UNIVERSIDADE ESTADUAL DO OESTE DO PARANÁ
PROGRAMA DE PÓS GRADUAÇÃO EM MATEMÁTICA
MESTRADO PROFISSIONAL EM REDE NACIONAL

Uma breve introdução à infinidade dos números primos

Outubro de 2023

UNIVERSIDADE ESTADUAL DO OESTE DO PARANÁ
PROGRAMA DE PÓS GRADUAÇÃO EM MATEMÁTICA
MESTRADO PROFISSIONAL EM REDE NACIONAL - PROFMAT

Uma breve introdução à infinidade dos números primos

Willian Cleyson Fritsche

Dissertação apresentada ao programa de pós graduação em matemática como parte dos requisitos para obtenção do título de Mestre pelo Mestrado Profissional em Matemática em Rede Nacional - PROFMAT.

Banca examinadora:
Profa. Dra. Raquel Lehrer - Unioeste (Orientadora)
Prof. Dr. Raimundo de Araújo Bastos Júnior - UnB
Prof. Dr. Clézio Aparecido Braga - Unioeste

Cascavel, Outubro de 2023.

Ficha de identificação da obra elaborada através do Formulário de Geração Automática do Sistema de Bibliotecas da Unioeste.

Fritsche, Willian Cleyson
Uma breve introdução à infinidade dos números primos / Willian Cleyson Fritsche; orientadora Raquel Lehrer. -- Cascavel, 2023.
100 p.

Dissertação (Mestrado Profissional Campus de Cascavel) -- Universidade Estadual do Oeste do Paraná, Centro de Ciências Exatas e Tecnológicas, Programa de Pós-Graduação em Matemática - Mestrado Profissional, 2023.

1. Números primos. 2. Infinidade dos números primos. 3. Testes de primalidade. 4. Atividades sobre números primos. I. Lehrer, Raquel, orient. II. Título.

unioeste
Universidade Estadual do Oeste do Paraná

PARANÁ
GOVERNO DO ESTADO

WILLIAN CLEYSON FRITSCHE

Uma breve introdução à infinidade dos números primos

Dissertação apresentada ao Programa de Pós-graduação em Matemática - PROFMAT em cumprimento parcial aos requisitos para obtenção do título de Mestre em Matemática, área de concentração Álgebra, linha de pesquisa Teoria dos números, APROVADO(A) pela seguinte banca examinadora:

Orientador(a) - Raquel Lehrer

Universidade Estadual do Oeste do Paraná - Campus de Cascavel (UNIOESTE)

Raimundo de Araújo Bastos Júnior

UNIVERSIDADE DE BRASÍLIA (UNB)

Clezio Aparecido Braga

Universidade Estadual do Oeste do Paraná - Campus de Cascavel (UNIOESTE)

Cascavel, 16 de novembro de 2023

Agradecimentos

Agradecer significa retribuir. Mas como? Como retribuir os ensinamentos preciosos dos professores que percorreram o percurso comigo? Com certeza, tenho muito a agradecer a minha orientadora Dra. Raquel Lehrer, principalmente pela paciência que teve comigo, e convenhamos, precisou de muita paciência. Os seus ensinamentos e apontamentos acolhidos foram muito importantes para o desenvolvimento deste trabalho.

Ademais, lembro-me das valiosas aulas do professor Dr. Paulo Conejo, que contribuíram para o desenvolvimento do presente trabalho, e do professor Dr. Clezio Braga que com a sua simpatia e grande conhecimento tornava as aulas uma obra de valor inestimável. De maneira geral, todos os professores do curso serão sempre lembrados e quero aqui agradecer-lhes pelo conhecimento outorgado.

Agradeço também aos colegas de turma pelos bons momentos, especialmente ao Daniel Schreiner, cuja amizade levarei com grande apreço, assim como, à Luana Bontempo que me presenteou com as questões antigas do ENQ, não me esquecerei da gentileza.

Agradecer significa retribuir. Mas como? Como retribuir a compreensão da ausência em momentos que a presença é desejada? Como retribuir as pessoas que estiveram ao seu lado nos ataques de ansiedade e devaneios cognitivos? Não existe retribuição para isso, porque é um preço que foi pago sem reembolso.

Dedico esse trabalho como tentativa de retribuição, principalmente à minha esposa, Mayara C. Tramontin Fritsche, pelo apoio fornecido de diversas maneiras, uma parte de nós reside nessas páginas. Dedico também esse trabalho aos meus filhos, que são uma quantidade prima, Arthur T. Fritsche, Felipe T. Fritsche e Yasmin T. Fritsche, para eles um dia será o dia.... Aos meus pais, Germano Fritsche e Gessy B. Fritsche agradeço imensamente o apoio e a ajuda fornecida, muitas coisas foram possíveis somente porque eles estavam presentes.

Agradeço profundamente à Deus, não há palavras que manifestem a minha gratidão, mas sei que Sabes. Confio com a certeza de que nada seria possível sem Ti, como sei que não seria nada se não fosse vós.

Mais alguém a agradecer além de mim mesmo?

Resumo

O presente trabalho apresenta uma coleção de 22 demonstrações da infinidade dos números primos e uma coleção de 7 testes de primalidade, incluindo o teste que origina o crivo de Eratóstenes e os testes com congruência de E. Lucas. Para concluir é apresentada uma coleção de 11 atividades que envolvem os números primos para o Ensino Fundamental II, algumas destas atividades possuem curta duração e podem ser utilizadas conjuntamente em uma mesma aula, outras atividades são adequadas para o reforço conceitual.

Palavras-Chave: Números primos; Atividades sobre números primos; Infinidade dos números primos; Testes de primalidade.

Abstract

The present work presents a collection of 22 demonstrations of the infinity of prime numbers and a collection of 7 primality tests, including the test that originates the sieve of Eratosthenes and the congruence tests of E. Lucas. To conclude, a collection of 11 activities involving prime numbers for Elementary School II is presented. Some of these activities are short in duration and can be used together in the same class, other activities are suitable for conceptual reinforcement.

Keywords: Prime numbers; Activities about prime numbers; Infinity of prime numbers; Primality tests.

Demonstrações utilizadas para a infinidade dos números primos

Número da Demonstração	Autor	Referência utilizada
1	Euclides	Página 1 de [29]
2	C. Hermite	Página 4 de [22]
3	T. Stieltjes	Página 4 de [22]
4	G. Métrod	Página 9 de [29]
5	L. Euler	Página 7 de [22]
6	C. Goldbach	Página 4 de [29]
7	F. Saidak	Página 36 de [8]
8	M. Wunderlich	Página 9 de [22]
9	A. Granville	Página 2 de [15]
10	A. Granville	Página 2 de [15]
11	A. Thue	Página 7 de [29]
12	A. Auric	Página 9 de [29]
13	A. Granville	Página 2 de [15]
14	L. Euler	Página 6 de [29]
15	A. Yaglom e I. Yaglom	Página 14 de [1]
16	P. Erdös	Página 16 de [1]
17	J. Whang	Página 181 de [34]
18	H. Furstenberg	Página 15 de [1]
19	A. Engel	Página 37 de [8]
20	S. Northshield	Página 466 de [23]
21	D. Wegener	Página 449 de [33]
22	R. Bellman e R. Buck	Página 23 de [21]

Sumário

Introdução

Os números primos, do grego *protoi arithmós*, são objeto de investigação desde os primórdios da matemática. Os gregos antigos possuíam muito interesse no estudo dos números, em especial, dos números primos. Não à toa, acredita-se que a concepção de número primo apareceu em meados de 530 a.C. através de Pitágoras e dos pitagóricos ([13], página 79).

Diversos matemáticos gregos buscaram determinar a quantidade de números primos existentes, Eratóstenes no século III a.C. conseguiu desenvolver um engenhoso método para determinar quando um número é primo, denominado Crivo de Eratóstenes. Um dos maiores matemáticos gregos, Euclides, fez as maiores contribuições da matemática grega para os números primos, no seu livro: Os Elementos; de 300 a.C., provou o importante Teorema Fundamental da Aritmética e posteriormente provou que existem infinitos números primos.

Estes matemáticos gregos foram os precursores de grandes matemáticos que estudaram os números primos, entre os quais podemos citar P. Fermat, L. Euler e C. Gauss, cada qual fez as suas contribuições fundamentais para o desenvolvimento dos primos. Atualmente, os números primos são a chave de sistemas criptográficos importantes, como o RSA, que são fundamentais para a proteção dos dados no mundo digital.

O presente trabalho possui o objetivo de apresentar uma breve introdução à infinidade dos números primos e dos testes de primalidade. Motivamo-nos nas palavras do ilustre matemático B. Riemann, que contribuiu significativamente no estudo dos números primos com um brilhante artigo em 1859. Riemann salienta nesse artigo que o trabalho sobre os números primos é "um tema que talvez não pareça totalmente indigno de tal comunicação, dado o interesse que os próprios Gauss e Dirichlet demonstraram por ele durante um longo período"([30], página 1).

O trabalho foi dividido em 3 Capítulos e tem a seguinte estrutura. O Capítulo 1 deste trabalho reúne 22 demonstrações da infinidade dos números primos. Buscou-se diversificar as demonstrações apresentando diversos métodos para reobter o clássico resultado de Euclides. As seções do Capítulo 1 apresentam na primeira seção os resultados

preliminares e nas demais seções as demonstrações da infinidade dos números primos divididas conforme os conceitos e resultados de cada uma das áreas matemáticas apresentadas, com a última seção reservada às demonstrações com resultados diversos.

No Capítulo 2 são apresentados 7 testes de primalidade para testar os números inteiros positivos. Buscou-se com os 7 métodos selecionados mostrar a complexidade, diversidade e custo de tempo que a determinação da primalidade dos inteiros positivos apresenta, principalmente se o número possuir fatores primos grandes ou for um primo grande. As seções do Capítulo 2 são divididas em testes de primalidade clássicos que não dependem de congruências, uma rápida busca por caracterizações dos números primos, e testes de primalidade clássicos que dependem de congruências. A determinação da primalidade de inteiros positivos é de grande importância, de fato, Gauss comentou no seu famoso trabalho Disquisitiones Arithmeticae que "o problema de distinguir os números primos dos números compostos e de exprimir estes últimos à custa de seus fatores primos deve ser considerado como um dos mais importantes e dos mais úteis em Aritmética" ([29], página 13).

Por fim, no Capítulo 3 são apresentadas 11 sugestões de atividades práticas sobre os números primos que podem ser desenvolvidas no Ensino Fundamental II, para o ensino ou para o reforço conceitual dos estudantes. Cada seção do Capítulo 3 é dedicada a uma atividade que pode ser aplicada para complementar uma aula ou pode ser aplicada em conjunto com outras atividades para reforçar o conhecimento. Para a seleção das atividades, buscou-se condizer com a habilidade da BNCC que estabelece o objetivo do estudante "classificar números naturais em primos e compostos, estabelecer relações entre números, expressas pelos termos 'múltiplo de', 'divisor de', 'fator de' "([6], página 301).

Capítulo 1

Neste capítulo apresentaremos alguns resultados preliminares que serão utilizados no decorrer do trabalho, bem como 22 demonstrações para a infinidade dos números primos. Este capítulo está assim dividido: na Seção 1.1 apresentamos os resultados preliminares, onde tentamos incluir todas as demonstrações dos mesmos para tornar a leitura mais acessível. Na Seção 1.2 apresentamos a demonstração clássica atribuída à Euclides na sua escrita original e nas Seções seguintes apresentamos as 22 demonstrações agrupadas por áreas de conhecimentos na Matemática.

1.1 Resultados Preliminares

Para convencionar a notação, realizamos inicialmente algumas considerações. Definimos o conjunto dos números naturais como sendo $\mathbb{N} = \{1, 2, 3, \ldots\}$, os demais conjuntos numéricos, como convencionado, são o conjunto dos números inteiros $\mathbb{Z}$, o conjunto dos números inteiros não negativos $\mathbb{Z}_+$, o conjunto dos números racionais $\mathbb{Q}$, o conjunto dos números reais $\mathbb{R}$ e o conjunto dos reais positivos $\mathbb{R}_+^*$.

Lembramos que $n! = 1 \times 2 \times \ldots \times n$ e $|x|$ é o módulo de um número real x, definido como x se $x \geq 0$ e $-x$ se $x < 0$.

Começamos enunciando o Princípio da Boa Ordenação, o Princípio da Indução e alguns resultados primordiais que serão utilizados no decorrer do trabalho, utilizamos como referência a Seção 1.4 de [16].

Definição 1.1. *(Princípio da Boa Ordenação) Se S é um subconjunto não vazio de $\mathbb{Z}$ e limitado inferiormente, então S possui um menor elemento.*

Teorema 1.2. *(Princípio de Indução Matemática) Sejam S um subconjunto de $\mathbb{Z}$ e $a \in \mathbb{Z}$ tais que*

i) $a \in S$;

ii) S é fechado com respeito à operação de "somar 1"a seus elementos, ou seja, $\forall\ n$, $n \in S \Longrightarrow n+1 \in S$.

Então, $\{x \in \mathbb{Z}\,;\, x \geq a\} \subset S$.

Demonstração. Seja $S' = \{x \in \mathbb{Z}\,;\, x \geq a\}$ e suponha que $S' \not\subset S$, logo $S' - S \neq \emptyset$. Como este conjunto S' é limitado inferiormente por a, existe um menor elemento $c \in S' - S$ e pelo fato de $c \in S'$ e $c \notin S$, temos que $c > a$, já que $a \in S$ por i), portanto $(c-1) \in S'$ e $(c-1) \in S$. Pela hipótese ii) sobre S, temos que $c = (c-1)+1 \in S$, como $c \in S'$ obtemos uma contradição com o fato de $c \in S' - S$, logo, $S' \subset S$. □

Teorema 1.3. *(Prova por Indução) Seja $a \in \mathbb{Z}$ e $P(n)$ uma propriedade do número natural n. Suponha que*

i) $P(a)$ é verdadeira;

ii) $\forall\ n \geq a$, $P(n) \Longrightarrow P(n+1)$ é verdadeira.

Então, $P(n)$ é verdadeira para todo $n \geq a$.

Demonstração. Seja $V = \{n \in \mathbb{Z}\,;\, P(n)\}$, ou seja, V é o conjunto dos elementos de $\mathbb{Z}$ para os quais $P(n)$ é verdadeira. Por i), $a \in V$ e por ii) para todo n, $n \in V \Longrightarrow (n+1) \in V$. Segue pelo Teorema 1.2 que $\{x \in \mathbb{Z}\,;\, x \geq a\} \subset V$. □

Será utilizado também o chamado Princípio da Indução Completa, para o seu enunciado basta substituir o item ii) no Teorema 1.3, por

ii') $\forall\ n$, $P(a)$, $P(a+1)$, ..., $P(n)$ verdadeiras $\Longrightarrow P(n+1)$ é verdadeira.

E a conclusão segue a mesma. A demonstração do Princípio da Indução Completa segue do Teorema 1.18 de [16].

A diferença entre os dois tipos de indução é que a completa necessita como hipótese que a sentença seja verdadeira para todos os valores menores ou iguais a n, por outro lado para a primeira basta a hipótese ser verdadeira para algum n. Para um estudo mais aprofundado sobre o Princípio da Indução recomendamos o capítulo 1 de [16].

Um resultado elementar importante é o Princípio das Gavetas, que pode ser encontrado na página 10 de [20].

Teorema 1.4. *(Princípio das Gavetas) Se temos $kn+1$ objetos e n gavetas, então existirá uma gaveta onde haverá pelo menos $k+1$ objetos.*

Demonstração. O número médio de objetos por gaveta é maior ou igual a $\dfrac{kn+1}{n} > k$. Portanto, existe uma gaveta com pelo menos $k+1$ objetos. □

Vamos agora rever alguns resultados elementares da Teoria dos Números. Para um estudo mais aprofundado recomendamos as referências aqui utilizadas [16] e [20].

Definição 1.5. *Sejam dois números inteiros a e b, diremos que a divide b, representando $a \mid b$, quando existir $k \in \mathbb{Z}$ tal que $b = ak$.*

Proposição 1.6. *Sejam $a, b \in \mathbb{Z}$, se $a \mid b$ e $a \mid c$ então $a \mid (b + c)$.*

Demonstração. Pela hipótese inicial, existem $k, k' \in \mathbb{Z}$ tal que $b = ak$ e $c = ak'$, portanto, $b + c = ak + ak' = a(k + k')$, logo, $a \mid (b + c)$. □

Um resultado bastante óbvio, mas que será utilizado em diversos momentos durante o presente trabalho, é apresentado abaixo.

Proposição 1.7. *Sejam $a, b \in \mathbb{Z}$, onde $b \neq 0$, temos que se $a \mid b$ então $|a| \leq |b|$.*

Demonstração. Como $a \mid b$, existe $k \in \mathbb{Z}$ tal que $b = ak$, assumindo módulos temos que $|b| = |a||k|$. Como $b \neq 0$, então, $a \neq 0$ e $1 \leq |k|$, consequentemente, $|a| \leq |a||k| = |b|$. □

Proposição 1.8. *Sejam $a, b \in \mathbb{Z}$, com $a \neq 0$, então existe $n \in \mathbb{Z}$ tal que $na > b$.*

Demonstração. Como $|a| \geq 1$, temos que $(|b|+1)|a| \geq |b|+1 > |b| \geq b$, tomando $n = |b|+1$ se $a > 0$ e $n = -(|b| + 1)$ se $a < 0$, segue que $na > b$. □

Lema 1.9. *Dado $a, b, c \in \mathbb{Z}$, se $a \mid (b + c)$, então $a \mid b$ se, e somente se, $a \mid c$.*

Demonstração. Suponha que $a \mid (b + c)$ e $a \mid b$, então $b + c = ka$ e $b = ga$ com $k, g \in \mathbb{Z}$, assim $ga + c = ka$, isto é, $c = a(k - g)$ com $(k - g) \in \mathbb{Z}$, logo $a \mid c$. A implicação contrária é análoga e o resultado segue. □

Lema 1.10. *Dados $a, b, c \in \mathbb{Z}$. Se $a \mid b$ e $b \mid c$, então $a \mid c$.*

Demonstração. Se $a \mid b$ e $b \mid c$, então existem $f, g \in \mathbb{Z}$ tais que $b = fa$ e $c = gb$, assim obtemos $c = gb = g(fa) = (gf)a$ e como $gf \in \mathbb{Z}$, concluímos que $a \mid c$. □

Teorema 1.11. *(Divisão Euclidiana) Sejam a e b dois números inteiros com $a \neq 0$. Existem dois únicos números inteiros c e r tais que*

$$b = ac + r,$$

com $0 \leq r < |a|$.

Demonstração. Considere o conjunto $S = \{x = b - ay \, ; \, y \in \mathbb{Z}\} \cap (\mathbb{N} \cup \{0\})$. Pela Proposição 1.8, existe $n \in \mathbb{Z}$ tal que $n(-a) > -b$, logo $b - na > 0$ então S é não vazio. O conjunto S é limitado inferiormente por 0, logo pelo Princípio da Boa Ordenação, temos que S possui um menor elemento $r \geq 0$. Suponha que $r = b - ac$ com $c \in \mathbb{Z}$. Suponhamos por absurdo que $r \geq |a|$, portanto existe $s \in \mathbb{N} \cup \{0\}$ tal que $r = |a| + s$, logo, $0 \leq s < r$, mas isso contradiz o fato de r ser o menor elemento de S, pois $s = b - a(c \pm 1) \in S$, com $s < r$. Portanto, $0 \leq r < |a|$.

Agora para a unicidade, suponha que $b = ac + r = ac' + r'$, onde $c, c', r, r' \in \mathbb{Z}$ e $0 \leq r, r' < |a|$. Assim, observamos que $-|a| < -r \leq r' - r \leq r' < |a|$, logo $|r' - r| < |a|$, por outro lado, $a(c - c') = r' - r$, o que implica que $|a||c - c'| = |r' - r| < |a|$, o que ocorre se, e somente se, $c = c'$ e consequentemente $r = r'$. □

Denominamos b como *dividendo*, a como *divisor*, c como *quociente* e r como o *resto* da divisão. Observamos que quando $r = 0$, temos que $b = ac$, isto é, $a \mid b$

A definição mais importante deste trabalho é a de número primo:

Definição 1.12. *Um número natural maior do que* 1 *que só possui como divisores positivos o* 1 *e ele próprio, é chamado de número primo.*

Decorre diretamente da definição que dado um número primo p e qualquer $d \in \mathbb{N}$ tal que $d \mid p$, então $d = 1$ ou $d = p$.

Definição 1.13. *(Máximo Divisor Comum) Dizemos que um número inteiro $d \geq 0$ é um máximo divisor comum dos números inteiros a e b, se possuir as seguintes propriedades:*

i) d é um divisor comum de a e b;

ii) d é divisível por todo divisor comum de a e b.

Representamos o máximo divisor comum por $(a, b) = (b, a) = d$ e para $a = b = 0$ convencionamos que $(0, 0) = 0$.

Sejam $a, b \in \mathbb{Z}$, quando $(a, b) = 1$ dizemos que a e b são *primos entre si*. Obviamente, dado um número primo p e qualquer $a \in \mathbb{Z}$, temos que $(p, a) = 1$ se $p \nmid a$ e $(p, a) = p$ se $p \mid a$, de maneira geral, se $a \mid b$ então $(a, b) = |a|$. O próximo lema é muito utilizado para obter resultados importantes envolvendo o máximo divisor comum.

Lema 1.14. *Sejam $a, b, n \in \mathbb{Z}$, temos que $(a, b - na) = (a, b)$.*

Demonstração. Seja $d = (a, b - na)$, como $d \mid a$ e $d \mid (b - na)$ segue que d divide $b = (b - na) + na$, logo d é um divisor comum de a e b. Suponha que c seja um divisor

comum de a e b, assim, c é um divisor comum de a e $b - na$, portanto, $c \mid d$, isto é, pela Definição 1.13, $d = (a, b)$. □

A demonstração do teorema que segue foi baseada no Teorema 6.3 de [14] e no Teorema 1.7 de [20].

Teorema 1.15. *(Bézout) Sejam $a, b \in \mathbb{Z}$, então existem $x, y \in \mathbb{Z}$ tais que $ax+by = (a, b)$. Em particular, se $k \in \mathbb{Z}$ é tal que $k \mid a$ e $k \mid b$ então $k \mid (a, b)$.*

Demonstração. Se $a = b = 0$ segue trivialmente que $x = y = 0$. Se $a = 0$ e $b \neq 0$, então $(0, b) = |b|$, assim basta tomar $x = 0$ e $y = \pm 1$, dependendo do sinal de b, o caso $a \neq 0$ e $b = 0$ é análogo. Portanto, consideramos $a \neq 0$ e $b \neq 0$, além disso, como $(a, b) = (|a|, |b|)$, sem perda de generalidade, podemos supor que $a > 0$ e $b > 0$.

