UNIVERSIDADE ESTADUAL DA PARAÍBA
CENTRO DE CIÊNCIAS EXATAS E SOCIAIS APLICADAS
CURSO DE LICENCIATURA PLENA EM MATEMÁTICA

Marcos Thadeu Lúcio da Silva

DEZ DEMONSTRAÇÕES DA INFINITUDE DOS NÚMEROS PRIMOS

PATOS
2016

Marcos Thadeu Lúcio da Silva

DEZ DEMONSTRAÇÕES DA INFINITUDE DOS NÚMEROS PRIMOS

Monografia submetida à Coordenação do Curso de Licenciatura Plena em Matemática, da Universidade Estadual da Paraíba, como requisito parcial para obtenção do grau de Licenciado em Matemática.

Orientador: Prof. Dr. Francisco Sibério Bezerra Albuquerque.

Patos
2016

S586d Silva, Marcos Thadeu Lúcio da
Dez demonstrações da infinitude dos números primos [manuscrito] / Marcos Thadeu Lucio da Silva. - 2016.
49 p.

Digitado.
Trabalho de Conclusão de Curso (Graduação em Matemática) - Universidade Estadual da Paraíba, Centro de Ciências Exatas e Sociais Aplicadas, 2016.
"Orientação: Prof. Dr. Francisco Sibério Bezerra Albuquerque, CCEA".

1. Teoria dos Números. 2. Infinitude numérica. 3. Números Primos. I. Título.

21. ed. CDD 512.72

Marcos Thadeu Lúcio da Silva

DEZ DEMONSTRAÇÕES DA INFINITUDE DOS NÚMEROS PRIMOS

Monografia a submetida Coordenação do Curso de Licenciatura Plena em Matemática, da Universidade Estadual da Paraíba, como requisito parcial para obtenção do grau de Licenciado em Matemática.

Área de concentração: Matemática.

Aprovada em 25 de maio de 2016

BANCA EXAMINADORA

Francisco Sibério B. Albuquerque

Prof. Dr. Francisco Sibério Bezerra Albuquerque (Orientador)
Universidade Estadual da Paraíba (UEPB)

Vilmar Vaz da Silva

Prof. Me. Vilmar Vaz da Silva
Universidade Estadual da Paraíba (UEPB)

UNIVERSIDADE ESTADUAL DA PARAÍBA
CCT
Prof. Vandenberg Lopes Vieira
Chefe do Dept° de Matemática
Mat. 122386-1

Prof. Dr. Vandenberg Lopes Vieira
Universidade Estadual da Paraíba (UEPB)

Aos meus pais Joelma e Edgar e às minhas tias Elita e Luzia.

AGRADECIMENTOS

Em primeiro lugar a Deus, pela força a qual Ele me deu o tempo inteiro;

Aos meus pais Maria Joelma Lúcio da Silva e Edgar Moreira da Silva, e a minha irmã Márcia Thaysa Lúcio da Silva, por toda a esperança depositada em mim, durante toda a minha vida, por serem os 3 grandes motivos de todo o meu esforço e dedicação;

Às minhas tias Elita, Dalva, Helena, Joana, Jocilda, Josenilda, Josiane, Luzia e Maria, e aos meus tios Elias, Erivaldo, Francisco, Heleno, José Moreira, Josué e Silvo por acreditarem em mim;

Ao professor Dr. Francisco Sibério, pelas orientações importantíssimas e pela escolha deste belo tema que tive o privilégio de estudar;

Ao professor Me. Vilmar Vaz da Silva, por ter me incentivado a seguir pelos caminhos da matemática desde cedo, pelas correções importantíssimas nesse texto e pelos valiosos conselhos;

À minha amiga, professora e mentora Me. Syana Monteiro, por sempre estar do meu lado me dando forças pra conseguir continuar, por ser a pessoa que mais me apoiou durante todo o meu percurso, pelos valiosos conselhos e exemplos de vida, por me ajudar sempre que necessito e por tudo que me proporciona até hoje;

À professora Rozana Bandeira e o professor Dr. Marcelo Vieira por serem valiosos amigos, por me darem apoio durante todo o curso.

Aos meus amigos Aline Marques, Ana Tereza, Annielly Sayonara, Bruno Dayvid, Claudineide Gomes, Daniel Farias, Ellen Priscylla, Enderson Nobre, Lívia Pedro, Luzia Valesca, Pedro Neto, Yan Linhares, entre outros, por serem os melhores amigos que eu sempre desejei ter, por estarem do meu lado me apoiando, não me deixando desistir jamais;

À professora Ma. Tatiana Rocha por ser um grande exemplo de vida e dedicação, e por ter sido uma excelente professora e amiga, no pouco tempo em que estivemos próximos.

Aos Professores Janine Dantas, Lidiane Campelo e Wilker Lima pelas valiosas aulas que foram ministradas durante a graduação;

Por fim, a todos que me desejaram sorte e boas energias ao fim dessa caminhada, e que me contribuíram de alguma forma para o desenvolvimento dessa monografia e da minha graduação.

"If you forget the way to go
And lose where you came from
If no one is standing baside you
Be still and know I am"

Trecho de *"Be Still", The Fray.*

RESUMO

O estudo das propriedades dos números inteiros positivos é o objetivo central da Teoria dos Números. São três os principais ramos em que ela se divide: Teoria Elementar, Teoria Analítica e Teoria Algébrica. Dentro da Teoria Elementar, tomamos conhecimento dos números primos, ou seja, aqueles inteiros positivos maiores do que 1 cujos únicos divisores positivos são apenas 1 e eles mesmos. Um dos primeiros e principais resultados envolvendo números primos é a famosa infinitude dos primos. Nessa direção, o objetivo principal do nosso trabalho é exibir dez diferentes demonstrações desse belíssimo resultado. Nos convencemos de que essa quantidade razoável de demonstrações da infinitude dos primos, além de ser algo bastante curioso visto que é muito pouco explorado nos cursos regulares de graduação, pode possibilitar o interesse no estudo desta área, Teoria dos Números, que ultimamente vem crescendo de maneira exponencial conjuntamente com os avanços computacionais e tecnológicos em geral.

Palavras Chave: Teoria dos Números; infinitude; demonstrações; primos.

ABSTRACT

The study of the properties of positive integers is the central goal of Number Theory. There are three main branches in it which is divided: Elementary Theory, Analytical Theory and Algebraic Theory. Within the elementary theory we know the prime numbers, that is, those positive integers bigger than 1 whose only positive divisors are only 1 and themselves. One of the first and main results involving prime numbers is the famous infinity of primes. In this direction, the main objective of our work is to show ten different proofs of this beautiful result. We are convinced that this reasonable amount of proofs from infinity of primes, beside being something rather curious, since it is little explored in regular undergraduate courses, may permit interest in the study of this area, Number Theory, which has lately growing exponentially in conjunction with the computational and technological advances in general.

Keywords: Number Theory; infinity; proofs; primes.

Sumário

Introdução

O estudo das propriedades dos números inteiros é o tema central da Teoria dos Números. Ela se divide em três principais ramos: A Teoria Analítica, a Teoria Elementar e a Teoria Algébrica.

Um número inteiro positivo é dito ser um primo se ele for divisível apenas por 1 e por ele mesmo. Essa simples afirmação define um dos mais essenciais e importantes números da matemática. Dentre os ramos da Teoria dos Números, o que nos mostra os conceitos de números primos é a Teoria Elementar, e uma das primeiras coisas que nos é mostrada é que existem infinitos números desse tipo.

Du Sautoy afirma que "Os primos são as pérolas que adornam a vastidão infinita do universo de números que os matemáticos exploram ao longo dos séculos" (DU SAUTOY, Marcus. 2004). Os números primos são uma das pedras fundamentais da matemática. É através deles que podemos encontrar todos os outros. Sautoy ainda afirma que, mesmo que não conhecêssemos os primos, mesmo que nossa capacidade de raciocínio não fosse suficiente para tanto, ainda existiriam números primos, pois a natureza os escolheu.

O objetivo desse trabalho é exibir dez demonstrações para a infinitude dos números primos, fazendo uma conexão desse resultado com a Análise, a Álgebra, a Contagem e a Topologia.

No **Capítulo 1**, enunciamos e demonstramos alguns resultados preliminares, os quais serão importantes para compreensão das demonstrações da infinitude dos primos. Ele é dividido em três seções: a primeira é dedicada aos resultados da Teoria dos Números; na segunda fazemos uma introdução à Teoria de Grupos e na terceira definimos alguns conceitos básicos de Topologia Geral.

O **Capítulo 2** é dedicado às 10 demonstrações dos números primos. Nas três primeiras, devidas a Euclides, Metrod e Kummer, fazemos uso apenas da Teoria Elementar dos Números.

A primeira demonstração, devida a Euclides de Alexandria (aproximadamente 300 a.C.), é a mais conhecida, simples e elegante prova desse fato, a qual utiliza a famosa técnica de redução ao absurdo, tão comum nas demonstrações de diversos resultados em Teoria dos Números. A segunda e a terceira são demonstrações semelhantes a de Euclides, e utilizam as mesmas ferramentas, porém de formas diferentes. Na quarta demonstração, devida a Thue, usamos de forma um pouco mais técnica, o Teorema Fundamental da Aritmética e propriedades dos logaritmos e funções. Na quinta demonstração, devida a Goldbach, são introduzidos os números de Fermat, os quais mostraremos serem relativamente primos, acarretando assim a infinitude dos primos. Na sexta demonstração, devida a Lagrange, fazemos uso dos tão procurados primos de Mersenne conjuntamente com o Teorema de Lagrange, o qual diz que se G é um grupo finito e H é um subgrupo de G, então a ordem de H divide a ordem de G. Na sétima demonstração, não apenas mostramos nosso resultado, mas também outro de grande importância, que é a divergência da série dos recíprocos dos primos, estudada por Euler e mais tarde por Clarkson, e cuja prova é devida a Erdös; A oitava demonstração, devida a Euler, é um tanto técnica. Definimos inicialmente o conjunto formado por todos os primos menores ou iguais a um número real dado e comparamos a cardinalidade desse conjunto com o logaritmo desse número real definido da sua melhor forma, isto é, por uma integral. A nona demonstração devida a Pinasco, faz uso do Princípio de Inclusão e Exclusão, muito estudado no campo da contagem. Após nove provas puramente analíticas e algébricas, é a vez de uma prova topológica; esse é o teor da décima demonstração da infinitude dos primos, dada por Hillel Furstenberg e publicada em 1955, na qual é definida uma topologia sobre o conjunto dos inteiros.

Por fim, nas **Considerações Finais**, apresentamos outras demonstrações da infinitude dos números primos, que faz uso de resultados mais avançados no campo da Teoria dos Números, como o Teorema de Dirichlet, e o Teorema de Green e Tao. Comentamos alguns fatos e curiosidades acerca deles e também apresentamos resultados ainda não demonstrados, dentro dessa área. ..

Capítulo 1

Preliminares

1.1 Teoria dos Números

Aqui, estão enunciados e demonstrados os principais resultados necessários ao entendimento das demonstrações do Capítulo 2.

