C} \to \mathbb{C}$ *é holomorfa em todo ponto de* $\mathbb{C}$, *então* f *é dita "inteira".*

Em geral, as regras de derivação de funções complexas se assemelham às regras para funções reais.

Exemplo 4.5.13. *Sendo* $f : \mathbb{C} \to \mathbb{C}$, *onde* $f(z) = z^n$, f *é inteira e* $f'(z) = nz^{n-1}$.

De fato. Seja $z_0 \in \mathbb{C}$, *então*

$$\begin{aligned} \lim_{z\to z_0} \frac{f(z)-f(z_0)}{z-z_0} &= \lim_{z\to z_0} \frac{z^n - z_0^n}{z-z_0} \\ &= \lim_{z\to z_0} \frac{(z-z_0)(z^{n-1} + z^{n-2}\cdot z_0 + \cdots + z\cdot z_0^{n-2} + z_0^{n-1})}{z-z_0} \\ &= \lim_{z\to z_0} (z^{n-1} + z^{n-2}\cdot z_0 + \cdots + z\cdot z_0^{n-2} + z_0^{n-1}) \\ &= z_0^{n-1} + z_0^{n-2}\cdot z_0 + \cdots + z_0\cdot z_0^{n-2} + z_0^{n-1} \\ &= n\cdot z_0^{n-1} \end{aligned}$$

A seguir, temos um exemplo de função holomorfa aplicada à função logaritma.

Exemplo 4.5.14. *Seja* $B \subset \mathbb{C}^*$ *um aberto simplesmente conexo. Um ramo de logaritmo é uma função contínua* $f : B \to \mathbb{C}$, *inversa da função exponencial, ou seja,*

$$e^{f(z)} = z, \forall z \in B.$$

Esta função é holomorfa [15], e

$$f'(z) = \frac{1}{\exp'(f(z))} = \frac{1}{\exp(f(z))} = \frac{1}{z}.$$

Seja $B = \{\rho e^{i\theta} \in \mathbb{C} \mid \rho > 0, \theta \in (-\pi, \pi)\}$. *Este conjunto é um aberto simplesmente conexo. Na seção 3.2, a definição 4.2.9 trata sobre o ramo principal de logaritmo como sendo a função*

$$\begin{array}{rccc} \log\colon & B & \to & \mathbb{C} \\ & \rho e^{i\theta} & \longmapsto & \log(\rho) + i\theta. \end{array}$$

Então, log *é holomorfa em* B *e* $\log'(z) = \dfrac{1}{z}$ *para todo* $z \in B$.

A partir deste ponto, todas as vezes que nos referírmos à função log, estaremos nos referindo à função definida como no Exemplo 4.5.14.

Definição 4.5.15. *Uma série de potências centrada no número complexo* z_0 *é uma série da forma*

$$\sum_{n=0}^{\infty} a_n (z - z_0)^n \, , a_n \in \mathbb{C}.$$

O maior número real $R > 0$ *para o qual esta série converge em todo ponto do disco* $\mathbb{D}(z_0, R)$ *é denominado "raio de convergência" da série.*

Observe que se $\displaystyle\sum_{n=0}^{\infty} a_n (z - z_0)^n$ converge no disco $\mathbb{D}(z_0, R)$, então esta série define uma função $f : \mathbb{D}(z_0, R) \to \mathbb{C}$. Assim, chegamos à seguinte definição.

Definição 4.5.16. *Sejam um conjunto aberto* $\Omega \subset \mathbb{C}$ *e* $f : \Omega \longrightarrow \mathbb{C}$. *A função* f *é dita analítica em* Ω, *se para todo* $z_0 \in \Omega$, f *se expressa como uma série de potências de centro* z_0 *com raio de convergência positivo.*

$$f(z) = \sum_{n=0}^{\infty} a_n (z - z_0)^n$$

Teorema 4.5.17. *Sejam um conjunto aberto* $\Omega \subset \mathbb{C}$ *e* $f : \Omega \longrightarrow \mathbb{C}$ *uma função analítica em* Ω. *Se* f *se expressa como uma série de potências de centro* z_0

$$f(z) = \sum_{n=0}^{\infty} a_n (z - z_0)^n$$

com raio de convergência positivo R, *então*

$$f'(z) = \sum_{n=1}^{\infty} n a_n (z - z_0)^{n-1}$$

para qualquer $z \in \mathbb{D}(z_0, R)$.

Demonstração. Uma demonstração para este teorema se encontra em [15]. □

Corolário 4.5.18. *Sejam um conjunto aberto* $\Omega \subset \mathbb{C}$ *e* $f : \Omega \longrightarrow \mathbb{C}$ *uma função analítica em* Ω. *Se* f *se expressa como uma série de potências de centro* z_0

$$f(z) = \sum_{n=0}^{\infty} a_n (z - z_0)^n$$

com raio de convergência positivo R, então $f(z)$ é dada pela série de Taylor centrada em z_0 expressa por

$$f(z) = \sum_{n=0}^{\infty} \frac{f^{(n)}(z_0)}{n!}(z - z_0)^n$$

onde tal série converge absolutamente para todo $z \in \mathbb{D}(z_0, R)$.

Perceba que tanto a função analítica quanto a função holomorfa envolvem a ideia de derivabilidade. Algumas literaturas expressam tais conceitos como equivalentes. Não daremos detalhes sobre tal temática neste trabalho, mas deixamos o seguinte teorema.

Teorema 4.5.19. *Toda função holomorfa é analítica.*

Demonstração. A demonstração para este teorema é encontrada em [1]. □

Com base neste teorema, podemos dizer que no campo complexo, os termos função analítica e função holomorfa expressam ideias equivalentes.

Exemplo 4.5.20. *Considere a função $f(z) = \log(1 + z)$. Temos que $f(0) = 0$ e*

$$f^{(k)}(z) = (-1)^{k+1} \cdot \frac{(k-1)!}{(1+z)^k}$$

então,

$$f^{(k)}(0) = (-1)^{k+1} \cdot (k-1)!.$$

Então, a expansão da função $f(z)$ em série de potências em torno de $z_0 = 0$ é dada por

$$\sum_{k=1}^{\infty} \frac{(-1)^{k+1} z^k}{k}.$$

Chamando $a_k = \dfrac{(-1)^{k+1}}{k}$, temos que o raio de convergência desta série é dado por

$$\lim_{k \to +\infty} \left| \frac{a_{k+1}}{a_k} \right| = 1,$$

ou seja, a série converge para $|z| < 1$.

4.6 Integrais, pólos e resíduos

Antes de finalizar nosso capítulo com alguns detalhes envolvendo a teoria dos resíduos e das singularidades, precisamos entender um pouco acerca da integração para funções de variáveis complexas. Comecemos com a definição de uma integral de variável complexa.

Definição 4.6.1. *Considere duas funções $f, g : [a, b] \to \mathbb{R}$ contínuas. Então*

$$\int_a^b (f(t) + ig(t))dt = \int_a^b f(t)dt + i \int_a^b g(t)dt.$$

Perceba que podemos desmembrar a integral de uma função complexa em parte real e parte imaginária. A partir desta definição, seguem as propriedades de linearidade e produto por escalar, válidas para integrais de funções reais. No entanto, a grande diferença entre a integral no campo complexo para o campo real consiste na ideia de *caminho de integração.*

Definição 4.6.2. *Seja Ω um aberto de $\mathbb{C}$. Um caminho em Ω é uma função contínua $\gamma : [a, b] \to \Omega$ tal que*

$$\gamma(t) = x(t) + iy(t).$$

Se $x(t)$ e $y(t)$ são funções que possuem derivada de 1^a ordem, e estas são contínuas, dizemos que o caminho γ é suave. Neste caso, denotamos o vetor tangente a γ no ponto $\gamma(t)$ por

$$\gamma'(t) = x'(t) + iy'(t).$$

Se o caminho γ consistir em n caminhos suaves $\gamma_1, \gamma_2, \gamma_3, ..., \gamma_n$ unidos sequencialmente, diremos que γ é um caminho suave por partes.

Se $\gamma(a) = \gamma(b)$, dizemos que o caminho γ é fechado. Chamaremos uma integral sobre um caminho fechado de *integral de contorno.*

Se $\mathbb{C} - \gamma$ possui exatamente duas componentes conexas, a curva γ em $\mathbb{C}$ é chamada *Curva de Jordan.*

Definição 4.6.3. *Seja Ω um aberto de $\mathbb{C}$. Sejam também f uma função contínua em Ω e $\gamma : [a, b] \to \Omega$ um caminho qualquer. Definimos a integral de f sobre o caminho γ*

$$\int_\gamma f(z)dz = \int_a^b f(\gamma(t))\gamma'(t)dt$$

Exemplo 4.6.4. *Vamos calcular a integral da função $f(z) = |z|$ ao longo do segmento retilíneo de $z_1 = 0$ a $z_2 = -2 + 3i$.*

Tomaremos a seguinte parametrização: $z = \gamma(t) = -2t + 3ti$, onde $0 \leq t \leq 1$. Então

$$|z| = |-2t + 3ti| = \sqrt{13}t$$

e ainda

$$dz = (-2 + 3i)dt$$

Logo,

$$\begin{aligned}
\int_\gamma f(z)dz &= \int_\gamma |z|dz \\
&= \int_0^1 \sqrt{13}t \cdot (-2 + 3i)dt \\
&= \sqrt{13}(-2 + 3i) \int_0^1 t\, dt \\
&= \sqrt{13}(-2 + 3i) \cdot \frac{t^2}{2}\Big|_0^1 \\
&= \frac{\sqrt{13}(-2 + 3i)}{2}
\end{aligned}$$

Perceba que a parametrização orienta o caminho de acordo com a variação dos valores da variável t, dando uma orientação de a até b.

Apesar da ideia de tormarmos caminhos diferentes para a integração, há uma importante relação entre as integrais sobre um caminho suave.

Teorema 4.6.5. *Sejam $\Omega \subset \mathbb{C}$ uma região e F uma função holomorfa em Ω tal que F' é contínua. Seja também γ um caminho em Ω com extremidades em z_0 e z_1, originando-se em z_0. Então*

$$\int_\gamma F'(z)dz = F(z_1) - F(z_0)$$

Demonstração. Tomando uma parametrização $\gamma(t)$, $\gamma : [a, b] \to \Omega$. Uma vez que a função F' possui uma primitiva, o Teorema Fundamental do Cálculo nos permite escrever

$$\begin{aligned} \int_\gamma F'(z)dz &= \int_a^b F'(\gamma(t))\gamma'(t)dt \\ &= F(\gamma(b)) - F(\gamma(a)) \\ &= F(z_1) - F(z_0) \end{aligned}$$

□

Teorema 4.6.6 (Teorema de Cauchy). *Sejam $\Omega \subset \mathbb{C}$ uma região simplesmente conexa e $p \in \Omega$. Se f é uma função contínua em Ω e holomorfa em $\Omega - \{p\}$, então $f = F'$, para alguma F holomorfa em Ω. Logo*

$$\int_\gamma f(z)dz = 0$$

para todo caminho γ fechado e suave por partes em Ω.

Demonstração. A demonstração deste teorema se encontra em [1]. □

Corolário 4.6.7. *Sejam $\Omega \subset \mathbb{C}$ uma região simplesmente conexa e f uma função holomorfa em Ω. Sejam $z_1, z_2 \in \Omega$ e γ_1 e γ_2 caminhos que ligam z_1 a z_2. Então*

$$\int_{\gamma_1} f(z)dz = \int_{\gamma_2} f(z)dz$$

Estes resultados nos permitem dizer que a integral complexa de uma função analítica em uma região simplesmente conexa depende, apenas, do ponto inicial e do ponto final do caminho de integração γ.

O teorema a seguir nos permite analisar os valores de uma função holomorfa em uma região, conhecendo seus valores no contorno da região.

Teorema 4.6.8 (Fórmula Integral de Cauchy). *Seja Ω uma região simplesmente conexa e seja $\gamma \subset \mathbb{C}$ uma curva de Jordan suave por partes. Seja f uma função holomorfa em Ω. Se z está na componente simplesmente conexa de $\Omega - \gamma$, então*

$$f(z) = \frac{1}{2\pi i} \int_\gamma \frac{f(w)}{w - z} dw.$$

Demonstração. A demonstração deste teorema se encontra em [1]. □

Enfim, embasados neste resultados a respeito das integrais, vejamos algumas definições importantes acerca de pólos e resíduos. Para tanto, usaremos a seguinte notação: sejam r_1 e r_2 números reais tais que $0 \leq r_1 < r_2$, $a \in \mathbb{C}$. O anel $A(a, r_1, r_2)$ é o conjunto aberto definido por

$$A(a, r_1, r_2) = \{z \in \mathbb{C} : r_1 < |z - a| < r_2\}.$$

Definição 4.6.9. *Seja f uma função holomorfa no anel $A(z_0, 0, r)$. A série de Laurent em torno de z_0 é definida por*

$$f(z) = \sum_{m=1}^{\infty} b_m \frac{1}{(z - z_0)^m} + a_0 + \sum_{n=1}^{\infty} a_n (z - z_0)^n,$$

Se cada b_m da série de Laurent for nulo, então esta coincide com a série de Taylor. Considerando esta representação em série de potências, precisamos analisar o que ocorre com a função $f(z)$ em z_0.