Consideramos o conjunto $S = \{ax+by \ ; \ ax+by > 0 \ \ e \ \ x, y \in \mathbb{Z}\}$, obviamente S é não vazio, pois como $a > 0$ então $a = a \,.\, 1 + b \,.\, 0$ é positivo e pertence a S. Como os elementos do conjunto S são inteiros positivos, ou seja, S é limitado inferiormente, pelo Princípio da Boa Ordenação, S possui um menor elemento $d > 0$, logo, podemos escrever $d = ax_0 + by_0$ com $x_0, y_0 \in \mathbb{Z}$. Por conseguinte, pela Divisão Euclidiana dos inteiros a e d, obtemos os inteiros c e r tais que $a = dc + r$ com $0 \leq r < d$. Assim, segue que

$$r = a - dc = a - (ax_0 + by_0)c = a(1 - cx_0) + b(-cy_0)$$

ou seja, o resto r é uma combinação linear inteira de a e b, mas como $0 \leq r < d$ e $d > 0$ é o elemento mínimo de S, temos que $r = 0$, pois caso contrário $r \in S$, o que é uma contradição pela minimalidade de d. Portanto, obtemos que $a = dc$, isto é, $d \mid a$. Analogamente, pela Divisão Euclidiana nos inteiros b e d, obtemos que $d \mid b$.

Dessa maneira, d é um divisor comum de a e b, além disso, suponha que existe $d_1 \in \mathbb{Z}$ com $d_1 > 0$ tal que $d_1 \mid a$ e $d_1 \mid b$, logo, $d_1 \mid (aw + bs)$ para quaisquer $w, s \in \mathbb{Z}$, em particular, $d_1 \mid (ax_0 + by_0)$, ou seja, $d_1 \mid d$ e concluímos que d é divisível por todo divisor comum de a e b, isto é, $d = (a, b)$. □

Corolário 1.16. *Sejam $a, b, c \in \mathbb{Z}$. A equação $ax + by = c$ admite solução inteira em x e y se, e somente se, $(a, b) \mid c$.*

Demonstração. Se a equação $ax+by = c$ admite solução inteira, então $(a, b) \mid a$ e $(a, b) \mid b$, logo, $(a, b) \mid c$. Reciprocamente, se $(a, b) \mid c$ então $c = k(a, b)$ com $k \in \mathbb{Z}$, pelo Teorema 1.15, existem inteiros x_0 e y_0 tais que $ax_0 + by_0 = (a, b)$ e multiplicando ambos os lados da equação por k obtemos que $x = kx_0$ e $y = ky_0$ são solução da equação $ax+by = c$. □

Lema 1.17. *(Lema de Gauss) Sejam $a, b, c \in \mathbb{Z}$. Se $a \mid bc$ e $(a, b) = 1$, então $a \mid c$.*

Demonstração. Se $a \mid bc$ e $(a, b) = 1$, então pelo Teorema 1.15, existem $x, y \in \mathbb{Z}$ tal que $ax + by = 1$, logo, $acx + bcy = c$, como $a \mid acx$ e $a \mid bcy$, temos que $a \mid c$. □

Corolário 1.18. *Seja p um número primo e $a_1, \ldots, a_m \in \mathbb{Z}$. Se $p \mid a_1 \ldots a_m$, então $p \mid a_i$ para algum índice i, com $1 \leq i \leq m$.*

Demonstração. Utilizando o Lema 1.17, o corolário segue por Indução em m. □

O próximo teorema, conhecido como Teorema Fundamental da Aritmética, encontra-se fragmentado no livro Os Elementos de Euclides. Este importante teorema torna o presente trabalho possível, pois figura em diversas demonstrações.

Teorema 1.19 (Teorema Fundamental da Aritmética)**.** *Todo número natural maior do que 1, ou é primo ou se escreve de modo único, a menos da ordem dos fatores, como um produto de números primos.*

Demonstração. Provaremos pelo Princípio da Indução Completa a fatoração em números primos. Se $n = 2$, temos um número primo e $P(2)$ é verdadeiro. Suponha que todo número natural $2 \leq k \leq n$ é primo ou é escrito como produto de números primos. Assim, se $n+1$ é primo, $P(n+1)$ é verdadeiro e o resultado segue. Se $n+1$ é composto, então existem $a, b \in \mathbb{N}$ tal que $n + 1 = ab$ com $1 < a < n + 1$ e $1 < b < n + 1$, portanto, pela hipótese de indução temos que $a = p_1 p_2 \ldots p_s$ e $b = q_1 q_2 \ldots q_{s'}$, logo, $n + 1 = p_1 p_2 \ldots p_s q_1 q_2 \ldots q_{s'}$, isto é, $n + 1$ é escrito como produto de números primos, portanto $P(n + 1)$ é verdadeiro e pelo Princípio da Indução Completa a fatoração em números primos segue.

Para a unicidade da fatoração, suponha que $n+1$ seja o menor número que têm duas fatorações distintas, isto é, $n + 1 = p_1 p_2 \ldots p_r = q_1 q_2 \ldots q_{r'}$, com $p_1 \leq p_2 \leq \ldots \leq p_r$ e $q_1 \leq q_2 \leq \ldots \leq q_{r'}$. Como $p_1 \mid (n + 1)$ então $p_1 \mid q_i$ para algum índice $1 \leq i \leq r'$, como q_i é primo temos que $p_1 = q_i$, assim $p_1 \geq q_1$, analogamente obtemos que $p_1 \leq q_1$, logo, $p_1 = q_1$. Portanto, observamos que $\frac{n+1}{p_1} = p_2 \ldots p_r = q_2 \ldots q_{r'}$ têm fatoração única pela minimalidade de $n + 1$, logo, $r = r'$ e $p_i = q_i$ para todo índice i, o que contradiz a dupla fatoração de $n + 1$. Portanto, a fatoração em números primos é única. □

Corolário 1.20 (Fatoração Única)**.** *Dado um número inteiro positivo $n \neq 1$, existem primos $p_1 < p_2 < \ldots < p_r$ e $\alpha_1, \alpha_2, \ldots, \alpha_r \in \mathbb{N}$, univocamente determinados, tais que $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$.*

Demonstração. O corolário segue do Teorema 1.19, por um agrupamento dos fatores primos repetidos e ordenação dos primos em ordem crescente. □

Um conceito muito importante da Teoria do Números é a congruência modular, que definimos a seguir.

Definição 1.21. *Dizemos que dois números inteiros a e b são congruentes módulo m com $m > 1$ inteiro, escrevendo-se $a \equiv b \mod m$, quando o resto da divisão euclidiana de a por m é igual ao resto da divisão euclidiana de b por m.*

As proposições que seguem apresentam propriedades fundamentais sobre a congruência modular.

Proposição 1.22. *Dado $a, b, m \in \mathbb{Z}$, com $m > 1$, tem-se que $a \equiv b \mod m$ se, e somente se, $m \mid (b - a)$.*

Demonstração. Seja $a = mc+r$, com $0 \leq r < m$ e $b = mc'+r'$, com $0 \leq r' < m$, as divisões euclidianas de a e b por m, respectivamente. Portanto, temos que $b-a = m(c'-c)+(r'-r)$, logo, se $a \equiv b \mod m$ então $r = r'$, isto é, $b-a = m(c'-c)$, em contrapartida, se $m \mid (b-a)$ então $m \mid (r' - r)$, mas como $r' - r < m$ temos que $r' - r = 0$, isto é, $r = r'$ e segue que $a \equiv b \mod m$. □

Proposição 1.23. *Para quaisquer $a, b, c, d, m \in \mathbb{Z}$, com $m > 1$, temos que valem as seguintes propriedades:*

1. *(Reflexividade): $a \equiv a \mod m$;*
2. *(Simetria): Se $a \equiv b \mod m$, então $b \equiv a \mod m$;*
3. *(Transitividade): Se $a \equiv b \mod m$ e $b \equiv c \mod m$, então $a \equiv c \mod m$;*
4. *(Compatibilidade com a soma): Podemos somar (ou subtrair) "membro a membro":*

$$\begin{cases} a \equiv b \mod m \\ c \equiv d \mod m \end{cases} \implies a + c \equiv b + d \mod m.$$

   Em particular, se $a \equiv b \mod m$, então $ka \equiv kb \mod m$, para todo $k \in \mathbb{Z}$.

5. *(Compatibilidade com o produto): Podemos multiplicar "membro a membro":*

$$\begin{cases} a \equiv b \mod m \\ c \equiv d \mod m \end{cases} \implies ac \equiv bd \mod m.$$

   Em particular, se $a \equiv b \mod m$, então $a^k \equiv b^k \mod m$, para todo $k \in \mathbb{Z}$.

6. *(Cancelamento): Se $(c, m) = 1$, então*

$$ac \equiv bc \mod m \iff a \equiv b \mod m.$$

Demonstração. (1) Basta observar que $m \mid (a - a) = 0$;

(2) Se $m \mid (b-a)$ então $m \mid -(b-a) = (a-b)$;

(3) Se $m \mid (a-b)$ e $m \mid (b-c)$ então $m \mid ((a-b)+(b-c)) = (a-c)$;

(4) Se $m \mid (a-b)$ e $m \mid (c-d)$ então $m \mid ((a-b)+(c-d)) = ((a+c)-(b+d))$, em particular, se $m \mid (a-b)$ então $m \mid k(a-b) = ak - bk$;

(5) Se $m \mid (a-b)$ e $m \mid (c-d)$ então $m \mid (a-b)c$ e $m \mid (c-d)b$, assim concluímos que $m \mid ((a-b)c + (c-d)b) = (ac-bd)$, em particular, se $m \mid (a-b)$, pelo que foi provado acima, $m \mid (a^2 - b^2)$ e recursivamente $m \mid (a^k - b^k)$;

(6) Como $(c, m) = 1$ temos que $m \mid (ac - bc) = (a-b)c$ e pelo Lema 1.17, concluímos que $m \mid (a-b)$.

□

Teorema 1.24. *Sejam $a, m \in \mathbb{Z}$, com $m > 1$. A congruência $aX \equiv 1 \mod m$ possui solução se, e somente se, $(a, m) = 1$. Além disso, se $x_0 \in \mathbb{Z}$ é uma solução, então x também é uma solução da congruência se, e somente se, $x \equiv x_0 \mod m$.*

Demonstração. A congruência tem solução x_0 se, e somente se, $m \mid (ax_0 - 1)$, assim existe $y \in \mathbb{Z}$ tal que $ax_0 + m(-y) = 1$ e pelo Corolário 1.16, concluímos que $(a, m) \mid 1$, logo, $(a, m) = 1$. Por conseguinte, se x_0 e x são soluções da congruência $aX \equiv 1 \mod m$, então $ax \equiv ax_0 \mod m$ e $(a, m) = 1$, assim $x \equiv x_0 \mod m$, por outro lado, se x_0 é solução da congruência $aX \equiv 1 \mod m$ e $x \equiv x_0 \mod m$, então x também é solução, pois $ax \equiv ax_0 \equiv 1 \mod m$. □

As duas definições que seguem são primordiais em diversos momentos do presente trabalho.

Definição 1.25. *Denominamos de sistema de resíduos módulo m, todo conjunto de números inteiros cujos restos pela divisão por m são os inteiros $0, 1, \ldots, m-1$; sem repetições e em uma ordem qualquer.*

O sistema de resíduos módulo m apresenta todas as possibilidades de restos na divisão de um inteiro qualquer a por m. Uma consequência da Definição acima é que, se $a_1, a_2, \ldots a_m$; são m inteiros, dois a dois, não congruentes módulo m, eles formam um sistema de resíduos módulo m.

Definição 1.26. *Um sistema reduzido de resíduos módulo m é um conjunto de números inteiros $b_1, b_2, \ldots, b_r$; tais que*

i) $(b_i, m) = 1$ *para todo* $i = 1, 2, \ldots, r$;

ii) $b_i \not\equiv b_j \mod m$, *se* $i \neq j$;

iii) Para cada $a \in \mathbb{Z}$ *tal que* $(a, m) = 1$, *existe* i *tal que* $a \equiv b_i \mod m$.

É possível obter um sistema reduzido de resíduos módulo m a partir de um sistema de resíduos módulo m, bastando eliminar os elementos a_i, do sistema de resíduos, que não são primos com m. Para saber mais sobre sistema reduzido de resíduos módulo m, veja Capítulo 10 de [16].

O lema que segue será oportunamente muito importante e possui uma notável simplicidade.

Lema 1.27. *Sejam* $a, m, n \in \mathbb{Z}$ *e* p *primo. Se* $a^n \equiv 1 \mod p$ *e* $a^m \equiv 1 \mod p$, *então* $a^g \equiv 1 \mod p$ *com* $g = (n, m)$.

Demonstração. Pelo Teorema 1.15 existem $x, y \in \mathbb{Z}$ tais que $nx + my = (n, m)$, portanto se $a^n \equiv 1 \mod p$ e $a^m \equiv 1 \mod p$, pelas propriedades da Proposição 1.23, temos que $a^{nx} \equiv a^{my} \equiv 1 \mod p$, logo, $a^{nx}a^{my} = a^{nx+my} = a^{(n,m)} \equiv 1 \mod p$. □

Para o importante resultado conhecido como Pequeno Teorema de Fermat, utilizamos o próximo teorema e o próximo lema.

Teorema 1.28. *(Fórmula do Binômio de Newton) Sejam* a *e* b *números reais e seja* $n \in \mathbb{N} \cup \{0\}$. *Tem-se que*

$$(a+b)^n = a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \ldots + \binom{n}{n-1}ab^{n-1} + b^n,$$

onde $\binom{n}{i} = \dfrac{n!}{i!(n-i)!}$, *com* $0 \leq i \leq n$ *inteiro.*

Demonstração. Teorema 2.8 de [16]. □

Lema 1.29. *Seja* p *um número primo. Os números* $\binom{p}{i}$, *onde* $0 < i < p$, *são todos divisíveis por* p.

Demonstração. Para $i = 1$ o resultado é trivial. Suponha que $1 < i < p$, portanto, como $(i!, p) = 1$ obtemos

$$\binom{p}{i} = p\frac{(p-1)\ldots(p-i+1)}{i!}.$$

Verifica-se facilmente que $\binom{p}{i} \in \mathbb{N}$, logo, $i! \mid (p-1)\ldots(p-i+1)$ e o resultado segue. □

Teorema 1.30 (Pequeno Teorema de Fermat)**.** *Se* p *é um número primo e se* a *é um número natural, então* $a^p \equiv a \mod p$. *Em particular, se* p *não divide* a, *ou seja, se* $(a, p) = 1$ *então temos que* $a^{p-1} \equiv 1 \mod p$.

Demonstração. Se $p = 2$, como $a^2 - a = a(a-1)$ concluímos que $2 \mid a(a-1)$, pois a ou $a-1$ é par, isto é, $a^2 \equiv a \mod 2$. Seja p um número primo ímpar, por indução em a temos que $p \mid (1^p - 1)$, portanto $P(1)$ é verdadeira. Suponha que $p \mid (a^p - a)$ para algum $a \in \mathbb{N}$, assim para $a+1$ e pela Fórmula do Binômio de Newton, obtemos

$$(a+1)^p - (a+1) = (a^p - a) + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \ldots + \binom{p}{p-1}a$$

pela hipótese de indução e o Lema 1.29, segue que $p \mid ((a+1)^p - (a+1))$, ou seja, $P(a+1)$ é verdadeira. Assim, pelo Princípio da Indução o resultado segue. Particularmente, se $(a,p) = 1$, então $p \mid a(a^{p-1} - 1) \iff p \mid (a^{p-1} - 1)$, logo, $a^{p-1} \equiv 1 \mod p$. □

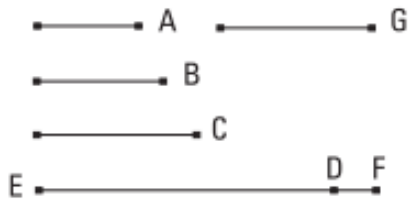
1.2 A Infinidade dos Números Primos

É enunciado a seguir o principal Teorema do presente trabalho, o Teorema de Euclides da Infinidade dos Números Primos. A primeira demonstração deste Teorema é atribuída à Euclides, por volta do ano 300 a.C. publicada no seu famoso livro, Os Elementos. A demonstração que será apresentada inicialmente é a original, que foi retirada na íntegra do livro Os Elementos - Euclides, uma tradução de I. Bicudo, e se encontra na página 342 de [5].

Teorema 1.31. *Existem infinitos números primos.*

Demonstração Original. (Euclides)

Sejam os números primos que tenham sido propostos A, B, C; digo que os números primos são 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. □

A seguir, apresentamos 22 demonstrações diferentes para o Teorema 1.31. Em certas demonstrações, foi necessário incluir mais algumas definições e resultados, que não foram utilizados em outras demonstrações.

1.3 Demonstrações com Teoria dos Números

Uma versão moderna da demonstração de Euclides é fornecida em seguida e foi baseada na página 1 de [29].

Demonstração 1. (Euclides)
Suponha que o conjunto $\mathfrak{P} = \{p_1, p_2, \ldots, p_r\}$ dos números primos seja finito. Considere $N = p_1 p_2 \ldots p_r + 1$, pelo Teorema 1.19, existe um número primo $q \leq N$ tal que $q \mid N$, mas se $q \in \mathfrak{P}$ então q divide $N - p_1 p_2 \ldots p_r = 1$, o que é um absurdo. Logo, $q \notin \mathfrak{P}$, isto é, existem infinitos números primos. □

A demonstração que segue, baseada na página 4 de [22], é atribuída à C. Hermite, desenvolvida no século 19, é uma elegante variação da demonstração de Euclides.

Demonstração 2. (Hermite)
Para cada $n \in \mathbb{N}$, seja $N = n! + 1$, pelo Teorema 1.19, existe um primo q tal que $q \mid N$, mas $q > n$, pois caso contrário q dividiria $N - n! = 1$. Logo, sempre existe pelo menos um número primo $q > n$ para cada $n \in \mathbb{N}$, isto é, existem infinitos números primos. □

Outra variação da demonstração de Euclides foi dada em 1890 por T. Stieltjes, a demonstração que segue foi baseada na página 4 de [22].

Demonstração 3. (Stieltjes)
Suponha que o conjunto $\mathfrak{P} = \{p_1, p_2, \ldots, p_r\}$ dos números primos seja finito. Considere $N = p_1 p_2 \ldots p_r = mn$, uma fatoração qualquer de N em inteiros positivos m e n maiores do que 1. Para todo primo $p_i \in \mathfrak{P}$, se $p_i \mid m$ temos que $p_i \nmid n$ e se $p_i \mid n$ então $p_i \nmid m$, logo, pela contrapositiva do Lema 1.9, $p_i \nmid (m + n)$, isto é, não existe $p_i \in \mathfrak{P}$ tal que $p_i \mid (m + n)$, o que é um absurdo pelo Teorema 1.19. Portanto, o conjunto dos números primos é infinito. □

Uma expansão da ideia de Stieltjes foi abordada por G. Métrod em 1917 e esta demonstração pode ser encontrada na página 9 de [29].

Demonstração 4. (Métrod)
Suponha que o conjunto dos números primos $\mathfrak{P} = \{p_1, p_2, \ldots, p_r\}$ seja finito. Considere

$N = p_1 p_2 \dots p_r$ e para cada índice $i = 1, 2, \dots, r$; seja $Q_i = \dfrac{N}{p_i}$. Consideramos $S = \sum_{i=1}^{r} Q_i$ e dado o número primo q tal que $q \mid S$, observamos pelo Lema 1.9 que $q \neq p_i$ para todo índice i, pois $p_i \mid Q_j$ para todo $j \neq i$, mas $p_i \nmid Q_i$. Portanto, $q \notin \mathfrak{P}$ o que é um absurdo, logo, o conjunto dos números primos é infinito. □

L. Euler em 1736 publicou uma demonstração do Teorema 1.31, encontrada na página 7 de [22], utilizando argumentos totalmente novos. Definimos para tal demonstração a função φ de Euler.

Definição 1.32. *Para todo inteiro $n \geq 1$, definimos a função $\varphi : \mathbb{N} \to \mathbb{N}$, denominada de função φ de Euler, como a quantidade de inteiros m, com $1 \leq m < n$ tais que $(m, n) = 1$. Portanto, $\varphi(n)$ é a quantidade de números naturais menores ou iguais a n que não possuem divisores inteiros positivos comuns, diferentes de 1, com n.*

Segue direto da definição que se $n = p$ é primo, tem-se $\varphi(p) = p - 1$, além disso, $\varphi(1) = 1$. Também vamos precisar do importante teorema que segue, baseado na página 49 de [20], para a demonstração recomendamos rever as propriedades da Proposição 1.23.

Teorema 1.33. *Se $a, b \in \mathbb{N}$ e $(a, b) = 1$, então, $\varphi(ab) = \varphi(a)\varphi(b)$.*

Demonstração. Consideramos os números $1, 2, \dots, ab$; organizados de forma matricial com b linhas e a colunas:

$$\begin{array}{ccccc} 1 & 2 & 3 & \dots & a \\ a+1 & a+2 & a+3 & \dots & 2a \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a(b-1)+1 & a(b-1)+2 & a(b-1)+3 & \dots & a(b-1)+a \end{array}$$

Pelo Lema 1.14 temos que $(ai + j, a) = (j, a)$, assim, se um número nessa lista é primo com a, então todos os números na presente coluna são primos com a. Logo, existem $\varphi(a)$ colunas tais que todos os números são primos com a. Por outro lado, como temos b inteiros tais que se $ai_1 + j \equiv ai_2 + j \mod b$, então, $i_1 \equiv i_2 \mod b$, pois $(a, b) = 1$, portanto, como $0 \leq i_1, i_2 < b$, devemos ter $i_1 = i_2$, logo, toda coluna possui um sistema de resíduos módulo b, isso permite utilizar a Definição 1.32 para concluir que em cada coluna existem exatamente $\varphi(b)$ números que são primos com b. Portanto, o total de números nessa lista que são simultaneamente primos com a e b, ou seja, primos com ab, são $\varphi(b)$ números em cada uma das $\varphi(a)$ colunas, ou seja, são $\varphi(a)\varphi(b)$, logo, $\varphi(ab) = \varphi(a)\varphi(b)$. □

Demonstração 5. (Euler)(1)
Suponha que o conjunto ordenado dos números primos $\mathfrak{P} = \{2, 3, p_3, \dots, p_r\}$ seja finito.