1.1.1 Números inteiros e propriedades

O conjunto dos números inteiros, é o conjunto

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}.$$

Sejam a, b e c números inteiros. O conjunto $\mathbb{Z}$ munido das operações de adição $(+)$ e multiplicação $(\cdot)$ goza das seguintes propriedades:

$P1 : a + b = b + a$ e $a \cdot b = b \cdot a$ (comutativa);
$P2 : (a + b) + c = a + (b + c)$ e $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ (associativa);
$P3$: Existem $0, 1 \in \mathbb{Z}$ tais que $a + 0 = 0 + a = a$ e $a \cdot 1 = 1 \cdot a = a$ (existência de elemento neutro da adição e multiplicação);
$P4$: Existe $-a \in \mathbb{Z}$, tal que $-a = (-1) \cdot a$ e $a + (-a) = 0$ (existência de elemento oposto);
$P5 : a \cdot (b + c) = a \cdot b + a \cdot c$ e $(a + b) \cdot c = a \cdot c + b \cdot c$ (distributiva);
$P6 : 0 \cdot a = 0$ e se $a \cdot b = 0$ então ou $a = 0$ ou $b = 0$ (não existência de divisores de zero);

Além disso, as relações "$>$" e "$<$", ou seja, "maior que" e "menor que", gozam das seguintes propriedades:

$P7$: Se $a \neq 0$, então ou $a > 0$ ou $a < 0$ (tricotomia);

$P8$: Se $a < b$ e $b < c$, então $a < c$ (transitividade da ordem);

$P9$: Se $a < b$, então $a + c < b + c$ (compatibilidade da ordem com a adição);

$P10$: Se $a < b$ e $c > 0$, então $a \cdot c < b \cdot c$ (compatibilidade da ordem com a multiplicação);

$P11$: Se $a < b$ e $c < 0$, então $b \cdot c < a \cdot c$(compatibilidade da ordem com a multiplicação).

Notação. Se $a < b$ ou $a = b$, então denotaremos por $a \leqslant b$. Analogamente, se $a > b$ ou $a = b$, então $a \geqslant b$.

1.1.2 Indução

Temos nessa seção a discussão de indispensáveis ferramentas na demonstração de muitos teoremas: o Princípio da Boa Ordenação e o Princípio de Indução Finita.

Princípio da boa ordenação (PBO): Seja A um subconjunto não-vazio dos inteiros não-negativos. Nessas condições, A possui elemento mínimo.

Proposição 1.1 (Primeira Forma do Princípio da Indução Finita)**.** *Seja B um subconjunto dos inteiros positivos. Se B possui as duas seguintes propriedades:*

(i) $1 \in B$*;*

(ii) $k + 1 \in B$ *sempre que* $k \in B$*,*

então B contém todos os inteiros positivos, isto é, $B = \mathbb{N}$.

Proposição 1.2 (Segunda Forma do Princípio da Indução Finita)**.** *Seja B um subconjunto dos inteiros positivos. Se B possui as duas seguintes propriedades:*

(i) $1 \in B$*;*

(ii) $k + 1 \in B$ *sempre que* $1, 2, \ldots, k \in B$*,*

então B contém todos os inteiros positivos, isto é, $B = \mathbb{N}$.

O PBO, a primeira e a segunda forma do princípio de indução são equivalentes. A demonstração desse fato pode ser encontrado em [3] e em [12].

1.1.3 Divisibilidade

Dentro do conceito de divisibilidade, serão destacadas algumas propriedades. O resultado principal dentro desse conceito é o Algoritmo de Euclides, que nos dá a forma mais eficiente de se encontrar o máximo divisor comum entre números inteiros.

Definição 1.3. *Sejam $a, b \in \mathbb{Z}$ com $a \neq 0$. Diz-se que a divide b, denota-se por $a \mid b$, se e somente se, existe $k \in \mathbb{Z}$, tal que $b = k \cdot a$.*

Observações.

i) $a \nmid b$ lê-se a não divide b

ii) A relação $a \mid b$ denomina-se **relação de divisibilidade em** $\mathbb{Z}$.

Teorema 1.4. *Dados $a, b, c \in \mathbb{Z}$, temos que:*

i) $a \mid 0$, $1 \mid a$ *e* $a \mid a$;

ii) *Se* $a \mid 1$, *então* $a = \pm 1$;

iii) *Se* $a \mid b$ *e* $c \mid d$, *então* $ac \mid bd$;

iv) *Se* $a \mid b$ *e* $b \mid c$, *então* $a \mid c$;

v) *Se* $a \mid b$ *e* $b \mid a$, *então* $a = \pm b$;

vi) *Se* $a \mid b$ *e* $b \neq 0$, *então* $|a| \leq |b|$;

vii) *Se* $a \mid b$ *e* $a \mid c$, *então* $a \mid bx + cy$, *para todos* $x, y \in \mathbb{Z}$.

Demonstração: *i)* $a \mid 0$ pois $0 = 0 \cdot a$, $1 \mid a$ e $a \mid a$ pois $a = a \cdot 1$.

ii) Como $a \mid 1$, então $0 \leqslant \mid a \mid \leqslant 1$. Como $a \neq 1$, então $0 < \mid a \mid \leqslant 1$. Assim, pelo PBO, $\nexists x \in \mathbb{Z}$ tal que $0 < x < 1$. Por isso, $\mid a \mid = 1 \Leftrightarrow a \pm 1$

iii) $a \mid b \Leftrightarrow b = k_1 \cdot a$ e $c \mid d \Leftrightarrow d = k_2 \cdot c$, $k_1, k_2 \in \mathbb{Z}$. Multiplicando, membro a membro essas duas última equações, obtemos

$$bd = \underbrace{(k_1 k_2)}_{= k_3 \in \mathbb{Z}} \cdot ac \Leftrightarrow bd = k_3 \cdot ac.$$

iv) $a \mid b \Leftrightarrow b = k_1 \cdot a$ e $b \mid c \Leftrightarrow c = k_2 \cdot b$, $k_1, k_2 \in \mathbb{Z}$. Daí, segue-se que

$$c = \underbrace{(k_1 k_2)}_{=k_3 \in \mathbb{Z}} \cdot a \Leftrightarrow c = k_3 \cdot a.$$

Logo, $a \mid c$.

v) $a \mid b \Leftrightarrow b = k_1 \cdot a$ e $b \mid a \Leftrightarrow a = k_2 \cdot b$, $k_1, k_2 \in \mathbb{Z}$. Daí, segue-se que

$$a = k_1 k_2 \cdot a \Rightarrow (k_1 k_2 - 1) \cdot a = 0.$$

Se a for diferente de zero, então

$$k_1 k_2 = 1 \Rightarrow k_1 = k_2 = 1 \Rightarrow (a = b)$$

ou

$$k_1 = k_2 = -1 \Rightarrow (a = -b).$$

Agora, se a for igual a zero, então b também é igual a zero, já que $b = k_1 \cdot a$.

vi) Se $a \mid b$ e $b \neq 0$, então $b = k \cdot a$, $k \in \mathbb{Z}^*$. Daí, $|b| = |k| \cdot |a|$. Como $k \neq 0$, segue-se que $|k| \geq 1$. Logo, $|b| \geq |a|$, ou seja, $|a| \leq |b|$.

vii) $a \mid b \Leftrightarrow b = k_1 \cdot a$ e $a \mid c \Leftrightarrow c = k_2 \cdot a$, $k_1, k_2 \in \mathbb{Z}$. Multiplicando a 1^{a} equação por x, a 2^{a} por y e logo após somando seus resultados membro a membro, obtemos: $bx + cy = \underbrace{(k_1 \cdot x + k_2 \cdot y)}_{=k_3 \in \mathbb{Z}} \cdot a$. Portanto, $a \mid bx + cy$, para todos $x, y \in \mathbb{Z}$.

□

Definição 1.5. *Chama-se divisor comum de $a, b \in \mathbb{Z}$ todo inteiro não-nulo d tal que $d \mid a$ e $d \mid b$.*

Notação. $D(a, b) = \{x \in \mathbb{Z} : x \mid a \text{ e } x \mid b\}$.

1.1.4 Algoritmo da divisão

O algoritmo da divisão é considerado um dos mais familiares resultados sobre os números inteiros e será bastante útil para algumas propriedades desses números, inclusive para se

demonstrar o Algoritmo de Euclides.

Teorema 1.6. *Dados quaisquer inteiros a e b, com $a > 0$, existem inteiros unicamente determinados q e r tais que $b = a \cdot q + r$, $0 \leq r < a$. Se $a \nmid b$, então $r \neq 0$.*

Demonstração: *i)* **Existência:** Consideremos a sequência de inteiros

$$\ldots, b - 2a, b - a, b, b + a, b + 2a, \ldots$$

Seja r o menor inteiro não-negativo dessa sequência. Observe que não ocorre que $r \geq a$. De fato, caso ocorresse, teríamos que $r - a$ seria um elemento da sequência e menor que r, o que é uma contradição pela minimalidade de r. Logo, $r = b - q \cdot a$, ou seja, $b = a \cdot q + r$ com $0 \leq r < a$.

ii) **Unicidade:** Supondo $b = q'a + r'$ com $0 \leq r' < a$, temos que

$$q'a + r' = qa + r \Rightarrow r' - r = (q - q')a \Rightarrow a \mid r' - r.$$

Como $0 \leq r' < a$, segue-se que $-a < -r' \leq 0$. Logo, $-a < -r' \leq 0$ e $0 \leq r < a$. Combinando ambas as expressões, obtemos

$$-a < r' - r < a \Rightarrow |r' - r| < a.$$

Como $a \mid r' - r$ e $|r' - r| < a$, só pode ocorrer que $r' - r = 0$, ou seja, $r' = r$ e, consequentemente, $q' = q$. Portanto, *i)* e *ii)* demonstram o teorema.

□

1.1.5 O máximo divisor comum

O máximo divisor comum é bastante útil para se solucionar algumas questões da Teoria dos Números, e é fundamental para conceitos trabalhados posteriormente neste texto, como o conceito de dois números primos entre si.

Definição 1.7. *O máximo divisor comum de dois inteiros (não simultaneamente nulos) a e b é o maior inteiro que divide a e b.*

Notação. (a, b).

Teorema 1.8. *Se $d = (a, b)$, então existem inteiros n_0, m_0 tais que $d = n_0a + m_0b$.*

Demonstração: Seja $A = \{na + mb : n, m \in \mathbb{Z}\}$. Obviamente, o subconjunto $A_+ \subset A$ dos elementos positivos de A é não vazio. De fato, basta tomar $n = a$ e $m = b$. Usando o PBO, concluímos que existe $c \in A$, o menor elemento positivo de A. Escrevemos $c = n_0a + m_0b$. Afirmamos que $c = d$, ou seja, c é o máximo divisor comum de a e b. Provemos que $c \mid a$. De fato, caso contrário, teríamos: $a = cq + r$ com $0 < r < c$. Daí,

$$r = a - q(n_0a + m_0b) = (1 - qn_0)a + (-qm_0)b \in A.$$

Mas isso é uma contradição pela minimalidade de c. Então $c \mid a$, e de forma análoga podemos mostrar que $c \mid b$). Daí, c é divisor comum de a e b, logo $c \leq d$. Como $d \mid c$, temos que $d \leq c$. Logo, $c = d$. □

Definição 1.9. *Os inteiros a, b são relativamente primos (ou primos entre si) se $(a, b) = 1$.*

Proposição 1.10. *Para todo inteiro positivo m vale: $(ma, mb) = m(a, b)$.*

Demonstração: De fato, usando a notação da prova do teorema anterior, temos:

$$A = \{xa + yb : x, y \in \mathbb{Z}\}$$
$$B = \{x(ma) + y(mb) : x, y \in \mathbb{Z}\} = m \cdot A.$$

Logo, o menor inteiro positivo de B, ou seja, (ma, mb), é m vezes o menor inteiro positivo de A, ou seja, (a, b). Portanto, $(ma, mb) = m(a, b)$. □

Encontrar o máximo divisor comum de números inteiros "pequenos" é uma tarefa não muito trabalhosa. Porém, para números grandes, como por exemplo 23999 e 9138, a tarefa é algo um pouco mais trabalhosa. Para isso, Euclides criou um algoritmo de divisões sucessivas que ajuda consideravelmente a fazer esse cálculo de maneira muito mais rápida. O Teorema a seguir é ferramenta necessária pra a aplicação do Algoritmo de Euclides.