Definição 4.6.10. *Seja f definida como em 4.6.9, e sua respectiva expansão em série de Laurent. Dizemos que z_0 é uma singularidade removível de f se $b_m = 0$ para $m \geq 1$. Se $b_k \neq 0$ e $b_m = 0$ para $m > k$, z_0 é um pólo de ordem k de f. Se $b_m \neq 0$ para uma infinidade de valores de m, dizemos que z_0 é uma singularidade essencial de f.*

Se a função possui pólo de ordem 1 em z_0, dizemos que este é um pólo simples.

Exemplo 4.6.11. *Considere a função $f(z) = \dfrac{e^z}{z^2}$ numa vizinhança de $z = 0$. Observe que*

$$\begin{aligned} f(z) &= \frac{1}{z^2} \cdot e^z \\ &= \frac{1}{z^2} \cdot \left(\sum_{n=0}^{\infty} \frac{z^n}{n!} \right) \\ &= \frac{1}{z^2} + \frac{1}{z} + \sum_{n=0}^{\infty} \frac{z^n}{(n+2)!}. \end{aligned}$$

Logo, $f(z)$ possui pólo de ordem 2 em $z = 0$.

Além do polo da função, precisamos ainda definir um outro elemento da representação em série de Laurent: o resíduo.

Definição 4.6.12. *Seja uma função f holomorfa no anel $A(z_0, 0, r)$. O resíduo de f em z_0, denotado por $\operatorname{res}(f, z_0)$, é o coeficiente b_1 do termo $\dfrac{1}{z - z_0}$ de sua série de Laurent com centro em z_0.*

Exemplo 4.6.13. *Uma vez que a função $f(z) = \dfrac{e^z}{z^2}$, numa vizinhança de $z = 0$, é dada por*

$$\frac{1}{z^2} + \frac{1}{z} + \sum_{n=0}^{\infty} \frac{z^n}{(n+2)!}$$

então, $f(z)$ possui resíduo 1 em $z = 0$. Ou seja, $\operatorname{res}(f, 0) = 1$.

Observe que as funções de variável complexa possuem algumas propriedades diferentes em relação às funções de variável real. Em particular, se duas funções $f : A \to \mathbb{C}$ e $g : B \to \mathbb{C}$ são analíticas numa mesma região Ω, e estas funções coincidirem em $A \cap B$, então f é dita uma continuação analítica de g, como ilustra a imagem 4.3. Neste caso, existe uma função $F : A \cup B \to \mathbb{C}$ tal que $F(z) = f(z)$ em A e $F(z) = g(z)$ em B, sendo F única [1].

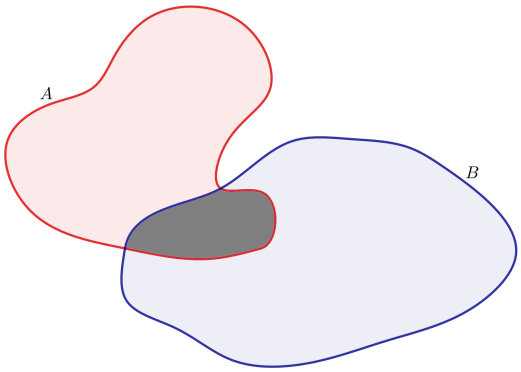

Figura 4.3: *Conjuntos A e B onde F é analítica*

Capítulo 5

A distribuição dos números primos

Em 1.890, o eminente matemático Charles Hermite propôs que o *Grand Prix des Sciences Mathématiques* da Academia de Paris fosse dedicado ao personagem que apresentasse uma prova para a conjectura de Gauss, ou seja, mostrar que a quantidade de números primos até dado valor x era aproximadamente $\frac{x}{\log x}$. Hermite acreditava que seu amigo, o holandês Thomas Stieltjes, realizasse tal façanha. Mas, para surpresa de todos, um aluno de Hermite, o jovem Jacques Hadamard, se inscreveu no concurso, apresentando um artigo com ideias suficientes para receber tal prêmio. Apesar da prova não ser completa, Hadamard conseguira mostrar que a função zeta de Riemann não possuía zeros no semiplano $\operatorname{Re} s > 1$. Esta contribuição de Hadamard, aprimorada posteriormente para uma prova, juntamente com a simultânia apresentação de uma demonstração por Charles de la Vallée-Poussin para o Teorema dos Números Primos, despertou o interesse de matemáticos durante o século XX em busca de mais resultados que se relacionassem à hipótese Riemann [14].

Este capítulo se destina a apresentar a função Zeta de Riemann e mostrar uma prova para o Teorema dos Números Primos diferente das apresentadas por Hadamard e Poussin. Tal demonstração será realizada apresentando uma relação entre a função Zeta de Riemann e umas das funções do matemático Pafnuty Chebyshev: a função $\psi(x)$. Para tanto, usaremos as seguintes notações:

- Sendo x real, $\lfloor x \rfloor$ corresponde ao maior inteiro menor do que ou igual a x.
- Uma função $f : \mathbb{R}^+ \to \mathbb{R}^+$ é $O(x)$, se existir alguma contante C para a qual $f(x) \leq Cx$, para todo $x > x_0$, $x_0 \in \mathbb{R}$ fixo.
- Quando nos referirmos ao número p, p é um número primo.
- $E_p(n)$ é o maior número inteiro não negativo k tal que p^k divide n.

5.1 As funções de Chebyshev

Apesar de não apresentar uma prova acerca do Teorema dos Números Primos, Pafnuty Chebyshev trouxe uma análise muito importante acerca da razão entre $\pi(x)$ e $x/\log(x)$ em 1.850, na cidade de São Petersburgo [14]. Para entender sua análise, vejamos alguns resultados importantes. O primeiro deles se refere à maior potência de base p que divide $n!$.

Proposição 5.1.1. *Seja $n \in \mathbb{N}$. Então*

$$E_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots$$

Demonstração. Façamos a prova por indução sobre n.
Para $n = 1$, temos

$$E_p(1!) = 0 = \left\lfloor \frac{1}{p} \right\rfloor.$$

Agora, suponha que a afirmação seja válida para todo número natural m, onde $m < n$. Listando os números de 1 a n, os números múltiplos de p são

$$p, 2p, ..., \left\lfloor \frac{n}{p} \right\rfloor p.$$

Ou seja, temos $\left\lfloor \frac{n}{p} \right\rfloor$ múltiplos de p. Cada um destes gera, ao menos, um fator p para $n!$. Para verificar se há mais fatores p, basta identificar na lista dos números de 1 a $\left\lfloor \frac{n}{p} \right\rfloor$ quais números também são múltiplos de p. Isso equivale a escrever que

$$E_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + E_p\left(1 \cdot 2 \cdot 3 \cdots \left\lfloor \frac{n}{p} \right\rfloor\right),$$

ou ainda

$$E_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + E_p\left(\left\lfloor \frac{n}{p} \right\rfloor!\right).$$

Pela hipótese de indução, como $\left\lfloor \frac{n}{p} \right\rfloor < n$,

$$E_p\left(\left\lfloor \frac{n}{p} \right\rfloor!\right) = \left\lfloor \frac{\left\lfloor \frac{n}{p} \right\rfloor}{p} \right\rfloor + \left\lfloor \frac{\left\lfloor \frac{n}{p} \right\rfloor}{p^2} \right\rfloor + \left\lfloor \frac{\left\lfloor \frac{n}{p} \right\rfloor}{p^3} \right\rfloor + \cdots,$$

e uma vez que

$$\left\lfloor \frac{\left\lfloor \frac{n}{p} \right\rfloor}{p^k} \right\rfloor = \left\lfloor \frac{n}{p^{k+1}} \right\rfloor,$$

onde $k \in \mathbb{N}$, então, segue-se o resultado. □

Vejamos um exemplo que ilustra a contagem de fatores p em dado número fatorial.

Exemplo 5.1.2. *Vamos verificar quantos fatores 2 possui o número 15!. Para tanto, precisamos analisar cada número pertencente ao intervalo $[1, 15]$, ou seja,*

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15.$$

Note que os números que fornecem fator 2 são

$$2, 4, 6, 8, 10, 12, 14,$$

os números que fornecem fator 2^2 *são*

$$4, 8, 12,$$

e, o único número que fornece fator 2^3 *é* 8. *Sendo assim, verificamos que a contagem de fatores* 2 *para* 15! *pode ser expressa como*

$$\begin{aligned} E_2(15!) &= 7 + E_2(7!) \\ &= 7 + 3 + E_2(3!) \\ &= 7 + 3 + 1 = 11. \end{aligned}$$

Vejamos a seguir um resultado interessante acerca dos fatores primos de $\binom{2n}{n}$.

Proposição 5.1.3. *Sejam* $n \in \mathbb{N}$ *e* k_p *o inteiro tal que* $p^{k_p} \leq 2n < p^{k_p+1}$. *Então,* $E_p\left(\binom{2n}{n}\right) \leq k_p$. *Em particular, se* $p > \sqrt{2n}$, *então* $E_p\left(\binom{2n}{n}\right) \leq 1$. *Se* $\frac{2}{3}n < p < n$, *então* p *não divide* $\binom{2n}{n}$.

Demonstração. Sejam $\alpha = E_p((2n)!)$ e $\beta = E_p(n!)$. Como $\binom{2n}{n} = \frac{(2n)!}{n!n!}$, então

$$\begin{aligned} E_p\left(\binom{2n}{n}\right) &= \alpha - 2\beta \\ &= \left\lfloor \frac{2n}{p} \right\rfloor + \left\lfloor \frac{2n}{p^2} \right\rfloor + \cdots + \left\lfloor \frac{2n}{p^{k_p}} \right\rfloor - 2\left(\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots + \left\lfloor \frac{n}{p^{k_p}} \right\rfloor \right) \\ &= \left(\left\lfloor \frac{2n}{p} \right\rfloor - 2\left\lfloor \frac{n}{p} \right\rfloor \right) + \left(\left\lfloor \frac{2n}{p^2} \right\rfloor - 2\left\lfloor \frac{n}{p^2} \right\rfloor \right) + \cdots + \left(\left\lfloor \frac{2n}{p^{k_p}} \right\rfloor - 2\left\lfloor \frac{n}{p^{k_p}} \right\rfloor \right) \\ &= \sum_{i=1}^{k_p} \left(\left\lfloor \frac{2n}{p^i} \right\rfloor - 2\left\lfloor \frac{n}{p^i} \right\rfloor \right). \end{aligned}$$

Mas, para todo x real,

$$2x - 1 < \lfloor 2x \rfloor \leq 2x \qquad \text{e} \qquad -2x \leq -2\lfloor x \rfloor < 2 - 2x,$$

assim,

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

de onde temos que

$$0 \leq \left\lfloor \frac{2n}{p^i} \right\rfloor - 2\left\lfloor \frac{n}{p^i} \right\rfloor \leq 1$$

Então,

$$E_p\left(\binom{2n}{n}\right) \leq \sum_{i=1}^{k_p} 1 = k_p.$$

Uma vez que $\frac{2}{3}n < p < n$, então

$$p < n < 2p < 2n < 3p.$$

Ou seja, $\alpha = 2$ e $\beta = 1$. Logo, $E_p\left(\binom{2n}{n}\right) = 0$. □

Corolário 5.1.4. *Todo número p que satisfaz a condição $n < p < 2n$, onde n é um número natural, divide $\binom{2n}{n}$. Ou seja, existe um $c \in \mathbb{N}$ tal que*

$$\binom{2n}{n} = c \cdot \frac{(2n)\#}{n\#}.$$

Corolário 5.1.5. *Para todo n natural,* $\text{mmc}(1, 2, 3, ..., 2n) \geq \binom{2n}{n}$.

Exemplo 5.1.6. $\binom{20}{10}$ *é divisível por* $11, 13, 17$ *e* 19. *Mas, uma vez que* $7 < \frac{20}{2}$, *então* $\binom{20}{10}$ *não é divisível por tal primo. Perceba também que nenhum* $p > 20$ *divide* $\binom{20}{10}$.

Em sua análise, Chebyshev conseguiu mostrar que a função $\pi(x)$ possui uma relação com a expressão $x/\log x$. Para tanto, usou o binômio $\binom{2n}{n}$ para mapear os primos pertencentes ao intervalo $(n, 2n]$. A proposição a seguir mostra a relação entre $\binom{2n}{n}$ e $\pi(x)$ proposta por Chebyshev.