Seja $N = 2 \cdot 3 \cdot p_3 \cdot \ldots \cdot p_r$, o produto de todos os números primos, observando a função φ de Euler aplicada em N, lembrando que $\varphi(p_i) = p_i - 1$ com $p_i \in \mathfrak{P}$, temos que

$$\varphi(N) = \varphi(2)\varphi(3)\varphi(p_3)\ldots\varphi(p_r) = \prod_{i=1}^{r}(p_i - 1) \geq 2,$$

portanto, além de $(1, N) = 1$, existe um inteiro $2 \leq n \leq N$ tal que $(n, N) = 1$, ou seja, como todos os primos dividem N e $(n, N) = 1$, o inteiro $n > 1$ não possui nenhum divisor primo, o que é um absurdo pelo Teorema 1.19. Assim, existem infinitos números primos. □

1.4 Demonstrações com inteiros primos entre si

A primeira demonstração posterior a Euclides é creditada à C. Goldbach e divulgada em uma carta para L. Euler em 1730. Esta demonstração, baseada na página 4 de [29], utiliza um método totalmente diferente para demonstrar o Teorema 1.31.

Definimos os *números de Fermat* como $F_n = 2^{2^n} + 1$ para todo inteiro $n \geq 0$. Por exemplo, $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$ e assim sucessivamente. Um interessante resultado que utilizaremos é apresentado no próximo Lema.

Lema 1.34. *Sejam os números de Fermat F_n, temos que $F_n - 2 = F_0F_1\ldots F_{n-1}$, para $n \geq 1$.*

Demonstração. Faremos por indução em n, como $F_0 = 3$ e $F_1 = 5$, temos que $P(1)$ é verdadeiro, pois $F_1 - 2 = F_0$. Suponha que $F_n - 2 = F_0F_1\ldots F_{n-1}$ para algum $n \in \mathbb{N}$, então multiplicando F_n na igualdade temos que $(F_n)^2 - 2F_n = F_0F_1\ldots F_{n-1}F_n$, mas

$$(F_n)^2 - 2F_n = \left(2^{2^n} + 1\right)^2 - 2(2^{2^n} + 1) = 2^{2^{n+1}} + 1 - 2 = F_{n+1} - 2$$

portanto, $P(n+1)$ é verdadeiro. Logo, pelo Princípio da Indução o resultado segue. □

Demonstração 6. (Goldbach)
Consideramos os números de Fermat $F_n = 2^{2^n} + 1$. Seja $m < n$, pelo Lema 1.34, temos que $F_m \mid (F_n - 2)$, então suponha que $F_m \mid F_n$, pelo Lema 1.9, $F_m \mid F_n \iff F_m \mid 2$, o que é um absurdo, pois $F_m \neq 1$ e $F_m \neq 2$, logo, $F_m \nmid F_n$. Como $F_n - 2 = kF_m$ com $k \in \mathbb{N}$, verifica-se facilmente que

$$1 = (2^{2^n} - 1, 2) = (2^{2^n} - 1, 2^{2^n} + 1) = (F_n - 2, F_n) = (kF_m, F_n) = (F_m, F_n).$$

Portanto, $(F_m, F_n) = 1$, $\forall\ m, n \in \mathbb{N} \cup \{0\}$ com $m < n$, isto é, todos os números de Fermat F_n são, dois a dois, primos entre si. Pelo Teorema 1.19, existe um número primo $p_1 \mid F_0$, $p_2 \mid F_1$, ..., $p_n \mid F_{n-1}$, ...; e todos são números primos distintos. Logo, existem infinitos números primos, visto que existem infinitos números de Fermat. □

Existe uma grande quantidade de variações da demonstração de Goldbach. Uma elegante variação dessa demonstração, que pode ser encontrada na página 36 de [8], foi publicada em 2006 por F. Saidak.

Demonstração 7. (Saidak)
Pelo Teorema 1.19, todo número natural maior que 1 possui pelo menos 1 fator primo e, além disso, dado um número natural $n > 1$ temos que $(n, n+1) = 1$, isto é, os fatores primos de n são todos distintos dos fatores primos de $n+1$, portanto temos que o número $n(n+1)$ possui pelo menos 2 fatores primos distintos, por conseguinte, como $(n(n+1), n(n+1)+1) = 1$, temos que o número $n(n+1)[n(n+1)+1]$ possui pelo menos 3 fatores primos distintos.

Seguindo esse processo recursivamente, definimos a sequência dada por $a_1 = n$ e $a_k = a_{k-1}(a_{k-1}+1)$ para $k \geq 2$, que possui pelo menos k fatores primos distintos para o seu k-ésimo termo, logo, como a sequência $(a_k)_{k\geq 2}$ possui infinitos termos, temos que $k \to \infty$, isto é, existem infinitos números primos. □

Para a próxima demonstração utilizamos os *números de Fibonacci* T_n, que são definidos por $T_1 = T_2 = 1$ e recursivamente por $T_{n+2} = T_{n+1} + T_n$ para todo $n \in \mathbb{N}$. Por exemplo, $T_1 = 1$, $T_2 = 1$, $T_3 = 2$, $T_4 = 3$, $T_5 = 5$, $T_6 = 8$, $T_7 = 13$, $T_8 = 21$ e assim sucessivamente. Necessitamos também dos resultados que seguem, baseados nos Capítulos 2 e 6 de [16], convém para as demonstrações lembrarem do Lema 1.14.

Lema 1.35. *Temos que* $T_{m+n} = T_m T_{n-1} + T_{m+1} T_n$ *para todo* $m, n \in \mathbb{N}$ *com* $n \geq 2$.

Demonstração. Fixado o inteiro $n \geq 2$, faremos indução completa em m. Para $m = 1$ obtemos que $T_1 T_{n-1} + T_2 T_n = T_{n-1} + T_n = T_{1+n}$ e $P(1)$ é verdadeiro. Suponha que para todo $k \leq m$ é válido $T_{k+n} = T_k T_{n-1} + T_{k+1} T_n$, assim, pela hipótese, temos que $T_{m+n} = T_m T_{n-1} + T_{m+1} T_n$ e $T_{m-1+n} = T_{m-1} T_{n-1} + T_m T_n$. Somando membro a membro essas igualdades, obtemos

$$T_{m+n} + T_{m-1+n} = T_m T_{n-1} + T_{m+1} T_n + T_{m-1} T_{n-1} + T_m T_n,$$

$$T_{m+n} + T_{m-1+n} = T_{n-1}\left(T_m + T_{m-1}\right) + T_n\left(T_{m+1} + T_m\right),$$

$$T_{m+1+n} = T_{m+1} T_{n-1} + T_{m+2} T_n.$$

Logo, $P(m+1)$ é verdadeira. Se fixado $m \in \mathbb{N}$, como $n \geq 2$, basta fazer $n - 1 = m'$ e $n = m' + 1$, então, analogamente se prova indução completa em n. Assim, o resultado segue pelo Princípio de Indução. □

Lema 1.36. $(T_n, T_{n+1}) = 1$ *para todo* $n \in \mathbb{N}$.

Demonstração. Por indução em n obtemos, para $n = 1$ que $(T_1, T_2) = 1$ e supondo que $(T_n, T_{n+1}) = 1$ para algum $n \in \mathbb{N}$, segue para $n + 1$ que

$$(T_{n+1}, T_{n+2}) = (T_{n+1}, T_{n+1} + T_n) = (T_{n+1}, T_n) = 1.$$

E o resultado segue. □

Teorema 1.37. *Os números de Fibonacci satisfazem* $(T_m, T_n) = T_{(m,n)}$ *para todo* $m, n \in \mathbb{N}$.

Demonstração. Provaremos por indução completa em m, se $m = 1$ ou $m = 2$ temos que

$$(T_m, T_n) = (1, T_n) = 1 = T_1 = T_2 = T_{(1,n)} = T_{(2,n)} = T_{(m,n)}, \tag{1.1}$$

para qualquer $n \in \mathbb{N}$, assim, $P(1)$ e $P(2)$ são verdadeiros. Suponha que $(T_m, T_n) = T_{(m,n)}$ para todo $m < k$ com $k \geq 3$ inteiro e para todo $n \in \mathbb{N}$, para provar $P(k)$ faremos indução em n com k fixado. Primeiramente, note que de maneira análoga à igualdade (1.1), obtemos que $(T_k, T_n) = T_{(k,n)}$ para $n = 1$ e $n = 2$, agora suponha que $(T_k, T_n) = T_{(k,n)}$ para todo inteiro positivo $2 < n < t$, logo, fazendo $n = t$, pelo Lema 1.35, temos que $T_t = T_{(t-k)+k} = T_{t-k}T_{k-1} + T_{t-k+1}T_k$, assim

$$(T_k, T_t) = (T_k, T_{t-k}T_{k-1} + T_{t-k+1}T_k) = (T_k, T_{t-k}T_{k-1}),$$

pelo Lema 1.36, $(T_{k-1}, T_k) = 1$ e pela hipótese de indução em n, já que $t - k < t$, concluímos que

$$(T_k, T_{t-k}T_{k-1}) = (T_k, T_{t-k}) = T_{(k,t-k)} = T_{(k,t)}.$$

Logo, $(T_k, T_n) = T_{(k,n)}$ para todo $n \in \mathbb{N}$, portanto, concluímos a indução em n e verificamos que $P(k)$ é verdadeiro, assim, o resultado segue pela indução em m. □

Corolário 1.38. *Se* $(m, n) = 1$ *então* $(T_m, T_n) = 1$

Demonstração. Se $(m, n) = 1$, pelo Teorema 1.37, $(T_m, T_n) = T_{(m,n)} = T_1 = 1$ □

A demonstração seguinte foi publicada em 1965 por M. Wunderlich e pode ser encontrada na página 9 de [22].

Demonstração 8. (Wunderlich)
Suponha que o conjunto ordenado $\mathfrak{P} = \{2, 3, p_3, \ldots, p_r\}$ dos números primos seja finito. Sabemos que $(p_a, p_b) = 1$ para quaisquer números primos $p_a, p_b \in \mathfrak{P}$ distintos, portanto, pelo Corolário 1.38 temos que os números de Fibonacci com índices primos são primos entre si, isto é, $(T_{p_a}, T_{p_b}) = 1$. Como $T_{p_i} > 1$ para todo $p_i \in \mathfrak{P}$ tal que $i \neq 1$, ou seja, para os índices $i = 2, 3, \ldots, r$; pelo Teorema 1.19 cada um dos números T_{p_i} possuem

pelo menos um fator primo e são todos distintos entre si, já que todos os T_{p_i} são primos entre si. Portanto, temos $r-1$ números de Fibonacci, todos com fatores primos distintos, e r números primos, assim, utilizando o Princípio das Gavetas, observamos que com a exceção de um único número de Fibonacci $T_{p_{i'}}$ que possui exatamente dois fatores primos distintos, todos os números de Fibonacci T_{p_i} com $i \neq i' \neq 1$ possuem exatamente um fator primo, isto é, a sua fatoração possui apenas um número primo distinto.

Sabe-se que $19, 37$ e 113 são números primos e $T_{19} = 4181 = 37 \,.\, 113$, portanto $T_{p_{i'}} = T_{19}$ e todos os demais T_{p_i} possuem exatamente um fator primo, contudo, $31, 557$ e 2417 são números primos tal que $T_{31} = 1346269 = 557 \,.\, 2417$, o que é um absurdo. Logo, existem infinitos números primos. □

1.5 Demonstrações com Congruência Modular

A próxima demonstração utiliza congruência modular e pode ser encontrada na página 2 de [15], como não é atribuída a um matemático específico, nomeamos esta demonstração em nome de A. Granville, autor do artigo em 2017 onde a demonstração é encontrada. Precisamos para a demonstração, os números de Mersenne M_q e o Lema 1.27.

Definimos os *números de Mersenne* como $M_q = 2^q - 1$ com q um número primo. Por exemplo, $M_2 = 3$, $M_3 = 7$, $M_5 = 31$, $M_7 = 127$, $M_{11} = 2047$ e assim sucessivamente.

Demonstração 9. (Granville)(1)
Suponha que o conjunto ordenado dos números primos $\mathfrak{P} = \{p_1, p_2, \ldots, q\}$ seja finito, onde q é o maior número primo. Se $p \in \mathfrak{P}$ é um fator primo do número de Mersenne $M_q = 2^q - 1$, então $2^q - 1 \equiv 0 \mod p$, isto é, $2^q \equiv 1 \mod p$ e como $(p, 2) = 1$, já que M_q é ímpar, pelo Teorema 1.30, sabemos que $2^{p-1} \equiv 1 \mod p$. Portanto, pelo Lema 1.27, concluímos que $2^g \equiv 1 \mod p$ com $g = (p-1, q)$. Como $g \mid q$, então $g = 1$ ou $g = q$, mas $g \neq 1$, pois se ocorrer $g = 1$ temos que $2^g - 1 = 2^1 - 1 = 1 \equiv 0 \mod p$, ou seja, $p \mid 1$ o que é um absurdo, logo, $g = q$. Por conseguinte, como $g = q$ temos que $q \mid (p-1)$, portanto, $q \leq p - 1 < p$, o que é um absurdo, pois q é o maior número primo de $\mathfrak{P}$. Logo, existem infinitos números primos. □

A próxima demonstração também utiliza congruência modular, novamente atribuímos esta demonstração a A. Granville, autor do artigo [15] em 2017, onde a demonstração é encontrada na página 2.

Demonstração 10. (Granville)(2)
Suponha que o conjunto ordenado dos números primos $\mathfrak{P} = \{2, 3, p_3, \ldots, p_r\}$ seja finito.

Seja 2^n a maior potência de 2 que divide algum dos números da forma $p_i - 1$ com $i = 1, 2, \ldots, r$. Consideramos o número de Fermat $F_n = 2^{2^n} + 1$ e $p_k \in \mathfrak{P}$ um fator primo de F_n, observamos que $2^{2^{n+1}} - 1 = (F_n - 1)^2 - 1 = F_n(F_n - 2) \equiv 0 \mod p_k$, já que $p_k \mid F_n$, ou seja, $2^{2^{n+1}} \equiv 1 \mod p_k$. Como $(p_k, 2) = 1$, já que F_n é ímpar, pelo Teorema 1.30, temos que $2^{p_k - 1} \equiv 1 \mod p_k$, portanto, pelo Lema 1.27, obtemos que $2^g \equiv 1 \mod p_k$ com $g = (2^{n+1}, p_k - 1)$, mas como $g \mid 2^{n+1}$ então g é 1 ou g é uma potência de 2 com expoente natural, logo, podemos escrever $g = 2^m$ com $m \in \mathbb{N} \cup \{0\}$. Temos ainda que $m \leq n$, pois 2^n é a maior potência de 2 que divide algum dos números da forma $p_i - 1$ e $g = 2^m \mid (p_k - 1)$. Logo, pelo que obtemos acima, como $2^g \equiv 1 \mod p_k$ concluímos que

$$0 \equiv F_n = 2^{2^n} + 1 = \left(2^{2^m}\right)^{2^{n-m}} + 1 = (2^g)^{2^{n-m}} + 1 \equiv 1^{2^{n-m}} + 1 = 2 \mod p_k$$

portanto, $2 \equiv 0 \mod p_k$, o que é um absurdo, pois $p_k \neq 2$. Logo, existem infinitos números primos. □

1.6 Demonstrações com Combinatória

Em 1897 A. Thue forneceu uma demonstração do Teorema 1.31 utilizando combinatória. Nos baseamos na página 7 de [29] para a demonstração.

Lema 1.39. *Temos que* $1 + 2k^2 < 2^{2k}$ *para todo* $k \geq 1$.

Demonstração. Provaremos por indução em k, para $k = 1$ temos que $3 < 4$ e $P(1)$ é verdadeira. Suponha que $1 + 2k^2 < 2^{2k}$ para algum $k \in \mathbb{N}$, observamos que $4k < 1 + 6k^2$, disso obtemos facilmente que $2(k+1)^2 + 1 < 4 + 8k^2$ e pela hipótese de indução obtemos que $4 + 8k^2 < 2^{2(k+1)}$, logo $2(k+1)^2 + 1 < 2^{2(k+1)}$ e $P(k+1)$ é verdadeiro. Pelo Princípio da Indução o resultado segue. □

Demonstração 11. (Thue)
Sejam os inteiros positivos k e $n > 1$ tais que $(n+1)^k < 2^n$. Considere o conjunto ordenado $\{2, 3, \ldots, p_r\}$ de todos os r números primos tais que $p_i < 2^n$ com $i = 1, 2, \ldots, r$. Suponha que $r \leq k$, assim, pelo Corolário 1.20, todo inteiro $1 \leq m \leq 2^n$ se escreve de maneira única como $m = 2^{\alpha_1} 3^{\alpha_2} \ldots p_r^{\alpha_r}$, onde $0 \leq \alpha_1, \alpha_2, \ldots, \alpha_r \leq n$. Obviamente, temos $(n+1)^r$ combinações possíveis de expoentes para gerar os inteiros positivos m, mas nem todas essas combinações geram um número m tal que $m \leq 2^n$, logo, temos que $2^n < (n+1)^r$, portanto, $2^n < (n+1)^r \leq (n+1)^k < 2^n$, o que é um absurdo, logo, $r \geq k + 1$.

Pelo Lema 1.39, temos que $1 + 2k^2 < 2^{2k}$ para todo $k \geq 1$, portanto, obtemos que $(1 + 2k^2)^k < 2^{2k^2} = 4^{k^2}$, fazendo $n = 2k^2$, obtemos que $(1 + n)^k < 2^n$, logo, como $r \geq k + 1$, existem pelo menos $k + 1$ números primos $p_i < 2^n = 4^{k^2}$. Como k pode ser tomado tão grande quanto se queira, existem infinitos números primos. □

Para a próxima demonstração utilizaremos a definição do denominado *piso* $\lfloor x \rfloor$ de x, que também utilizaremos em vários outros momentos durante o trabalho.

Definição 1.40. *Dado $x \in \mathbb{R}$, definimos o piso $\lfloor x \rfloor$ de x como sendo o único $k \in \mathbb{Z}$ tal que $k \leq x < k+1$.*

Observe que segue direto da Definição acima que $\lfloor x \rfloor \leq x$. Em todo o trabalho escrevemos o *logaritmo natural* do número real $x > 0$ como $\log x$ e definimos esta função utilizando o conceito de integral. O objetivo desta definição é utilizar o fato de uma integral definida ser a área sob a curva de uma função, para saber mais sobre a definição apresentada, veja a página 440 de [17]. Ficam também assumidas as propriedades dos logaritmos, veja Seção 7.3 de [17].

Definição 1.41. *A função logarítmica natural* $\log : \mathbb{R}_+^* \to \mathbb{R}$ *é definida como*

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

A demonstração fornecida por A. Auric em 1915 é também simples, nos baseamos na página 9 de [29]. Utilizamos nessa demonstração o fato da *função exponencial* $e : \mathbb{R} \to \mathbb{R}_+^*$ definida como $e(x) = a^x$ com $a > 0$ real e $a \neq 1$, crescer mais rapidamente que qualquer função polinomial $p : \mathbb{R} \to \mathbb{R}$ definida como $p(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ com $a_n, a_{n-1}, \ldots, a_0$ números reais e $a_n \neq 0$, o que pode ser verificado pelo limite $\lim\limits_{x \to +\infty} \dfrac{p(x)}{e(x)} = 0$, facilmente demonstrado por sucessivas aplicações da regra de L'Hôpital, veja Teorema 11.1.4 de [17]. Para um estudo mais detalhado dessas funções apresentadas, veja [19].

Demonstração 12. (Auric)
Suponha que o conjunto ordenado $\mathfrak{P} = \{2, 3, p_3, \ldots, p_r\}$ dos números primos seja finito, com p_r o maior número primo. Sejam os inteiros $t \geq 1$ e p_r^t, pelo Corolário 1.20, cada inteiro $1 \leq m \leq p_r^t$ pode ser escrito como $m = 2^{\alpha_1} 3^{\alpha_2} \ldots p_r^{\alpha_r}$, onde $\alpha_1, \alpha_2, \ldots, \alpha_r \geq 0$ e $p_i^{\alpha_i} \leq p_r^t$ para todo $i = 1, 2, \ldots, r$; assim, observamos que a sequência $\alpha_1, \alpha_2, \ldots, \alpha_r$; é definida de maneira única para cada inteiro positivo m. Como $2^{\alpha_i} \leq p_i^{\alpha_i} \leq p_r^t$, então obtemos facilmente que $\alpha_i \leq t \left\lfloor \frac{\log p_r}{\log 2} \right\rfloor$, assim α_i é, no máximo, igual a $t \left\lfloor \frac{\log p_r}{\log 2} \right\rfloor$ para cada índice i e já que $\left\lfloor \frac{\log p_r}{\log 2} \right\rfloor > 1$ para $p_r > 3$, existe $\alpha_k > t$ com $k \in \{1, 2, \ldots, r\}$ tal que a sequência $\alpha_k, 0, \ldots, 0$; gera um número menor que p_r^t, mas a sequência $\alpha_k, \alpha_k, \ldots, \alpha_k$; gera um número maior que p_r^t, logo, temos que a quantidade p_r^t de inteiros m é estritamente menor que a quantidade existente de sequências distintas $\alpha_1, \alpha_2, \ldots, \alpha_r$; com $\alpha_i \leq t \left\lfloor \frac{\log p_r}{\log 2} \right\rfloor$, que a propósito, é igual a $\left(t \left\lfloor \frac{\log p_r}{\log 2} \right\rfloor + 1 \right)^r$. Assim, temos satisfeita a desigualdade

$$p_r^t < \left(t \left\lfloor \frac{\log p_r}{\log 2} \right\rfloor + 1 \right)^r \leq \left(\left\lfloor \frac{\log p_r}{\log 2} \right\rfloor + 1 \right)^r t^r, \tag{1.2}$$

a desigualdade da direita segue do fato de $t \geq 1$. Mas observe que o exponencial p_r^t cresce mais rápido do que qualquer polinômio, que é o caso de at^r com $a \in \mathbb{R}$, portanto, para t suficientemente grande a desigualdade (1.2) não é válida, o que é um absurdo. Logo, existe uma quantidade infinita de números primos. □

1.7 Demonstrações com Análise e Topologia

Utilizaremos oportunamente os seguintes teoremas sobre séries, que podem ser encontradas no decorrer do Capítulo 12 de [17]:

Teorema 1.42. *Se* $\sum_{n=1}^{\infty} u_n$ *for uma série convergente de termos positivos, a ordem dos termos pode ser rearranjada e a série resultante será também convergente com a mesma soma que a série inicialmente dada.*

Demonstração. Teorema 12.5.5 de [17]. □

Teorema 1.43. *Seja* (s_n) *a sequência das somas parciais de uma dada série convergente* $\sum_{n=1}^{\infty} u_n$*, então para todo* $\epsilon > 0$*, existe um número* N *tal que se* $r > N$ *e* $t > N$ *então* $|s_r - s_t| < \epsilon$.