Teorema 1.11. *Se a e b são inteiros e $a = qb+r$, onde q e r são inteiros, então $(a, b) = (b, r)$.*

Demonstração: Como $a = qb + r$, segue-se que todo divisor comum de b e r também é divisor de a. Mas podemos escrever $r = a - qb$, o que nos diz que todo divisor comum de a e b também é divisor de r. Logo, os conjuntos dos divisores comuns de a e b é igual ao conjunto dos divisores comuns de b e r. Portanto, $(a, b) = (b, r)$. □

Teorema 1.12 (Algoritmo de Euclides)**.** *Sejam a e b inteiros positivos. Aplicamos o algoritmo da divisão sucessivamente para obtermos as equações:*

$$\begin{aligned}
a &= bq_1 + r_1,\ 0 < r_1 < b \\
b &= r_1q_2 + r_2,\ 0 < r_2 < r_1 \\
r_1 &= r_2q_3 + r_3,\ 0 < r_3 < r_2 \\
&\cdots\cdots\cdots\cdots \\
r_{j-2} &= r_{j-1}q_j + r_j,\ 0 < r_j < r_{j-1} \\
r_{j-1} &= r_jq_{j+1} + 0
\end{aligned}$$

O máximo divisor comum de a e b é r_j, ou seja, o último resto não nulo do processo de divisões sucessivas acima.

Demonstração: Se $d = (a, b)$ e olhando o processo acima de "cima para baixo", então $d \mid r_1 \Rightarrow d \mid r_2 \Rightarrow \ldots \Rightarrow d \mid r_j \Rightarrow d \leq r_j$. Por outro lado, olhando de "baixo para cima", percebemos que $r_j \mid r_{j-1} \Rightarrow r_j \mid r_{j-2} \Rightarrow \ldots \Rightarrow r_j \mid r_1 \Rightarrow r_j \mid b \Rightarrow r_j \mid a$. Logo, r_j é divisor comum de a e b e, por definição, $r_j \leq d$. Portanto, $r_j = d = (a, b)$. □

1.1.6 Números primos e compostos

A classe dos números primos é uma das mais importantes dentro do conjunto dos números inteiros. Eles são, pelo Teorema Fundamental da Aritmética, suficientes para gerar todos os outros inteiros, diferentes de $-1, 0, 1$.

Definição 1.13. *Um inteiro $n > 1$ é primo se possuir apenas dois divisores positivos, a saber, 1 e n. Se $n > 1$ não é primo dizemos que n é composto.*

Proposição 1.14. *Se p é primo e $p \mid ab$, então $p \mid a$ ou $p \mid b$.*

Demonstração: Se $p \mid a$, o resultado está demonstrado. Se $p \nmid a$, então $(p, a) = 1$. Mas então $p \mid b$. □

Proposição 1.15. *O menor divisor positivo maior que* 1 *de um inteiro* $a > 1$ *é primo.*

Demonstração: Seja d o menor divisor maior que 1 de a. Suponhamos, por absurdo, que d não seja primo. Sendo assim, d possui um divisor n maior que 1 e menor que d. Esse número é divisor de a, pois $n \mid d$ *e* $d \mid a \Rightarrow n \mid a$, com n maior que 1 e menor que d. Absurdo! □

1.1.7 Teorema Fundamental da Aritmética

O resultado a seguir será utilizado durante todo esse trabalho, por se tratar de um dos resultados mais importantes da matemática.

Teorema 1.16 (Teorema Fundamental da Aritmética)**.** *Todo inteiro maior que* 1 *pode ser representado de maneira única (a menos da ordem) como produto de números primos.*

Demonstração: *i*) **Existência:** Seja n o inteiro maior que 1. Se n for primo, acabamos. Caso contrário, existe p_1 o menor divisor positivo de n maior que 1. Daí, $n = p_1 \cdot n_1$, com p_1 primo. Se n_1 for primo, acabamos. Caso contrário, existe p_2 o menor divisor de n_1 (logo, de n) maior que 1. Daí, $n_1 = p_2 \cdot n_2 \Rightarrow n = p_1 \cdot p_2 \cdot n_2$. Se n_2 for primo, acabamos. Caso contrário, repetimos o processo e obtemos:

$$n = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_s \cdot n_s.$$

Como $n > n_1 > n_2 > \ldots > n_s$, o processo acaba e obtemos:

$$n = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_r,$$

decomposição em produto de primos.

ii) **Unicidade :** Suponha

$$n = p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_s = q_1 \cdot q_2 \cdot q_3 \cdot \ldots \cdot q_r$$

duas decomposições de n como produto de primos. Suponhamos que $s \geq r$. Como q_1 é primo e divide $p_1 \cdot p_2 \cdot p_3 \cdot \ldots \cdot p_s$, segue-se que existe $1 \leq j \leq s$ tal que $q_1 \mid p_j$, logo

$q_1 = p_j$. A menos de uma reordenação, podemos supor que $j = 1$. Assim, $p_1 = q_1$ e obtemos $p_2 \cdot p_3 \cdot \ldots \cdot p_s = q_2 \cdot q_3 \cdot \ldots \cdot q_r$. Repetimos o raciocínio r vezes e obtemos:

$$p_1 = q_1,\ p_2 = q_2,\ \ldots,\ p_r = q_r$$

e se $s > r$, temos

$$p_{r+1} \cdot \ldots \cdot p_s = 1,$$

o que é um absurdo! Logo, $r = s$ e $p_i = q_i$, $\forall i = 1, \ldots, r$.

□

1.1.8 Conguências

Definição 1.17. *Dado $m > 0$, diremos que os inteiros a e b são congruentes módulo m se $m \mid (a - b)$.*

Notação. $a \equiv b\,(mod\,m)$. Se $m \nmid (a - b)$, então denotamos por $a \not\equiv b\,(mod\,m)$.
Observação. $a \equiv b\,(mod\,m) \Leftrightarrow \exists k \in \mathbb{Z}$ tal que $a = b + km$.

Proposição 1.18. *A congruência é uma relação de equivalência*[1] *em $\mathbb{Z}$, isto é, valem as seguintes propriedades:*

i) $a \equiv a\,(mod\,m)$ *(reflexiva);*

ii) *Se* $a \equiv b\,(mod\,m)$, *então* $b \equiv a\,(mod\,m)$ *(simétrica);*

iii) *Se* $a \equiv b\,(mod\,m)$ *e* $b \equiv c\,(mod\,m)$, *então* $a \equiv c\,(mod\,m)$ *(transitiva).*

As provas de $i), ii)$ e $iii)$ seguem diretamente das propriedades de divisibilidade, (c.f. [8]).

Proposição 1.19. *Se a, b, c, d e $m > 0$ são inteiros tais que $a \equiv b\,(mod\,m)$ e $c \equiv d\,(mod\,m)$, então:*

i) $a + c \equiv b + d\,(mod\,m)$;

ii) $ac \equiv bd\,(mod\,m)$.

[1] Ver Seção 1.2.1

Demonstração: *i)* $a \equiv b\,(mod\,m) \Leftrightarrow m \mid (a-b)$ e $c \equiv d\,(mod\,m) \Leftrightarrow m \mid (c-d)$. Logo,

$$m \mid [(a+c)-(b+d)] \Leftrightarrow a+c \equiv b+d\,(mod\,m).$$

Em particular, tomando $c = d$, temos que $a + c \equiv b + c\,(mod\,m)$, uma vez que $c \equiv c(mod\,m)$.

ii) $a \equiv b\,(mod\,m) \Leftrightarrow m \mid (a-b) \Leftrightarrow \exists k \in \mathbb{Z}$ tal que $a = b + km$, e $c \equiv d\,(mod\,m) \Leftrightarrow m \mid (c-d) \Leftrightarrow \exists t \in \mathbb{Z}$ tal que $c = d + tm$. Logo,

$$\begin{aligned} ac &= (b+km)(d+tm) \\ &= bd + btm + dkm + ktm^2 \\ &= bd + sm \\ &\Leftrightarrow m \mid (ac - bd) \\ &\Leftrightarrow ac \equiv bd\,(mod\,m). \end{aligned}$$

Em particular, $ac \equiv bc\,(mod\,m)$ e $a^k \equiv b^k\,(mod\,m)$, supondo, é claro, $a \equiv b\,(mod\,m)$

□

Observação. $ac \equiv bc\,(mod\,m)$ não implica necessariamente que $a \equiv b\,(mod\,m)$. De fato, basta considerar o contra-exemplo:

$$2 \equiv 4\,(mod\,2) \nRightarrow 1 \equiv 2\,(mod\,2).$$

Proposição 1.20. *Se a, b, c e m são inteiros e $ac \equiv bc\,(mod\,m)$, então*

$$a \equiv b\left(mod\,\frac{m}{(m,c)}\right).$$

Demonstração:

$$ac \equiv bc\,(mod\,m) \Leftrightarrow m \mid (a-b)c \Rightarrow \frac{m}{(m,c)} \mid (a-b)\frac{c}{(m,c)}.$$

Mas como $\left(\frac{m}{(m,c)}, \frac{c}{(m,c)}\right) = \frac{(m,c)}{(m,c)} = 1$, segue-se que

$$\frac{m}{(m,c)} \mid a - b \Leftrightarrow a \equiv b \left(mod\, \frac{m}{(m,c)}\right).$$

□

1.1.9 A função maior inteiro

A **Função Maior Inteiro** é definida por

$$\begin{aligned} f : \mathbb{R} &\longrightarrow \mathbb{Z} \\ x &\mapsto \lfloor x \rfloor \end{aligned}$$

onde $\lfloor x \rfloor$ indica o maior inteiro menor ou igual a x.

Proposição 1.21. *A função $\lfloor x \rfloor$ tem as seguintes propriedades:*

i) $\lfloor x + m \rfloor = \lfloor x \rfloor + m$ *se* $m \in \mathbb{Z}$;

ii) $\lfloor x \rfloor + \lfloor -x \rfloor = 0$ *ou* -1, *conforme* x *é um inteiro ou não;*

iii) $\left\lfloor \frac{x}{n} \right\rfloor = \left\lfloor \frac{\lfloor x \rfloor}{n} \right\rfloor$, *em que* $n \in \mathbb{N}$;

iv) $\lfloor x \rfloor + \lfloor y \rfloor \leqslant \lfloor x + y \rfloor$ *para quaisquer* x *e* y *reais.*

As demonstrações da proposição acima são simples e podem ser encontrada em [8] e [12].

Proposição 1.22. *O número de inteiros do conjunto* $\{1, 2, \ldots, n\}$ *que são divisíveis por* a *é dado por* $\left\lfloor \frac{n}{a} \right\rfloor$.

Demonstração: Observe que $n = \left\lfloor \frac{n}{a} \right\rfloor \cdot a + r,\ 0 \leqslant r < a$, o que completa a prova. □

1.2 Estruturas Algébricas

1.2.1 Relação de equivalência e operações binárias

Definição 1.23. *Dados dois conjuntos A e B, chamamos de* **relação** *R entre A e B a todo subconjunto de $A \times B = \{(a, b) : a \in A, b \in B\}$.*

Notação. Dada uma relação R entre dois conjuntos, denotamos por xRy, quando $(x, y) \in R$.

Definição 1.24. *Dado um conjunto A, uma relação R de A em A é uma* **relação de equivalência** *quando as seguintes propriedades são satisfeitas:*

i) $xRx, \forall x \in A$;

ii) $xRy \Rightarrow yRx, \forall x, y \in A$;

iii) xRy *e* $yRz \Rightarrow xRz, \forall x, y, z \in A$.

Definição 1.25. *Seja A um conjunto não vazio. Uma* **operação binária** *em A é uma relação $*$ tal que:*

$$* : A \times A \longrightarrow A$$
$$(a, b) \longmapsto a * b.$$

Notação. Se G é um conjunto e "$*$" uma operação binária em G, dizemos que G é um conjunto munido de $*$, e denotamos por $(G, *)$.

Definição 1.26. *Seja $\sim$ uma relação de equivalência sobre um conjunto A. Para cada $a \in A$, o conjunto de todos os elementos x em A, tais que $x \sim a$, chama-se* **classe de equivalência de a** *e indica-se por $\overline{a}$. Ou seja,*

$$\overline{a} = \{x \in A : x \sim a\}.$$

Um elemento $b \in \overline{a}$ é dito um representante da classe $\overline{a}$. O conjunto de todas as classes de equivalência segundo a relação $\sim$ chama-se conjunto quociente de A por $\sim$ e indica-se por $A/\sim$. Assim,

$$A/\sim = \{\overline{a} : a \in A\}$$

.