Proposição 5.1.7. *Existem $c, C \in \mathbb{R}_+^*$ tais que, para $x \geq 2$,*

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

Demonstração. Como $\binom{2n}{n}$ é apenas um dos elementos da linha $2n$ do triângulo de Pascal, então

$$\binom{2n}{n} \leq 2^{2n}.$$

Daí, pelo Corolário 5.1.4, temos que

$$\frac{(2n)\#}{n\#} < 2^{2n}.$$

Por outro lado, observe que a quantidade de números primos pertencentes ao intervalo $(n, 2n]$ é menor que n, e, por sua vez, cada p pertencente a este intervalo é maior que n. Então, vale a desigualdade

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

Ou seja,

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

Aplicando o logaritmo em ambos os membros desta desigualdade última desigualdade, temos que

$$(\pi(2n) - \pi(n)) \log n < 2n \log 2,$$

e como $\log n > 0$, então

$$\pi(2n) - \pi(n) < \frac{2n \log 2}{\log n}. \tag{5.1}$$

Afirmamos: para $k \geq 5$, natural,

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

De fato. Usemos o princípio da indução finita para provar esta afirmação. Observe que, para $k \leq 5$,

$$\begin{array}{rcccccl}
k=1 & : & \pi(2^{1+1}) = \pi(4) & = & 2 & < & \dfrac{5 \cdot 2^1}{1} \\
k=2 & : & \pi(2^{2+1}) = \pi(8) & = & 4 & < & \dfrac{5 \cdot 2^2}{2} \\
k=3 & : & \pi(2^{3+1}) = \pi(16) & = & 6 & < & \dfrac{5 \cdot 2^3}{3} \\
k=4 & : & \pi(2^{4+1}) = \pi(32) & = & 11 & < & \dfrac{5 \cdot 2^4}{4} \\
k=5 & : & \pi(2^{5+1}) = \pi(64) & = & 18 & < & \dfrac{5 \cdot 2^5}{5}.
\end{array}$$

Agora, suponha que a afirmação seja válida para algum $k \geq 5$, ou seja,

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

Pela equação 5.1, temos que

$$\begin{array}{rcl}
\pi(2^{k+2}) - \pi(2^{k+1}) & < & \dfrac{2 \cdot 2^{k+1} \log 2}{\log 2^{k+1}} \\
& = & \dfrac{2^{k+2}}{k+1}.
\end{array}$$

Reorganizando a desigualdade e aplicando a hipótese da indução,

$$\begin{array}{rcl}
\pi(2^{k+2}) & < & \pi(2^{k+1}) + \dfrac{2^{k+2}}{k+1} \\
& < & \dfrac{5 \cdot 2^k}{k} + \dfrac{4 \cdot 2^k}{k+1} \\
& = & \left(\dfrac{5}{k} + \dfrac{4}{k+1}\right) \cdot 2^k.
\end{array}$$

Se $k \geq 5$, então

$$5k + 5 \leq 5k + k$$

Logo

$$\frac{5}{k} \leq \frac{5+1}{k+1}$$

Então,

$$\begin{array}{rcl}
\left(\dfrac{5}{k} + \dfrac{4}{k+1}\right) \cdot 2^k & < & \left(\dfrac{6}{k+1} + \dfrac{4}{k+1}\right) \cdot 2^k \\
& = & \dfrac{10}{k+1} \cdot 2^k \\
& = & \dfrac{5}{k+1} \cdot 2^{k+1}
\end{array}$$

Logo, $\pi(2^{k+1}) < \dfrac{5 \cdot 2^k}{k}$ para todo k natural pelo Princípio da Indução.

Por outro lado, como $f(x) = x \log 2 / \log x$ é uma função crescente para $x \geq 3$, se $2^k < x \leq 2^{k+1}$, temos que

$$\begin{aligned} \pi(x) &\leq \pi(2^{k+1}) \\ &< \frac{5 \cdot 2^k}{k} \\ &= 5 \cdot \frac{2^k}{\log 2^k} \cdot \log 2 \\ &\leq 5 \log 2 \cdot \frac{x}{\log x}. \end{aligned}$$

Ou seja, $\pi(x) < C \cdot \dfrac{x}{\log x}$, onde $C = 5 \log 2$.

Para a segunda parte da nossa demonstração, precisamos mostrar que existe um c real positivo tal que $c \cdot \dfrac{x}{\log x} < \pi(x)$. Para tanto, considerando a forma fatorada canônica de $\binom{2n}{n}$, temos

$$\binom{2n}{n} = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r} = \prod_{i=1}^{r} p_i^{\alpha_i},$$

onde p_i é o i-ésimo número primo, $r = \pi(2n)$, e α_i é um número inteiro não negativo. Como cada $p_i^{\alpha_i} \leq 2n$,

$$\begin{aligned} \log \binom{2n}{n} &= \log \prod_{i=1}^{r} p_i^{\alpha_i} \\ &\leq \log \prod_{i=1}^{r} (2n) \\ &= \log (2n)^r \\ &= \pi(2n) \log(2n). \end{aligned}$$

Uma vez que

$$\binom{2n}{n} = \frac{2n}{n} \cdot \frac{2n-1}{n-1} \cdots \frac{n+1}{1},$$

e que, para $0 \leq k < n$

$$\frac{2n-k}{n-k} = 2 + \frac{k}{n-k} \geq 2,$$

então $\binom{2n}{n} \geq 2^n$. Logo,

$$\begin{aligned} \pi(2n) &\geq \frac{\log \binom{2n}{n}}{\log(2n)} \\ &\geq \frac{n \log 2}{\log(2n)} \\ &= \frac{2n \log 2}{2 \log(2n)}. \end{aligned}$$

Ou seja, para todo x par,

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

e como $\pi(2k) = \pi(2k-1)$, para $k > 1$, segue-se o resultado. □

Curiosamente, trazemos outra limitação para $\binom{2n}{n}$, desenvolvida por *James Stirling.*

Proposição 5.1.8. *Para todo n natural*

$$\binom{2n}{n} \sim \frac{2^{2n}}{\sqrt{\pi n}},$$

e, em particular,

$$\binom{2n}{n} < \frac{2^{2n}}{\sqrt{\pi n}}.$$

Demonstração. A demonstração desta proposição pode ser conferida em [9]. □

A Proposição 5.1.7 mostrou que a função $\pi(x)$ é $O(x/\log x)$. Logo, faz-se necessário estudar funções que relacionem números primos a logaritmos. Com esse intuito, apresentamos a primeira e a segunda funções de Chebyshev.

Definição 5.1.9. *A função $\vartheta : \mathbb{R}^+ \to \mathbb{R}$, denominada primeira função de Chebyshev, é definida por*

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

Alternativamente, fazendo uso de números primoriais,

$$\vartheta(x) = \log(x\#).$$

Exemplo 5.1.10. $\vartheta(10) = \log 2 + \log 3 + \log 5 + \log 7 = \log(10\#) = \log 210.$

Definição 5.1.11. *A função $\psi : \mathbb{R}^+ \to \mathbb{R}$, denominada segunda função de Chebyshev, é definida por*

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

onde

$$\Lambda(n) = \begin{cases} \log p, & \text{se } n \text{ é uma potência cuja base é } p; \\ 0, & \text{caso contrário.} \end{cases}$$

A função $\Lambda(n)$ é denominada função de Von Mangoldt.
Alternativamente, podemos escrever

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

Uma vez que, para todo x real não nulo, existe um k inteiro tal que

$$p^k \leq x < p^{k+1},$$

então

$$k \leq \log_p x < k + 1.$$

Logo, a segunda função de Chebyshev também pode ser dada por

$$\psi(x) = \sum_{p \leq x} \left\lfloor \frac{\log x}{\log p} \right\rfloor \log p = \log \operatorname{mmc}(1, 2, 3, ..., \lfloor x \rfloor)$$

Exemplo 5.1.12. *Para $\psi(10)$, temos:*

$$\begin{aligned}\psi(10) &= 3\log 2 + 2\log 3 + \log 5 + \log 7 \\ &= \log(2^3 \cdot 3^2 \cdot 5 \cdot 7) \\ &= \log 2.520\end{aligned}$$

Como a primeira e a segunda funções de Chebyshev fazem uso de logaritmos, podemos relacioná-las.

Proposição 5.1.13. *Seja x um número real. Então*

$$\psi(x) = \sum_{k=1}^{r} \vartheta\left(x^{\frac{1}{k}}\right),$$

onde $r = \left\lfloor \dfrac{\log x}{\log 2} \right\rfloor$.

Demonstração. Se $p^k \leq x$ então $p \leq x^{1/k}$, onde $k \in \mathbb{N}$. Logo,

$$\begin{aligned}\psi(x) &= \sum_{k=1}^{\infty} \sum_{p^k \leq x} \log p \\ &= \sum_{k=1}^{\infty} \vartheta\left(x^{\frac{1}{k}}\right)\end{aligned}$$

Uma vez que, para dado r inteiro, $2^r \leq x < 2^{r+1}$,

$$r \leq \frac{\log x}{\log 2}$$

então, $\vartheta\left(x^{\frac{1}{k}}\right) = 0$ para todo $k > r$. □

A partir da igualdade estabelecida entre $\vartheta(x)$ e $\psi(x)$ na Proposição 5.1.13, chegamos ao seguinte teorema.

Teorema 5.1.14. *Seja x um número real positivo. Então*

$$\lim_{x \to +\infty} \left(\frac{\psi(x)}{x} - \frac{\vartheta(x)}{x} \right) = 0.$$

Demonstração. Observe que

$$\begin{aligned}0 \leq \psi(x) - \vartheta(x) &= \sum_{n=1}^{\infty} \vartheta\left(x^{\frac{1}{n}}\right) - \vartheta(x) \\ &= \sum_{2 \leq n \leq \log_2 x} \vartheta\left(x^{\frac{1}{n}}\right).\end{aligned}$$

Por outro lado,

$$\begin{aligned}\vartheta(x) &= \log x\# \\ &\leq \log x^x \\ &= x \log x\end{aligned}$$

logo,

$$\begin{aligned} 0 \leq \sum_{2 \leq n \leq \log_2 x} \vartheta\left(x^{\frac{1}{n}}\right) &\leq \sum_{2 \leq n \leq \log_2 x} x^{1/n} \log x^{1/n} \\ &\leq (\log_2 x) x^{1/2} \log x^{1/2} \\ &\leq \frac{\sqrt{x}(\log x)^2}{2 \log 2}. \end{aligned}$$

Como $x > 0$, temos que

$$0 \leq \frac{\psi(x)}{x} - \frac{\vartheta(x)}{x} \leq \frac{(\log x)^2}{2\sqrt{x} \log 2}.$$

Daí, como

$$\lim_{x \to +\infty} \frac{(\log x)^2}{2\sqrt{x} \log 2} = 0,$$

temos que

$$\lim_{x \to +\infty} \left(\frac{\psi(x)}{x} - \frac{\vartheta(x)}{x} \right) = 0.$$

□

Observe que, pelo Teorema 5.1.14, para um x grande,

$$\frac{\psi(x)}{\vartheta(x)} \sim \frac{\frac{\psi(x)}{x}}{\frac{\vartheta(x)}{x}} \sim 1$$

Mesmo diante deste fato, nosso foco será comparar a função $\pi(x)$ com a função $\psi(x)$. Sendo assim, trazemos a equivalência a seguir.

Proposição 5.1.15.

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

Demonstração. Temos que

$$\begin{aligned} \psi(x) &= \sum_{p \leq x} \left\lfloor \frac{\log x}{\log p} \right\rfloor \log p \\ &\leq \log x \sum_{p \leq x} 1. \end{aligned}$$

Ou seja,

$$\psi(x) \leq \pi(x) \cdot \log x. \tag{5.2}$$

Por outro lado, tomando y real tal que $1 < y < x$, estabelecemos a seguinte relação entre a quantidade de números primos pertencentes ao intervalo $(y, x]$.

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

Note que, para $x > e$,

$$1 < \frac{x}{(\log x)^2} < x,$$

logo, fazendo $y = \dfrac{x}{(\log x)^2}$

$$\begin{aligned} \pi(x) &< \frac{x}{(\log x)^2} + \frac{\psi(x)}{\log\left(x/(\log x)^2\right)} \\ &= \frac{x}{(\log x)^2} + \frac{\psi(x)}{\log x - 2\log\log x}. \end{aligned} \tag{5.3}$$

A partir das desigualdades 5.2 e 5.3, escrevemos

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

Uma vez que $x > 0$,

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

Assim, como $\lim\limits_{x\to+\infty} \dfrac{1}{\log x} = 0$ e $\lim\limits_{x\to+\infty} \dfrac{\log x}{\log x - 2\log\log x} = 1$,

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

□

Observe que para concluírmos a demonstração do Teorema dos Números Primos dependemos da análise da função $\psi(x)/x$ e da prova de que $\lim\limits_{x\to+\infty} \dfrac{\psi(x)}{x} = 1$. Iniciaremos este processo mostrando o comportamento assintótico da função $\psi(x)$, de modo análogo à Proposição 5.1.7. Tal resultado confirma o fato posto na Proposição 5.1.15.