Demonstração. Teorema 12.3.4 de [17]. □

Teorema 1.44. *Uma série infinita de termos positivos será convergente se e somente se sua sequência de somas parciais tiver um limitante superior.*

Demonstração. Teorema 12.5.1 de [17]. □

Teorema 1.45. *Se a série infinita* $\sum_{n=1}^{\infty} u_n$ *for absolutamente convergente, então, será convergente.*

Demonstração. Teorema 12.8.3 de [17]. □

Teorema 1.46. *Se a série infinita* $\sum_{n=1}^{\infty} u_n$ *for convergente então* $\lim_{n\to\infty} u_n = 0$.

Demonstração. Teorema 12.3.3 de [17]. □

Teorema 1.47 (Teste da Razão)**.** *Seja* $\sum_{n=1}^{\infty} u_n$ *uma série infinita dada para a qual todo* u_n *é não nulo. Então, considerando o limite* $\lim_{n\to\infty} \left|\frac{u_{n+1}}{u_n}\right| = L \geq 0$*, se* $L < 1$ *a série dada*

é absolutamente convergente, se $L > 1$ ou $L \to \infty$ a série dada é divergente e se $L = 1$ nenhuma conclusão quanto à convergência pode ser tirada do teste.

Demonstração. Teorema 12.8.4 de [17]. □

Teorema 1.48. *(Série geométrica) A série geométrica de razão r é definida como $\sum_{k=0}^{\infty} ar^k = a + ar + ar^2 + \ldots$; sendo convergente para $\frac{a}{1-r}$ quando $|r| < 1$ e divergente quando $|r| \geq 1$.*

Demonstração. Teorema 12.3.5 de [17]. □

A demonstração que segue é interessante por depender da irracionalidade do número real π. A demonstração da irracionalidade do número π pode ser encontrada a partir da página 9 de [12].

Esta demonstração do Teorema 1.31 é encontrada na página 2 de [15], não é atribuída a um matemático específico, portanto à denominaremos em homenagem a A. Granville, autor em 2017 do artigo em que a demonstração é encontrada. Para a demonstração necessitamos da convergência da seguinte série alternada:

Teorema 1.49.

$$\sum_{n=0}^{\infty} \frac{(-1)^n}{2n+1} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \ldots = \frac{\pi}{4}.$$

Demonstração. Exemplo 4 e Ilustração 3 do Capítulo 13.3 de [17]. □

Demonstração 13. (Granville)(3)
Suponha que o conjuntos $\mathfrak{P} = \{2, 3, 5, \ldots, p_r\}$ dos números primos seja finito. Sabemos que

$$\frac{\pi}{4} = 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \ldots;$$

dividindo a igualdade por 3 e somando o resultado com a mesma, obtemos

$$\frac{\pi}{4} + \frac{\pi}{12} = \left(1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \ldots\right) + \left(\frac{1}{3} - \frac{1}{9} + \frac{1}{15} - \frac{1}{21} + \ldots\right),$$

ou seja,

$$\left(\frac{3+1}{3}\right)\frac{\pi}{4} = 1 + \frac{1}{5} - \frac{1}{7} - \frac{1}{11} + \ldots;$$

dividindo a igualdade acima por 5 e subtraindo o resultado da mesma, obtemos

$$\left(\frac{3+1}{3}\right)\frac{\pi}{4} - \left(\frac{3+1}{3}\right)\frac{\pi}{20} = \left(1 + \frac{1}{5} - \frac{1}{7} - \frac{1}{11} + \ldots\right) - \left(\frac{1}{5} + \frac{1}{25} - \frac{1}{35} - \frac{1}{55} + \ldots\right),$$

ou seja,

$$\left(\frac{3+1}{3}\right)\left(\frac{5-1}{5}\right)\frac{\pi}{4} = 1 - \frac{1}{7} - \frac{1}{11} + \frac{1}{13} + \ldots;$$

seguimos repetindo o processo acima.

Veja que os termos da soma original são positivos quando $(2n+1) \equiv 1 \mod 4$ e negativos quando $(2n+1) \equiv 3 \mod 4$ com $n \in \mathbb{N} \cup \{0\}$, mas se dividirmos todos os termos por um primo $p_i \equiv 3 \mod 4$, os termos das somas com valores iguais, quando comparado os termos da soma original com a nova soma obtida, terão sinais opostos, assim, para anulá-los basta somá-los. Por outro lado, se dividirmos por um primo $p_i \equiv 1 \mod 4$, os termos das somas com valores iguais, quando comparado os termos da soma original com a nova soma obtida, terão sinais iguais, assim, para anulá-los basta subtraí-los.

De maneira geral, seguimos dividindo por todos os números primos $p_i \in \mathfrak{P}$ ímpares, somando quando $p_i \equiv 3 \mod 4$ e subtraindo quando $p_i \equiv 1 \mod 4$, sempre da expressão anteriormente obtida. Pelo Teorema 1.19, como todo número natural maior do que 1 possui pelo menos um fator primo, quando percorrermos todos os primos de $\mathfrak{P}$, concluímos que

$$\left(\prod_{p_i \equiv 3 \mod 4} \frac{p_i+1}{p_i}\right)\left(\prod_{p_{i'} \equiv 1 \mod 4} \frac{p_{i'}-1}{p_{i'}}\right)\left(\frac{\pi}{4}\right) = 1,$$

ou seja,

$$\frac{\pi}{4} = \left(\prod_{p_i \equiv 3 \mod 4} \frac{p_i}{p_i+1}\right)\left(\prod_{p_{i'} \equiv 1 \mod 4} \frac{p_{i'}}{p_{i'}-1}\right). \tag{1.3}$$

Sabemos que π é irracional, portanto, $\frac{\pi}{4}$ é irracional, mas o lado direito da igualdade (1.3), como existem finitos números primos, é um produto finito de números racionais, portanto é racional, o que é um absurdo. Logo, existem infinitos números primos. □

L. Euler forneceu em 1737 uma demonstração, que nos baseamos na página 6 de [29], completamente inovadora para o Teorema 1.31. Para a demonstração observamos que quando multiplicamos duas séries geométricas convergentes, termo a termo, o resultado é uma série tal que os seus termos são combinações de todos os termos das séries anteriores. Por exemplo, dados p e q números primos, com as séries geométricas $\sum_{k=0}^{\infty} \frac{1}{p^k}$ e $\sum_{k'=0}^{\infty} \frac{1}{q^{k'}}$, obtemos

$$\left(\sum_{k=0}^{\infty} \frac{1}{p^k}\right) \times \left(\sum_{k'=0}^{\infty} \frac{1}{q^{k'}}\right) = 1 + \frac{1}{q} + \frac{1}{q^2} + \ldots + \frac{1}{p} + \frac{1}{pq} + \frac{1}{pq^2} + \ldots + \frac{1}{p^2} + \frac{1}{p^2 q} + \frac{1}{p^2 q^2} + \ldots \quad . \tag{1.4}$$

Portanto, obtemos a soma dos inversos de todos os números naturais da forma $p^k q^{k'}$ com $k, k' \geq 0$, cada um contado uma única vez. Além disso, precisamos do resultado da divergência da série harmônica, que é definida como a soma de todos os inversos dos números naturais, isto é, $\sum_{n=1}^{\infty} \frac{1}{n} = +\infty$. Uma prova dessa divergência é apresentada na Seção 12.3, Ilustração 3 de [17].

Demonstração 14. (Euler)(2)
Suponha que o conjunto $\mathfrak{P} = \{p_1, p_2, \ldots, p_r\}$ dos números primos seja finito. Seja a soma dos termos de uma progressão geométrica de razão $\frac{1}{p_i}$, para cada $i = 1, 2, \ldots, r$; temos que

$$\sum_{k=0}^{\infty} \frac{1}{p_i^k} = 1 + \frac{1}{p_i} + \frac{1}{p_i^2} + \frac{1}{p_i^3} + \ldots = \frac{1}{1 - \frac{1}{p_i}},$$

realizando a multiplicação da soma dos termos de todas as progressões geométricas de razão $\frac{1}{p_i}$ com $p_i \in \mathfrak{P}$, obtemos

$$\prod_{i=1}^{r} \left(\sum_{k=0}^{\infty} \frac{1}{p_i^k} \right) = \prod_{i=1}^{r} \frac{1}{1 - \frac{1}{p_i}}, \tag{1.5}$$

conforme visto na igualdade (1.4), os termos do produto das séries, no lado esquerdo da igualdade (1.5), formam todas as combinações existentes dos números primos e, pelo Teorema 1.19 e Corolário 1.20, obtemos a soma de todos os inversos dos números naturais, cada um somado apenas uma vez, e como todos os termos são positivos podem ser reorganizados sem alterar o resultado. Assim, concluímos que

$$\sum_{n=1}^{\infty} \frac{1}{n} = \prod_{i=1}^{r} \frac{1}{1 - \frac{1}{p_i}}, \tag{1.6}$$

como existem finitos números primos, o produto do lado direito da igualdade (1.6) é finito, mas a série harmônica $\sum_{n=1}^{\infty} \frac{1}{n}$ é divergente, o que é um absurdo. Logo, o conjunto dos números primos é infinito. □

A demonstração a seguir foi baseada na página 14 de [1], é atribuída a A. Yaglom e I. Yaglom em 1954 ([21], página 21). Esta demonstração utiliza propriedades interessantes de Análise, além da função de *contagem de números primos* $\pi(x)$.

Definição 1.50. *A função de contagem de números primos $\pi : \mathbb{R} \to \mathbb{N}$, representada por $\pi(x)$, é definida como a quantidade de números primos $p \leq x$.*

Exemplo 1.51. *Temos que $\pi(10) = 4$, pois temos 4 números primos menores ou iguais a 10. Também tomamos como exemplo: $\pi(\sqrt{2}) = 0$, $\pi(e) = 1$, $\pi(100) = 25$ e $\pi(1000) = 168$.*

O desenvolvimento que segue é fundamental para a demonstração do Teorema 1.31. Sejam os números primos p_i com $i = 1, 2, \ldots, r$; introduzimos a notação $p_i \mid\!! \; m$ para dizer que o inteiro positivo m é dividido **exclusivamente** pelos números primos p_i tal que $i = 1, 2, \ldots, r$; além disso, lembramos que o símbolo lógico $\vee$ significa "ou". Dependemos também do fato que $\lim\limits_{x \to +\infty} \log x = +\infty$, o que pode ser verificado na página 446 de [17].

Dada a função $f : [1, +\infty) \to \mathbb{R}$ definida por $f(t) = \dfrac{1}{t}$, conforme a Definição 1.41, o logaritmo natural $\log x$ é definido pela integral $\displaystyle\int_1^x \frac{dt}{t}$, isto é, utilizaremos $\log x$ como a área sob a curva definida pela função f no intervalo $[1, x]$. Consideramos ainda a função chamada de *degrau superior* $g : [1, +\infty) \to \mathbb{R}$ definida por $g(x) = \dfrac{1}{n}$ para $n \leq x < n + 1$ com $n \in \mathbb{N}$.

Comparando as áreas sob as curvas das funções f e g, observamos que temos $\dfrac{1}{n} > \log(n + 1) - \log n$, portanto, segue facilmente para $n \leq x \leq n + 1$ que

$$\log x < 1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n} \leq \sum_{\substack{m=1 \, \vee \\ p_i \mid\!! \; m; \; p_i \leq x}} \frac{1}{m}, \tag{1.7}$$

onde o somatório se estende sobre todos os $m \in \mathbb{N}$ tal que $m = 1$ ou que m têm somente divisores primos $p_i \leq x$ com $i = 1, 2, \ldots, r_x$.

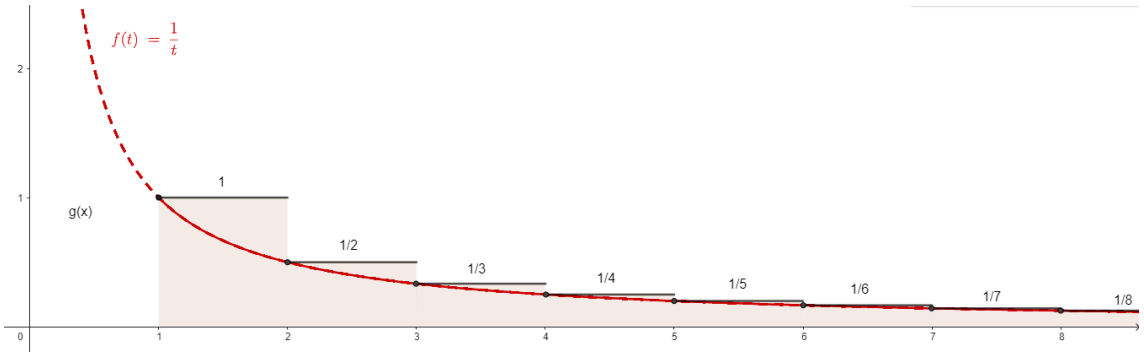


Figura 1: Comparação das áreas sob as curvas das funções f e g.
Fonte: Arquivo pessoal do autor.

Observe que $\displaystyle\sum_{\substack{m=1 \, \vee \\ p_i \mid\!! \; m; \; p_i \leq x}} \frac{1}{m} = 1$ para $1 \leq x < 2$, mas para $x \geq 2$ esta soma possui infinitos termos, pois existem infinitos números que são divisíveis somente pelos números primos $2 \leq p_i \leq x$, além disso, os n primeiros termos da soma são iguais aos n primeiros inversos dos números naturais, isso justifica a desigualdade da direita em (1.7).

Considere $x \geq 2$ para dispormos de números primos $p_i \leq x$, pelo Corolário 1.20, podemos escrever de modo único $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_{r_x}^{\alpha_{r_x}}$ com $\alpha_1, \alpha_2, \ldots, \alpha_{r_x} \geq 0$, portanto, considerando o mesmo desenvolvimento da igualdade (1.4), como a soma pode ser

rearranjada sem alterar o seu resultado, concluímos que

$$\sum_{\substack{m=1 \vee \\ p_i \,|!\, m;\ p_i \leq x}} \frac{1}{m} = 1+\frac{1}{p_1}+\frac{1}{p_2}+\ldots+\frac{1}{p_1 p_2}+\frac{1}{p_1 p_2^2}+\ldots+\frac{1}{p_1^{\alpha_1}\ldots p_{r_x}^{\alpha_{r_x}}}+\ldots = \prod_{i=1}^{r_x}\left(\sum_{k=0}^{\infty}\frac{1}{p_i^k}\right). \quad (1.8)$$

Demonstração 15. (Yaglom)
Considere o número real $x \geq 2$, dada a desigualdade (1.7) e a igualdade (1.8), obtemos

$$\log x < \sum_{\substack{m=1 \vee \\ p_i \,|!\, m;\ p_i \leq x}} \frac{1}{m} = \prod_{i=1}^{r_x}\left(\sum_{k=0}^{\infty}\frac{1}{p_i^k}\right),$$

pela convergência da soma de uma progressão geométrica de razão $\frac{1}{p_i}$ e pela Definição 1.50, já que r_x é a quantidade de números primos $p_i \leq x$, obtemos que

$$\log x < \prod_{i=1}^{r_x}\left(\sum_{k=0}^{\infty}\frac{1}{p_i^k}\right) = \prod_{i=1}^{r_x}\frac{1}{1-\frac{1}{p_i}} = \prod_{i=1}^{r_x}\frac{p_i}{p_i-1} = \prod_{i=1}^{\pi(x)}\frac{p_i}{p_i-1},$$

obviamente, como os números primos sempre são maiores do que os seus índices, obtemos que $p_i \geq i+1$, portanto $\frac{1}{i} \geq \frac{1}{p_i-1}$, assim

$$\frac{p_i}{p_i-1} = 1+\frac{1}{p_i-1} \leq 1+\frac{1}{i} = \frac{i+1}{i},$$

logo,

$$\log x < \prod_{i=1}^{\pi(x)}\frac{p_i}{p_i-1} \leq \prod_{i=1}^{\pi(x)}\frac{i+1}{i} = \frac{2}{1}\times\frac{3}{2}\times\frac{4}{3}\times\ldots\times\frac{\pi(x)}{\pi(x)-1}\times\frac{\pi(x)+1}{\pi(x)} = \pi(x)+1.$$

Concluímos que $\log x < \pi(x)+1$ para todo número real $x \geq 2$, logo, como $\lim_{x\to+\infty}\log x = +\infty$ temos que $\lim_{x\to+\infty}(\pi(x)+1) = +\infty$, isto é, $\pi(x)$ não é limitado e, portanto, existem infinitos números primos. □

A próxima demonstração, baseada na página 16 de [1], é atribuída a P. Erdös em 1938 e prova que a soma $\sum_{p\in\mathfrak{P}}\frac{1}{p}$ sobre todos os números primos $p \in \mathfrak{P}$ é divergente, portanto, essa soma possui infinitos termos.

Demonstração 16. (Erdös)
Considere o conjunto de todos os números primos $\mathfrak{P} = \{p_1, p_2, p_3, \ldots\}$, este sendo finito ou infinito. Suponha que a soma $\sum_{p_i\in\mathfrak{P}}\frac{1}{p_i}$ sobre todos os números primos $p_i \in \mathfrak{P}$ é convergente, logo, por consequência dos Teorema 1.43 e Teorema 1.44, existe um número natural k suficientemente grande tal que

$$\sum_{i\geq k+1}\frac{1}{p_i} < \frac{1}{2}.$$

Considerando ainda o número k, denominamos $S_p = \{p_1, p_2, \ldots, p_k\} \cup \{1\}$ o conjunto dos números primos "pequenos" união com o 1 e $S_g = \{p_{k+1}, p_{k+2}, p_{k+3}, \ldots\}$ o conjunto dos números primos "grandes". Para um número inteiro positivo arbitrário N, temos que

$$\sum_{i \geq k+1} \frac{N}{p_i} < \frac{N}{2} \tag{1.9}$$

e seja N_p a quantidade de inteiros positivos $n \leq N$ que são divisíveis somente por números primos "pequenos", contando o número 1, e N_g a quantidade de inteiros positivos $n \leq N$ que são divisíveis por pelo menos um número primo "grande". Observe que, pelo Teorema 1.19, cada inteiro positivo $n \leq N$ é contado uma única vez em N_p ou N_g, portanto, temos que $N = N_p + N_g$.

Observe que $\left\lfloor \frac{N}{p_i} \right\rfloor$ é a quantidade de inteiros positivos $n \leq N$ que são múltiplos do primo $p_i \in S_g$, além disso, podem existir inteiros positivos n múltiplos de mais do que um número primo "grande", que serão contados mais de uma vez em $\sum_{i \geq k+1} \left\lfloor \frac{N}{p_i} \right\rfloor$, portanto, comparando essa contagem com N_g e pela desigualdade (1.9), percebe-se que

$$N_g \leq \sum_{i \geq k+1} \left\lfloor \frac{N}{p_i} \right\rfloor \leq \sum_{i \geq k+1} \frac{N}{p_i} < \frac{N}{2}. \tag{1.10}$$

Por conseguinte, dado $a_n, b_n \in \mathbb{N}$, escrevemos como $n = a_n b_n^2$ todos os inteiros positivos $n \leq N$ que é 1 ou que é divisível somente por números primos "pequenos" $p_{i'} \in S_p$, onde a_n não é um quadrado perfeito diferente de 1. Portanto, todo número a_n é 1 ou é um produto de números primos "pequenos" distintos, assim, cada um dos k números primos "pequenos"$p_{i'} \in S_p$ pode estar ou não estar no produto que gera a_n, e se nenhum número primo está no produto então $a_n = 1$, logo, existem precisamente 2^k possibilidades para os números a_n.

Além disso, como $b_n^2 \leq n \leq N$, obtemos que $b_n \leq \sqrt{n} \leq \sqrt{N}$, portanto b_n é, no máximo, igual à $\sqrt{N}$, isto é, existem $\left\lfloor \sqrt{N} \right\rfloor$ possibilidades para os números b_n. Observe que temos N_p números $n = a_n b_n^2$, mas também temos 2^k possibilidades para a_n **e** $\left\lfloor \sqrt{N} \right\rfloor$ possibilidades para b_n, que podem resultar em mais de N_p inteiros positivos, logo, concluímos que

$$N_p \leq 2^k \left\lfloor \sqrt{N} \right\rfloor \leq 2^k \sqrt{N}. \tag{1.11}$$

Assim, pela desigualdade (1.10) e desigualdade (1.11), obtemos que

$$N = N_g + N_p < \frac{N}{2} + 2^k \sqrt{N}, \tag{1.12}$$

contudo, sempre que ocorre $2^k \sqrt{N} \leq \frac{N}{2}$ ou $2^{k+1} \leq \sqrt{N}$, a desigualdade (1.12) não é

verdadeira. Portanto, basta assumir $N = 2^{2k+2}$ que obtemos

$$N = 2^{2k+2} < \frac{2^{2k+2}}{2} + 2^k\sqrt{2^{2k+2}} = 2^{2k+1} + 2^k.\,2^{k+1} = 2^{2k+2} = N,$$

o que é um absurdo. Logo, a soma $\sum_{p_i \in \mathfrak{P}} \frac{1}{p_i}$ é divergente e, portanto, possui infinitos termos, ou seja, $\mathfrak{P}$ é infinito, isto é, existem infinitos números primos. □

Para a próxima demonstração do Teorema 1.31 observamos que uma das principais aplicações de $\lfloor x \rfloor$ é o lema que segue, conforme a página 30 de [20]:

Lema 1.52. *(Fatores do Fatorial) Seja p um número primo, então a maior potência de p que divide $n!$ é p^α, onde*

$$\alpha = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \ldots = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

Observe que a soma acima tem uma quantidade finita de termos não nulos, pois os termos $\left\lfloor \frac{n}{p^k} \right\rfloor$ eventualmente serão zero.