Teorema 1.27. *Seja $\sim$ uma relação de equivalência sobre um conjunto A. Então,*

i) $\overline{x} = \overline{y}$ *se, e somente se* $x \sim y, \forall x, y \in A$;

ii) Se $\overline{x} \cap \overline{y} \neq \emptyset$, *então* $\overline{x} = \overline{y}, \forall x, y \in A$;

iii) $\bigcup_{x \in A} \overline{x} = A$.

A demonstração desse teorema decorre das definições anteriores e pode ser encontrada com mais detalhes em [11].

1.2.2 Grupos e subgrupos

Definição 1.28. *Seja G um conjunto não vazio, munido de uma operação binária $*$. Dizemos que $(G, *)$ é um* **grupo** *quando as seguintes propriedades são satisfeitas:*

i) $a * (b * c) = (a * b) * c, \forall a, b, c \in G$;

ii) *Existe um elemento $e \in G$ tal que $e * a = a * e = a, \forall a \in G$;*

iii) *Para todo $a \in G$, existe $b \in G$ tal que $a * b = b * a = e$.*

Observações.

i) O elemento e é único e é chamado **identidade** de G;

ii) Se G, além das propriedades acima, satisfizer $a * b = b * a, \forall a, b \in G$, dizemos que G é um **grupo Abeliano**.

Notações. O elemento b em *iii)* é chamado de **inverso** de a e será denotado por $b = a^{-1}$. Além disso, a partir de agora, utilizaremos G para denotarmos $(G, *)$ e ab para $a * b$.

Definição 1.29. *Seja G um grupo e $x \in G$. Se $n \in \mathbb{Z}$, definimos x^n como segue:*

$$x^n = \begin{cases} e, & se\ n = 0 \\ x^{n-1}x, & se\ n > 0 \\ (x^{-n})^{-1}, & se\ n < 0. \end{cases}$$

Se um grupo G possui n elementos, dizemos que a **ordem de G é** n, e denotamos por $| G | = n$. Se G possui infinitos elementos, dizemos que a **ordem de G é infinita**.

Sejam G um grupo e $a \in G$. Se existe $n \in \mathbb{N}$ tal que $a^n = e$, diz-se que o elemento a tem **ordem finita**, e o menor inteiro m tal que $a^m = e$ chama-se de **ordem de** a, a qual denotaremos por $O(a)$. Caso não exista nenhum $n \in \mathbb{N}$ satisfazendo tal propriedade, então o elemento a é dito de **ordem infinita**.

Definição 1.30. *Seja G um grupo e $H \subseteq G$ não vazio. Se H munido da operação binaria de G é um grupo, dizemos que H é um* **subgrupo** *de G.*

Notação. $H \leq G$

Proposição 1.31. *Sejam G um subgrupo e H um subgrupo de G. Então,*

i) A identidade de H é igual a identidade de G;

ii) Para todo $a \in H$, tem-se que h^{-1} é o inverso multiplicativo de h em H, e coincide com o inverso multiplicativo de h em G.

A demonstração desse fato segue do fato de H também ser um grupo, e pode ser vista com detalhes em [12].

Proposição 1.32. *Sejam G um grupo e H um subconjunto não vazio de G. Então H é um subgrupo de G se, e somente se, o menos uma das seguintes condições são satisfeitas:*

i) $ab \in H$ e $b^{-1} \in H, \forall a, b \in H$;

ii) $ab^{-1} \in H, \forall a, b \in H$.

Demonstração: Se H é subgrupo de G, então ficam claros os itens $i)$ e $ii)$.
Reciprocamente, suponhamos que H satisfaz a condição $i)$. Logo, para qualquer a em H, temos $a^{-1} \in H$. Assim, $e = a \cdot a^{-1} \in H$, o que nos leva a conclusão que H é subgrupo de G. Finalmente, se H satisfaz $ii)$, então dados $a, b \in H$,

$$e = b \cdot b^{-1} \in H \Rightarrow b^{-1} = eb^{-1} \in H$$

Daí,

$$a \cdot b = a \cdot (b^{-1})^{-1} \in H$$

Portanto, H é um subgrupo de G. □

1.2.3 Grupos cíclicos

Definição 1.33. *Sejam G um grupo e $a \in G$.*

i) O conjunto de todas as potencias de a, dado por

$$H = \{a^n : n \in \mathbb{Z}\}$$

é um subgrupo de G, e o chamamos de **subgrupo cíclico gerado por a**;

Notação. $H = \langle a \rangle$.

ii) Dizemos que G é um grupo cíclico quando existe $a \in G$, com $G = \langle a \rangle$.

Proposição 1.34. *Todo grupo cíclico é abeliano.*

Demonstração: Seja G um grupo cíclico e $a \in G$ tal que

$$G = \langle a \rangle = \{a^n : n \in \mathbb{Z}\}.$$

Dados, x_1, $x_2 \in G$, digamos $x_1 = a^{n_1}$ e $x_2 = a^{n_2}$,

$$x_1 \cdot x_2 = a^{n_1} \cdot a^{n_2} = a^{n_1+n_2} = a^{n_2+n_1} = a^{n_2} \cdot a^{n_1} = x_2 \cdot x_1.$$

Ou seja, G é abeliano. □

Teorema 1.35. *Seja G um grupo e $a \in G$.*

i) Se $a^n = e$ para algum $n \in \mathbb{N}$, então $O(a)$ divide n;

ii) Se $O(a) = m$, então para qualquer $k \in \mathbb{Z}$, então $a^k = a^r$, com r sendo o resto da divisão de k por m;

iii) $O(a) = m$ se, e somente se, $| \langle a \rangle | = m$.

Demonstração: *i)* Como $a^n = e$, então a tem ordem finita. Seja $O(a) = m$, pelo Algoritmo da Divisão, existem $q, r \in \mathbb{Z}$ tais que $n = mq + r$ com $0 \leq r < m$. Logo,

$$e = a^n = (a^m)^q \cdot a^r = e^q \cdot a^r \Rightarrow a^r = e.$$

Pela minimalidade de m, concluímos que $r = 0$. Portanto, $n = mq$;

ii) Note que para cada $k \in \mathbb{Z}$, $k = mq + r$, com $q, r \in \mathbb{Z}$ e $0 \leq r < m$. Portanto, pelo item *i)*, temos que $a^k = a^r$.

iii) Se $O(a) = m$, segue que os elementos $e, a, a^2, \ldots, a^{m-1}$ são todos distintos. Com efeito, se $a^i = a^j$, para $0 \leq i < j \leq m-1$, então $a^{j-i} = e$, e $j - i < m$, o que é uma

contradição, pois $O(a) = m$. Agora, seja $H = \langle a \rangle$. Pelo item $ii)$, sabemos que dado $k \in \mathbb{Z}$, $a^k = a^r$, sendo $r \in \{0, 1, \ldots, m-1\}$. Por isso,

$$H = \langle a \rangle = \{a^k : k \in \mathbb{Z}\} = \{a^r : r = 0, 1, \ldots, m-1\}$$

tem ordem m.

Reciprocamente, suponhamos que $H = \langle a \rangle$ tem ordem finita. Isto nos diz que as potências a^i, com $i \in \mathbb{Z}$, não podem ser todas distintas. Por isso, existem $i, j \in \mathbb{Z}$, com $i < j$, de maneira que $a^i = a^j$, isto é, $a^{j-i} = e$. Mas isso implica que a tem ordem finita, digamos $O(a) = m$. Assim, como dito anteriormente, os elementos $e, a, a^2, \ldots, a^{m-1}$ são todos distintos. Pelo item $ii)$

$$H = \langle a \rangle = \{a^r : r = 0, 1, \ldots, m-1\} = \{e, a, a^2, \ldots, a^{m-1}\}$$

ou seja, a ordem de H é m.

□

1.2.4 Classes laterais e o Teorema de Lagrange

Seja G um grupo e H um subgrupo de G. Seja a relação de equivalência "$\equiv (mod\, H)$" dada, para quaisquer $a, b \in G$, por

$$a \equiv b (mod\, H) \Leftrightarrow a^{-1}b \in H.$$

Proposição 1.36. *A classe de equivalência de um elemento $g \in G$, relativa a esta relação, é dada por $\{gh : h \in H\}$.*

Demonstração: Dado $g \in G$, seja $\overline{g}$ a classe de equivalência de g relativa à relação $\equiv$. Por definição, $\overline{g} = \{x \in G : g \equiv x (mod\, H)\}$. Então, para $x \in G$,

$$x \in \overline{g} \Leftrightarrow g \equiv x (mod\, H) \Leftrightarrow g^{-1}x \in H,$$

ou seja, $g^{-1}x = h \in H \Rightarrow x = gh \in \{gh : h \in H\}$. Portanto, $\overline{g} \subset \{gh : h \in H\}$.

Se $x \in \{gh : h \in H\}$, então existe $h \in H$ tal que $x = gh$, ou seja, $g^{-1}x = h$. O que implica que $g \equiv x(mod\, H)$ e assim, $x \in \overline{g}$. Portanto, $\{gh : h \in H\} \subset \overline{g}$. □

Vamos denotar a classe de equivalência $\overline{g}$ por gH, e a chamaremos de **classe lateral de g à esquerda**. Assim,

$$gH = \{gh : h \in H(mod\, H)\}.$$

O conjunto de todas as classes laterais à esquerda de H, será denotado por H_E, ou seja,

$$H_E = \{gH : g \in G\}.$$

Como gH é uma classe de equivalência, então pelo Teorema 1.27, temos:

i) $G = \bigcup_{g \in G} gH$;

ii) Se $x, y \in G$, então $xH \cap yH = \emptyset$ ou $xH = yH$.

Definição 1.37. *Sejam G um grupo e H um subgrupo de G. A cardinalidade do conjunto H_E chama-se de* **o índice de H em G** *e será denotado por $(G : H)$.*

Teorema 1.38. *Sejam G um grupo finito e H um subgrupo de G. Então, toda classe lateral à esquerda tem a mesma cardinalidade de H.*

Demonstração: Para cada $g \in G$, consideremos a função

$$f : H \to gH$$
$$h \mapsto gh.$$

É claro que f é sobrejetora[2]. Além disso, dados $h_1, h_2 \in H$, obtemos

$$f(h_1) = f(h_2) \Rightarrow gh_1 = gh_2 \Rightarrow h_1 = h_2.$$

Logo f é injetora[3], e portanto, bijetora[4]. Assim a cardinalidade de gH é a mesma de H. □

[2]Dizemos que uma função f qualquer é sobrejetora se a imagem de f for igual ao contradomínio de f, ou seja, se $Im(f) = CD(f)$.

[3]Dizemos que uma função f qualquer é injetora se para todo $x, y \in D(f)$, tem-se $f(x) = f(y) \Rightarrow x = y$.

[4]Uma função é bijetora quando ela é injetora e sobrejetora.

Teorema 1.39 (Teorema de Lagrange)**.** *Sejam G um grupo finito e H um subgrupo de G. Então, a ordem de H divide a ordem de G. Especificamente,*

$$|G| = |H| \cdot (G : H).$$

Demonstração: Como G é finito, então $(G : H)$ também o é, digamos $(G : H) = r$. Seja $H_E = \{a_1H, a_2H, \ldots, a_rH\}$. Como H_E é uma partição de G, então

$$\dot{\bigcup_{i=1}^{r}} a_iH$$

Desse modo, pela Proposição 1.38, temos

$$|G| = \underbrace{|H| + |H| + \ldots + |H|}_{r\,vezes} = |H| \cdot r,$$

ou seja, $|G| = |H| \cdot (G : H)$. □

Corolário 1.40. *Sejam G um grupo finito e $g \in G$. Então, a ordem de g divide a ordem de G. Em particular, $g^{|G|} = e$.*

Demonstração: Pelo item *iii*) do Teorema 1.35, temos que $O(g) = |\langle g \rangle|$. Logo, aplicando o Teorema de Lagrange ao subgrupo $|\langle g \rangle|$, segue que $O(g) = \lambda$ divide $|G|$. Portanto existe $k \in \mathbb{N}$ tal que $|G| = \lambda \cdot k$. Assim,

$$g^{|G|} = g^{\lambda \cdot k} = (g^{\lambda})^k = e^k = e.$$

□

1.3 Alguns conceitos topológicos

Vamos definir o que é uma topologia sobre um conjunto e algumas propriedades importantes. Para mais informações consulte [6].