Proposição 5.1.16. *A função $\psi(x)$ é $O(x)$.*

Demonstração. Do Corolário 5.1.4, temos que

$$\frac{(2n)\#}{n\#} \leq \binom{2n}{n} < 2^{2n}.$$

Ou seja,

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

Daí, temos que

$$\log\left((2n)\#\right) - \log(n\#) < 2n\log 2,$$

ou ainda,

$$\vartheta(2n) - \vartheta(n) < 2n\log 2.$$

Em particular, para k inteiro positivo, vale a desigualdade

$$\vartheta(2^k) - \vartheta(2^{k-1}) < 2^k \log 2.$$

Assim, temos que

$$\begin{array}{rcl} \vartheta(2^k) - \vartheta(2^{k-1}) & < & 2^k \log 2 \\ \vartheta(2^{k-1}) - \vartheta(2^{k-2}) & < & 2^{k-1} \log 2 \\ & \vdots & \\ \vartheta(2^2) - \vartheta(2) & < & 2^2 \log 2 \\ \vartheta(2) & < & 2 \log 2. \end{array}$$

Fazendo a soma telescópica das desigualdades, obtemos

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

Como, para todo x real, existe um k inteiro tal que $2^{k-1} < x \leq 2^k$, então

$$\begin{aligned} \vartheta(x) &\leq \vartheta(2^k) \\ &< 2^{k+1} \log 2 \\ &= (4 \log 2) \cdot 2^{k-1} \\ &< (4x \log 2). \end{aligned}$$

Para $p > 0$, temos que se $p^r \leq x$, então $p \leq x^{r^{-1}}$. Logo, para $r \geq 2$ fixo,

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

Pela Proposição 5.1.13,

$$\begin{aligned} \psi(x) &= \sum_{n=1}^{r} \vartheta\left(x^{\frac{1}{n}}\right) \\ &= \vartheta(x) + \vartheta(x^{1/2}) + \vartheta(x^{1/3}) + \cdots + \vartheta(x^{1/r}). \end{aligned}$$

onde $r \in \mathbb{Z}$, e $r = \left\lfloor \dfrac{\log x}{\log 2} \right\rfloor$. Então,

$$\begin{aligned} \psi(x) &\leq 4x \log 2 + \sum_{i=2}^{r} 4x^{1/i} \log 2 \\ &\leq 4x \log 2 + \sum_{i=2}^{r} 4x^{1/2} \log 2 \\ &= 4x \log 2 + 4x^{1/2} \log 2 \sum_{i=2}^{r} 1 \\ &= 4x \log 2 + 4x^{1/2} \log 2 \cdot (r-1) \\ &< 4x \log 2 + 4x^{1/2} \log 2 \cdot \frac{\log x}{\log 2} \\ &= 4x \log 2 + 4x^{1/2} \log x. \end{aligned}$$

Visto que

$$\lim_{x\to+\infty}\frac{4x\log 2}{4x^{1/2}\log x}=\lim_{x\to+\infty}\frac{x^{1/2}\log 2}{\log x}=+\infty,$$

então, existe $a>0$ real,

$$\begin{aligned}4x\log 2+4x^{1/2}\log x &< 4x\log 2+4x\log 2\\ &= 8x\log 2\end{aligned}$$

para todo $x>a$, mostrando que $\psi(x)$ é $O(x)$. □

5.2 A função Zeta

O primeiro matemático a estudar a função zeta foi Leonard Euler, no século XVII. Mesmo sendo um matemático brilhante, algumas vezes usou artifícios para convergência de somas finitas para afirmar que séries infinitas covergiam. Ainda assim, conseguiu obter resultados verdadeiros e brilhantes, que mudaram o rumo da história da Matemática. Em 1735, Euler apresentou a solução para o famoso *Problema da Basiléia*, que relaciona a soma dos inversos dos quadrados dos números naturais, fazendo referência à função zeta.

Na referida demonstração, Euler usou a expansão em séries de potência para a função $\operatorname{sen} x$

$$\operatorname{sen} x=x-\frac{x^3}{3!}+\frac{x^5}{5!}+\cdots.$$

Em seguida, considerou que, para $x\neq 0$, vale a igualdade

$$\frac{\operatorname{sen} x}{x}=1-\frac{x^2}{3!}+\frac{x^4}{5!}+\cdots.$$

Assim, considerando $x\neq 0$, afirmou que os zeros para a função $f(x)=(\operatorname{sen} x)/x$ coincidiam com os zeros de sua respectiva representação em série de potências. Uma vez que os zeros para a função $(\operatorname{sen} x)/x$ eram da forma $x=\pm n\pi$, com $n\neq 0$, Euler considerou válida a igualdade

$$\begin{aligned}\frac{\operatorname{sen} x}{x} &= \prod_{k=1}^{\infty}\left(1-\frac{x}{\pi k}\right)\left(1+\frac{x}{\pi k}\right)\\ &= \prod_{k=1}^{\infty}\left(1-\frac{x^2}{\pi^2k^2}\right),\end{aligned}$$

sem verificar se, de fato, o produtório convergia para a série de potências. Assim, concluiu que

$$\prod_{k=1}^{\infty}\left(1-\frac{x^2}{\pi^2k^2}\right)=1-\frac{x^2}{3!}+\frac{x^4}{5!}+\cdots.$$

Comparando o termo em x^2 obtido após o desenvolvimento do produtório pertencente ao primeiro membro, com o termo $-x^2/3!$ pertencente ao segundo membro, obteve a igualdade

$$\frac{1}{\pi^2}\sum_{n=1}^{\infty}\frac{1}{n^2}=\frac{1}{3!},$$

de onde tem-se que

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}.$$

Esta demonstração recebeu críticas, uma vez que as devidas observações mais rigorosas no campo analítico foram ignoradas. Ainda assim, a identidade é válida. Uma prova rigorosa do Problema da Basiléia é encontrada em [10], fazendo-se o uso de uma interpretação geométrica.

Em 1858, Riemann estudou o conhecido *Produto de Euler* utilizando técnicas de variáveis complexas, e fundamentou suas afirmações na teoria das funções analíticas. A função estudada por Riemann foi intitulada *função Zeta de Riemann.*

Definição 5.2.1. *A função $\zeta(s)$, denominada função zeta de Riemann, é a única extensão da função dada pela série $\sum_{n=1}^{\infty} \frac{1}{n^s}$, para o plano complexo $\mathbb{C}$, onde $\operatorname{Re} s > 1$. Esta extensão representa uma função analítica, à exceção dos polos.*

Ou seja, para cada valor $s \in \mathbb{C}$, com $\operatorname{Re} s > 1$, a série $\sum_{n=1}^{\infty} \frac{1}{n^s}$ converge.

Em sua análise, Riemann relacionou a convergência de $\sum_{n=1}^{\infty} \frac{1}{n^s}$ à convergência do produtório $\prod_{p} \frac{1}{1-p^{-s}}$. Esta relação é chamada de produto de Euler.

Teorema 5.2.2. *Seja $s \in \mathbb{C}$. Se $\operatorname{Re} s > 1$, então valem:*

(a)(Fórmula de Euler)

$$\zeta(s) = \prod_{p} \frac{1}{1-p^{-s}}$$

(b) $\zeta(s) \neq 0$.

Demonstração. Conside $s \in \mathbb{C}$ fixo, onde $\operatorname{Re} s > 1$. Temos que a série geométrica $\sum_{n=0}^{\infty} \frac{1}{p^{ns}}$ converge para $\frac{1}{1-p^{-s}}$. Daí, escrevemos

$$\left(1 + \frac{1}{2^s} + \frac{1}{(2^s)^2} + \frac{1}{(2^s)^3} + \cdots\right)\left(1 + \frac{1}{3^s} + \frac{1}{(3^s)^2} + \frac{1}{(3^s)^3} + \cdots\right)$$
$$= 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{6^s} + \frac{1}{8^s} + \frac{1}{9^s} + \cdots$$

Perceba que cada parcela deste último somatório é da forma $\frac{1}{(2^{k_1} \cdot 3^{k_2})^s}$, onde $k_1, k_2 \in \mathbb{N} \cup \{0\}$.

De modo análogo, desenvolvendo o produto

$$\left(1 + \frac{1}{2^s} + \frac{1}{(2^s)^2} + \frac{1}{(2^s)^3} + \cdots\right)\left(1 + \frac{1}{3^s} + \frac{1}{(3^s)^2} + \frac{1}{(3^s)^2} + \cdots\right)\left(1 + \frac{1}{5^s} + \frac{1}{(5^s)^2} + \frac{1}{(5^s)^3} + \cdots\right)$$

obtemos um somatório com infinitas, cada uma delas é da forma $\frac{1}{(2^{k_1}\cdot 3^{k_2}\cdot 5^{k_3})^s}$, onde $k_1, k_2, k_3 \in \mathbb{N}\cup\{0\}$. Tomando um produto finito de séries absolutamente convergentes, temos que

$$\prod_{p\leq x}\frac{1}{1-p^{-s}} = \sum_{n\in N_x}\frac{1}{n^s},$$

onde N_x é o conjunto dos números naturais cujos fatores primos são menores ou iguais a x. Como qualquer número natural pertencente ao intervalo $[1,x]$ também é elemento de N_x, então

$$\left|\zeta(s) - \prod_{p\leq x}\frac{1}{1-p^{-s}}\right| \leq \sum_{n>x}\left|\frac{1}{n^s}\right|$$

Pela Proposição 4.5.5, a série $\sum_{n=1}^{\infty}\frac{1}{n^s}$ converge absolutamente em $\operatorname{Re} s > 1$, ou seja, $\lim_{x\to\infty}\sum_{n>x}\left|\frac{1}{n^s}\right| = 0$. Consequentemente, $\prod_{p\leq x}\frac{1}{1-p^{-s}}$ tende a $\zeta(s)$. Isto prova (a).

Para provar a afirmativa (b), basta mostrar que

$$\frac{1}{|\zeta(s)|} < +\infty.$$

Para tanto, partiremos da igualdade provada em (a). Observe que, para todo α real pertencente ao intervalo $(1, \operatorname{Re} s]$, pela desigualdade triangular vale

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

Denotemos por p_i o i-ésimo número primo. Observe que

$$\log\prod_{i=1}^{n}\left(1+\frac{1}{p_i^\alpha}\right) = \sum_{i=1}^{n}\log\left(1+\frac{1}{p_i^\alpha}\right). \tag{5.4}$$

Como consequência do Exemplo 4.5.2, $\sum_{i=1}^{\infty}\frac{1}{p_i^\alpha}$ converge. Denotemos $\sum_{i=1}^{\infty}\frac{1}{p_i^\alpha} = \frac{S}{2}$ e $\frac{1}{p_i^\alpha} = c_i$. Fazendo uso da representação em série de potências como no Exemplo 4.5.20, e considerando $m\in\mathbb{N}$, temos que

$$\begin{aligned}
\log\prod_{i=1}^{n}(1+c_i) &= \sum_{i=1}^{n}\sum_{m\geq 1}\frac{(-1)^{m+1}c_i^m}{m} \\
&\leq \sum_{i=1}^{n}\sum_{m\geq 1}c_i^m \\
&= \sum_{i=1}^{n}c_i + \sum_{i=1}^{n}\sum_{m\geq 2}c_i^m.
\end{aligned}$$

Uma vez que $\sum_{m\geq 2} c_i^m$ converge,

$$\begin{aligned}\log\prod_{i=1}^{n}(1+c_i) &\leq \sum_{i=1}^{n} c_i + \sum_{i=1}^{n}\frac{c_i^2}{1-c_i}\\ &= \sum_{i=1}^{n} c_i + \sum_{i=1}^{n} c_i\cdot\frac{c_i}{1-c_i}.\end{aligned}$$

Como, para todo i, $c_i < \frac{1}{2}$, tem-se que $\frac{c_i}{1-c_i} < 1$. Então

$$\begin{aligned}\log\prod_{i=1}^{n}(1+c_i) &\leq 2\sum_{i=1}^{n} c_i\\ &\leq 2\sum_{i=1}^{\infty} c_i.\end{aligned}$$

Note que, por maior que seja n, o logaritmo do produtório em 5.4 é finito e limitado por S. Assim, podemos escrever que,

$$\lim_{n\to\infty}\prod_{i=1}^{n}\left(1+\frac{1}{p_i^{\alpha}}\right)\leq e^{S},$$

de onde concluímos que

$$\prod_{p}\left(1+\frac{1}{p^{\alpha}}\right)^{-1}\geq e^{-S}>0.$$

□

Este teorema traz uma grande ferramenta para o estudo da função zeta. Uma vez que tal função não se anula para $\operatorname{Re} s > 1$, podemos tomar logaritmos da função para quaisquer valores de s sobre esta região do plano complexo. Com base neste resultado, vamos analisar a demonstração proposta por Euler para o Teorema de Euclides acerca da infinitude dos números primos.