Demonstração. No produto $n! = 1 \times 2 \times \ldots \times n$, $\left\lfloor \frac{n}{p} \right\rfloor$ é a quantidade de múltiplos de p menores ou iguais a n, dentre esse, os múltiplos de p^2 possuem um fator primo extra que é contado por $\left\lfloor \frac{n}{p^2} \right\rfloor$, os múltiplos de p^3 possuem mais um fator primo extra, em relação à p^2, que é contado por $\left\lfloor \frac{n}{p^3} \right\rfloor$, e assim sucessivamente até $p^k > n$, onde não haverá mais múltiplos menores ou iguais a n para contar e teremos $\left\lfloor \frac{n}{p^k} \right\rfloor = 0$. □

Consideramos ainda o limite $\lim_{n\to\infty} \frac{M^n}{n!} = 0$ para $M \in \mathbb{R}^*$. Observe que pelo Teste da razão, veja Teorema 1.47, obtemos que a série $\sum_{n=1}^{\infty} \frac{M^n}{n!}$ é absolutamente convergente, portanto, é convergente e, pelo Teorema 1.46, sabemos que o limite do termo geral da série dada quando $n \to \infty$ é zero, logo, concluímos que para qualquer $M \in \mathbb{R}^*$ temos que

$$\lim_{n\to\infty} \frac{M^n}{n!} = 0. \tag{1.13}$$

A demonstração que segue é baseada na página 181 de [34], foi desenvolvida em 2010 por J. Whang e é uma demonstração analítica muito simples.

Demonstração 17. (Whang)
Suponha que o conjunto dos números primos $\mathfrak{P} = \{p_1, p_2, \ldots, p_r\}$ seja finito. Pela fatoração única em primos, Corolário 1.20, escrevemos

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

e seja $p_i^{\alpha_i}$ a maior potência do primo $p_i \in \mathfrak{P}$ que divide $n!$, assim, pelo Lema 1.52 e pela convergência da série geométrica, obtemos que

$$\alpha_i = \left\lfloor \frac{n}{p_i} \right\rfloor + \left\lfloor \frac{n}{p_i^2} \right\rfloor + \ldots = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p_i^k} \right\rfloor \leq \sum_{k=1}^{\infty} \frac{n}{p_i^k} = \frac{\frac{n}{p_i}}{1 - \frac{1}{p_i}} = \frac{n}{p_i - 1} \leq n. \tag{1.14}$$

Considere $\prod_{i=1}^{r} p_i = M \in \mathbb{R}^*$, então, obtemos pela desigualdade (1.14), sobre a maior potência de cada um dos números primos $p_i \mid n!$, que

$$n! = \prod_{i=1}^{r} p_i^{\alpha_i} \leq \prod_{i=1}^{r} p_i^n = \left(\prod_{i=1}^{r} p_i \right)^n = M^n, \tag{1.15}$$

dividindo a desigualdade (1.15) por $n!$, obtemos para cada $n \in \mathbb{N}$ que

$$1 \leq \frac{M^n}{n!}, \tag{1.16}$$

mas observando o limite de (1.16) quando $n \to \infty$, conforme o resultado obtido no limite (1.13), concluímos que

$$1 \leq \lim_{n \to \infty} \frac{M^n}{n!} = 0,$$

o que é um absurdo. Logo, existem infinitos números primos. □

A demonstração apresentada a seguir, concedida por H. Furstenberg em 1955, é uma das demonstrações mais extraordinárias já desenvolvidas, pois é construída sobre a Topologia. Apresentaremos alguns conceitos importantes de topologia, baseados no Capítulo 3 de [18].

Definição 1.53. *Uma topologia em um conjunto X é uma coleção τ de subconjuntos de X, chamados os subconjuntos abertos (segundo a topologia τ) satisfazendo às seguintes condições:*

1) X e o subconjunto vazio $\emptyset$ são abertos;

2) a reunião de uma família qualquer de subconjuntos abertos é um subconjunto aberto;

3) a interseção de uma família finita de subconjuntos abertos é um subconjunto aberto.

Definição 1.54. *Chamamos de espaço topológico X o par ordenado (X, τ), onde X é um conjunto e τ é uma topologia em X.*

Definição 1.55. *Dado um subconjunto $A \subset X$, chama-se complementar de A o conjunto $X - A$ formado pelos elementos do conjunto X que não pertencem ao subconjunto A.*

Definição 1.56. *Dizemos que um subconjunto F de um espaço topológico X é fechado quando o seu complementar $X - F$ é aberto.*

Observe que se $F \subset X$ é um conjunto fechado então existe um conjunto aberto A tal que $A = X - F$, pela Definição 1.55, temos que $X = A \cup F$ e os conjuntos A e F são *disjuntos*, isto é, $A \cap F = \emptyset$, logo, $X - A = F$, isto é, um conjunto A é aberto se o seu complementar F é fechado.

Os conjuntos fechados possuem também as seguintes propriedades:

Teorema 1.57. *Os subconjuntos fechados de um espaço topológico X, possuem as propriedades:*

i) X e o subconjunto vazio $\emptyset$ são fechados;

ii) a interseção de uma família qualquer de subconjuntos fechados é um subconjunto fechado;

iii) a reunião de uma família finita de subconjuntos fechados é um subconjunto fechado.

Demonstração. Proposição 15 de [18]. □

A demonstração do Teorema 1.31 utilizando topologia foi baseada na página 15 de [1], iniciamos definindo um espaço topológico $(\mathbb{Z}, \mathbb{Z}(a, b))$ formado pela família dos conjuntos abertos $\mathbb{Z}(a, b)$.

Dado $a, b \in \mathbb{Z}$ com $b > 0$, definimos

$$\mathbb{Z}(a, b) = \{a + nb\,;\ n \in \mathbb{Z}\},$$

ou seja, cada conjunto $\mathbb{Z}(a, b)$ é uma progressão aritmética de razão b e infinita nos dois sentidos, positivo e negativo, inclusive, se $a = 0$ e $b = 1$ obtemos que $\mathbb{Z}(0, 1) = \mathbb{Z}$. Observamos agora que:

1) Dizemos que um conjunto $S \subseteq \mathbb{Z}$ é aberto se S é vazio ou se para cada $a \in S$ existe algum $b > 0$ com $\mathbb{Z}(a, b) \subseteq S$.

2) Observamos que a união arbitrária dos conjuntos abertos $\mathbb{Z}(a, b)$ é também um conjunto aberto, pois trivialmente satisfaz a definição de conjunto aberto dada acima.

3) Por fim, dados S_1 e S_2 abertos, se $a \in S_1 \cap S_2$ com $\mathbb{Z}(a, b_1) \subseteq S_1$ e $\mathbb{Z}(a, b_2) \subseteq S_2$, então existe $\mathbb{Z}(a, b_1 b_2)$ tal que $\mathbb{Z}(a, b_1 b_2) \subseteq S_1 \cap S_2$, isto é, como a interseção finita de conjuntos sempre pode ser vista como a interseção de apenas dois conjuntos, essa interseção finita de conjuntos abertos é também um conjunto aberto.

Logo, pela Definição 1.53, definimos um espaço topológico em $\mathbb{Z}$ dada pela família dos conjuntos abertos $\mathbb{Z}(a, b)$. Pela definição do espaço topológico $(\mathbb{Z}, \mathbb{Z}(a, b))$, temos a propriedade:

Propriedade 1. Qualquer conjunto não vazio e aberto do espaço topológico $(\mathbb{Z}, \mathbb{Z}(a, b))$ é infinito.

Também ocorre que

$$\bigcup_{i=1}^{b-1} \mathbb{Z}(a + i, b) = \mathbb{Z} - \mathbb{Z}(a, b),$$

e $\bigcup_{i=1}^{b-1} \mathbb{Z}(a + i, b)$ é um conjunto aberto pela Definição 1.53, ou seja, o complementar do conjunto $\mathbb{Z}(a, b)$ é aberto, logo, pela Definição 1.56 temos a propriedade:

Propriedade 2. O conjunto $\mathbb{Z}(a, b)$ é um conjunto fechado.

Demonstração 18. (Furstenberg)
Suponha que o conjunto dos números primos $\mathfrak{P} = \{p_1, p_2, \ldots, p_r\}$ seja finito. Pelo Teorema 1.19, todos os números inteiros $m \neq 1$ e $m \neq -1$ tem um divisor primo $p_i \in \mathfrak{P}$, logo, para todo $m \in \mathbb{Z} - \{-1, 1\}$ temos que $m \in \mathbb{Z}(0, p_i)$ para algum $i = 1, 2, \ldots, r$; portanto

$$\mathbb{Z} - \{-1, 1\} = \bigcup_{i=1}^{r} \mathbb{Z}(0, p_i),$$

e o conjunto $\mathbb{Z} - \{-1, 1\}$, que é o complementar de $\{-1, 1\}$, é fechado, pois pela Propriedade 2 e pelo Teorema 1.57 sabemos que $\bigcup_{i=1}^{r} \mathbb{Z}(0, p_i)$ é a união finita de conjuntos fechados, portanto, é também um conjunto fechado, consequentemente, o conjunto $\{-1, 1\}$ é aberto. Logo, $\{-1, 1\}$ é um conjunto não vazio, aberto e finito no espaço topológico $(\mathbb{Z}, \mathbb{Z}(a, b))$, o que é uma contradição para a Propriedade 1, portanto, existem infinitos conjuntos $\mathbb{Z}(0, p_i)$, isto é, existem infinitos números primos. □

1.8 Outras demonstrações interessantes

A próxima demonstração foi publicada por A. Engel em 1998 e pode ser encontrada na página 37 de [8], esta demonstração é bem simples e utiliza o Princípio da Indução aplicada em uma função sabiamente definida.

Sejam as funções $f : \mathbb{N} \to \mathbb{N}$ dada por $f(n) = 2^{2^{n+1}} + 2^{2^n} + 1$ e $g : \mathbb{R} \to \mathbb{R}$ dada por $g(x) = x^4 + x^2 + 1 = (x^2 + x + 1)(x^2 - x + 1)$. Considerando $x = 2^{2^{n-1}}$ para todo $n \in \mathbb{N}$, obtemos

$$g\left(2^{2^{n-1}}\right) = \left(2^{2^{n-1}}\right)^4 + \left(2^{2^{n-1}}\right)^2 + 1 = 2^{2^{n+1}} + 2^{2^n} + 1 = f(n), \tag{1.17}$$

além disso, pelo Lema 1.14, temos que

$$\left(2^{2^{n+1}} + 2^{2^n} + 1, 2^{2^{n+1}} - 2^{2^n} + 1\right) = \left(2^{1+2^n}, 2^{2^{n+1}} - 2^{2^n} + 1\right) = 1,$$

para todo $n \in \mathbb{N}$, pois 2^{1+2^n} é uma potência de 2 e $\left(2^{2^{n+1}} - 2^{2^n} + 1\right)$ é ímpar, não possuindo fatores maiores do que 1 em comum.

Demonstração 19. (Engel)
Provaremos pelo Princípio de Indução que $f(n)$ tem pelo menos $n + 1$ fatores primos distintos. Temos que $f(1) = 16 + 4 + 1 = 21 = 7 \,.\, 3$, que possui $1 + 1 = 2$ fatores primos distintos, portanto $P(1)$ é verdadeira. Suponha que $P(n)$ é verdadeira para $n \in \mathbb{N}$, isto é, $f(n) = 2^{2^{n+1}} + 2^{2^n} + 1$ possui pelo menos $n + 1$ fatores primos distintos. Assim, para $n + 1$, considerando a igualdade (1.17), temos que

$$f(n+1) = g\left(2^{2^n}\right) = \left(2^{2^{n+1}} + 2^{2^n} + 1\right)\left(2^{2^{n+1}} - 2^{2^n} + 1\right) = f(n)\left(2^{2^{n+1}} - 2^{2^n} + 1\right),$$

como o máximo divisor comum $\left(f(n), 2^{2^{n+1}} - 2^{2^n} + 1\right) = 1$ e $\left(2^{2^{n+1}} - 2^{2^n} + 1\right) > 1$, pelo Teorema 1.19, temos que $\left(2^{2^{n+1}} - 2^{2^n} + 1\right)$ tem pelo menos um fator primo tal que são todos distintos dos fatores primos de $f(n)$, que por hipótese têm $n + 1$ fatores primos distintos, logo, $f(n)\left(2^{2^{n+1}} - 2^{2^n} + 1\right)$ possui pelo menos $n + 2$ fatores primos distintos. Portanto, $P(n + 1)$ é verdadeira e pelo Princípio de Indução, $f(n)$ possui pelo menos $n + 1$ fatores primos distintos para cada $n \in \mathbb{N}$, logo, como $f(n)$ não é limitada, existem infinitos números primos. □

A próxima demonstração foi fornecida por S. Northshield em 2015 e pode ser encontrada na página 466 de [23], é uma demonstração simples, originalmente apresentada em apenas uma linha é diferente por envolver a função seno e algumas de suas propriedades. Inicialmente vamos relembrar os conceitos que utilizaremos.

Dada a função $\text{sen} : \mathbb{R} \to \mathbb{R}$, conhecida como *função seno*, sabemos que essa função é *periódica* de período 2π, isto é, $\text{sen}(x + 2k\pi) = \text{sen}(x)$ para todo $x \in \mathbb{R}$

e $k \in \mathbb{Z}$. Assim, como $\text{sen}(0) = \text{sen}(\pi) = 0$, pela periodicidade da função seno, é imediato que $\text{sen}(t\pi) = 0$ para todo $t \in \mathbb{Z}$, observamos também que para todo número real $2k\pi < x < 2k\pi + \pi$ temos que $\text{sen}(x) > 0$ e para $2k\pi - \pi < x < 2k\pi$ temos que $\text{sen}(x) < 0$, em especial, nos interessa que para $0 < x < \pi$ ocorre $\text{sen}(x) > 0$. Para saber mais sobre a definição da função seno, recomendamos o Capítulo 9 de [19].

Demonstração 20. (Northshield)
Suponha que o conjunto $\mathfrak{P} = \{p_1, p_2, \ldots, p_r\}$ dos números primos seja finito. Observamos que $\text{sen}\left(\frac{\pi}{p_i}\right) = \text{sen}\left(\frac{\pi}{p_i} + 2k\pi\right)$ tal que $p_i \in \mathfrak{P}$ com $i = 1, 2, \ldots, r$ e $k \in \mathbb{Z}$. Fazendo $N = p_1 p_2 \ldots p_r$ e seja $k = \frac{N}{p_i}$, temos que

$$\text{sen}\left(\frac{\pi}{p_i}\right) = \text{sen}\left(\frac{\pi}{p_i} + \frac{2N\pi}{p_i}\right) = \text{sen}\left(\frac{1+2N}{p_i}\pi\right), \tag{1.18}$$

como $0 < \frac{\pi}{p_i} < \pi$ para qualquer $p_i \in \mathfrak{P}$, temos que $\text{sen}\left(\frac{\pi}{p_i}\right) > 0$ para todo número primo p_i, logo, sabemos que $\prod_{i=1}^{r} \text{sen}\left(\frac{\pi}{p_i}\right) > 0$. Contudo, pelo Teorema 1.19 observamos que existe pelo menos um número primo $p_{i'} \in \mathfrak{P}$ tal que $p_{i'} \mid (1 + 2N)$, isto é, $\frac{1+2N}{p_{i'}} \in \mathbb{Z}$, logo, $\text{sen}\left(\frac{1+2N}{p_{i'}}\pi\right) = 0$, por conseguinte, $\prod_{i=1}^{r} \text{sen}\left(\frac{1+2N}{p_i}\pi\right) = 0$, pois pelo menos um dos valores da função seno, no produtório, é zero. Portanto, pela igualdade (1.18), concluímos que

$$0 < \prod_{i=1}^{r} \text{sen}\left(\frac{\pi}{p_i}\right) = \prod_{i=1}^{r} \text{sen}\left(\frac{1+2N}{p_i}\pi\right) = 0,$$

o que é um absurdo. Logo, existem infinitos números primos. □

A próxima demonstração foi dada por D. Wegener em 1981, pode ser encontrada na página 449 de [33]. É uma demonstração, em certo sentido, similar à demonstração de Euclides, contudo, a utilização de triplas pitagóricas a torna especial. Os resultados apresentados a seguir podem ser encontrados na página 132 de [20].

Definição 1.58. *As triplas de números inteiros positivos (x, y, z) que satisfazem a equação $x^2 + y^2 = z^2$, são denominadas de triplas pitagóricas. Se para uma tripla pitagórica os termos x, y e z são, dois a dois, primos entre si, denominam-na de tripla pitagórica primitiva.*

Teorema 1.59. *Todas as triplas pitagóricas primitivas são dadas, sem duplicação, por*

$$x = 2mn; \qquad y = m^2 - n^2; \qquad z = m^2 + n^2; \tag{1.19}$$

com números naturais $m > n$ primos entre si e $m + n$ ímpar. Além disso, quaisquer $m, n \in \mathbb{N}$, com $(m, n) = 1$, $m > n$ e $m+n$ ímpar, produzem através das igualdades (1.19) uma tripla pitagórica primitiva.

Demonstração. Dada uma tripla pitagórica primitiva (x, y, z), temos que x e y não podem ser ambos pares, pois $(x, y) = 1$, portanto, podemos supor sem perda de generalidade que y é ímpar, além disso, para $k \in \mathbb{Z}$ temos que $(2k+1)^2 = 4k^2 + 4k + 1 \equiv 1 \mod 4$ e $(2k)^2 = 4k^2 \equiv 0 \mod 4$, ou seja, quadrados perfeitos são congruentes ou a 1 ou a 0 módulo 4, se o inteiro que é elevado ao quadrado for ímpar ou par, respectivamente, assim, x não pode ser ímpar, pois caso contrário $z^2 = x^2 + y^2 \equiv 2 \mod 4$, o que é um absurdo. Logo, temos que x é par, y é ímpar e como os quadrados conservam a paridade, concluímos que z é ímpar.

Por outro lado, temos que $x^2 = z^2 - y^2 = (z-y)(z+y)$ e observamos que $(y, x) = (y^2, x^2) = (y^2, x^2 + y^2) = (y^2, z^2) = (y, z) = 1$, assim, temos que $(z, z+y) = 1$ e $z + y$ é par, pois é a soma de dois ímpares, logo, $(z-y, z+y) = (2z, z+y) = 2$.

Logo, $\dfrac{z+y}{2}$ e $\dfrac{z-y}{2}$ são inteiros positivos primos entre si e seu produto é um quadrado perfeito, portanto, pela unicidade no Teorema 1.19, como temos dois fatores distintos, primos entre si, que multiplicados formam um quadrado perfeito, cada um desses fatores deve ser o quadrado de um inteiro positivo, isto é,

$$\left(\frac{z+y}{2}\right)\left(\frac{z-y}{2}\right) = \left(\frac{x}{2}\right)^2 = m^2 n^2.$$

Portanto, com a organização adequada para x e a resolução de um sistema com as equações obtidas $z + y = 2m^2$ e $z - y = 2n^2$, concluímos que $x = 2mn$; $y = m^2 - n^2$; $z = m^2 + n^2$, com $(m, n) = 1$. Para concluir, como $z = m^2 + n^2$ é ímpar, m e n possuem paridades distintas, portanto $m + n$ é ímpar, na realidade, a condição de $m + n$ ser ímpar garante a primitividade da tripla pitagórica.

Reciprocamente, observamos que dado quaisquer $m, n \in \mathbb{N}$ que satisfazem as condições de $(m, n) = 1$, $m > n$ e $m + n$ ímpar, temos que

$$y^2 + x^2 = \left(m^2 - n^2\right)^2 + (2mn)^2 = m^4 + 2m^2n^2 + n^4 = \left(m^2 + n^2\right)^2 = z^2.$$

Assim, concluímos a demonstração. □

Demonstração 21. (Wegener)
Suponha que o conjunto ordenado dos números primos $\mathfrak{P} = \{2, p_2, p_3, \ldots, p_r\}$ seja finito, sendo p_r o maior número primo. Seja $m = 2p_2p_3 \ldots p_r$ e $n = 1$, então m e n satisfazem as condições do Teorema 1.59, isto é, temos uma tripla pitagórica primitiva dada por $x = 2(2p_2p_3 \ldots p_r)$, $y = (2p_2p_3 \ldots p_r)^2 - 1$ e $z = (2p_2p_3 \ldots p_r)^2 + 1$. Considerando o Teorema 1.19, analisaremos a soma $x + y$, assim se for um número primo

$$x + y = 2(2p_2p_3 \ldots p_r) + (2p_2p_3 \ldots p_r)^2 - 1 > p_r,$$

o que é um absurdo pela maximalidade de $p_r \in \mathfrak{P}$. Se $x+y$ é um número composto, existe um número primo $q \in \mathfrak{P}$ tal que $q \mid (x + y)$, mas como $q \mid x$, pelo Lema 1.9, temos que $q \mid y$ o que é um absurdo, pois $(x, y) = 1$. Logo, existem infinitos números primos. □

A próxima demonstração utiliza o fato do número de Euler e ser transcendente, o que pode ser verificado a partir da página 29 de [12], além disso, também precisamos da bela expressão que é apresentada no lema abaixo, que envolve essa constante e uma das funções mais importantes da Teoria dos Números, a função μ de Möbius, definida a seguir, conforme página 189 de [20].

Definição 1.60. *Definimos a função de Möbius $\mu : \mathbb{N} \to \mathbb{Z}$, como*

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

Para o desenvolvimento da demonstração pretendida, precisamos dos seguintes resultados a respeito da classificação dos números reais como números algébricos e transcendentes. Os resultados que seguem podem ser encontrados no Capítulo 4 de [12] ou no artigo [32].

Definição 1.61. *Qualquer solução real de uma equação polinomial da forma:*

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = 0,$$

onde $n \in \mathbb{N}$, $a_i \in \mathbb{Q}$ para $i = 0, 1, 2, \ldots, n$; e $a_n \neq 0$, é chamado de número algébrico.

Definição 1.62. *Os números reais que não são algébricos são denominados de números transcendentes.*

O teorema que segue, sobre as operações com números algébricos, é muito importante para a demonstração que faremos.

Teorema 1.63. *Sejam a e b números algébricos, temos que:*

i) $a \pm b$ é um número algébrico;

ii) $a \,.\, b$ é um número algébrico;

iii) Se $a \neq 0$ então a^{-1} é um número algébrico.

Demonstração. Página 17 de [12]. □

O lema apresentado a seguir foi proposto por R. Bellman em 1943 e solucionado por R. Buck em 1944, é o lema central para a demonstração do Teorema 1.31, cuja baseamo-nos na página 23 de [21].