Definição 1.41. *Seja X um conjunto e $\mathcal{T}$ uma coleção de subconjuntos de X. Dizemos que $\mathcal{T}$ é uma topologia em X, se satisfaz as seguintes condições*

i) $\emptyset$ *e* X *estão em* $\mathcal{T}$*;*

ii) A união qualquer de elementos de $\mathcal{T}$ *ainda pertence a* $\mathcal{T}$*;*

iii) A interseção finita de quaisquer elementos de X *pertence a* $\mathcal{T}$*.*

Um **espaço topológico**, é um par $(X, \mathcal{T})$, onde X é um conjunto e $\mathcal{T}$ é uma topologia em X. Desde que não haja confusão, chamaremos de X o espaço $(X, \mathcal{T})$. Cada elemento de $\mathcal{T}$ é chamado de **conjunto aberto**.

Exemplo 1.42. *Seja* X *um conjunto com* 3 *elementos* $X = \{a, b, c\}$*, e tome* $\mathcal{T} = \{\{a, b\}, \{b\}, \{b, c\}, \emptyset, X\}$ *É fácil ver que* $\mathcal{T}$ *é uma topologia sobre* X*. Tome agora* $\mathcal{T} = \{\{a\}, \{b\}, \emptyset, X\}$*. Observe que a união de dois subconjuntos de* $\mathcal{T}$ *nem sempre é aberta, pois* $\{a\} \cup \{b\} = \{a, b\} \notin \mathcal{T}$*.*

Exemplo 1.43. *Seja* X *um conjunto qualquer. A coleção de todos os subconjuntos de* X *é claramente uma topologia sobre* X*. Chamamos essa topologia de* **topologia discreta**. *A coleção* $\emptyset$ *e* X*, é também uma topologia e é chamada de* **topologia trivial**.

Exemplo 1.44. *Seja* $X = \mathbb{R}$ *e tome a seguinte coleção :*

$$\mathcal{T} = \{\emptyset, A \subset \mathbb{R}\},$$

onde $A \in \mathcal{T}$ *se, e somente se para todo* $x \in A$ *existe um intervalo aberto* (a, b) *tal que* $x \in (a, b) \subset A$*.*

Afirmação. $\mathcal{T}$ *é uma topologia sobre* $\mathbb{R}$*.*

i) Claramente $\emptyset$ *e* $\mathbb{R} \in \mathcal{T}$*;*

ii) Se tomarmos $\{A_\alpha \in \mathcal{T} : \alpha \in \Gamma\}$*, então*

$$\bigcup_{\alpha \in \Gamma} A_\alpha \in \mathcal{T}.$$

De fato, se $x \in \bigcup_{\alpha \in \Gamma} A_\alpha$*, então existe* $\alpha_0 \in \Gamma$ *tal que* $x \in A_{\alpha_0} \in \mathcal{T}$*. Logo existe* (a, b) *e:*

$$x \in (a, b) \subset A_{\alpha_0} \subset \bigcup_{\alpha \in \Gamma} A_\alpha;$$

iii) Sejam B_1 e $B_2 \in \mathcal{T}$. Dado $x \in B_1 \cap B_2$, temos que $x \in B_1 \in \mathcal{T}$ e $x \in B_2 \in \mathcal{T}$, logo existem (a_1, b_1) e (a_2, b_2) tais que $x \in (a_1, b_1) \subset B_1$ e $x \in (a_2, b_2) \subset B_2$. Se denotarmos por $a = \max\{a_1, a_2\}$ e $b = \min\{b_1, b_2\}$, então $x \in (a, b) \subset B_1 \cap B_2$.

Definição 1.45. *Um subconjunto A de um espaço topológico X é dito um* **Conjunto Fechado**, *se $X - A$[5] é um Conjunto Aberto.*

Teorema 1.46. *Seja X um espaço topológico. Então*

i) $\emptyset$ e X são conjuntos fechados;

ii) Uma interseção qualquer de conjuntos fechados é fechada;

iii) Uma união finita de conjuntos fechados é fechada.

Demonstração: *i)* O complementar de $\emptyset$ é X e o complementar de X é $\emptyset$. Ambos são conjuntos abertos, portanto, $\emptyset$ e X são conjuntos fechados;

ii) Dada uma coleção de conjuntos fechados $\{A_j\}_{j\in\lambda}$, temos que

$$X - \bigcap_{j\in\lambda} A_j = \bigcup_{j\in\lambda} (X - A_j).$$

Como $X - A_j$ é aberto para todo $j \in \lambda$, então $\bigcup_{j\in\lambda}(X - A_j)$ é aberto e portanto, $\bigcap_{j\in\lambda} A_j$ é fechado;

ii) Sejam $A_1, A_2, \ldots, A_n$, com $n \in \mathbb{N}$, temos

$$X - \bigcup_{j=1}^{n} A_j = \bigcap_{j=1}^{n} (X - A_j).$$

De forma similar ao item *ii)*, como cada A_j é fechado, então $(X - A_j)$ é aberto e portanto $\bigcap_{j=1}^{n}(X - A_j)$ é aberto. Assim, $\bigcup_{j=1}^{n} A_j$ é fechado.

□

[5] $X - A$ é o complementar de A em relação a X.

Capítulo 2

Dez demonstrações da infinitude dos números primos

O Teorema de Euclides, enunciado a seguir, será demonstrado de dez formas diferentes ao decorrer desse capítulo.

Teorema 2.1. *O conjunto dos números primos possui infinitos elementos.*

2.1 Demonstrações no campo da teoria dos números

A demonstração dada por Euclides, é a mais conhecida pelos matemáticos de todo o mundo. Na Proposição 20, do volume 9 de [2], Euclides faz a seguinte demonstração:

> "Os números primos são mais numerosos do que toda quantidade que tenha sido proposta de números primos.
> Sejam os números primos que tenham sido propostos A,B, C; digo que os números primos sejam mais numerosos do que os A,B, C. Fique, pois, tomado o menor medido pelos A,B, C e seja o DE, e fique acrescida a unidade DF ao DE. Então, o EF ou é primo ou não. Primeiramente, seja primo; portanto, os números primos A,B, C, EF achados são mais numerosos do que os A,B, C. Mas, então, não seja primo o EF; portanto, é medido por algum número primo. Seja medido pelo primo G; digo que o G não é o mesmo que algum dos A,B, C. Pois, se possível, seja. Mas os A,B, C medem o DE; portanto, o G também medirá o DE. E também mede o EF; e o G, sendo um número, medirá a unidade DF restante; o que é absurdo. Portanto, o G não é o mesmo que algum dos A B, C. E foi suposto primo. Portanto, os números primos achados, A,B, C, G são mais numerosos do que a quantidade que tenha sido proposta dos A,B, C; o que era preciso provar."

Apresentada dessa forma ela é trabalhosa de se entender, devido á linguagem utilizada. Assim, a mesma demonstração pode ter uma releitura de forma mais clara, utilizando uma linguagem matemática mais atual, como veremos a seguir. Essa demonstração utiliza apenas os conceitos de divisibilidade da Teoria dos Números, vistos na seção 1.1.3, e pode ser encontrada em [8].

Demonstração do Teorema 2.1. Suponha que há um número finito de elementos no conjunto $\mathbb{P}$ dos números primos, ou seja, $\mathbb{P} = \{p_1, p_2, \ldots, p_k\}$. Tome o número inteiro

$$P = p_1 \cdot p_2 \cdot \ldots \cdot p_k + 1.$$

Como $P \neq p_i, i = 1, 2, \ldots, k$, então exite p primo, com $p \mid P$. Mas $p = p_i$, para algum $i = 1, 2, \ldots, k$. Assim,

$$p \mid (P - p_1 \cdot p_2 \cdot \ldots \cdot p_k)$$

ou seja, $p \mid 1$. Absurdo! Portanto, há uma infinidade de números primos. □

A segunda demonstração, semelhante à de Euclides, é atribuída a Métrod (1917) e também utiliza ferramentas simples da teoria dos números, como o conceito de divisibilidade.

Demonstração do Teorema 2.1. Suponha que $p_1 < p_2 < \ldots < p_k$, é a lista dos k números

primos existentes. Seja

$$N = p_1 \cdot p_2 \cdot \ldots \cdot p_k$$

e para cada $i = 1, 2, \ldots, k$ considere

$$Q_i = \frac{N}{p_i} = p_1 \cdot p_2, \cdot \ldots \cdot p_{i-1} \cdot p_{i+1} \cdot \ldots \cdot p_k.$$

Observe que p_i não divide Q_i, mas divide Q_j para $j \neq i$.

Seja

$$S = \sum_{j=1}^{k} Q_j.$$

Como

$$S = p_2 \cdot \ldots \cdot p_n + \ldots + p_1 \cdot \ldots \cdot p_{i-1} \cdot p_{i+1} \cdot \ldots \cdot p_n + \cdot \ldots \cdot + p_1 \cdot p_2 \cdot \ldots \cdot p_{n-1},$$

então S é maior que cada p_i, o que implica que S não é nenhum dos p_i. Pelo Teorema 1.16, algum p_i divide S, com $i = 1, 2, \ldots, k$. Assim,

$$p_i \mid (S - \sum_{j \neq i} Q_j) \Longleftrightarrow p_i \mid Q_i$$

O que é um absurdo! □

Kummer (1873), utilizou um fato conhecido de simples verificação, que diz que todo par de inteiros positivos consecutivos são primos entre si, para se concluir a infinitude dos números primos.

Lema 2.2. *Para todo $n > 2$ inteiro positivo, $(n, n-1) = 1$. Em particular se $n = p_1 p_2, \ldots p_k > 2$, então deve existir $p \neq p_1$, para todo $i = 1, \ldots, k$, tal que $p \mid (n-1)$.*

Demonstração: Suponhamos que $(n, n-1) = d \neq 1$. Como $n = (n-1) \cdot 1 + 1$, pela Proposição 1.11, $(n, n-1) = (n-1, 1)$ Logo, $d = 1$. Absurdo! Em Particular, para $n = p_1 p_2 \ldots p_k > 2$, temos que, como $(n, n-1) = 1$, se $p_i \mid n \Rightarrow p_i \nmid (n-1), i = 1, \ldots, k$. Então temos duas opções para $n-1$: Ou $n-1$ é primo, ou ele é composto. Como garante o Teorema 1.16, existe um p primo diferente de todo p_i, $\forall i = 1, \ldots, k$ tal que $p \mid (n-1)$. □

Demonstração do Teorema 2.1. Sejam $p_1, p_2, \ldots, p_k$ todos os primos e $n = p_1 \cdot p_2 \cdot \ldots \cdot p_k > 2$. Como $(n, n-1) = 1$ e existe $p \neq p_i$ tal que $p \mid (n-1)$, então pelo Lema 2.2, p é um primo diferente de todos os p_i. Absurdo!

□

2.2 A demonstração de Thue

Aqui, temos uma variação da demonstração de Thue (1897), um pouco mais ricas em detalhes, onde vemos a utilização de conceitos de logaritmos, e funções.