Pela Fórmula de Euler, tomando um valor real $a > 1$, vale a igualdade

$$\log\zeta(a) = \log\left(\sum_{n=1}^{\infty}\frac{1}{n^a}\right) = -\sum_{p}\log\left(1-\frac{1}{p^a}\right).$$

De modo análogo à demonstração do Teorema 5.2.2 (b), sendo $m\in\mathbb{N}$,

$$\begin{aligned}\log\zeta(a) &= \sum_{p}\sum_{m=1}^{\infty}\frac{1}{mp^{ma}}\\ &= \sum_{p}\frac{1}{p^a}+\sum_{p}\sum_{m=2}^{\infty}\frac{1}{mp^{ma}}\\ &< \sum_{p}\frac{1}{p^a}+\sum_{p}\sum_{m=2}^{\infty}\frac{1}{p^m}.\end{aligned}$$

Como $\sum_{m=2}^{\infty} \frac{1}{p^m}$ converge para $\frac{1}{p(p-1)}$, temos que

$$\begin{aligned}
\log \zeta(a) &< \sum_p \frac{1}{p^a} + \sum_p \frac{1}{p(p-1)} \\
&< \sum_p \frac{1}{p^a} + \sum_{n=2}^{\infty} \frac{1}{n(n-1)} \\
&= \sum_p \frac{1}{p^a} + 1 \\
&< \sum_p \frac{1}{p} + 1.
\end{aligned}$$

Assim, a convergência de $\sum_p \frac{1}{p^a}$ está atrelada à convergência de $\sum_{n=1}^{\infty} \frac{1}{n^a}$. Se $\sum_p \frac{1}{p}$ converge, então $\lim_{a \to +\infty} \log \zeta(a) < +\infty$, ou seja, $\sum_{n=1}^{\infty} \frac{1}{n}$ converge. Assim, conclui-se que há infinitos números primos.

Antes de enunciarmos uma aplicação para a função zeta, precisamos definir um tipo especial de número composto: os números livres de quadrados.

Definição 5.2.3. *Um número natural n é dito livre de quadrados se n não existe p tal que $p^2 \mid n$.*

Esta noção pode ser estendida para inteiros livres de cubos, de potência 4, e assim sucessivamente.

Vejamos um problema pertinente envolvendo a função $\zeta(s)$, o produto de Euler a ideia de inteiros livres de quadrados.

Exemplo 5.2.4. *O espaçamento médio entre inteiros não-negativos livres de quadrados é $\frac{\pi^2}{6}$.*

De fato. Observe a tabela 5.1.

1	2	3	4	5	6	7	8	9	10	11	12
13	14	15	16	17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32	33	34	35	36

Tabela 5.1: Números livres de fator 2^2 pertencentes ao intervalo $[0, 36]$.

Perceba que a cada 4 números interios, um é múltiplo de 2^2. Logo, no intervalo $[0, 36]$, a distância média entre inteiros livres de fatores 2^2 é $\frac{4}{3}$ ou, aproximadamente, 1,333.

Na tabela 5.2, pode-se observar ainda o intervalo $[0, 36]$, onde destacamos os números que são divisíveis por 4 ou por 9.

Perceba que a distância média entre os inteiros livres de fator 2^2 ou 3^2 é $\frac{4}{3} \cdot \frac{9}{8} = \frac{3}{2} = 1{,}5$.

1	2	3	4	5	6	7	8	9	10	11	12
13	14	15	16	17	18	19	20	21	22	23	24
25	26	27	28	29	30	31	32	33	34	35	36

Tabela 5.2: Números livres de fatores 2^2 ou 3^2 pertencentes ao intervalo $[0, 36]$.

Recursivamente, temos que, no intervalo $[0, (p_k\#)^2]$, *a distância média entre inteiros livres de fatores* 2^2, 3^2, ..., p_k^2, *onde* k *é o* k*-ésimo número primo é*

$$\frac{2^2}{2^2-1} \cdot \frac{3^2}{3^2-1} \cdots \frac{p_k^2}{p_k^2-1}$$

Esta distância média permanece inalterada se tomarmos o intervalo $[0, (p_k\#)^2]$, *para* $c \in \mathbb{N}$.

Fazendo $k \to \infty$, *temos que o espaçamento médio entre inteiros livres de quadrados é dada por*

$$\prod_{i=1}^{\infty} \left(1 - \frac{1}{p_i^2}\right)^{-1}$$

Pelo Teorema 5.2.2

$$\prod_{i=1}^{\infty} \left(1 - \frac{1}{p_i^2}\right)^{-1} = \sum_{n=1}^{\infty} \frac{1}{n^2} = \zeta(2),$$

e, pelo problema da Basileia,

$$\zeta(2) = \frac{\pi^2}{6}.$$

Logo, a distância média entre inteiros não-negativos livres de quadrados é

$$\frac{\pi^2}{6} \approx 1{,}645$$

De modo análago, temos que o espaçamento médio entre inteiros livres de cubos é dada por

$$\frac{2^3}{2^3-1} \cdot \frac{3^3}{3^3-1} \cdots \frac{p^3}{p^3-1} \cdots = \prod_{i=1}^{\infty} \left(1 - \frac{1}{p_i^3}\right)^{-1} = \zeta(3)$$

Sendo assim, concluímos que o espaçamento médio entre livres de fatores do tipo p^n é $\zeta(n)$, $n \in \mathbb{N}$, com $n > 1$.

Uma consequência para o Exemplo 5.2.4 é observada no cálculo da probabilidade em obtermos um número natural n livre de quadrados, tomado aleatoriamente. Escolhendo n pertencente ao intervalo $[0, 36c]$, $c \in \mathbb{N}$, a probabilidade n não ser divisível por 2^2 é

$$1 - \frac{1}{4} = \frac{3}{4}$$

e a probabilidade de n não ser divisível por 3^2 é

$$1 - \frac{1}{9} = \frac{8}{9}.$$

Logo, a probabilidade de n, tomado aleatoreamente num intervalo $[0, 36c]$, não ser divisível por 2^2 ou por 3^2 é

$$\left(1-\frac{1}{4}\right)\left(1-\frac{1}{9}\right).$$

Seguindo os mesmos passos do Exemplo 5.2.4, observamos que a probabilidade de um número natural n, tomado aleatoriamente, ser livre de quadrados é dado por

$$\prod_{i=1}^{\infty}\left(1-\frac{1}{p_i^2}\right)=\frac{1}{\zeta(2)}=\frac{6}{\pi^2}$$

ou, aproximadamente, 60,79%.

De posse do Teorema 5.2.2 e da Proposição4.5.5, onde mostramos que $\sum_{n=1}^{\infty}\frac{1}{n^s}$ não converge para $s=1$, nossa análise se baseará na investigação da existência de *polos* para a função zeta.

Vejamos um lema que nos ajudará a identificar os polos para a função zeta em $\operatorname{Re} s > 0$, particularmente, para $s=1$. Este lema relaciona uma função expressa por uma série de potências e a definição de integral. Tal lema é conhecido por *Lema da representação integral.*

Lema 5.2.5. *Sejam $f(s)$ uma função analítica, à exceção dos polos, e $(a_n)_{n\in\mathbb{N}}$ uma sequência de números complexos tal que $f(s)=\sum_{n=1}^{\infty}\frac{a_n}{n^s}$, em $\operatorname{Re} s > a$, para dado $a\in\mathbb{R}$. Sendo $P(x)=\sum_{n\leq x}a_n$, se $\sum_{n=1}^{\infty}\frac{P(n)}{n^s}$ e $\sum_{n=1}^{\infty}\frac{P(n-1)}{n^s}$ convergem em $\operatorname{Re} s > b$, e $\int_1^{\infty}P(x)x^{-1-s}dx$ representa uma função analítica em $\operatorname{Re} s > c$, para certos $b, c\in\mathbb{R}$, então*

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

em $\operatorname{Re} s > c$.

Demonstração. Para $\operatorname{Re} s > \max\{a, b\}$, vale que

$$f(s) \;=\; \sum_{n=1}^{\infty}\frac{a_n}{n^s}.$$

Observe que se $x<1$, então $P(x)=0$. Daí, temos que

$$f(s) \;=\; \sum_{n=1}^{\infty}\frac{P(n)}{n^s}-\sum_{n=1}^{\infty}\frac{P(n-1)}{n^s}.$$

Reescrevendo o último somatório,

$$\begin{aligned} f(s) &= \sum_{n=1}^{\infty}\frac{P(n)}{n^s}-\sum_{n=1}^{\infty}\frac{P(n)}{(n+1)^s} \\ &= \sum_{n=1}^{\infty}P(n)\left(\frac{1}{n^s}-\frac{1}{(n+1)^s}\right), \end{aligned}$$

e, fazendo o uso da definição de integral,

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

Uma vez que $g(s) = s$ é uma função analítica, bem como $h(s) = \displaystyle\int_1^{\infty} P(x)x^{-1-s}dx$, e o produto de duas funções analíticas é uma função analítica, então $f(s)$ também é analítica em $\operatorname{Re} s > c$. □

Com base no Lema 5.2.5, podemos analisar a função zeta na proposição a seguir.

Proposição 5.2.6. *A função $\zeta(s)$ possui um único polo em $\operatorname{Re} s > 0$, sendo este polo simples em $s = 1$, com resíduo 1.*

Demonstração. Nosso objetivo será verificar se a função $\zeta(s)$ possui singularidade em $s = 1$. Seja $P(x) = \lfloor x \rfloor$. Então temos que

$$\sum_{n=1}^{\infty}\frac{P(n)}{n^s} = \sum_{n=1}^{\infty}\frac{1}{n^{s-1}} \qquad \text{e} \qquad \sum_{n=1}^{\infty}\frac{P(n-1)}{n^s} = \sum_{n=1}^{\infty}\left(\frac{1}{n^{s-1}} - \frac{1}{n^s}\right)$$

são séries convergentes em $\operatorname{Re} s > 2$. Além disso, $f(s) = \displaystyle\int_1^{\infty} P(x)x^{-1-s}dx$ representa uma função analítica em $\operatorname{Re} s > 1$. Então, pelo Lema 5.2.5

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

Daí, temos que

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

Como esta última integral é convergente em $\operatorname{Re} s > 0$, representa uma função analítica neste domínio, de onde concluímos que $\zeta(s)$ possui pólo em $s = 1$, com resíduo 1. □

Uma vez que podemos tomar logaritmos para quaisques valores de $\zeta(s)$ tais que $\operatorname{Re} s > 1$, precisamos analisar a existência de pólos para $\dfrac{\zeta'(s)}{\zeta(s)}$. Para tanto, vejamos a seguinte proposição.