Lema 1.64. *Dado $x \in \mathbb{R}$ tal que $|x| < 1$, temos que*

$$e^{-x} = \prod_{n=1}^{\infty} (1-x^n)^{\frac{\mu(n)}{n}} = \frac{(1-x)\,(1-x^6)^{\frac{1}{6}}\,(1-x^{10})^{\frac{1}{10}} \cdots}{(1-x^2)^{\frac{1}{2}}\,(1-x^3)^{\frac{1}{3}}\,(1-x^5)^{\frac{1}{5}} \cdots} \tag{1.20}$$

Demonstração. Página 410 de [7]. □

Demonstração 22. (Bellman-Buck)
Considerando $x = -\dfrac{1}{2}$ na fórmula 1.20 do Lema 1.64, obtemos

$$\prod_{n=1}^{\infty} \left(1 - \left(-\frac{1}{2}\right)^n\right)^{\frac{\mu(n)}{n}} = e^{\frac{1}{2}}.$$

Suponha que o conjunto $\mathfrak{P} = \{p_1, p_2, \ldots, p_r\}$ dos números primos seja finito e seja o produto de todos os números primos $N = p_1 p_2 \ldots p_r$, logo, $\mu(m) = 0$ para todo $m > N$, pois pelo Princípio das Gavetas, todo $m > N$ possui pelo menos um primo quadrado em sua fatoração, portanto, $\displaystyle\prod_{n=N+1}^{\infty} \left(1 - \left(-\frac{1}{2}\right)^n\right)^0 = 1$, assim, obtemos

$$\prod_{n=1}^{\infty} \left(1 - \left(-\frac{1}{2}\right)^n\right)^{\frac{\mu(n)}{n}} = \prod_{n=1}^{N} \left(1 - \left(-\frac{1}{2}\right)^n\right)^{\frac{\mu(n)}{n}} = A = e^{\frac{1}{2}},$$

ou seja,

$$\prod_{n=1}^{N} \left(1 - \left(-\frac{1}{2}\right)^n\right)^{\frac{\mu(n)}{n}} = \left(1 - \left(-\frac{1}{2}\right)\right)\left(1 - \left(-\frac{1}{2}\right)^2\right)^{-\frac{1}{2}} \cdots \left(1 - \left(-\frac{1}{2}\right)^N\right)^{\frac{\mu(N)}{N}} = A = e^{\frac{1}{2}}.$$

Portanto, temos uma multiplicação finita de números algébricos não nulos e diferentes de 1, ou seja, esse produto $A = e^{\frac{1}{2}}$ é um número algébrico, logo, $A \,.\, A = A^2 = e$ também é um número algébrico, o que é um absurdo, pois e é um número transcendente. Logo, existem infinitos números primos. □

Capítulo 2

Neste capítulo será apresentado alguns métodos para verificar se um determinado número $m \in \mathbb{N}$ é primo ou composto. Existem vários métodos para o teste de primalidade, no presente trabalho apresentaremos 7 métodos, 2 que dependem da determinação de fatores do número m e 5 que dependem de congruências específicas.

A escolha dos testes de primalidade apresentados ocorreu pela possibilidade de execução do teste para qualquer inteiro ímpar maior do que 1, mesmo que o custo de tempo seja elevado, e pela importância histórica na Teoria dos Números de cada um dos métodos.

2.1 Crivo de Eratóstenes e Fatoração de Fermat

De maneira geral, para determinar se um número $m \in \mathbb{N}$ é primo, basta realizar a divisão de m por todos os números primos $p_1 < p_2 < \ldots < p_r < m$, assim caso existir algum número primo $p_i \mid m$ com $i = 1, 2, \ldots, r$; o número m é composto, caso contrário, se $p_i \nmid m$ para todo $i = 1, 2, \ldots, r$; o número m é primo. Este é o método que segue diretamente da definição de número primo.

Exemplo 2.1.

O número 351 *é composto, pois* $3 \mid 351$. *Felizmente foram necessárias apenas duas etapas, pois existem* 70 *números primos menores que* 351.

O número 71 *é primo, pois não é divisível por nenhum número primo menor. No caso foram necessárias* 19 *verificações, que é a quantidade de números primos menores que* 71.

É também de interesse matemático determinar os fatores primos de um número composto m. Para isso basta fazer, conforme acima, reiteradas verificações de primalidade, por exemplo, determina-se que um inteiro m é composto, assim ele é divisível por um número primo p_1 e podemos escrever $m = p_1 m_1$, agora se executa o método no inteiro

m_1, se for primo a fatoração está completa, caso contrário, se for composto então é divisível por um número primo p_2 e podemos escrever $m = p_1 p_2 m_2$, executa-se o método no inteiro m_2 e assim sucessivamente. Em uma quantidade finita de etapas podemos determinar todos os fatores primos de um inteiro composto m.

Esse método de verificar a primalidade é simples, mas requer uma quantidade demasiada de etapas, principalmente se o número investigado for grande e se revelar um número primo. Felizmente podemos aprimorar o método reduzindo consideravelmente a quantidade de etapas a serem realizadas pelo seguinte lema, que pode ser encontrado no Capítulo 1 de [24].

Lema 2.2. *Dado $m \in \mathbb{N}$ composto. Então existe um primo $p \leq \sqrt{m}$ tal que $p \mid m$.*

Demonstração. Como m é composto, existem $m_1, m_2 \in \mathbb{N}$ com $1 < m_1 \leq m_2 < m$ tais que $m = m_1 m_2$. Suponha que $m_1 > \sqrt{m}$, logo, $m = m_1 m_2 \geq m_1 m_1 > \sqrt{m}\sqrt{m} = m$, o que é um absurdo, portanto, $m_1 \leq \sqrt{m}$. Como m_1 pode ser escrito como produto de fatores primos, basta tomar o primo p tal que $p \mid m_1$, assim, concluímos que $p \leq m_1 \leq \sqrt{m}$ onde $p \mid m$. □

Exemplo 2.3. *Como $\lfloor \sqrt{71} \rfloor = 8$, basta testar os números primos $2, 3, 5$ e 7 para determinar que 71 é primo, ou seja, reduzimos as 19 verificações necessárias anteriormente para apenas 4 verificações.*

Esse método é sintetizado no próximo teorema, que recebe o nome de Crivo de Eratóstenes, em homenagem a seu idealizador no século III a.C., o matemático grego Eratóstenes. A demonstração pode ser encontrada no Capítulo 1 de [24].

Teorema 2.4. *(Teste 1: Crivo de Eratóstenes) Sejam $m \in \mathbb{N}$ e $p_1 < p_2 < \ldots < p_r$ todos os números primos menores ou igual que $\sqrt{m}$. Então, m é primo se, e somente se, $p_i \nmid m$ para qualquer $i = 1, 2, \ldots, r$.*

Demonstração. Se m é um número primo, por definição, temos que $p_i \nmid m$ para qualquer $p_1 < \ldots < p_r \leq \sqrt{m} < m$ com $i = 1, 2, \ldots, r$. Para a recíproca, observe que se $p_i \nmid m$ para todo $p_1 < \ldots < p_r \leq \sqrt{m} < m$ com $i = 1, 2, \ldots, r$; pelo Lema 2.2, o natural m não pode ser composto, pois caso contrário haveria um primo $p_i \leq \sqrt{m}$ tal que $p_i \mid m$, logo, m é primo. □

O Crivo de Eratóstenes é comumente utilizado para determinar todos os números primos $p \leq m$ com $m \in \mathbb{N}$. Como exemplo do algoritmo desenvolvido para este fim, vamos determinar todos os números primos menores do que 150, para isso inicialmente construímos uma lista com todos os números de 1 a 150.

Observamos que precisaremos inspecionar, para o exemplo, os números primos $p \leq \lfloor \sqrt{150} \rfloor = 12$, mas não precisamos saber quais são estes números primos inicialmente, pois a cada etapa executada no crivo, o primeiro número não eliminado na sequência dos números naturais é primo, então basta utilizá-lo na próxima etapa.

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
101	102	103	104	105	106	107	108	109	110
111	112	113	114	115	116	117	118	119	120
121	122	123	124	125	126	127	128	129	130
131	132	133	134	135	136	137	138	139	140
141	142	143	144	145	146	147	148	149	150.

Por convenção o número 1 não é primo, então podemos eliminá-lo, o próximo número não eliminado é o 2, então esse número é primo, assim eliminamos todos os outros números múltiplos de 2, pois são todos compostos:

	2	3	5	7	9
11		13	15	17	19
21		23	25	27	29
31		33	35	37	39
41		43	45	47	49
51		53	55	57	59
61		63	65	67	69
71		73	75	77	79
81		83	85	87	89
91		93	95	97	99
101		103	105	107	109
111		113	115	117	119
121		123	125	127	129
131		133	135	137	139
141		143	145	147	149.

O próximo número, depois do 2, que não foi eliminado é o 3, logo, esse é um número primo, assim eliminaremos todos os outros números múltiplos de 3. Observamos que na sequência restará o número 5, que é primo, e após eliminar os outros múltiplos de 5, restará o número 7, que é primo, e após eliminar os outros múltiplos do 7, obtemos:

	2	3	5	7	
11		13		17	19
		23			29
31				37	
41		43		47	
		53			59
61				67	
71		73			79
		83			89
				97	
101		103		107	109
		113			
121				127	
131				137	139
		143			149.

O próximo número da sequência que não foi eliminado é o 11, que é primo, como o 12 já foi eliminado, essa é a última etapa que é necessária, logo, após a eliminação dos outros números múltiplos de 11, restarão na lista apenas os números que são primos. Portanto, os números primos menores que 150 são os que seguem:

	2	3	5	7	
11		13		17	19
		23			29
31				37	
41		43		47	
		53			59
61				67	
71		73			79
		83			89
				97	
101		103		107	109
		113			
				127	
131				137	139
					149.

Notamos que existem 35 números primos menores que 150, se recordarmos da Definição 1.50, a função responsável por realizar essa contagem é chamada de função de contagem dos números primos $\pi(x)$, assim, $\pi(150) = 35$.

O Crivo de Eratóstenes é eficiente, contudo, o tempo de processamento desfavorece o método para valores muito grandes, pois o processo de dividir por todos os números primos $p \leq \sqrt{m}$ é consideravelmente custoso para valores muito grandes pela elevada quantidade de números primos utilizados.

P. Fermat desenvolveu um método de fatoração para um inteiro m ímpar que dispensa a necessidade de conhecer os números primos $p \leq m$. A ideia desenvolvida por Fermat consiste na existência de $x, y \in \mathbb{Z}_+$ tais que $m = x^2 - y^2 = (x + y)(x - y)$, assim $(x + y)$ e $(x - y)$ são fatores de m e dependendo dos valores de x e y, o inteiro m é composto ou primo.

Os resultados seguintes foram baseados e adaptados do Capítulo 2 de [10].

Lema 2.5. *Seja o inteiro ímpar $m = ab \geq 1$ com $a, b \in \mathbb{Z}$. Então, existem com $x, y \in \mathbb{Z}_+$ tal que $m = x^2 - y^2 = (x - y)(x + y)$, mais ainda, $x = \dfrac{b + a}{2}$ e $y = \dfrac{b - a}{2}$.*

Demonstração. Considere o inteiro $m \geq 1$ ímpar, existem $a, b \in \mathbb{Z}$ com $1 \leq a \leq b \leq m$ tal que $m = ab$. Suponha que $m = x^2 - y^2$, assim segue que $m = ab = x^2 - y^2 = (x - y)(x + y)$ e como $x - y \leq x + y$, concluímos que $a = x - y$ e $b = x + y$. Logo, resolvendo o sistema de equações, obtemos

$$\begin{cases} x + y = b \\ x - y = a \end{cases} \Longrightarrow \begin{cases} x = \dfrac{b + a}{2} \\ y = \dfrac{b - a}{2} \end{cases},$$

notemos que $m \geq 1$ é inteiro ímpar e como a multiplicação de apenas dois ímpares é ímpar, a e b são inteiros ímpares e segue que $b + a$ e $b - a$ são inteiros não negativos pares, pois $b \geq a$ e a adição/subtração de inteiros ímpares é par, logo, $x = \dfrac{b + a}{2}$ e $y = \dfrac{b - a}{2}$ são inteiros não negativos. Em contrapartida, suponha que $x = \dfrac{b + a}{2}$ e $y = \dfrac{b - a}{2}$ são inteiros não negativos com a e b inteiros ímpares, assim obtemos que

$$x^2 - y^2 = \left(\frac{b + a}{2}\right)^2 - \left(\frac{b - a}{2}\right)^2 = ab = m$$

e m é um inteiro ímpar. Logo, o resultado segue. □

Adaptamos levemente a Fatoração de Fermat, apresentada a seguir, para utilizar como teste de primalidade.

Teorema 2.6. *(Teste 2: Fatoração de Fermat) Seja $m = 2k$ com $k \in \mathbb{N}$, então, m é primo se, e somente se, $k = 1$. Mas se $m > 1$ é um inteiro ímpar, existem $x, y \in \mathbb{Z}_+$ tais que $m = x^2 - y^2$ com $y = \sqrt{x^2 - m}$ e $\lfloor \sqrt{m} \rfloor \leq x \leq \dfrac{m+1}{2}$, assim, considere a solução $x \geq \lfloor \sqrt{m} \rfloor$ tal que $\sqrt{x^2 - m} = y \in \mathbb{Z}_+$, logo:*

i) Se $x < \dfrac{m+1}{2}$, então, m é composto;

ii) Se $x = \dfrac{m+1}{2}$, então, m é primo.

Demonstração. O resultado para $m = 2k$ é trivial. Agora, pelo Lema 2.5, todo inteiro ímpar $m = ab > 1$ com $1 \leq a \leq b \leq m$ pode ser escrito como $x^2 - y^2$ com $x, y \in \mathbb{Z}_+$ tal que $x = \dfrac{b+a}{2}$ e $y = \dfrac{b-a}{2}$.

Portanto, se $m = ab$ é primo ímpar, pela própria definição de número primo, a única solução é $a = 1$ e $b = m$, disso segue que $x = \dfrac{m+1}{2}$. Se $m = ab$ é composto ímpar, então $1 < a \leq b < m$. Caso $m = a^2$, isto é, $a = b$ temos que $x = a = |a| = \sqrt{a^2}$ e observamos ainda que $x = a < \dfrac{m+1}{2}$, pois $2a < a^2 + 1$ para $a > 1$. Agora, caso $m = ab$ é composto com $1 < a < b < m$, como $(a-1) > 0$ e $b > 1$ temos que $(a-1)b > a - 1$ então $ab + 1 > a + b$, isto é, $x = \dfrac{b+a}{2} < \dfrac{m+1}{2}$.

Observe do exposto acima que $x \leq \dfrac{m+1}{2}$ com a igualdade ocorrendo se, e somente se, m é primo, além disso, como $m = x^2 - y^2$ então $y = \sqrt{x^2 - m} \in \mathbb{Z}_+$ e por $y \geq 0$ então $x \geq \sqrt{m} \geq \lfloor \sqrt{m} \rfloor$. E o resultado segue. □

Para determinar os inteiros x e y necessários no Teste 2 sem conhecer os fatores a e b do inteiro ímpar $m > 1$, exatamente o que é pretendido com o teste, tomamos o menor inteiro positivo possível para x, ou seja, tomamos $x = \lfloor \sqrt{m} \rfloor$ e testamos se $y = \sqrt{x^2 - m} \in \mathbb{Z}_+$, se a resposta for afirmativa, foram determinados x e y e concluímos que m é composto, em contrapartida, se a resposta for negativa, assumimos $x = \lfloor \sqrt{m} \rfloor + 1$ e testamos novamente se $y = \sqrt{x^2 - m} \in \mathbb{Z}_+$, caso isso não ocorra, tomamos $x = \lfloor \sqrt{m} \rfloor + 2$ e testamos novamente se $y = \sqrt{x^2 - m} \in \mathbb{Z}_+$, e assim sucessivamente.

Ocorre que, conforme a demonstração do Teorema 2.6, se m for composto ímpar encontraremos $x < \dfrac{m+1}{2}$ tal que $y = \sqrt{x^2 - m} \in \mathbb{Z}_+$, mas caso m é primo ímpar encontraremos $x = \dfrac{m+1}{2}$ e segue que $y = \sqrt{\left(\frac{m+1}{2}\right)^2 - m} = \sqrt{\left(\frac{m-1}{2}\right)^2} = \left|\dfrac{m-1}{2}\right| \in \mathbb{Z}_+$.

Esse teste de primalidade é mais eficiente que o teste do Crivo de Eratóstenes quando o inteiro m é composto e possui o menor fator primo $p \mid m$ próximo de $\sqrt{m}$, lembre-se que $p \leq \sqrt{m}$. Contudo, o custo de tempo ainda é demasiadamente elevado para

números grandes, principalmente se $m = p$ for um número primo ímpar, a sua verificação exigiria $\frac{p+1}{2} - \lfloor\sqrt{p}\rfloor + 1$ etapas.

Exemplo 2.7. *Se* $m = 37$*, observamos que* $\lfloor\sqrt{37}\rfloor = 6 \leq x \leq 19 = \frac{37+1}{2}$*, portanto*

x	$y = \sqrt{x^2 - 37}$
6	*não existe em* $\mathbb{R}$,
7	$3,46...$
8	$5,19...$
9	$6,63...$
10	$7,93...$
11	$9,16...$
12	$10,34...$
13	$11,48...$
14	$12,60...$
15	$13,71...$
16	$14,79...$
17	$15,87...$
18	$16,94...$
19	18.

Logo, como $x = 19$*, podemos concluir que* 37 *é um número primo.*

Exemplo 2.8. *Se* $m = 371$*, observamos que* $\lfloor\sqrt{371}\rfloor = 19 \leq x \leq 186 = \frac{371+1}{2}$*, portanto*

x	$y = \sqrt{x^2 - 371}$
19	*não existe em* $\mathbb{R}$,
20	$5,38...$
21	$8,36...$
22	$10,63...$
23	$12,56...$
24	$14,31...$
25	$15,93...$
26	$17,46...$
27	$18,92...$
28	$20,32...$
29	$21,67...$
30	23.

Logo, como $x = 30 < 186$*, podemos concluir que* 371 *é um número composto.*

Exemplo 2.9. *Se* $m = 169$*, observamos que* $\lfloor \sqrt{169} \rfloor = 13 \leq x \leq 85 = \dfrac{169+1}{2}$*, portanto*

x	$y = \sqrt{x^2 - 169}$
13	0.

Logo, como $x = 13 < 85$*, podemos concluir que* 169 *é um número composto.*

Exemplo 2.10. *Se* $m = 33$*, observamos que* $\lfloor \sqrt{33} \rfloor = 5 \leq x \leq 17 = \dfrac{33+1}{2}$*, portanto*

x	$y = \sqrt{x^2 - 33}$
5	*não existe em* $\mathbb{R}$,
6	1, 73...
7	4.

Logo, como $x = 7 < 17$*, podemos concluir que* 33 *é um número composto.*

2.2 Caracterização dos Primos e o Teste de Wilson

Para prosseguir vamos precisar de alguns teoremas que caracterizem os números primos, iremos analisar três teoremas. Entende-se como caracterizar os números primos quando existe uma propriedade que é satisfeita por todos os números primos, contudo, não é satisfeita por nenhum número composto, isto é, estabelecemos um conectivo lógico bicondicional entre os números primos e a propriedade adquirida.

Para a primeira busca pela caracterização dos números primos, precisamos do Teorema de Wilson, a demonstração do teorema e da sua recíproca podem ser encontradas no Capítulo 10 de [16].

Teorema 2.11. *(Teorema de Wilson) Se* p *é número primo, então* $(p-1)! \equiv -1 \mod p$.

Demonstração. Obviamente temos que $-1 \equiv (2-1)! \mod 2$ e $-1 \equiv (3-1)! \mod 3$, então suponha que $p \geq 5$ primo. Observe que pelo Teorema 1.24 podemos concluir que para todo $i \in \{1, 2, \ldots, p-1\}$ a congruência $iX \equiv 1 \mod p$ possui uma única solução módulo p, ou seja, dado $i \in \{1, 2, \ldots, p-1\}$ existe um único $j \in \{1, 2, \ldots, p-1\}$ tal que $ij \equiv 1 \mod p$. Caso $i = j$ temos que $i^2 \equiv 1 \mod p$, então, $p \mid (i^2-1) = (i+1)(i-1)$, o que significa que $p \mid (i+1)$ ou $p \mid (i-1)$ e isso ocorre se, e somente se, $i = p-1$ ou $i = 1$. Assim, dado $i \neq j$ temos que para cada $i \in \{2, \ldots, p-2\}$ existe um único $j \in \{2, \ldots, p-2\}$ tal que $ij \equiv 1 \mod p$, logo, organizando essa congruência adequadamente podemos concluir que

$$2 \cdot 3 \cdot \ldots \cdot (p-2) \equiv 1 \mod p \Longrightarrow 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-2) \cdot (p-1) \equiv p-1 \equiv -1 \mod p,$$

portanto, concluímos que $(p-1)! \equiv -1 \mod p$ para p primo. □

Teorema 2.12. *(Recíproca do Teorema de Wilson) Seja o inteiro $m \geq 2$. Se ocorre $(m-1)! \equiv -1 \mod m$, então m é um número primo.*

Demonstração. Obviamente temos que $-1 \equiv (2-1)! \mod 2$ e $-1 \equiv (3-1)! \mod 3$ e os números 2 e 3 são primos, contudo, para $m = 4$ temos que $-1 \not\equiv (4-1)! \equiv -2 \mod 4$ e 4 não é primo. Suponha que $m > 4$ e não é um número primo, portanto, $m = ab$ com $a, b \in \mathbb{Z}$ e $1 < a \leq b < m$, então, tanto o fator a quanto o fator b de m são também fatores de $(m-1)!$, logo, $m \mid (m-1)!$ e concluímos que $m \nmid ((m-1)! + 1)$, pois caso contrário $m \mid 1$, o que é um absurdo, portanto, $(m-1)! \not\equiv -1 \mod m$.

Logo, se m é composto, $(m-1)! \not\equiv -1 \mod m$, em contrapartida, se ocorrer $(m-1)! \equiv -1 \mod m$, então, $m = p$ é um número primo. □

O Teorema de Wilson satisfaz a primeira exigência da caracterização dos números primos e a sua recíproca satisfaz a segunda exigência da caracterização, logo, temos uma maneira de caracterizar os números primos, isto é,

$$m \text{ é primo} \iff (m-1)! \equiv -1 \mod m.$$

Em especial, a recíproca do Teorema de Wilson comumente é assumida como um teste de primalidade, mas também podemos utilizar a caracterização dos números primos determinada acima, o que atesta os Teoremas de Wilson, Teorema 2.11 e Teorema 2.12 juntos, como um método para verificar a primalidade de inteiros positivos. Vamos formalizar este teste:

Corolário 2.13. *(Teste 3: Teoremas de Wilson) Seja o inteiro $m > 1$. Então, m é primo se, e somente se, $(m-1)! \equiv -1 \mod m$.*

Demonstração. Segue direto do Teorema 2.11 e Teorema 2.12. □

Teoricamente é muito simples determinar a primalidade de um inteiro $m > 1$ pelo Teste 3 de primalidade, pois basta calcular um fatorial e verificar uma congruência módulo m, contudo, o tempo de execução do Teste 3 é demasiadamente longo, já que é necessário calcular $(m-1)!$ e não é conhecida uma maneira rápida de obter esse valor.