Lema 2.3. *Fixado $n \in \mathbb{N}$, existe k suficientemente grande tal que $2^k > (k+1)^n$.*

Demonstração: Sejam as funções $f(x) = 2^x$ e $g(x) = (x+1)^n$. Vamos mostrar que

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

Usando as Regras de l'Hôpital[1], temos:

$$\begin{aligned}
\lim_{x \to +\infty} \frac{f(x)}{g(x)} &= \lim_{x \to +\infty} \frac{2^x}{(x+1)^n} \\
&= \lim_{x \to +\infty} \frac{ln\,2 \cdot e^{x \cdot ln\,2}}{(n) \cdot (x+1)^{n-1}} \\
&= \ldots \\
&= \lim_{x \to +\infty} \frac{(ln\,2)^{n-1} \cdot e^{x \cdot ln\,2}}{(n)! \cdot (x+1)} \\
&= \lim_{x \to +\infty} \frac{(ln\,2)^{n} \cdot e^{x \cdot ln\,2}}{(n)!} \\
&= \frac{(ln\,2)^n}{(n)!} \cdot \lim_{x \to +\infty} e^{x \cdot ln\,2} = +\infty.
\end{aligned}$$

[1] As Regras de l'Hôpital são ferramentas do cálculo que auxiliam no cálculo de limites de funções, onde aparecem indeterminações matemáticas do tipo $\frac{\infty}{\infty}$ ou $\frac{0}{0}$. Elas dizem que se $\lim_{x \to p} f(x) = +\infty$ e $\lim_{x \to p} g(x) = +\infty$, então:

$$\lim_{x \to p} \frac{f(x)}{g(x)} = \lim_{x \to p} \frac{f'(x)}{g'(x)}.$$

Assim, para todo $A > 0$, existe $B > 0$ tal que

$$x > B \Rightarrow \frac{2^x}{(x+1)^n} > A.$$

Em particular, tome $A = 1$, logo $2^x > (x+1)^n$. □

Demonstração do Teorema 2.1. Suponha que exista um total de n primos $p_1 = 2, p_2, \ldots, p_n$. Tome k suficientemente grande tal que $2^k > (k+1)^n$. Considere a função $f : \{1, 2, \ldots, 2^k\} \longrightarrow \{0, 1, \ldots, k\}^n$ definida por $f(x) := (e_1, e_2, \ldots, e_n)$, onde $x = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_n^{e_n}$. Pelo Teorema Fundamental da Aritmética (TFA), todo número natural pode ser escrito na forma $p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_n^{e_n}$. Logo a função esta bem definida. Resta-nos saber se $f(x) \in \{0, \ldots k\}^n$ para todo x do domínio.

Como $x \leqslant 2^k$, temos que

$$\begin{aligned} k = \log 2^k \geqslant \log x &= \log\left(p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_n^{e_n}\right) \\ &= e_1 \cdot \log p_1 + e_2 \cdot \log p_2 + \ldots + e_n \cdot \log p_n \\ &\geqslant e_1 + e_2 + \ldots + e_n \\ &\geqslant \max\{e_1, e_2, \ldots, e_n\} \end{aligned}$$

onde o logaritmo acima é tomado na base 2. Logo $0 \leqslant e_i \leqslant k$, com $i = 1, 2, \ldots, k$.Portanto $f(x) \in \{0, \ldots k\}^n$. Pelo TFA e assumindo a existência de apenas n primos, fica clara a injetividade da função, uma vez que se dois números possuem os mesmos expoentes em sua fatoração, eles são iguais. Porém, encontramos uma função injetiva de um conjunto com cardinalidade 2^k em um outro conjunto com cardinalidade $(k+1)^n$. Portanto,

$$2^k \leqslant (k+1)^n.$$

Absurdo! □

2.3 A demonstração de Goldbach

Goldbach, em uma carta a Euler, datada de 20/31 de julho de 1730, fez uma demonstração da infinidade de números primos, encontrando uma sequência de números tais que dois a dois

são primos entre si. A fim desse objetivo, ele fez uso dos números de Fermat, para mostrar que, como eles são dois a dois primos entre si, então satisfazem a condição procurada, comprovando o resultado.

Definição 2.4. *Um número da forma* $F_n = 2^{2^n} + 1$ *é chamado de número de Fermat.*

Lema 2.5. $F_0 \cdot F_1 \cdot \ldots \cdot F_{n-1} = F_n - 2$.

Demonstração: Para isso utilizaremos indução finita na primeira forma Para $n = 1$, temos:

$$F_0 = 2^{2^0} + 1 = 3 = 4 + 1 - 2 = 2^{2^1} + 1 - 2 = F_1 - 2.$$

Suponha que $F_0 \cdot F_1 \cdot \ldots \cdot F_{n-1} = F_n - 2$. Então,

$$\begin{aligned} F_0 \cdot F_1 \cdot \ldots \cdot F_{n-1} \cdot F_n &= (F_n - 2) \cdot F_n \\ &= (2^{2^n} + 1 - 2) \cdot (2^{2^n} + 1) \\ &= (2^{2^n} - 1) \cdot (2^{2^n} + 1) \\ &= 2^{2^n} \cdot 2^{2^n} - 1 \\ &= 2^{2^n + 2^n} - 1 \\ &= 2^{2^{n+1}} - 1 \\ &= 2^{2^{n+1}} + 1 - 2 \\ &= F_{n+1} - 2. \end{aligned}$$

□

Lema 2.6. *Quaisquer dois números de Fermat distintos,* F_n *e* F_m*, são relativamente primos.*

Demonstração: Com efeito, tome $m > n$. Assim,

$$F_m - F_0 \cdot F_1 \cdot \ldots \cdot F_{m-1} = 2.$$

Portanto se d divide F_m e F_n, então d divide 2. Mas F_n é impar e portanto $d = 1 \Rightarrow (F_n, F_m) = 1$. □

Demonstração do Teorema 2.1. A sequência dos números $F_0, F_1, \ldots, F_n, \ldots$ é infinita, e pelo Lema 2.6, é composta apenas de números naturais relativamente primos. Então, pelo

TFA, para cada F_i existem primos p_i, tais que se p_1 é um fator primo de F_1, p_2 é um fator primo de $F_2, \ldots, p_n$ é um fator primo de $F_n, \ldots$, então $p_1, p_2, \ldots, p_n, \ldots$ são todos distintos. Portanto existem infinitos primos. □

2.4 A demonstração de Lagrange

A próxima demonstração utiliza argumentos algébricos, como o Teorema de Lagrange.

Demonstração: Suponha que o conjunto dos números primos seja finito, com p sendo o maior primo. Consideremos o Primo de Mersenne[2] $2^p - 1$ e mostremos que qualquer fator primo q de $2^p - 1$ é maior que p. Para tanto, tome q um divisor primo de $2^p - 1 \Rightarrow 2^p \equiv 1(mod\ q)$. Como p é primo, então isso significa que o elemento 2 tem ordem p no grupo multiplicativo $\mathbb{Z}_q - \{\overline{0}\}$ Como $\mathbb{Z}_q - \{\overline{0}\}$ possui $q - 1$ elementos, pelo Corolário 1.40,

$$p \mid (q-1) \Rightarrow p < q.$$

□

2.5 A demonstração de Erdös

Aqui, veremos um resultado forte sobre os números primos. A divergência da série dos recíprocos primos foi provado inicialmente por Euler. Porém, a demonstração aqui apresentada se deve a Erdös. Como veremos a seguir, esse fato implica a infinitude dos números primos.

Lema 2.7. *Para todo $n \in \mathbb{N}$, existem a_n e b_n, também naturais, com a_n livre de quadrados, tais que $n = a_n \cdot (b_n)^2$.*

Demonstração: Observe que, pelo Teorema 1.16, para todo $n \in \mathbb{N}$,

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n}.$$

[2]Os primos de Mersenne são números inteiros da forma $2^p - 1$, onde p é um primo.

Como cada $\alpha_i \in \mathbb{N}$, então ou α_i é par ou é ímpar. Seja $S = \{i \in S : \alpha_i \text{ é impar } \}$ e

$$\beta_i = \begin{cases} \alpha_i, \ se \ i \ \in \ S \\ \alpha_i \ - \ 1, \ se \ i \ \notin \ S \end{cases}.$$

Assim, escrevemos

$$n = \prod_{j \in S} p_j \cdot \prod_{i \in \mathbb{N}} p_i^{\beta_i}.$$

Note que cada β_i é par, e $\beta_i = 2 \cdot \gamma_i$, assim,

$$n = \prod_{j \in S} p_j \cdot \left(\prod_{i \in \mathbb{N}} p_i^{\gamma_i} \right)^2.$$

Portanto, tomando $a_n = \prod_{j \in S} p_j$ e $b_n = \prod_{i \in \mathbb{N}} p_i^{\gamma_i}$, temos que todo $n \in \mathbb{N}$ pode ser escrito da forma $n = a_n \cdot (b_n)^2$, onde $a_n, b_n \in \mathbb{N}$ e a_n é livre de quadrados. □

Lema 2.8. *A série dos inversos multiplicativos dos números primos diverge, ou seja*

$$\sum_{p \ primo} \frac{1}{p_i}$$

diverge.

Demonstração: Seja $p_1, p_2, \ldots$ a sequência dos números primos, e suponha que a série acima convirja. Logo, existe $k \in \mathbb{N}$ tal que $\sum_{i>k} \frac{1}{p_i} < \frac{1}{2}$.

Definiremos dois conjuntos de números naturais da seguinte forma: chamaremos de **primos pequenos** aos primos com índice menores que k, e de **primos grandes** a todos os outros. Para um $N \in \mathbb{N}$, tome N_g, como sendo a quantidade de naturais $n \leq N$ que são múltiplos de algum múltiplo grande, e N_p a quantidade de naturais $n \leq N$ que possuem apenas primos pequenos em sua fatoração. Dessa forma, é natural esperarmos que $N = N_p + N_g$, porém chegaremos a uma conclusão diferente, o que terminará a demonstração. Para isso, vamos estimar as quantidades N_p e N_g.

Para N_g, observe que, pela Proposição 1.22 a quantidade de múltiplos de um p_i menores ou iguais a N é exatamente $\left\lfloor \frac{N}{p_i} \right\rfloor$. Assim, como os primos grandes são aqueles em que $i > k$, então:

$$N_g = \sum_{i>k} \left\lfloor \frac{N}{p_i} \right\rfloor \leq \sum_{i>k} \frac{N}{p_i} = n \cdot \sum_{i>k} \frac{1}{p_i} < N \cdot \frac{1}{2} = \frac{N}{2}.$$

Para estimarmos N_p, temos que, como $n \leq N$ então, n pode ser escrito na forma $n = a_n \cdot (b_n)^2$, com a_n e b_n definidos no Lema 2.7. Assim, estimaremos as quantidades de a_n e b_n. Como a_n é livre de quadrados e possui apenas primos pequenos em sua fatoração, a quantidade de números dessa forma é a quantidade de subconjuntos do conjunto $\{p_1, p_2, \ldots, p_k\}$, que é 2^k. Note ainda que $(b_n)^2 \leq n \leq N \Rightarrow b_n \leq \sqrt{n} \leq \sqrt{N}$. Com isso vemos que temos no máximo $\sqrt{n}$ escolhas para b_n. Logo,

$$N_p \leq 2^k \cdot \sqrt{n}.$$

Assim, com os valores estimados para N_p e N_g, temos:

$$\begin{aligned} N = N_g + N_p < \frac{N}{2} + 2^k \cdot \sqrt{N} &\iff \frac{N}{2} < 2^k \cdot \sqrt{N} \\ &\iff \frac{N}{\sqrt{N}} < 2^k \\ &\iff \sqrt{N} < 2^{k+1} \\ &\iff N < 2^{2k+2}. \end{aligned}$$

Tomando $N = 2^{2k+2}$, temos um absurdo! Portanto a série diverge. □

Demonstração do Teorema 2.1. Se existisse uma quantidade finita de números primos, então a soma acima claramente convergiria. Porém, como a série diverge, então existem infinitos primos. □

2.6 A demonstração de Euler

Nessa demonstração, Euler usa conceitos da mais alta importância, e que são estudados na Teoria Analítica dos Números, como a função $\pi(x)$[3] de contagem de números primos. Essa função foi produto de pesquisas de matemáticos como Gauss(1792), Legendre(1808),

[3]Uma das grandes descobertas do final do século XIX, mais precisamente em 1896, a qual citamos aqui sem apresentar sua mais profunda demonstração, é o chamado Teorema dos Números Primos e que leva os nomes dos matemáticos Cauchy/Hadamard/de la Valée Poussin. Ele descreve o comportamento assintótico

Riemman(1859). Eles estudaram o comportamento dessa função, comparando-a à funções já conhecidas.