Proposição 5.2.7. *$\zeta(s) \neq 0$ sobre a fronteira do semiplano $\{z \in \mathbb{C} \mid \operatorname{Re}(s) > 1\}$.*

Demonstração. Faremos nossa prova por contradição. Antes disto, vejamos uma pequena estimativa acerca da expressão $3+4\cos(x)+\cos(2x)$. Observe que, para qualquer x real

$$\begin{aligned} 3+4\cos(x)+\cos(2x) &= 3+4\cos(x)+\cos(x)^2-\operatorname{sen}(x)^2 \\ &= 3+4\cos(x)+\cos(x)^2-(1-\cos(x)^2) \\ &= 2+4\cos(x)+2\cos(x)^2 \\ &= 2(1+\cos(x))^2 \geq 0. \end{aligned}$$

Voltando para a prova da nossa proposição, suponha que $\zeta(1+bi)=0$ para algum $b\in\mathbb{R}^*$. Além disso, uma vez que não temos uma expressão para a $\zeta(s)$ em $\operatorname{Re} s=1$, considere a função

$$\varphi(s)=\zeta^3(s)\zeta^4(s+ib)\zeta(s+2ib).$$

Por hipótese, $\zeta^4(s+ib)$ tem um zero de ordem, pelo menos, quatro em $s=1$. Assim, mesmo diante do polo de ζ em $s=1$, $\varphi(s)$ se anula neste ponto. Deste modo,

$$\lim_{s\to 1}\log|\varphi(s)|=-\infty. \tag{5.5}$$

Considere agora $s,t\in\mathbb{R}$, onde $s>1$. Então

$$\begin{aligned} \log|\zeta(s+it)| &= \log\left|\prod_p(1-p^{-s-it})^{-1}\right| \\ &= -\operatorname{Re}\sum_p\log(1-p^{-s-it}). \end{aligned}$$

e, pelo Exemplo 4.5.20

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

onde $a_n=1$, se n for primo, e $a_n=0$, caso contrário. Sendo assim,

$$\begin{aligned} \log|\varphi(s)| &= \operatorname{Re}\log|\zeta^3(s)\zeta^4(s+ib)\zeta(s+2ib)| \\ &= \operatorname{Re}\left(\log|\zeta(s)|^3+\log|\zeta(s+ib)|^4+\log|\zeta(s+2ib)|\right) \\ &= \operatorname{Re}\left(3\log|\zeta(s)|+4\log|\zeta(s+ib)|+\log|\zeta(s+2ib)|\right) \\ &= \operatorname{Re}\left(3\sum_{n=1}^{\infty}a_n n^{-s}+4\sum_{n=1}^{\infty}a_n n^{-s-ib}+\sum_{n=1}^{\infty}a_n n^{-s-2it}\right) \\ &= \operatorname{Re}\sum_{n=1}^{\infty}a_n n^{-s}(3+4n^{-ib}+n^{-2ib}) \end{aligned}$$

Como $\operatorname{Re} n^{-ib} = \cos(b \log n)$, e $\operatorname{Re} n^{-2ib} = \cos(2b \log n)$, então

$$\log |\varphi(s)| = \sum_{n=1}^{\infty} a_n n^{-s}(3 + 4\cos(b \log n) + \cos(2b \log n)) \geq 0$$

o que contradiz a igualdade 5.5. □

Vejamos uma função que dá um excelente suporte para o estudo da função zeta: a função gama.

Definição 5.2.8. *A função gama, $\Gamma(s)$, é a função analítica em $\mathbb{C} - \{0, -1, -2, \ldots\}$, dada pelo limite da sequência de funções*

$$\Gamma_n(s) = \frac{n! n^s}{s(s+1)\cdots(s+n)}$$

A função gama goza das seguintes propriedades:

a) $\Gamma(s)$ possui pólos em 0, −1, −2, ..., e todos estes são de ordem 1.

b) $\Gamma(s) \neq 0$ para todo $s \in \mathbb{C}$.

c) Se $x \in \mathbb{R}$, $x > 0$, então $\Gamma(x) > 0$.

d) $\Gamma(s+1) = s \cdot \Gamma(s)$ para todo $s \in \mathbb{C} - \{0, -1, -2, \ldots\}$.

Convém observar que a função gama é uma extensão da função fatorial

$$\Gamma(n+1) = n!$$

onde $n \in \mathbb{N}$.

Para um estudo detalhado acerca da função gama, recomendamos a leitura de [6].

Teorema 5.2.9. *A função $\Gamma(s)$ admite representação por integral, dada por*

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

para $\operatorname{Re} s > 0$.

Demonstração. Veja [6]. □

Com o auxílio desta função, obtem-se uma extensão da função zeta de Riemann para o plano complexo.

Proposição 5.2.10. *A função zeta de Riemann satisfaz uma equação denominada equação funcional de Riemann, dada por*

$$\pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \pi^{-(1-s)/2}\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s)$$

onde $s \in \mathbb{C}$.

Demonstração. Para a demonstração desta proposição, recomendamos a leitura de [6]. □

Como $\Gamma(s)$ possui pólos em 0, −1, −2, ..., chegamos ao seguinte corolário.

Corolário 5.2.11. *A função zeta de Riemann se anula para $s = -2, -4, -6, \ldots$. Estes zeros são chamados zeros triviais da função zeta.*

Diante dos resultados postos até aqui, precisamos analisar um pouco mais a função $\dfrac{\zeta'(s)}{\zeta(s)}$.

Proposição 5.2.12. *A função $-\dfrac{\zeta'(s)}{\zeta(s)} - \dfrac{1}{s-1}$ possui continuação analítica sobre a reta* $\operatorname{Re} s = 1$.

Demonstração. Na Proposição 5.2.6, vimos que

$$\zeta(s) = 1 + \frac{1}{s-1} + s\int_1^\infty (\lfloor x \rfloor - x)x^{-1-s}dx \tag{5.6}$$

mostrando que a função $\zeta(s)$ é analítica em $\operatorname{Re} s > 0$, e só possui um polo, sendo este simples em $s = 1$, com resíduo 1.

Da igualdade 5.6, podemos escrever

$$(s-1)\zeta(s) = (s-1) + 1 + (s-1)s\int_1^\infty (\lfloor x \rfloor - x)x^{-1-s}dx \tag{5.7}$$

Aplicando o logaritmo aos membros da equação 5.7,

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

de onde obtemos que

$$\log(s-1) + \log\zeta(s) = \log\left((s-1) + 1 + (s-1)s\int_1^\infty (\lfloor x \rfloor - x)x^{-1-s}dx\right) \tag{5.8}$$

Como na Proposição 5.2.7, garantimos que $\zeta(s) \neq 0$ em $\operatorname{Re} s = 1$, derivando ambos os membros da igualdade 5.8, temos que a função $-\dfrac{\zeta'(s)}{\zeta(s)} - \dfrac{1}{s-1}$ é analítica sobre a reta $\operatorname{Re} s = 1$, onde a função $-\dfrac{\zeta'(s)}{\zeta(s)}$ possui polo de tipo $\dfrac{1}{s-1}$ único, com resíduo igual a 1. Além disso, a Proposição 5.2.2 também garante que $-\dfrac{\zeta'(s)}{\zeta(s)} - \dfrac{1}{s-1}$ é analítica em $\operatorname{Re} s > 1$. □

De posse de todos os resultados desta seção, vamos estabelecer uma relação entre a função e $\zeta(s)$ a função $\pi(x)$, fazendo o uso da função $\psi(x)$. Assim, criaremos mais uma importante ferramenta para a demonstração do Teorema dos Números Primos.

Proposição 5.2.13. *A função $g(s) = s\displaystyle\int_1^\infty \psi(x)x^{-1-s}dx$ é analítica em $\operatorname{Re} s > 1$, e neste domínio $g(s) = -\dfrac{\zeta'(s)}{\zeta(s)}$.*

Demonstração. Como $\psi(n) = \log \operatorname{mmc}(1, 2, ..., n)$, temos que

$$\begin{aligned} \psi(x) &\leq \log x! \\ &\leq \log x^x \\ &\leq x \log x \end{aligned}$$

Então, $\displaystyle\int_1^\infty \psi(x) x^{-1-s} dx$ converge e $g(s)$ representa uma função analítica neste domínio.

Por outro lado, se $\operatorname{Re} s > 1$, pelo Teorema 5.2.2

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

Daí,

$$\begin{aligned} \log \zeta(s) &= -\sum_p \log(1 - p^{-s}) \\ &= \sum_p \sum_{m=1}^{\infty} \frac{1}{m p^{ms}}. \end{aligned}$$

Como, para todo s tal que $\operatorname{Re} s > 1$, esta última série converge, então, fazendo uso das regras de derivação:

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

Daí, pelo Exemplo 4.5.2,

$$\begin{aligned} -\frac{\zeta'(s)}{\zeta(s)} &= \sum_p \left(\sum_{j=1}^{\infty} p^{-js} \right) \log p \\ &= \sum_p \sum_{j=1}^{\infty} \log p \, (p^j)^{-s} \\ &= \sum_{n=1}^{\infty} \Lambda(n) n^{-s}. \end{aligned}$$

Por fim, tome $a_n = \Lambda(n)$ e $P(x) = \psi(x)$ aplicados ao Lema 5.2.5. Uma vez que $\psi(n) \leq n^2$, como $\displaystyle\int_1^\infty x^{-1-s} dx$ converge para $\operatorname{Re} s > 3$, então $\displaystyle\int_1^\infty \psi(x) x^{-1-s} dx$ também converge no mesmo domínio. Tomando

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

segue que

$$g(s) = \frac{\zeta'(s)}{\zeta(s)}$$

em $\operatorname{Re} s > 1$. □

5.3 Transformadas de Laplace e Mellin

A partir da Proposição 5.2.12, que analisou a existência de possíveis polos para a função $\zeta(s)$, conseguimos mostrar que a função $-\dfrac{\zeta'(s)}{\zeta(s)} - \dfrac{1}{s-1}$ possui continuação analítica sobre a reta $\operatorname{Re} s = 1$. Posteriormente, através da Proposição 5.2.13, conseguimos mostrar que a função $g(s) = s\displaystyle\int_1^\infty \psi(x)x^{-1-s}dx$ é analítica em $\operatorname{Re} s > 1$, e neste domínio $g(s) = -\dfrac{\zeta'(s)}{\zeta(s)}$, fazendo o uso do Lema 5.2.5 aplicado a séries de potências e à função $\psi(x)$. Além disso, como

$$\int_1^\infty \psi(x)x^{-1-s}dx = \int_1^\infty (\psi(x) + x - x)x^{-1-s}dx,$$

para $\operatorname{Re} s > 1$, então, pela Proposição 5.2.12, vale a identidade

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

Mas, diante desse cenário, faz-se necessário verificar se $\displaystyle\int_1^\infty (\psi(x) - x)x^{-1-s}dx$ converge para $\operatorname{Re} s = 1$. O objetivo central desta seção é mostrar a convergência de tal integral, e garantir que exista o limite da função $\dfrac{\psi(x)}{x}$ para $x \to +\infty$, onde tal limite será 1. Para tanto, faremos uso de alguns teoremas relacionados a transformadas de Laplace e Mellin, conhecidos como *Teoremas Tauberianos*.

Lema 5.3.1. *Seja a função $F : (0, \infty) \to \mathbb{R}$ limitada e integrável em qualquer subintervalo finito. Então sua transformada de Laplace, dada por*

$$G(s) = \int_0^\infty F(t)e^{-st}dt$$

está bem definida e é analítica no semiplano $\operatorname{Re} s > 0$.

Demonstração. Deixamos como referência para esta demonstração [7]. □

Lema 5.3.2. *Seja a função $f : [1, \infty) \to \mathbb{R}$ integrável em qualquer subintervalo finito e $O(x)$. Então sua transformada de Mellin, dada por*

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

está bem definida e é analítica no semiplano $\operatorname{Re} s > 1$.

Demonstração. Como a função f é $O(x)$, então existem $\lambda, C \in \mathbb{R}$, $C > 0$ e $\lambda > 1$, tal que para $x > \lambda$ e C real positivo fixo,

$$|f(x)| < C|x|.$$

Se $m \leq \operatorname{Re} s$ e $m > 1$, então

$$\begin{aligned}\left|\int_\lambda^\infty f(x)x^{-1-s}dx\right| &\leq \int_\lambda^\infty \left|\frac{f(x)}{x}\right| x^{-m}dx \\ &\leq \int_\lambda^\infty Cx^{-m}dx \\ &= C\cdot \lim_{t\to+\infty}\int_\lambda^t x^{-m}dx \\ &\leq C\cdot \lim_{t\to+\infty}\frac{-x^{1-m}}{1-m}\Big|_\lambda^t \\ &\leq \frac{C}{m-1}\lambda^{1-m}.\end{aligned}$$

Daí, temos que

$$\lim_{t\to+\infty}\int_1^t f(x)x^{-1-s}dx = \int_1^\infty f(x)x^{-1-s}dx$$

uniformemente em $m \in (1, \operatorname{Re} s]$. Portanto $g(s) = s\displaystyle\int_1^\infty f(x)x^{-1-s}dx$ é uma função analítica em $\operatorname{Re} s > 1$. □

No Lema 5.3.1, garantimos que a integral define uma função analítica em $\operatorname{Re} s > 0$. Precisamos investigar se a função $G(s)$ se estende sobre a reta $\operatorname{Re} = 0$.

Teorema 5.3.3. *Sejam a função $F : (0,\infty) \to \mathbb{R}$ limitada e integrável em qualquer subintervalo finito, e G a sua transformada de Laplace. Se G possui continuação analítica sobre a reta $\operatorname{Re} z = 0$, então a integral $\displaystyle\int_0^\infty F(t)dt$ converge e*

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

Demonstração. Precisamos analisar a continuação analítica da transformada de Laplace da função F na vizinhança do semiplano $\operatorname{Re} z \geq 0$. Denotemos esta continuação por $G(z)$. Vamos supor que $|F(t)| \leq 1$ e definir a função

$$G_\lambda(z) = \int_0^\lambda F(t)e^{-zt}dt,$$

onde $\lambda < +\infty$. Observe que $G_\lambda(z)$ é analítica em $\mathbb{C}$ para todo λ.