Os testes de primalidade que serão apresentados posteriormente necessitam da verificação de uma quantidade consideravelmente elevada de congruências para a verificação da primalidade de um inteiro $m > 1$ grande, o que torna o fato da necessidade de verificar apenas uma congruência, no Teste 3, especial. Veja nos próximos exemplos como o Teste 3 de primalidade pode ser utilizado.

Exemplo 2.14. *Vamos verificar se o número* 13 *é primo. Como* $12! = 479001600$ *e* $13 \mid 479001601$*, ou seja,* $12! \equiv -1 \mod 13$*. Concluímos pelo Teste* 3 *que o número* 13 *é primo.*

Exemplo 2.15. *Vamos verificar se o número* 17 *é primo. Como* $16! = 20922789888000$ *e* $17 \mid 20922789888001$*, ou seja,* $16! \equiv -1 \mod 17$*. Concluímos pelo Teste* 3 *que o número* 17 *é primo.*

Exemplo 2.16. *Vamos verificar se* 21 *é primo. Como* $20! = 2432902008176640000$ *e* $21 \nmid 2432902008176640001$*, ou seja,* $20! \not\equiv -1 \mod 21$*. Concluímos pelo Teste* 3 *que o número* 21 ***não*** *é primo.*

A próxima busca pela caracterização dos números primos envolve a função φ de Euler, reveja a Definição 1.32. Lembramos que para qualquer número primo p, $(a, p) = 1$ para todo $1 \leq a < p$, logo, $\varphi(p) = p - 1$, como todo número primo satisfaz essa condição, a primeira exigência da caracterização é satisfeita.

Agora, dado um inteiro positivo m, se $\varphi(m) = m - 1$ então, por definição, $(m, a) = 1$ para todo inteiro $1 \leq a < m$, em particular, isso significa que $a \nmid m$ para qualquer $1 < a < m$, portanto, m é primo. Assim, a segunda exigência da caracterização dos números primos é satisfeita e obtemos uma importante maneira de caracterizar os números primos, isto é,

$$m \text{ é primo} \iff \varphi(m) = m - 1.$$

Poder-se-ia utilizar essa caracterização como um teste de primalidade, mas isso não é prático, contudo, essa caracterização é fundamental para provar o último teste de primalidade que será apresentado, juntamente com os seus aprimoramentos

O próximo Teorema é uma generalização feita por Euler do Pequeno Teorema de Fermat, que envolve a função φ de Euler. A demonstração que segue pode ser encontrada no Capítulo 2 de [29]. Lembre-se que existem $\varphi(m)$ inteiros $1 \leq b \leq m$ tais que $(b, m) = 1$ e reveja a Definição 1.26 de sistema reduzido de resíduos módulo m.

Teorema 2.17. *(Teorema de Euler) Sejam* $a, m \in \mathbb{Z}$ *com* $m > 1$ *e* $(a, m) = 1$*, então* $a^{\varphi(m)} \equiv 1 \mod m$*.*

Demonstração. Sejam $b_1, b_2, \ldots, b_{\varphi(m)}$ um sistema reduzido de resíduos módulo m, se $(a, m) = 1$ temos que $(ab_i, m) = 1$ para $i = 1, 2, \ldots, \varphi(m)$, já que $(b_i, m) = 1$, além disso, pelo sistema reduzido de resíduos definido inicialmente, temos que $ab_1, ab_2, \ldots, ab_{\varphi(m)}$ são, dois a dois, não congruentes módulo m e para cada $k \in \mathbb{Z}$ com $(k, m) = 1$ existem $i, j \in \{1, 2, \ldots, \varphi(m)\}$ tal que $k \equiv ab_i \equiv b_j \mod m$, logo, $ab_1, ab_2, \ldots, ab_{\varphi(m)}$ também é um sistema reduzido de resíduos módulo m.

Portanto, o conjunto $\{b_1 \mod m, b_2 \mod m, \ldots, b_{\varphi(m)} \mod m\}$ é igual ao conjunto $\{ab_1 \mod m, ab_2 \mod m, \ldots, ab_{\varphi(m)} \mod m\}$ e podemos concluir que

$$\prod_{i=1}^{\varphi(m)} ab_i = a^{\varphi(m)} \prod_{i=1}^{\varphi(m)} b_i \equiv \prod_{i=1}^{\varphi(m)} b_i \mod m,$$

logo, pela propriedade de cancelamento, $a^{\varphi(m)} \equiv 1 \mod m$. □

A última busca de caracterização que investigaremos é o Pequeno Teorema de Fermat, pode-se recordá-lo através do Teorema 1.30, o mesmo afirma que se p é um número primo e se $a \in \mathbb{N}$ com $(a, p) = 1$, então $a^{p-1} \equiv 1 \mod p$. Como essa é uma propriedade satisfeita por todos os números primos, a primeira exigência de caracterização é garantida, contudo, existem números compostos m que satisfazem $(a, m) = 1$ tal que $a^{m-1} \equiv 1 \mod m$, logo, a segunda exigência da caracterização não é garantida.

Exemplo 2.18.

$(4, 5) = 1$, *mas* $5^3 \equiv 1 \mod 4$ *e obviamente* 4 *não é primo.*

$(6, 13) = 1$, *mas* $13^5 \equiv 1 \mod 6$ *e obviamente* 6 *não é primo.*

$(57, 37) = 1$, *mas* $37^{56} \equiv 1 \mod 57$ *e* 57 *não é primo.*

Os números compostos que compartilham alguma propriedade específica dos números primos são denominados de *pseudoprimos*, no caso de um inteiro composto m satisfazer a congruência $a^{m-1} \equiv 1 \mod m$ para o inteiro $a > 1$ com $(m, a) = 1$, denominamos m de *pseudoprimo de Fermat na base a.*

Exemplo 2.19.

341 é composto e $2^{340} \equiv 1 \mod 341$*, então 341 é um pseudoprimo de Fermat na base 2.*

645 é composto e $2^{644} \equiv 1 \mod 645$*, então 645 é um pseudoprimo de Fermat na base 2.*

91 é composto e $3^{90} \equiv 1 \mod 91$*, então 91 é um pseudoprimo de Fermat na base 3.*

15 é composto e $4^{14} \equiv 1 \mod 15$*, então 15 é um pseudoprimo de Fermat na base 4.*

33 é composto e $10^{32} \equiv 1 \mod 33$*, então 33 é um pseudoprimo de Fermat na base 10.*

Para conhecer mais sobre os pseudoprimos, veja o Capítulo 6 de [10]. A seguir provaremos que existem infinitos pseudoprimos de Fermat, o que de fato afeta diretamente a pretensão de obter um teste de primalidade dos inteiros positivos baseado no Pequeno

Teorema de Fermat. Para a demonstração que segue, considere os inteiros positivos m e $a > 1$, verifica-se facilmente por indução em m, conforme página 45 de [16], que

$$a^{m-1} + a^{m-2} + a^{m-3} + \ldots + a + 1 = \frac{a^m - 1}{a - 1} \in \mathbb{Z} \tag{2.1}$$

e

$$a^{2m} - a^{2m-1} + a^{2m-2} - \ldots - a + 1 = \frac{a^{2m+1} + 1}{a + 1} \in \mathbb{Z}. \tag{2.2}$$

Seja p um número primo ímpar que não divide $a(a^2-1)$. Considere que $m = p$ na igualdade (2.1), assim, determinamos o inteiro positivo n_1 como

$$n_1 = \frac{a^p - 1}{a - 1} = a^{p-1} + a^{p-2} + a^{p-3} + \ldots + a + 1.$$

Na igualdade (2.2), como p é primo ímpar, considere que $2m + 1 = p$ para algum inteiro $m \geq 1$, assim, determinamos o inteiro positivo n_2 como

$$n_2 = \frac{a^p + 1}{a + 1} = a^{p-1} - a^{p-2} + a^{p-3} - \ldots - a + 1.$$

Se o inteiro a é par, verifica-se facilmente que n_1 e n_2 são inteiros ímpares, já que podemos escrever $a = 2k$ para algum $k \in \mathbb{Z}$ e o produto de números pares é par, somando-se 1 no final. Caso o inteiro a é ímpar, escrevemos $a = 2k' + 1$ para algum $k' \in \mathbb{Z}$ e com o auxílio da Fórmula do Binômio de Newton, veja o Teorema 1.28, notamos que n_1 possui os termos que são pares e a soma de $p-1$ números 1, o que também é par porque p é ímpar, restando ainda 1 somado a esses pares, já para n_2 temos, além dos termos pares, uma soma de $p-1$ números 1 que se cancelam pela alternância dos sinais, restando ainda 1 somado a esses pares, logo, tanto n_1 quanto n_2 são ímpares. Concluímos que n_1 e n_2 são números ímpares maiores do que 1 independentemente da paridade do inteiro $a > 1$.

Teorema 2.20. *Para cada inteiro $a > 1$, existem infinitos pseudoprimos m de Fermat na base a.*

Demonstração. Seja p um número primo ímpar que não divide $a(a^2 - 1)$ com $a > 1$. Considere o inteiro

$$n_1 n_2 = \left(\frac{a^p - 1}{a - 1}\right)\left(\frac{a^p + 1}{a + 1}\right) = \frac{a^{2p} - 1}{a^2 - 1} = m,$$

obviamente, como n_1 e n_2 são números ímpares maiores do que 1, o inteiro m é composto e ímpar. Além disso, pelo Pequeno Teorema de Fermat, como $a^p \equiv a \mod p$, obtemos

$$n_1 = \frac{a^p - 1}{a - 1} \equiv \frac{a - 1}{a - 1} = 1 \mod p \qquad e \qquad n_2 = \frac{a^p + 1}{a + 1} \equiv \frac{a + 1}{a + 1} = 1 \mod p,$$

logo, $n_1 n_2 = m \equiv 1 \mod p$, ou seja, $p \mid (m-1)$, mas como m é ímpar, temos que $m-1$ é par e p é primo ímpar, logo, $2p$ também divide $(m-1)$, isto é, $m \equiv 1 \mod 2p$ e podemos escrever $m = 2pK+1$ para algum $K \in \mathbb{Z}$. Por conseguinte, como $m = \dfrac{a^{2p}-1}{a^2-1}$ temos que $(a^2-1)m = a^{2p}-1$, então, $m \mid (a^{2p}-1)$, ou seja, $a^{2p} \equiv 1 \mod m$.

Portanto, concluímos que

$$a^m = a^{2pK+1} = (a^{2p})^K a \equiv (1)^K a = a \mod m,$$

em particular, se $(a, m) = 1$ então $a^{m-1} \equiv 1 \mod m$, logo, m é um pseudoprimo de Fermat na base a.

Desse modo, obtemos um pseudoprimo m de Fermat diferente para cada número primo ímpar p que não divide $a(a^2-1)$ e existem infinitos números primos que satisfazem essa condição, logo, existem infinitos pseudoprimos de Fermat na base $a > 1$. □

O Pequeno Teorema de Fermat, apesar de não caracterizar os números primos pela existência dos infinitos pseudoprimos de Fermat, fornece um interessante **método para determinar quando um número não é primo**, isto é, sejam $m, a \in \mathbb{N}$ com $m > 1$ e $(a, m) = 1$ tais que $a^{m-1} \not\equiv 1 \mod m$, garantimos que m não é um número primo, conforme formalizaremos no próximo teste de primalidade, já que se $m = p$ primo satisfaria o Pequeno Teorema de Fermat para todo inteiro a com $p \nmid a$.

Exemplo 2.21.

$2^{86} \equiv 4 \mod 87$, *portanto* 87 *não é um número primo.*

$5^{38} \equiv 25 \mod 39$, *portanto* 39 *não é um número primo.*

$4^{50} \equiv 16 \mod 51$, *portanto* 51 *não é um número primo.*

Além disso, observamos que para um inteiro a', satisfazendo as condições iniciais, o inteiro $m > 1$ pode ser um pseudoprimo de Fermat na base a', contudo, se determinarmos que $a^{m-1} \not\equiv 1 \mod m$ para algum outro inteiro a com $(a, m) = 1$, ainda garantimos que m é composto.

Exemplo 2.22.

$2^{340} \equiv 1 \mod 341$, *mas* $3^{340} \equiv 56 \mod 341$. *Logo,* 341 *não é um número primo.*

$30^{48} \equiv 1 \mod 49$ *e* $31^{48} \equiv 1 \mod 49$, *mas* $32^{48} \equiv 22 \mod 49$. *Logo,* 49 *não é um número primo.*

$3^{90} \equiv 1 \mod 91$, $4^{90} \equiv 1 \mod 91$, $9^{90} \equiv 1 \mod 91$ *e* $10^{90} \equiv 1 \mod 91$*, entre outros valores, contudo,* $2^{90} \equiv 64 \mod 91$*. Logo,* 91 *não é um número primo.*

Mesmo que a base a com $(m, a) = 1$ possa ser qualquer, é suficiente considerar $1 \leq a < m$, pois os resíduos da congruência módulo m se repetem para $a > m$. De fato, sejam $a, m, n \in \mathbb{N}$ com $m > 1$ e $1 \leq a \leq m$, se $a^n \equiv r \mod m$ com $r \in \{0, 1, \ldots, m-1\}$, como $(a + m) \equiv a \mod m$ então $(a + m)^n \equiv a^n \equiv r \mod m$.

2.3 Testes de primalidade por congruência

Com o teste de várias bases no Pequeno Teorema de Fermat determinamos a não primalidade de vários números compostos e eliminamos vários pseudoprimos, mesmo os que satisfazem o Teorema 1.30 para mais de uma base. Contudo, precisa-se ainda ter precaução, pois o teste esporádico de algumas bases a não garante a primalidade de nenhum inteiro positivo.

De fato, existem números compostos m que satisfazem $a^{m-1} \equiv 1 \mod m$ para todo $1 \leq a \leq m - 1$ com $(m, a) = 1$, esses números são denominados de *números de Carmichael*. Em 1994 os matemáticos W. Alford, A. Granville e C. Pomerance provaram que *existem infinitos números de Carmichael*. A demonstração desse resultado está fora do escopo do presente trabalho, mas a demonstração se encontrada no artigo original [2]. Para saber mais sobre os números de Carmichael, veja o Capítulo 6 de [10].

Exemplo 2.23. *Exemplos de números de Carmichael são:* 561*,* 1105*,* 1729*,* 2465*,* 2821*,* 6601*,* 8911*,* 10585*, entre infinitos outros.*

Observe que se $m = p$ for um número primo, por sua própria definição, temos que $(a, p) = 1$ para todo inteiro $1 \leq a \leq m - 1$, caso contrário, se $(a, m) = d > 1$ então os inteiros a e m são divisíveis pelo inteiro $1 < d < m$, logo, m é um número composto e temos que $d^{m-1} \not\equiv 1 \mod m$ para os divisores d de m, conforme provado a seguir, o que nos fornece um teste de primalidade. Este teste foi adaptado do Capítulo 6 de [10] e devidamente demonstrado.

Teorema 2.24. *(Teste 4) Sejam os inteiros* a *e* $m > 1$*. Então,* m *é primo se, e somente se,* $a^{m-1} \equiv 1 \mod m$ *para todo* $1 \leq a \leq m - 1$*.*

Demonstração. Vamos mostrar que os números compostos sempre violam a congruência $a^{m-1} \equiv 1 \mod m$ para algum $1 < a < m$, mais especificamente, violam essa congruência para $a = d > 1$ com $d \mid m$. Seja $m > 1$ composto, então existe um inteiro $1 < d < m$ e $k \in \mathbb{Z}$ tal que $m = dk$. Suponha que $d^{m-1} \equiv 1 \mod m$, assim, existe $t \in \mathbb{Z}$ tal que

$mt = d^{m-1} - 1$, ou seja, $d\,(d^{m-2} - kt) = 1$, o que é um absurdo, pois $(d^{m-2} - kt) \in \mathbb{Z}$ e $d > 1$, logo, concluímos que $d^{m-1} \not\equiv 1 \mod m$ para $d \mid m$ com $d > 1$. Em contrapartida, se $a \nmid m$ para todo $1 < a < m$ então m é primo e a congruência $a^{m-1} \equiv 1 \mod m$ segue, pelo Teorema 1.30, para todo $1 \leq a \leq m - 1$. □

Dessa maneira, se a congruência $a^{m-1} \equiv 1 \mod m$ para todo $1 \leq a \leq m - 1$ então m é um número primo, contudo, se m é um número composto então existe $1 < d < m$ tal que $d^{m-1} \not\equiv 1 \mod m$. Observe que se $d \mid m$ com $d > 1$ então $d^{m-1} \not\equiv 1 \mod m$, mas a recíproca não é verdadeira.

Exemplo 2.25.

$561 = 3 \,.\, 11 \,.\, 17$ *é número de Carmichael e* $3^{560} \equiv 375 \not\equiv 1 \mod 561$.

$29341 = 13 \,.\, 37 \,.\, 61$ *é número de Carmichael e* $13^{29340} \equiv 18057 \not\equiv 1 \mod 29341$.

$334153 = 19 \,.\, 43 \,.\, 409$ *é número de Carmichael e* $19^{334152} \equiv 193458 \not\equiv 1 \mod 334153$

O Teste 4 de primalidade é bom para determinar se um inteiro m é composto, como já mencionado, mesmo quando for um pseudoprimo é relativamente fácil fazer essa verificação. O caso mais demorado para determinar que um inteiro m não é primo são os números de Carmichael, que violam o Teste 4 de primalidade somente para os inteiros d tal que $(d, m) = d > 1$, assim, se os fatores primos de m são grandes o custo de tempo não se torna viável. Quando m é um inteiro ímpar primo, que é o caso mais demorado para concluir o teste, são necessárias $m - 3$ congruências para confirmar a sua primalidade, já que as bases $a = 1$ e, nesse caso, $a = m - 1$ são trivialmente congruentes a 1 módulo m.

Ressaltamos que o Teste 4 é restringido à versão do Pequeno Teorema de Fermat com $(a, m) = 1$, ou seja, devemos utilizar nesse enunciado **exclusivamente** a congruência $a^{m-1} \equiv 1 \mod m$. Se utilizarmos a outra versão do Teorema 1.30, isto é, $a^m \equiv a \mod m$, o Teste 4 de primalidade é perdido juntamente com essa sutileza. Isso ocorre pela definição dos números de Carmichael depender da versão do Pequeno Teorema de Fermat utilizada.

Quando dispensamos a necessidade dos inteiros a e m serem primos entre si, considera-se o Pequeno Teorema de Fermat com $a^m \equiv a \mod m$, assim, observamos que um número de Carmichael satisfaz essa congruência para todo $1 \leq a \leq m-1$. A violação da congruência que ocorre no Teste 4 de primalidade para os números compostos é devida à própria definição dos números primos p, ou seja, $(a, p) = 1$ para todo $1 \leq a \leq p - 1$ e pelo Pequeno Teorema de Fermat sempre temos $a^{p-1} \equiv 1 \mod p$, em contrapartida, os números compostos e, em especial, os números m de Carmichael como são compostos, têm $(d, m) = d > 1$ para algum $1 < d < m$ e assim obtemos que $d^{m-1} \not\equiv 1 \mod m$, como

visto anteriormente, por esse motivo consideramos exclusivamente a versão do Pequeno Teorema de Fermat que é utilizada no enunciado do Teste 4.

Exemplo 2.26. *Vamos verificar se o número* 31 *é primo. Observe que:*

$1^{30} \equiv 1 \mod 31$; $2^{30} \equiv 1 \mod 31$; $3^{30} \equiv 1 \mod 31$; $4^{30} \equiv 1 \mod 31$;
$5^{30} \equiv 1 \mod 31$; $6^{30} \equiv 1 \mod 31$; $7^{30} \equiv 1 \mod 31$; $8^{30} \equiv 1 \mod 31$;
$9^{30} \equiv 1 \mod 31$; $10^{30} \equiv 1 \mod 31$; $11^{30} \equiv 1 \mod 31$; $12^{30} \equiv 1 \mod 31$;
$13^{30} \equiv 1 \mod 31$; $14^{30} \equiv 1 \mod 31$; $15^{30} \equiv 1 \mod 31$; $16^{30} \equiv 1 \mod 31$;
$17^{30} \equiv 1 \mod 31$; $18^{30} \equiv 1 \mod 31$; $19^{30} \equiv 1 \mod 31$; $20^{30} \equiv 1 \mod 31$;
$21^{30} \equiv 1 \mod 31$; $22^{30} \equiv 1 \mod 31$; $23^{30} \equiv 1 \mod 31$; $24^{30} \equiv 1 \mod 31$;
$25^{30} \equiv 1 \mod 31$; $26^{30} \equiv 1 \mod 31$; $27^{30} \equiv 1 \mod 31$; $28^{30} \equiv 1 \mod 31$;
$29^{30} \equiv 1 \mod 31$; $30^{30} \equiv 1 \mod 31$.

Portanto, como $a^{30} \equiv 1 \mod 31$ *para todo* $1 \leq a \leq 30$*, concluímos pelo Teste* 4 *que* 31 *é primo.*

Exemplo 2.27. *Vamos verificar se o número* 17 *é primo. Observe que:*

$1^{16} \equiv 1 \mod 17$; $2^{16} \equiv 1 \mod 17$; $3^{16} \equiv 1 \mod 17$; $4^{16} \equiv 1 \mod 17$;
$5^{16} \equiv 1 \mod 17$; $6^{16} \equiv 1 \mod 17$; $7^{16} \equiv 1 \mod 17$; $8^{16} \equiv 1 \mod 17$;
$9^{16} \equiv 1 \mod 17$; $10^{16} \equiv 1 \mod 17$; $11^{16} \equiv 1 \mod 17$; $12^{16} \equiv 1 \mod 17$;
$13^{16} \equiv 1 \mod 17$; $14^{16} \equiv 1 \mod 17$; $15^{16} \equiv 1 \mod 17$; $16^{16} \equiv 1 \mod 17$.