Lema 2.9. *Seja $m, p_i \in \mathbb{N}$ com p_i primo. Então*

$$\sum_{m=1}^{\infty} \frac{1}{m} = \prod_{i=1}^{\infty} \left(\sum_{k \geqslant 0} \frac{1}{{p_i}^k} \right).$$

Demonstração: Para a demonstração desse fato é só vermos que, pelo Teorema Fundamental da Aritmética, todo número pode ser escrito de maneira única como produto de potências de fatores primos. A expansão do produto do segundo membro da igualdade é

$$\begin{aligned}
\prod_{i=1}^{\infty} \left(\sum_{k \geqslant 0} \frac{1}{{p_i}^k} \right) &= \left(\sum_{k \geqslant 0} \frac{1}{{p_1}^k} \right) \cdot \left(\sum_{k \geqslant 0} \frac{1}{{p_2}^k} \right) \cdot \ldots \cdot \left(\sum_{k \geqslant 0} \frac{1}{{p_n}^k} \right) \cdot \ldots \\
&= \left(1 + \frac{1}{p_1} + \frac{1}{p_1^2} + \ldots + \frac{1}{p_1^n} + \ldots \right) \cdot \left(1 + \frac{1}{p_2} + \frac{1}{p_2^2} + \ldots + \frac{1}{p_2^n} + \ldots \right) \\
&\cdot \ldots \cdot \left(1 + \frac{1}{p_r} + \frac{1}{p_r^2} + \ldots + \frac{1}{p_r^n} + \ldots \right) \cdot \ldots \\
&= \left(1 + \frac{1}{p_1} + \frac{1}{p_2} + \ldots + \frac{1}{p_r} + \ldots \right) + \ldots + \left(\frac{1}{p_1^n} + \frac{1}{p_2^n} + \ldots + \frac{1}{p_r^n} + \ldots \right) \\
&+ \ldots + \left(\frac{1}{p_1 p_2} + \ldots \frac{1}{p_r^n p_{r+1}^n} + \ldots \right) + \ldots + \frac{1}{p_1^{n_1} p_2^{n_2} \ldots p_r^{n_r} \ldots}.
\end{aligned}$$

Note que os denominadores dos elemento da expansão do segundo membro da igualdade acima são todos os números naturais, pois o produto varia em todos os números primos. Logo, para todo $m \in \mathbb{N}$, $\frac{1}{m}$ está na expansão do produto do segundo membro. □

Demonstração do Teorema 2.1. Seja $\pi(x) = \#\{p \leq x : p \text{ é primo positivo}\}$ a função de contagem dos números primos e tome o logaritmo natural $\log x$, definido como

$$\log x = \int_1^x \frac{1}{t} dt$$

.

da função $\pi(x)$. Mais precisamente,

$$\lim_{x \longrightarrow \infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1.$$

Isto quer dizer que, se x é grande, a quantidade dos números primos menores do que ou iguais a x é dada, com aproximação cada vez melhor, por $\frac{x}{\ln x}$.

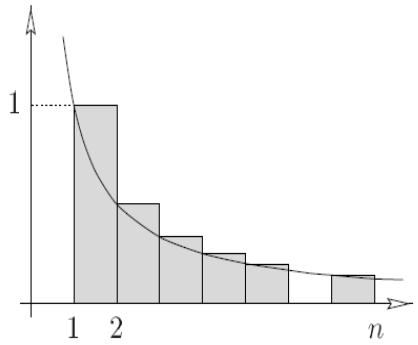

Figura 2.1: Gráfico da função $f(x) = \frac{1}{t}$.

Agora, vamos comparar a área sob o gráfico de $f(x) = \frac{1}{t}$, com a soma das áreas dos retângulos da figura 2.1.

$$1 + \frac{1}{2} + \ldots + \frac{1}{n} \geqslant \int_1^n \frac{1}{t} dt \Rightarrow \sum_{n=1}^{n} \frac{1}{n} \geqslant \log n.$$

Assim, para $n \leq x \leq n+1$, temos:

$$\log x \leqslant 1 + \frac{1}{2} + \ldots + \frac{1}{n} \leqslant \sum \frac{1}{m}$$

com $m \in \mathbb{N}$ tendo apenas divisores primos $p \leq x$. Pelo Teorema 1.16, todo m pode ser escrito como

$$m = \prod_{p \leqslant x} p^{k_p}.$$

Assim, pelo Lemma 2.9

$$\sum \frac{1}{m} = \prod_{\substack{p \leqslant x \\ p \text{ primo}}} \left(\sum_{k \geqslant 0} \frac{1}{p^k} \right).$$

Observe que as somas de dentro do produto são séries geométricas de razão p^{-1}. Então, elas convergem para $\frac{1}{1-\frac{1}{p}}$. Assim,

$$\log x \leqslant \prod_{\substack{p \leqslant x \\ p \text{ primo}}} \left(\frac{1}{1-\frac{1}{p}} \right) = \prod_{\substack{p \leqslant x \\ p \text{ primo}}} \frac{p}{p-1} = \prod_{k=1}^{\pi(x)} \frac{p_k}{p_k - 1}.$$

Claramente $p_k \geqslant k+1$, e

$$\frac{p_k}{p_k - 1} = 1 + \frac{1}{p_k - 1} \leqslant 1 + \frac{1}{k} = \frac{k+1}{k}.$$

Daí,

$$\log x \leqslant \prod_{k=1}^{\pi(x)} \frac{k+1}{k} = \frac{2}{1} \cdot \frac{3}{2} \cdot \frac{4}{3} \cdot \ldots \cdot \frac{\pi(x)}{\pi(x)-1} \cdot \frac{\pi(x)+1}{\pi(x)} = \pi(x) + 1.$$

Porém, $\log x$ é ilimitada, e portanto, $\pi(x)$ também é, o que conclui a demonstração. □

2.7 A demonstração de Pinasco

Pinasco, em 2009, publicou uma prova para a infinitude dos números usando o Princípio da Inclusão e Exclusão[4], clássico resultado do campo da contagem.

Lema 2.10. *Para $x, t > 0$, temos*

$$\lim_{x \longrightarrow \infty} \frac{1}{x} \cdot \left\lfloor \frac{x}{t} \right\rfloor = \frac{1}{t}.$$

Demonstração: Pela definição de $\left\lfloor \frac{x}{t} \right\rfloor$, temos

$$\left\lfloor \frac{x}{t} \right\rfloor \leqslant \frac{x}{t} \leqslant \left\lfloor \frac{x}{t} \right\rfloor + 1 \Rightarrow \frac{1}{x} \cdot \left\lfloor \frac{x}{t} \right\rfloor \leqslant \frac{1}{x} \cdot \frac{x}{t} \leqslant \frac{1}{x} \cdot \left\lfloor \frac{x}{t} \right\rfloor + \frac{1}{x}$$
$$\Rightarrow \frac{1}{t} - \frac{1}{x} \leqslant \frac{1}{x} \cdot \left\lfloor \frac{x}{t} \right\rfloor \leqslant \frac{1}{x} \cdot \frac{x}{t}.$$

Assim, como $\lim_{x \longrightarrow \infty} \frac{1}{t} - \frac{1}{x} = \frac{1}{t}$ e $\lim_{x \longrightarrow \infty} \frac{1}{x} \cdot \frac{x}{t} = \frac{1}{t}$, pelo Teorema do Confronto[5] chegamos ao resultado desejado. □

Lema 2.11.

$$\sum_{i=1}^{N} \frac{1}{p_i} - \sum_{i<j} \frac{1}{p_i \cdot p_j} + \sum_{i<j<k} \frac{1}{p_i \cdot p_j \cdot p_k} - \ldots + (-1)^{N+1} \cdot \frac{1}{p_1 \cdot p_2 \cdot \ldots \cdot p_N} = 1 - \prod_{i=1}^{N} \left(1 - \frac{1}{p_i}\right).$$

[4] O Princípio da Inclusão e Exclusão nos diz que, se $A_1, A_2, \ldots, A_n$ são conjuntos, e $\mid A_i \mid$ é a cardinalidade de A_i, então: $\mid \bigcup_{i=1}^{n} A_i \mid = \sum_{i=1}^{N} \mid A_i \mid - \sum_{i<j} \mid A_i \cap A_j \mid + \sum_{i<j<k} \mid A_i \cap A_j \cap A_k \mid - \ldots + (-1)^{N+1} \mid A_1 \cap A_2 \cap \ldots \cap A_N \mid$

[5] O Teorema do Confronto, aqui não demonstrado, é enunciado da seguinte forma "Sejam f, g e $h : \mathbb{R} \longrightarrow \mathbb{R}$ três funções e suponha que exista $r > 0$ tal que $f(x) \leqslant g(x) \leqslant h(x)$ para $0 < \mid x - p \mid < r$. Nestas condições, se $\lim_{x \to p} f(x) = L = \lim_{x \to p} h(x)$, então $\lim_{x \to p} g(x)$"

Demonstração: Vamos expandir ambos os membros da igualdade e comparar os resultados.

$$\begin{aligned}
&\sum_{i=1}^{N}\frac{1}{p_i}-\sum_{i<j}\frac{1}{p_ip_j}+\sum_{i<j<k}\frac{1}{p_ip_jp_k}-\ldots+(-1)^{N+1}\cdot\frac{1}{p_1p_2\ldots p_N}\\
&=\left(\frac{1}{p_1}+\frac{1}{p_2}+\ldots+\frac{1}{p_N}\right)-\left(\frac{1}{p_1p_2}+\frac{1}{p_1p_3}+\ldots+\frac{1}{p_{N-1}p_N}\right)\\
&+\left(\frac{1}{p_1p_2p_3}+\frac{1}{p_1p_3p_4}+\ldots+\frac{1}{p_{N-2}p_{N-1}p_N}\right)+\ldots+(-1)^{N+1}\cdot\frac{1}{p_1p_2\ldots p_N}.
\end{aligned}$$

e

$$\begin{aligned}
1-\prod_{i=1}^{N}\left(1-\frac{1}{p_i}\right)&=1-\left(1-\frac{1}{p_1}\right)\cdot\left(1-\frac{1}{p_2}\right)\cdot\ldots\cdot\left(1-\frac{1}{p_N}\right)\\
&=1-\left(1-\frac{1}{p_1}-\frac{1}{p_2}-\ldots-\frac{1}{p_N}+\frac{1}{p_1p_2}+\frac{1}{p_1p_3}+\ldots+\frac{1}{p_{N-1}p_N}-\right.\\
&\left.-\frac{1}{p_1p_2p_3}-\frac{1}{p_1p_3p_4}-\ldots-\frac{1}{p_{N-2}p_{N-1}p_N}+\ldots+(-1)^N\cdot\frac{1}{p_1p_2\ldots p_N}\right)\\
&=\left(\frac{1}{p_1}+\frac{1}{p_2}+\ldots+\frac{1}{p_N}\right)-\left(\frac{1}{p_1p_2}+\frac{1}{p_1p_3}+\ldots+\frac{1}{p_{N-1}p_N}\right)\\
&+\left(\frac{1}{p_1p_2p_3}+\frac{1}{p_1p_3p_4}+\ldots+\frac{1}{p_{N-2}p_{N-1}p_N}\right)+\ldots+(-1)^{N+1}\cdot\frac{1}{p_1p_2\ldots p_N}.
\end{aligned}$$

Como as expansões são iguais, a igualdade se verifica.