Queremos mostrar que

$$\lim_{\lambda\to\infty} G_\lambda(0) = G(0).$$

Para tanto, vamos analisar o disco fechado $\overline{D}\left(0, \dfrac{1}{\varepsilon}\right)$, para dado $\varepsilon > 0$. Pela definição vista no capítulo 3, considerando $R = \dfrac{1}{\varepsilon}$,

$$\overline{D}(0,R) = \{z \in \mathbb{C}; |z| \leq R\}.$$

Uma vez que a função $G(z)$ é analítica numa vizinhança do semiplano $\operatorname{Re} s \geq 0$, então, para cada valor R, existe um número real $\delta > 0$ pequeno o suficiente

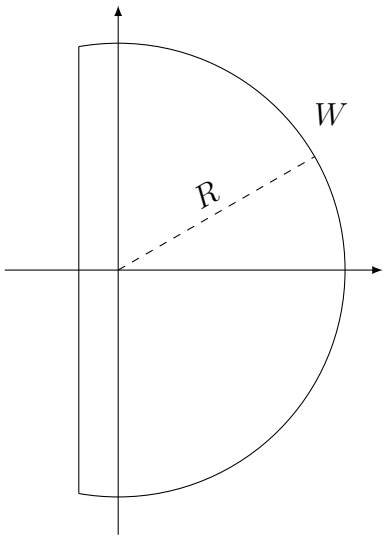

Figura 5.1: *Ilustração da curva W.*

para garantir que G seja analítica na região aberta que contém os pontos z pertencentes a $\overline{D}\left(0,\frac{1}{\varepsilon}\right) \cap \{\mathrm{Re}\, z \geq -\delta\}$. Note que a fronteira deste conjunto é uma curva fechada, a qual denotaremos por W, ilustrada pela imagem 5.1.

Pelo Teorema 4.6.8,

$$G(0) - G_\lambda(0) = \frac{1}{2\pi i}\int_W \frac{G(z) - G_\lambda(z)}{z} dz.$$

Seja $\varphi(z)$, uma função analítica em um domínio que contém

$$\overline{D}\left(0,\frac{1}{\varepsilon}\right) \cap \{\mathrm{Re}\, z \geq -\delta\}$$

então $\varphi(z)\cdot e^{\lambda\cdot z}$ também é analítica neste domínio. Assim, novamente pelo Teorema 4.6.8,

$$\varphi(0) = \frac{1}{2\pi i}\int_W \frac{\varphi(z)e^{\lambda z}}{z} dz, \tag{5.9}$$

e, uma vez que a função $h(z) = \dfrac{z\varphi(z)e^{\lambda z}}{R^2}$ é contínua em $\overline{D}\left(0,\frac{1}{\varepsilon}\right) \cap \{\mathrm{Re}\, z \geq -\delta\}$, temos que $h(0) = 0$. Como W é um caminho fechado

$$\int_W \frac{z\varphi(z)e^{\lambda z}}{R^2} dz = 0$$

Sendo assim,

$$\frac{1}{2\pi i}\int_W \frac{z\varphi(z)e^{\lambda z}}{R^2} dz = 0. \tag{5.10}$$

Somando termo a termo das equações (5.9) e (5.10), temos

$$\varphi(0) = \frac{1}{2\pi i}\left(\int_W \varphi(z)e^{\lambda z}\cdot\frac{1}{z}dz + \int_W \varphi(z)e^{\lambda z}\cdot\frac{z}{R^2}dz\right),$$

de onde temos que

$$\varphi(0) = \frac{1}{2\pi i}\int_W \varphi(z)e^{\lambda z}\left(\frac{1}{z}+\frac{z}{R^2}\right)dz.$$

Tomando $\varphi(z) = G(z) - G_\lambda(z)$, e $I(z) = (G(z) - G_\lambda(z))e^{\lambda z}\left(\frac{1}{z}+\frac{z}{R^2}\right)$, obtemos a igualdade

$$G(0) - G_\lambda(0) = \frac{1}{2\pi i}\int_W I(z)dz.$$

Agora, nosso objetivo será dividir o caminho de integração W em dois subconjuntos: $W^+ = \{z \in W;\ \mathrm{Re}\, z \geq 0\}$ e $W^- = \{z \in W;\ \mathrm{Re}\, z \leq 0\}$, conforme a figura 5.2.

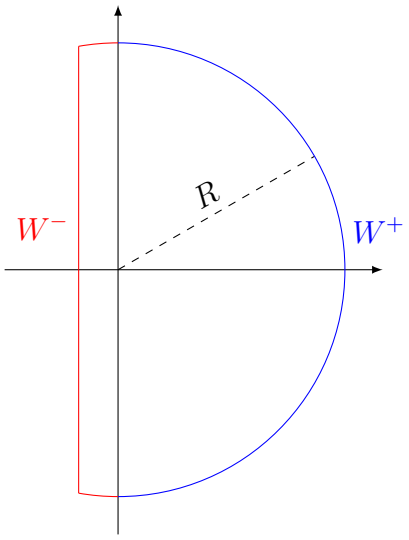

Figura 5.2: *Ilustração da divisão da fronteira W.*

Deste modo, teremos que

$$G(0) - G_\lambda(0) = \frac{1}{2\pi i}\left(\int_{W^+} I(z)dz + \int_{W^-} I(z)dz\right).$$

Para verificar a convergência de cada uma desta duas últimas integrais, precisamos subdividir W^-. Para tanto, observe que a função $G(z)\left(\frac{1}{z}+\frac{z}{R^2}\right)$ é analítica sobre W. Então, $\left|G(z)\left(\frac{1}{z}+\frac{z}{R^2}\right)\right|$ é limitada por um B real positivo, para todo $z \in W^-$. Então, vamos definir $\delta_1 > 0$ em função de ε, δ e B, onde $0 < \delta_1 < \delta$. Assim, tomaremos

$$W_2^- = \{z \in W^-;\ -\delta_1 \leq \mathrm{Re}\, z\},$$

de modo que

$$\frac{B}{2\pi}\int_{W_2^-} |dz| < \varepsilon.$$

Assim, W_2^- é o conjunto dado pelos pontos de W^- compreendidos entre a reta $\mathrm{Re}\, z = -\delta_1$ e $\mathrm{Re}\, z = 0$.

Vamos considerar também o conjunto W_1^-, dado por $W^- - W_2^-$.

$$W_1^- = \{z \in W^-;\ -\delta_1 > \operatorname{Re} z\}.$$

Por fim, considere o conjunto

$$W_*^- = \{z \in \mathbb{C};\ \operatorname{Re} z < 0 \ \text{ e } |z| = R\}.$$

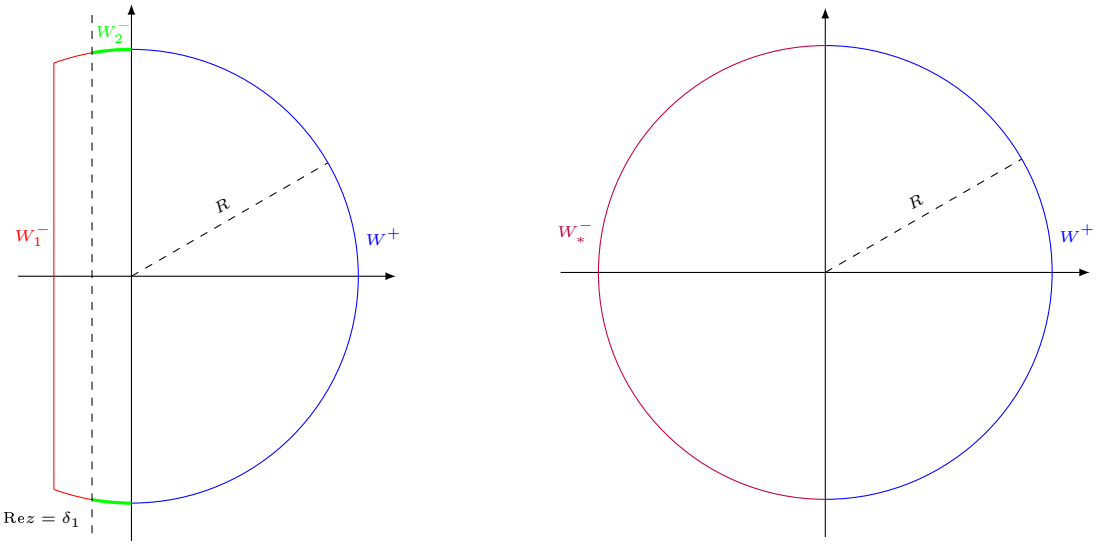

Figura 5.3: *Ilustração das subdivisões da fronteira* W^-.

Na figura 5.3, temos uma ilustração dos conjuntos W_1^-, W_2^- e W_*^-. Note que W_2^- é composto por dois arcos.

Vejamos algumas observações importantes. Se $x = \operatorname{Re} z$ e $|z| = R$, então

$$\frac{1}{z} + \frac{z}{R^2} = \frac{\overline{z}}{R^2} + \frac{z}{R^2} = \frac{2x}{R^2}. \tag{5.11}$$

Se, além disso, $x > 0$, uma vez que $|F(t)| \leq 1$, então

$$\begin{aligned}
|G(z) - G_\lambda(z)| &= \left| \int_0^\infty F(t)e^{-zt}dt - \int_0^\lambda F(t)e^{-zt}dt \right| \\
&= \left| \int_\lambda^\infty F(t)e^{-zt}dt \right| \\
&\leq \int_\lambda^\infty |F(t)|e^{-xt}dt \\
&\leq \int_\lambda^\infty e^{-xt}dt \\
&= \lim_{r\to+\infty} \int_\lambda^r e^{-xt}dt \\
&= \lim_{r\to+\infty} \frac{e^{-xt}}{-x}\Big|_\lambda^r
\end{aligned}$$

de onde obtemos que

$$|G(z) - G_\lambda(z)| \leq \frac{e^{-\lambda x}}{x}. \tag{5.12}$$

Mas, se $x < 0$,

$$\begin{aligned} |G_\lambda(z)| &= \left| \int_0^\lambda F(t)e^{-tz}dt \right| \\ &\leq \int_0^\lambda e^{-tx}dt \\ &= \frac{e^{-\lambda x}}{|x|} - \frac{1}{|x|}, \end{aligned}$$

de onde obtemos que

$$|G_\lambda(z)| < \frac{e^{-\lambda x}}{|x|}. \tag{5.13}$$

Em particular, se $z \in W_1^-$,

$$|e^{\lambda z}| = e^{\lambda x} \leq e^{-\delta_1 \lambda z}.$$

Vamos denotar $I_1(z) = G(z)e^{\lambda z}\left(\frac{1}{z} + \frac{z}{R^2}\right)$ e $I_2 = G_\lambda(z)e^{\lambda z}\left(\frac{1}{z} + \frac{z}{R^2}\right)$.
Como $G_\lambda(z)$ é analítica em $\mathbb{C}$, pelo Corolário 4.6.7,

$$\int_{W^-} I_2 dz = \int_{W_*^-} I_2 dz.$$

Sendo assim,

$$\begin{aligned} G(0) - G_\lambda(0) &= \frac{1}{2\pi i}\left[\int_{W^+} I(z)dz + \int_{W^-} (I_1(z) - I_2(z))dz\right] \\ &= \frac{1}{2\pi i}\left[\int_{W^+} I(z)dz + \int_{W^-} I_1(z)dz - \int_{W^-} I_2(z)dz\right] \\ &= \frac{1}{2\pi i}\left[\int_{W^+} I(z)dz + \int_{W_1^-} I_1(z)dz + \int_{W_2^-} I_1(z)dz - \int_{W_*^-} I_2(z)dz\right] \end{aligned}$$

Usando as estimativas 5.11, 5.12 e 5.13, temos para a 1ª integral

$$\begin{aligned} \left|\frac{1}{2\pi i}\int_{W^+} I(z)dz\right| &\leq \frac{1}{2\pi}\int_{W^+} e^{\lambda x}\cdot\frac{e^{-\lambda x}}{x}\cdot\frac{2x}{R^2}|dz| \\ &= \frac{1}{\pi R^2}\int_{W^+}|dz| \\ &= \frac{\pi R}{\pi R^2} \\ &= \frac{1}{R} = \varepsilon, \end{aligned}$$

para a 2ª integral

$$\begin{aligned} \left|\frac{1}{2\pi i}\int_{W_1^-} I_1(z)dz\right| &\leq \frac{1}{2\pi}\int_{W_1^-} B\cdot e^{-\lambda\delta_1}|dz| \\ &= \frac{B}{2\pi}\cdot e^{-\lambda\delta_1}\int_{W_1^-}|dz|, \end{aligned}$$

para a 3ª integral

$$\begin{aligned}\left|\frac{1}{2\pi i}\int_{W_2^-} I_1(z)dz\right| &\leq \frac{1}{2\pi}\int_{W_2^-} B\cdot e^{\lambda x}|dz| \\ &= \frac{B}{2\pi}\int_{W_2^-}|dz| < \varepsilon,\end{aligned}$$

e para a 4ª integral

$$\begin{aligned}\left|\frac{1}{2\pi i}\int_{W_*^-} I_2(z)dz\right| &\leq \frac{1}{2\pi}\int_{W_*^-} e^{\lambda x}\cdot\frac{e^{-\lambda x}}{|x|}\cdot\frac{2|x|}{R^2}|dz| \\ &= \frac{1}{\pi R^2}\int_{W_*^-}|dz| \\ &= \frac{\pi R}{\pi R^2} \\ &= \frac{1}{R} = \varepsilon.\end{aligned}$$

Logo, para um λ suficientemente grande

$$|G(0) - G_\lambda(0)| \leq 4\varepsilon.$$

□

Para encerrar essa seção, vejamos um último teorema antes de chegar à conclusão de que

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

Este teorema é inspirado no teorema de Ikehara-Wiener.

Teorema 5.3.4. *Seja $f:[1,+\infty)\to\mathbb{R}$ uma função integrável em qualquer subintervalo finito, não negativa, não decrescente, e $O(x)$. Seja também $g(s)$ a sua transformada de Mellin. Se existe $c\in\mathbb{R}$ constante tal que*

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

possui continuação analítica sobre a reta $\operatorname{Re} s = 1$, então

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

Demonstração. Inicialmente, vamos tomar $F(t) = \dfrac{f(e^t)}{e^t} - c$, onde $t > 0$. Como $F(t)$ é $O(x)$, então $F(t)$ é limitada em $[0,+\infty)$. Uma vez que f é $O(x)$, e integrável em qualquer subintervalo finito, $F(t)$ também o é. Sendo assim, sua transformada de Laplace G será

$$\begin{aligned}G(z) &= \int_0^\infty\left(\frac{f(e^t)}{e^t} - c\right)\cdot\frac{1}{e^{zt}}dt \\ &= \int_0^\infty\frac{f(e^t)}{(e^t)^{z+1}}dt - \int_0^\infty\frac{c}{(e^t)^z}dt\end{aligned}$$

Fazendo a mudança de variáveis $x = e^t$, temos que $dt = \frac{1}{e^t}dx$. Assim,

$$\begin{aligned} G(z) &= \int_1^\infty \frac{f(x)}{x^{z+1}} \cdot \frac{1}{x} dx - \int_1^\infty \frac{c}{x^z} \cdot \frac{1}{x} dx \\ &= \int_1^\infty \frac{f(x)}{x^{z+1}} \cdot \frac{1}{x} dx - \int_1^\infty \frac{c}{x^{z+1}} dx \\ &= \int_1^\infty \frac{f(x)}{x^{(z+1)+1}} dx + \frac{1}{z} \cdot \frac{c}{x^z}\Big|_1^\infty \\ &= \int_1^\infty \frac{f(x)}{x^{(z+1)+1}} dx - \frac{c}{z} \end{aligned}$$

Seja $g(z)$ a transformada de Mellin da função f, então

$$\begin{aligned} G(z) &= \frac{g(z+1)}{z+1} - \frac{c}{z} \\ &= \frac{1}{z+1}\left(g(z+1) - \frac{c}{z} - c\right) \end{aligned}$$

Por hipótese, $g(z+1) - \dfrac{c}{z}$ possui continuação analítica sobre $\mathrm{Re}(z+1) = 1$. Consequentemente, $G(z)$ possui continuação analítica sobre $\mathrm{Re}\, z = 0$. Desta maneira, podemos aplicar o Teorema 5.3.3 à função $F(t)$, de onde temos que

$$\begin{aligned} G(0) &= \int_0^\infty \left(\frac{f(e^t)}{e^t} - c\right) dt \\ &= \int_1^\infty \left(\frac{f(x)}{x} - c\right) \cdot \frac{1}{x} dt \\ &= \int_1^\infty \frac{f(x) - cx}{x^2} dx \end{aligned}$$

Agora, nosso objetivo será mostrar que se $\displaystyle\int_1^\infty \frac{f(x) - cx}{x^2} dx$ converge, então $\displaystyle\lim_{x\to+\infty} \frac{f(x)}{x} = c$. Para tanto, faremos uma demonstração por redução ao absurdo. Inicialmente, observe que $c \geq 0$. Caso contrário, teríamos que

$$\int_1^\infty \frac{f(x) - cx}{x^2} dx \geq \int_1^\infty \frac{-cx}{x^2} dx = +\infty,$$

ou seja, $\displaystyle\int_1^\infty \frac{f(x) - cx}{x^2} dx$ não converge. Sendo assim, suponha que se vale a desigualdade

$$\limsup \frac{f(x)}{x} > c,$$

então existe $\delta > 0$ tal que vale a desigualdade

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

Uma vez que $c \geq 0$, tome o número real $\rho = \dfrac{c + 2\delta}{c + \delta} > 1$. Considere também uma sequência $(y_n)_{n\in\mathbb{N}}$, onde $y_n \to +\infty$, e ainda,

$$f(y_n) > (c + 2\delta)y_n, \forall n \in \mathbb{N}.$$

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

$$y_n < x < \frac{c+2\delta}{c+\delta} y_n$$

$$(c+\delta)y_n < (c+\delta)x < (c+2\delta)y_n.$$

Ou seja,

$$f(x) \geq f(y_n) > (c+\delta)x,$$

de onde obtemos a desigualdade

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

Assim,

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

Uma vez que

$$G(0) = \int_1^{\infty} \frac{f(x)-cx}{x^2} dx,$$

dado $\varepsilon > 0$, existe um número real $M > 1$ tal que, para todo real $a \geq M$,

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

Em particular, tomando $0 < \varepsilon < \frac{\delta}{2} \log \rho$, como $y_n \to +\infty$, existe $n_0 \in \mathbb{N}$ tal que, para $a \geq y_{n_0}$,

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

Por outro lado,

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

o que é um absurdo. Logo, concluímos que $\limsup \frac{f(x)}{x} \leq c$.

Analogamente, para mostrar que $\liminf \frac{f(x)}{x} \geq c$, basta supor que $\liminf \frac{f(x)}{x} < c$, tomar

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

e seguir os mesmos passos tomados para a demonstração de que $\limsup \frac{f(x)}{x} \leq c$. □

5.4 O Teorema dos Números Primos

Esta seção tem por objetivo usar os resultados obtidos neste capítulo para provar o Teorema dos Números Primos.

Teorema 5.4.1.

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

Demonstração. Vimos que a função $\psi(x)$ é $O(x)$ na Proposição 5.1.16. Além disso, esta função é não decrescente, não negativa e integrável em intervalos finitos. Na Proposição 5.2.13, vimos que sua transformada de Mellin, dada por

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

é analítica em $\operatorname{Re} s > 1$, e $g(s) = -\dfrac{\zeta'(s)}{\zeta(s)}$. Por fim, vimos na Proposição 5.2.12 que a função $-\dfrac{\zeta'(s)}{\zeta(s)} - \dfrac{1}{s-1}$ possui continuação analítica sobre a reta $\operatorname{Re} s = 1$.

Aplicando o Teorema 5.3.4 à função $\psi(x)$, temos que

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

Uma vez que, pela Proposição 5.1.15,

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

obtemos o nosso resultado. □

5.5 Conclusão

Mesmo depois de séculos de estudos acerca dos números primos, ainda há muito mistério acerca deste tema. Desde o século XIX, quando o Teorema dos Números Primos foi anunciado por Gauss e Legendre e sua posterior prova foi realizada por Hadamard e Poussin, não havia uma nova e grandiosa descoberta no tocante ao espaçamento entre primos. Somente em 2.013, foi provado que existem infinitos pares de primos cuja distância é N, para algum $N \in \mathbb{N}$ menor que 70.000.000.

Apesar da temática dos números primos ser objeto da área da Teoria dos Números, vimos também que, através de técnicas de análise complexa, é possível mostrar que o espaçamento médio entre primos até um número natural n é aproximadamente $\log n$. Para tanto, a ideia de Riemann em associar a distribuição dos números primos à função zeta aplicada a números complexos foi fundamental. Ainda assim, sua teoria acerca dos zeros não triviais para a função zeta continua em aberto, bem como outras conjecturas que dependem da prova desta hipótese de Riemann.

Alguns pontos importantes sobre os primos já foram mostrados, como a infinitude deste conjunto, e testes de primalidade cada vez mais eficazes e interessantes. De igual modo, grandes aplicações na área de segurança do mundo eletrônico, bem como na Física Quântica, se tornaram evidentes e valiosas. Resta saber qual será a nova nota a ressoar na canção dos números primos.

Referências Bibliográficas

[1] AVILA, G. *Variáveis Complexas e Aplicações*. 3. ed. Rio de Janeiro: LTC, 2008.

[2] CLEMENT, P. A. *Congruences for Sets of Primes* v. 56, n. 1. The American Mathematical Monthly: JSTOR, 1949. Disponível em `https://doi.org/10.2307/2305816`. Acessado em 28/12/2022.

[3] EVES, H. *Introdução à história da matemática*. 1. ed. Campinas: Editora da UNICAMP, 2004.

[4] GONÇALVES, A.*Introdução à Álgebra*. 6. ed. Rio de Janeiro: IMPA, 2017.

[5] HEFEZ, A.*Aritmética*. 2. ed. Rio de Janeiro: Sociedade Brasileira de Matemática, 2016.

[6] LINS NETO, A. *Funções de uma Variável Complexa*. 2. ed. Rio de Janeiro: IMPA, 2008.

[7] MARTINEZ, F. E. R.; MOREIRA, C. G. T. A.; SALDANHA, N. C.; TENGAN, E. *Teoria dos Números: um passeio com primos e outros números familiares pelo mundo inteiro*. 3. ed. Rio de Janeiro: IMPA, 2013.

[8] MOTA, K. V. C. *O Mistério e a Beleza dos Números Primos*. 53 f. Dissertação (Mestrado em Matemática). Universidade Federal de Goiás, Goiânia, 2017.

[9] MUNIZ NETO, A.C.*Fundamentos do Cálculo*. 1. ed. Rio de Janeiro: Sociedade Brasileira de Matemática, 2015.

[10] OLIVEIRA, D. F.; SANTOS, J. J. *Uma prova geométrica do Problema da Basileia*. 14 f. Revista eletrônica da Sociedade brasileira de matemática. Disponível em `https://pmo.sbm.org.br/wp-content/uploads/sites/5/sites/5/2022/07/art22_vol10_PMO_SBM_2022.pdf`. PMO, v. 10, n. 3. SBM, 2022.

[11] PROBST, R. W. *NÚMEROS PRIMOS*. 53 f. Dissertação (Trabalho de conclusão do curso Matemática - Bacharelado). Universidade Regional de Blumenau, Blumenau, 2003.

[12] RIZEL, A. C. *NÚMEROS PRIMOS*. 60 f. Dissertação (Trabalho de conclusão do curso de especialização com ênfase em cálculo). Universidade Federal de Minas Gerais, Belo Horizonte, 2014.

[13] ROQUE, T; PITOMBEIRA, J.B.*Tópicos de História da Matemática*. 1. ed. Rio de Janeiro: SBM, 2012.

[14] SAUTOY, M. *A Música dos Números Primos: a História de um Problema não Resolvido*. Rio de Janeiro: Zahar, 2007.

[15] SOARES, M. G. *Cálculo em uma Variável Complexa*. 4. ed. Rio de Janeiro: IMPA, 2006.

Sites visitados

[FC] Chebyshev function. In: WIKIPEDIA: a enciclopédia livre. Wikimedia 2023. Disponível em https://en.wikipedia.org/wiki/Chebyshev_function. Acessado em 01/02/2023.

[FS] Fermat Search. Disponível em http://www.fermatsearch.org/news.html. Acessado em 09/03/2023

[MO] GIMPS: 2023. Disponível em https://www.mersenne.org/. Acessado em 09/03/2023.

[GIMPS] Great Internet Mersenne Prime Search. In: WIKIPEDIA: a enciclopédia livre. Wikimedia 2023. Disponível em https://en.wikipedia.org/wiki/Great_Internet_Mersenne_Prime_Search. Acessado em 27/04/2023.

[NPG] Números primos gemeos. In: WIKIPEDIA: a enciclopédia livre. Wikimedia 2022. Disponível em https://pt.wikipedia.org/wiki/N%C3%BAmeros_primos_g%C3%A9meos. Acessado em 29/12/2022.

[PP] PRIMEPAGES: 2022. Disponível em https://primes.utm.edu. Acessado em 09/03/2023.