□

Demonstração do Teorema 2.1. Suponha a existência de apenas uma quantidade finita de números primos, $2<p_1<\ldots<p_N$. Para $x\geq 1$, e $i=1,\ldots,N$, defina o conjunto A_i dos inteiros em $[1,x]$ que são múltiplos de p_i. E seja A o conjunto dos inteiros em $[1,x]$ que são múltiplos de algum primo. Devemos ter $A=\bigcup_{i=1}^{N}A_i$.
Pelo Princípio da Inclusão e Exclusão, temos:

$$\lfloor x\rfloor=1+\sum_{i=1}^{N}\mid A_i\mid-\sum_{i<j}\mid A_i\cap A_j\mid+\sum_{i<j<k}\mid A_i\cap A_j\cap A_k\mid-\ldots+(-1)^{N+1}\mid A_1\cap A_2\cap\ldots\cap A_N\mid.$$

Pela Proposição 1.22, o número de elementos de cada A_i é $\left\lfloor \frac{x}{p_i} \right\rfloor$. Assim,

$$\lfloor x \rfloor = 1 + \sum_{i=1}^{N} \left\lfloor \frac{x}{p_i} \right\rfloor - \sum_{i<j} \left\lfloor \frac{x}{p_i \cdot p_j} \right\rfloor + \sum_{i<j<k} \left\lfloor \frac{x}{p_i \cdot p_j \cdot p_k} \right\rfloor - \ldots + (-1)^{N+1} \cdot \left\lfloor \frac{x}{p_1 \cdot p_2 \cdot \ldots \cdot p_N} \right\rfloor.$$

Pelo Lema 2.10, multiplicando ambos os membros da igualdade acima por $\frac{1}{x}$, e tomando o limite quando x tende a infinito, temos:

$$1 = \sum_{i=1}^{N} \frac{1}{p_i} - \sum_{i<j} \frac{1}{p_i \cdot p_j} + \sum_{i<j<k} \frac{1}{p_i \cdot p_j \cdot p_k} - \ldots + (-1)^{N+1} \cdot \frac{1}{p_1 \cdot p_2 \cdot \ldots \cdot p_N}.$$

Pelo Lema 2.7 podemos escrever a soma acima de forma compactada, pelo produto abaixo:

$$1 = 1 - \prod_{i=1}^{N} \left(1 - \frac{1}{p_i}\right).$$

Como o produto é estritamente positivo, temos que $1 > 1$, o que é um absurdo. Portanto, existem infinitos primos. □

2.8 A demonstração de Furtenberg

Utilizando o conceito de Topologia, visto na Seção 1.3, vamos à demonstração da infinitude dos números primos, proposta por Furstenberg.

Definiremos inicialmente uma topologia no conjunto dos números inteiro, da seguinte forma. Para todo $a, b \in \mathbb{Z}$ com $b > 0$, seja

$$N_{a,b} = \{a + bn : n \in \mathbb{Z}\}.$$

Seja $\mathcal{T}$ uma família de subconjuntos de $\mathbb{Z}$ tal que $X \in \mathcal{T}$ (ou seja, X é aberto) se X é vazio ou se para todo $x \in X$, existe $b > 0$ tal que $N_{x,b} \subseteq X$.

Lema 2.12. *$\mathcal{T}$ definido da forma acima é uma topologia.*

Demonstração: *i)* $\emptyset$ e $\mathbb{Z}$ claramente estão em $\mathcal{T}$;

ii) Sejam $\{X_j\}_{j\in\Lambda}$ uma família qualquer de elementos de $\mathcal{T}$. Assim, se

$$x \in \bigcup_{j\in\Lambda} X_j$$

então $x \in X_i$, para algum $i \in \Lambda$. Daí, existe $b > 0$ tal que $N_{x,b} \subseteq X_i$, o que implica que

$$N_{x,b} \subseteq \bigcup_{j\in\Lambda} X_j.$$

Portanto a união de abertos é ainda aberto.

ii) Sejam X_j com $j = 1, \ldots, n$ conjuntos abertos. Se

$$x \in \bigcap_{j=1}^{n} X_j$$

então $x \in X_j$ para todo $j = 1, \ldots, n$. Assim, existem $b_j > 0$ com $j = 1, \ldots, n$, tais que $N_{x,b_j} \subseteq X_j$. Se tomarmos $b = b_1 \cdot b_2 \cdot \ldots \cdot b_n$, então

$$N_{x,b} \subseteq \bigcap_{j=1}^{n} X_j.$$

O que mostra que a interseção de n abertos é um aberto.

Portanto $\mathbb{Z}$ é um espaço topológico, com a topologia $\mathcal{T}$. □

Lema 2.13. *i) Todo conjunto aberto não vazio de $\mathbb{Z}$ é infinito.*

ii) Os conjuntos $N_{x,b}$ são conjuntos fechados.

Demonstração: *i)* Isso é claro, pois os conjuntos abertos não vazios de $\mathbb{Z}$ são os que contem $N_{a,b}$, e cada um deles é infinito por definição;

ii) Como

$$N_{a,b} = \mathbb{Z} - \bigcup_{i=1}^{b-1} N_{a-i,b}$$

Assim, como cada $N_{a-i,b}$ é aberto, segue que $N_{a,b}$ é fechado.

□

Demonstração do Teorema 2.1. Suponha que existem apenas n números primos. Assim, pelo Teorema 1.1.7 todo numero inteiro diferente de 1 e -1 pode ser escrito como produto de primos. Assim, N_{0,p_i} é o conjunto de todos os múltiplos de um primo p_i com $i = 1, \ldots n$. Assim,

$$\mathbb{Z} - \{-1, 1\} = \bigcup_{i=1}^{n} N_{0,p_i}$$

Dessa forma, pelo Lema 2.13 a união acima é uma união finita de conjuntos fechados, e pelo Teorema 1.46 é também um conjunto fechado. Logo $\{-1, 1\}$ é um conjunto aberto. Absurdo! Portanto, existem infinitos números primos. □

2.9 Outras Demonstrações

Há ainda outras demonstrações para esse mesmo resultado, porém utilizando ferramentas mais avançadas. Uma delas, utiliza um fato aparentemente simples, cuja demonstração não é, que é o Postulado de Bertrand, enunciado da seguinte forma:

Teorema 2.14 (Postulado de Bertrand)**.** *Para todo $n \in \mathbb{N}$, existe algum p primo tal que $n < p < 2n$.*

A demonstração desse fato pode ser encontrada em [8] e em [5]. Mas assumindo sua veracidade, construímos uma sequência $n < p_1 < 2n < p_2 < 4n < p_3 < 8n < \ldots$ que implica na infinidade dos números primos p_i, $i \in \mathbb{N}$.

Outro dado interessante é que existem infinitos números primos da forma $4n + 1$, por exemplo, como pode ser visto em [8]. Na verdade, e de forma mais geral, Dirichlet diz que:

Teorema 2.15 (Teorema de Dirichlet)**.** *Sejam a e b, números naturais primos entre si, então existem infinitos primos da forma $an + b$, onde $n \in \mathbb{N}$.*

A demonstração desse teorema, que não é simples e nem elementar, porém pode ser encontrada em [4].

Em 2008, Green e Tao demonstraram que:

Teorema 2.16. *Para todo $k \geqslant 3$, existe pelo menos uma progressão aritmética de k inteiros*

positivos que são números primos.[6]

Tomando esse resultado como verdade, suponha que existem apenas n primos. Se tomássemos $k = n + 1$, então existiria, pelo Teorema de Green e Tao, pelo menos uma progressão aritmética, com $n + 1$ termos primos, o que seria impossível.

Grandes resultados da teoria dos números, envolvendo os números primos, ainda estão em aberto. Podemos enunciar as seguintes conjecturas:

- Todo número par maior ou igual a 4 é a soma de dois números primos?[7]
- Existem infinitos primos gêmeos[8] ?
- Existem uma infinidade de números primos de Mersenne?
- Existem uma infinidade de números primos do tipo $p\# + 1$, onde $p\#$[9] denota o produto de todos os primos menores ou iguais a p?
- Existem uma infinidade de números da forma $N^2 + 1$?
- Existem infinitos números da forma $C_n = n \times 2^n + 1$[10]?

entre outras afirmações, que tem motivado estudiosos do mundo todo na busca por respostas pra todas elas. Caso haja maior interesse, o leitor interessado pode consultar [9] e [4].

[6] A demonstração desse fato rendeu a TAO uma Medalha Fields no Congresso Internacional de Matemática de 2006.

[7] Essa é a famosa *Conjectura de Goldbach.*

[8] Dizemos que dois primos são gêmeos se um se distancia do outro por 2 unidades.

[9] Chamamos tal notação de "primorial de p".

[10] Os números da forma $C_n = n \times 2^n + 1$ são chamados *números de Cullen*

Considerações Finais

Aqui neste trabalho, mostramos de diversas formas que existem infinitos primos, porém, não é de conhecimento do ser humano a listagem deles, ou a forma que eles se comportam. Não há uma fórmula que me mostre, por exemplo, o 100000^{o} número primo. Para se ter ideia de como é caótica essa listagem, existem saltos arbitrariamente grandes na sequência dos números primos.

Ao tomarmos conhecimento das demonstrações da infinitude dos primos aqui apresentadas, vemos que a ligação da Teoria dos Números com outras áreas é muito grande. A forma como consegue-se demonstrar o teorema sem que se use ferramentas apenas na Teoria do Números é uma prova desse fato.

A presente monografia traz uma poderosa ferramenta para professores e estudantes se inteirarem de uma quantidade razoável de demonstrações. Além disso, esse trabalho também se torna ferramenta impulsionadora do interesse de novos estudiosos no campo da Teoria dos Números, por se tratar de demonstrações pouco conhecidas, mas de pouca complexidade, em que se faz uso, em sua maioria, de resultados conhecidos por graduandos em sua fase final de um curso de matemática.

Além disso, da mesma forma que foi feito com a infinitude dos números primos, também poderíamos ter feito outras demonstrações de outros resultados, como por exemplo o tão importante Algoritmo de Euclides, ou o Teorema Fundamental da Aritmética.

Referências Bibliográficas

[1] Du Santoy, Marcus. *A música dos números primos: a história de um problema não resolvido na matemática*. 1 ed. Rio de Janeiro: Jorge Zahar, 2007.

[2] Euclides. *Os Elementos*. São Paulo: Editora UNESP, 2009

[3] Gonçalves, A. *Introdução à álgebra*. Rio de Janeiro: IMPA, 2000.

[4] Martinez, F. B.; *Teoria dos números: um passeio com primos e outros números familiares pelo mundo inteiro*. Rio de Janeiro: IMPA, 2011.

[5] Martin, A. Günter, M. Z. Karl, H. H. *Proofs from THE BOOK*. 3 ed. Berlin: Springer, 2009.

[6] Munkers, J. R. *Topology: A first course*. 2 ed. Prendice Hall Inc., 1975.

[7] Pinasco, J. P. *New Proofs of Euclid's and Euler's Theorems*. THE MATHEMATICAL ASSOCIATION OF AMERICA, Monthly 116. p. 172 - 173, 2009.

[8] Santos, J. P. D. O. *Introdução à teoria dos números*. Rio de Janeiro: Impa, 2011.

[9] Ribenboim, P. *Números Primos: Velhos mistérios e novos recordes*, 1 ed. Rio de Janeiro: IMPA, 2014.

[10] Sam, S. V. *Infinitude of primes*. Disponível em <http://math.mit.edu/∼ssam/writings/primes.pdf>. Acesso em 02 de maio de 2016.

[11] Vieira, V. L. *Álgebra abstrata para licenciatura*. 2 ed. Campina Grande: EDUEPB, 2015.

[12] Vieira, V. L. *Um curso básico em teoria dos números.* 1 ed. Campina Grande: EDUEPB; São Paulo: Livraria da Física, 2015.