Portanto, como $a^{16} \equiv 1 \mod 17$ *para todo* $1 \leq a \leq 16$*, concluímos pelo Teste* 4 *que* 17 *é primo.*

Exemplo 2.28. *Vamos verificar se o número* 33 *é primo. Observe que:*

$$1^{32} \equiv 1 \mod 33; \qquad 2^{32} \equiv 4 \not\equiv 1 \mod 33.$$

Portanto, como $a^{32} \not\equiv 1 \mod 33$ *para algum* $1 \leq a \leq 32$*, concluímos pelo Teste* 4 *que* 33 ***não*** *é primo.*

A justificativa da funcionalidade do Teste 4 de primalidade, conforme debatido anteriormente, é sintetizada pelo lema seguinte, que será oportunamente utilizado sem citação, cuja importância é devida à possibilidade de aplicar resultados matemáticos mais importantes quando satisfeita a hipótese de que $a^{m-1} \equiv 1 \mod m$.

Lema 2.29. *Sejam os inteiros positivos* a *e* $m > 1$*, se* $a^{m-1} \equiv 1 \mod m$ *então* $(a, m) = 1$.

Demonstração. Se $a^{m-1} \equiv 1 \mod m$ então existe $k \in \mathbb{Z}$ tal que $a^{m-1} - 1 = mk$, ou seja, $a\,(a^{m-2}) + m(-k) = 1$, assim pelo Corolário 1.16 temos que $(a, m) \mid 1$, logo, $(a, m) = 1$. □

Lembre-se do lema acima nas demonstrações dos testes de primalidade que serão apresentados nas páginas seguintes, pois esse lema é assumido como óbvio e não será citado nas demonstrações.

O matemático francês E. Lucas buscando simplificar os testes de primalidade através de uma maneira mais efetiva de filtrar os pseudoprimos de Fermat, obteve em 1876 o teste de primalidade mais famoso além do Crivo de Eratóstenes. Para demonstrá-lo consideraremos os próximos resultados, encontrados no Capítulo 1 de [20].

Definição 2.30. *Sejam os inteiros positivos a e $m > 1$ com $(a, m) = 1$, definimos a ordem de a módulo m como o menor expoente inteiro $i > 0$ tal que $a^i \equiv 1 \mod m$, escrevendo $i = ord_m a$.*

Podemos perceber pelo Teorema de Euler que sempre existe $ord_m a$ para $(a, m) = 1$, já que sempre ocorre $a^{\varphi(m)} \equiv 1 \mod m$, contudo, nem sempre $ord_m a$ será igual à $\varphi(m)$, podendo ser menor, logo, $ord_m a$ é no máximo $\varphi(m)$, isto é, $ord_m a \leq \varphi(m)$. Uma definição importante envolvendo ordem módulo m é a seguinte:

Definição 2.31. *Se $ord_m a = \varphi(m)$, dizemos que a é raiz primitiva módulo m.*

Além dessa definição, o próximo teorema também é extremamente importante para o nosso estudo.

Teorema 2.32. *Seja o inteiro positivo a e os inteiros $t > 1$, $m > 1$ com $(a, m) = 1$. Então, $a^t \equiv 1 \mod m$ se, e somente se, $ord_m a \mid t$.*

Demonstração. Sejam os inteiros $a > 0$, $t > 1$, $m > 1$ com $(a, m) = 1$ e seja $i = ord_m a$. Suponha que $a^t \equiv 1 \mod m$, logo, pela Divisão Euclidiana existem $c, r \in \mathbb{Z}$ com $0 \leq r < i$ tais que $t = ic + r$, considere que $r \neq 0$, assim, $a^t = a^{ic+r} = (a^i)^c a^r \equiv 1 \mod m$, como $a^i \equiv 1 \mod m$, temos que $(a^i)^c a^r \equiv a^r \mod m$ e concluímos que $a^r \equiv 1 \mod m$, o que é um absurdo, pois $r < i$ e i é a ordem de a módulo m, logo, $r = 0$ e $i \mid t$. Reciprocamente, suponha que $i \mid t$, assim existe $c \in \mathbb{Z}$ tal que $t = ic$, logo

$$a^t = a^{ic} = \left(a^i\right)^c \equiv 1^c = 1 \mod m,$$

o que conclui a prova. □

Corolário 2.33. *$ord_m a \mid \varphi(m)$.*

Demonstração. É imediato pelo Teorema 2.17 e pelo Teorema 2.32. □

Se m é um pseudoprimo de Fermat, ou seja, m é um inteiro composto com $1 < a < m$ e $(a, m) = 1$ tal que $a^{m-1} \equiv 1 \mod m$, então, pela caracterização dos números

primos temos que $\varphi(m) < m-1$ e pelo Corolário 2.33 obtemos que $ord_m a \leq \varphi(m)$, assim, $ord_m a \leq \varphi(m) < m-1$, logo, $ord_m a \neq m-1$ para todo inteiro $1 < a < m$, isto é, existe $1 < k < m-1$ tal que $a^k \equiv 1 \mod m$, ou seja, $m-1$ **nunca** será o menor inteiro positivo i tal que $a^i \equiv 1 \mod m$.

Em contrapartida, para todos os números primos p, como veremos adiante, sempre existe pelo menos um $1 \leq a < p$ tal que a ordem de a módulo p é igual a $p-1$.

Para demonstrar tal resultado, comentado acima, sobre os números primos, necessitamos dos dois lemas seguintes, que podem ser encontrados a partir da página 73 de [20].

Lema 2.34. $\sum_{d|m} \varphi(d) = m$ *para todo* $m \in \mathbb{N}$ *e divisor* d *de* m.

Demonstração. Seja d um divisor de $m \in \mathbb{N}$. Dado o inteiro $1 \leq b \leq m$, observamos que $d = (m, b)$ se, e somente se, $d \mid b$ e $\left(\frac{m}{d}, \frac{b}{d}\right) = 1$, logo, temos que a quantidade de inteiros b tais que $1 \leq b \leq m$ e $d = (m, b)$ é igual a $\varphi\left(\frac{m}{d}\right)$, já que $\varphi\left(\frac{m}{d}\right)$ fornece a quantidade de inteiros entre 1 e $\frac{m}{d}$, inclusos, que são primos com $\frac{m}{d}$. Além disso, o máximo divisor comum de cada um dos inteiros b com m é igual a algum $d \mid m$, ou seja, todos os m inteiros b são particionados unicamente segundo $(m, b) = d$ tal que $d \mid m$ e são contados uma única vez por $\varphi\left(\frac{m}{d}\right)$, portanto, obtemos que $\sum_{d|m} \varphi\left(\frac{m}{d}\right) = m$. Agora, sejam $1, d_2, \ldots, d_k, m$; todos os $(k+1)$ divisores de m, temos que

$$\sum_{d|m} \varphi\left(\frac{m}{d}\right) = \varphi(m) + \varphi\left(\frac{m}{d_2}\right) + \ldots + \varphi\left(\frac{m}{d_k}\right) + \varphi(1) = \varphi(m) + \varphi(d_k) + \ldots + \varphi(d_2) + \varphi(1) = \sum_{d|m} \varphi(d).$$

Logo, concluímos que $\sum_{d|m} \varphi(d) = m$. □

Para o próximo lema consideraremos a seguinte definição:

Definição 2.35. *Seja* p *um primo e* d *um divisor de* $p-1$*, definimos* $N(d)$ *como a quantidade de inteiros* $1 \leq a \leq p-1$ *tal que* $ord_p a = d$.

Um resultado importante que precisaremos na demonstração do próximo lema é que um polinômio não constante de grau n, $p(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$ com $a_n, a_{n-1}, \ldots, a_0$ números reais e $a_n \neq 0$, têm no máximo n raízes, veja Teorema 2.19 de [9]. Na realidade, essa é uma consequência de um resultado mais forte, o Teorema Fundamental da Álgebra, que estabelece através de uma das maneiras de enunciá-lo, que todo polinômio $p(x)$ não constante de grau n, definido no conjunto dos números complexos $\mathbb{C}$ e com coeficientes complexos, possui exatamente n raízes, não necessariamente distintas. Para saber mais sobre o Teorema Fundamental da Álgebra, veja [9]. Seguimos para o lema.

Lema 2.36. *Sejam p primo e $d \mid (p-1)$. Então $N(d) \leq \varphi(d)$.*

Demonstração. Se ocorrer $N(d) = 0$ então o resultado é trivial. Assim, suponha que $N(d) > 0$, portanto, existe pelo menos um inteiro positivo $1 \leq a \leq p-1$ tal que $ord_p a = d$, ou seja, o inteiro $d > 0$ é o menor expoente tal que $a^d \equiv 1 \mod p$ e, consequentemente, os resíduos $1 \mod p, a \mod p, a^2 \mod p, \ldots, a^{d-1} \mod p$; são todos distintos entre si. Como ocorre $\left(a^k\right)^d = \left(a^d\right)^k \equiv 1^k = 1 \mod p$ para todos os inteiros $0 \leq k \leq d-1$, os d elementos do conjunto $\{1 \mod p, a \mod p, a^2 \mod p, \ldots, a^{d-1} \mod p\}$ fornecem todas as soluções de x na congruência $x^d \equiv 1 \mod p$, já que essa congruência têm no máximo d soluções distintas módulo p porque o polinômio $x^d - (pt+1) = 0$ com $t \in \mathbb{Z}$ possui no máximo d soluções. Por outro lado, se ocorrer $ord_p(a^k) = d$ então temos que $(k,d) = 1$, pois caso $(k,d) = r > 1$ então $\left(a^k\right)^{\frac{d}{r}} = \left(a^d\right)^{\frac{k}{r}} \equiv (1)^{\frac{k}{r}} = 1 \mod p$, assim, obteríamos $ord_p(a^k) \leq \dfrac{d}{r} < d$.

Dessa forma, seja o inteiro $1 \leq b \leq p-1$, temos que

$$ord_p b = d \Longleftrightarrow b \in \{x \equiv a^k \mod p\,;\ 0 \leq k \leq d-1 \ \ e \ \ (k,d) = 1\},$$

observe que existem $\varphi(d)$ inteiros $0 \leq k \leq d-1$ tal que $(k,d) = 1$, que é exatamente a quantidade de elementos do conjunto $\{x \equiv a^k \mod p\,;\ 0 \leq k \leq d-1 \ \ e \ \ (k,d) = 1\}$, que são todas as possibilidades para os elementos $b \equiv a^k \mod p$ tal que $ord_p b = d$, ou seja, $N(d)$ é no máximo igual a $\varphi(d)$. Logo, concluímos que $N(d) \leq \varphi(d)$. □

Na verdade, não longínquo da demonstração realizada acima, podemos concluir que $N(d) = \varphi(d)$, essa conclusão surgirá na demonstração do próximo teorema, mas poderia se juntar ao lema acima sem problemas, a opção de não o fazer é pelo melhor desenvolvimento da demonstração que seguirá. Com esses lemas podemos provar o importante teorema que segue:

Teorema 2.37. *Se p é um número primo então existe um inteiro $1 < a < p$ que é raiz primitiva módulo p, ou seja, $ord_p a = \varphi(p) = p-1$.*

Demonstração. Seja p primo e $d \mid (p-1)$, como $a^{p-1} \equiv 1 \mod p$ para todo $1 \leq a \leq p-1$, cada um dos inteiros a possui $ord_p a \leq p-1$ e pelo Teorema 2.32, $ord_p a \mid (p-1)$. Portanto, cada um dos $p-1$ inteiros a é contado uma única vez por algum $N(d)$, considerando-se cada $d \mid (p-1)$, logo, temos que $\displaystyle\sum_{d|(p-1)} N(d) = p-1$. Pelo Lema 2.34, temos que $\displaystyle\sum_{d|(p-1)} \varphi(d) = p-1$, mas pelo Lema 2.36 sabemos que $N(d) \leq \varphi(d)$ e considerando a desigualdade para cada d, podemos concluir que

$$p-1 = \sum_{d|(p-1)} N(d) \leq \sum_{d|(p-1)} \varphi(d) = p-1,$$

logo, é imediata a conclusão que $N(d) = \varphi(d)$ para cada $d \mid (p-1)$.

Em Particular, $N(p-1) = \varphi(p-1) > 0$, logo, sempre existe pelo menos um inteiro $1 \leq a < p$ que é raiz primitiva módulo p, isto é, $ord_p a = \varphi(p) = p-1$. □

O teorema acima sintetiza que para todo número primo p, sempre existe um inteiro $1 \leq a < p$ tal que a ordem de a módulo p é igual a $p-1$, que é exatamente a garantia da funcionalidade do Teste de Lucas que veremos em seguida. Assim, com posse desse teorema e baseado na página 37 de [29], vejamos o teste de primalidade de Lucas.

Teorema 2.38. *(Teste 5: Teste de Lucas) Seja o inteiro $m > 1$. Então, m é primo se, e somente se, existe um inteiro $1 \leq a < m$ tal que:*

i) $a^{m-1} \equiv 1 \mod m$;

ii) $a^k \not\equiv 1 \mod m$ *para* $k = 1, 2, \ldots, (m-2)$.

Demonstração. Seja o inteiro $m > 1$. Suponha que existe um inteiro $1 \leq a < m$ tal que as condições $i)$ e $ii)$ sejam satisfeitas, assim, $m-1$ é o menor expoente inteiro que satisfaz a congruência dada em $i)$, logo, $ord_m a = m-1$ e pelo Corolário 2.33 temos que $ord_m a \mid \varphi(m)$, ou seja, $(m-1) \mid \varphi(m)$, portanto, como $\varphi(m) \leq m-1$ concluímos que $\varphi(m) = m-1$, logo, m é um número primo. Reciprocamente, pelo Teorema 2.37, se m é um número primo então sempre existe pelo menos um inteiro $1 \leq a < m$ tal que $ord_m a = m-1$, logo, as condições $i)$ e $ii)$ são satisfeitas. □

Este teste é quase perfeito, pois é simples e elegante, contudo, ainda exige uma quantidade demasiada de operações para m grande, pois é necessário realizar a verificação de $m-1$ congruências, além de encontrar uma base a adequada. Observe que a base $a = 1$ é utilizada apenas para verificar a primalidade do número 2, usando vacuidade na condição $ii)$, para os inteiros $m > 2$ basta considerar $1 < a < m$. O mesmo é válido para o Teste 4.

Exemplo 2.39. *Vamos verificar se o número 5 é primo. Observe que* $2^4 \equiv 1 \mod 5$*, além disso,*

$$2^1 \equiv 2 \not\equiv 1 \mod 5; \quad 2^2 \equiv 4 \not\equiv 1 \mod 5; \quad 2^3 \equiv 3 \not\equiv 1 \mod 5.$$

Logo, pelo Teste 5 o número 5 é primo.

Exemplo 2.40. *Vamos verificar se o número 11 é primo. Observe que* $6^{10} \equiv 1 \mod 11$*, além disso,*

$$\begin{array}{lll} 6^1 \equiv 6 \not\equiv 1 \mod 11; & 6^2 \equiv 3 \not\equiv 1 \mod 11; & 6^3 \equiv 7 \not\equiv 1 \mod 11; \\ 6^4 \equiv 9 \not\equiv 1 \mod 11; & 6^5 \equiv 10 \not\equiv 1 \mod 11; & 6^6 \equiv 5 \not\equiv 1 \mod 11; \\ 6^7 \equiv 8 \not\equiv 1 \mod 11; & 6^8 \equiv 4 \not\equiv 1 \mod 11; & 6^9 \equiv 2 \not\equiv 1 \mod 11. \end{array}$$

Logo, pelo Teste 5 *o número* 11 *é primo.*

Exemplo 2.41. *Vamos verificar se o número* 17 *é primo. Observe que* $5^{16} \equiv 1 \mod 17$*, além disso,*

$$5^1 \equiv 5 \not\equiv 1 \mod 17; \quad 5^2 \equiv 8 \not\equiv 1 \mod 17; \quad 5^3 \equiv 6 \not\equiv 1 \mod 17;$$
$$5^4 \equiv 13 \not\equiv 1 \mod 17; \quad 5^5 \equiv 14 \not\equiv 1 \mod 17; \quad 5^6 \equiv 2 \not\equiv 1 \mod 17;$$
$$5^7 \equiv 10 \not\equiv 1 \mod 17; \quad 5^8 \equiv 16 \not\equiv 1 \mod 17; \quad 5^9 \equiv 12 \not\equiv 1 \mod 17.$$
$$5^{10} \equiv 9 \not\equiv 1 \mod 17; \quad 5^{11} \equiv 11 \not\equiv 1 \mod 17; \quad 5^{12} \equiv 4 \not\equiv 1 \mod 17;$$
$$5^{13} \equiv 3 \not\equiv 1 \mod 17; \quad 5^{14} \equiv 15 \not\equiv 1 \mod 17; \quad 5^{15} \equiv 7 \not\equiv 1 \mod 17.$$

Logo, pelo Teste 5 *o número* 17 *é primo.*

Lembre-se que a condição i) do Teste 5 é satisfeita somente por números primos ou por números compostos que são pseudoprimos de Fermat na base a considerada, logo, **se um inteiro** m **não satisfazer a condição** i**), então,** m **é composto**. Mas satisfeita a condição i), verifica-se a condição ii) do Teste 5 e **se o inteiro** m **não satisfazer a condição** ii**), então, não podemos afirmar nada sobre** m, desse modo, precisamos analisar outra base $1 \leq a < m$.

Verifica-se que, se m for primo, a condição i) sempre será satisfeita para todas as bases $1 \leq a < m$ e, pelo Teorema 2.37, sempre haverá uma dessas bases a que satisfaz a condição ii), como desejado. Contudo, caso m for composto, a condição i) será violada para alguma base $1 \leq a < m$, conforme o que foi debatido no Teste 4 de primalidade, mas mesmo que a condição i) seja satisfeita para alguma base $1 \leq a' < m$, essa base não satisfará a condição ii), pois nesse caso, ainda que o inteiro composto m possuir uma raiz primitiva, **o que nem sempre ocorre**, temos que $ord_m a' = \varphi(m) < m - 1$, além disso, se m não possuir raiz primitiva temos que $ord_m a' < \varphi(m) < m - 1$, logo, em ambos os casos a condição ii) será violada.

Dessa forma, a base a do Teste 5 pode ser um pouco complicada de ser determinada, já que essa base deve satisfazer todas as congruências exigidas na condição ii) e, diferente da condição i), quando a base a não satisfazer uma das congruências, não podemos afirmar nada sobre o inteiro analisado, mas devemos considerar uma outra base $1 \leq a' < m$ e iniciar o Teste 5 novamente.

Por exemplo, para o número 17 vimos que a base $a = 5$ verifica a sua primalidade, contudo, se considerarmos a base $a = 2$ temos, na condição i), que $2^{16} \equiv 1 \mod 17$, contudo, também ocorre que $2^8 \equiv 1 \mod 17$, o que contradiz a condição ii). Da mesma maneira, o número 11 obteve a sua primalidade verificada com a base $a = 6$, mas a base $a = 3$ não poderia ser utilizada, pois $3^{10} \equiv 1 \mod 11$, para a condição i), mas também ocorre que $3^5 \equiv 1 \mod 11$, o que contradiz a condição ii).

O Teste 5 de primalidade obteve um refinamento desenvolvido por E. Lucas em 1891, substituindo o item *ii*) no Teorema 2.38, referente ao Teste 5, para a verificação apenas dos inteiros $d \mid (m-1)$ com $1 \leq d < m-1$. Baseado na página 37 de [29], vejamos o teste de primalidade de Lucas refinado.

Teorema 2.42. *(Teste 6: Teste de Lucas refinado) Seja o inteiro $m > 1$. Então, m é primo se, e somente se, existe um inteiro $1 \leq a < m$ tal que:*

i) $a^{m-1} \equiv 1 \mod m$;

ii') $a^d \not\equiv 1 \mod m$ *para todo divisor* d *de* $m-1$ *tal que* $1 \leq d < m-1$.

Demonstração. Seja o inteiro $m > 1$. Suponha que existe um inteiro $1 \leq a < m$ tal que as condições i) e ii') sejam satisfeitas, assim, pela condição i) e pelo Teorema 2.32 temos que $ord_m a \mid (m-1)$, mas pela condição ii'), nenhum dos divisores d de $m-1$ tal que $1 \leq d < m-1$ satisfaz a congruência $a^d \equiv 1 \mod m$, assim, novamente pelo Teorema 2.32 temos que $ord_m a \nmid d$, logo, $ord_m a = m-1$. Por conseguinte, pelo Corolário 2.33 temos que $ord_m a \mid \varphi(m)$, ou seja, $(m-1) \mid \varphi(m)$, portanto, como $\varphi(m) \leq m-1$ concluímos que $\varphi(m) = m-1$, logo, m é um número primo. Reciprocamente, pelo Teorema 2.37, se m é um número primo então sempre existe pelo menos um inteiro $1 \leq a < m$ tal que $ord_m a = m-1$, logo, as condições i) e ii') são satisfeitas. □

O Teste 6 de primalidade reduz a quantidade de congruências necessárias para a sua execução em comparação com o Teste 5 de primalidade, contudo, acrescenta o problema de determinar todos os divisores d de $m-1$ tal que $1 \leq d < m-1$, o que na maioria dos casos não é uma tarefa fácil para m grande.

Observaremos os mesmos 3 exemplos utilizados no Teste 5 de primalidade, executando-os agora com o Teste 6, para constatar a redução de congruências necessárias para a verificação da primalidade de um inteiro $m > 1$.

Exemplo 2.43. *Vamos verificar se o número* 5 *é primo. Observe que* $2^4 \equiv 1 \mod 5$, *além disso, os divisores* $1 \leq d < 4$ *de* 4 *são* 1 *e* 2, *portanto,*

$$2^1 \equiv 2 \not\equiv 1 \mod 5; \qquad 2^2 \equiv 4 \not\equiv 1 \mod 5.$$

Logo, pelo Teste 6 *o número* 5 *é primo. Observe que foi reduzido* 1 *congruência na sua verificação.*

Exemplo 2.44. *Vamos verificar se o número* 11 *é primo. Observe que* $6^{10} \equiv 1 \mod 11$, *além disso, os divisores* $1 \leq d < 10$ *de* 10 *são* $1, 2$ *e* 5, *portanto,*

$$6^1 \equiv 6 \not\equiv 1 \mod 11; \qquad 6^2 \equiv 3 \not\equiv 1 \mod 11; \qquad 6^5 \equiv 10 \not\equiv 1 \mod 11.$$

Logo, pelo Teste 6 *o número* 11 *é primo. Observe que foram reduzidas* 6 *congruências na sua verificação.*

Exemplo 2.45. *Vamos verificar se o número* 17 *é primo. Observe que* $5^{16} \equiv 1 \mod 17$*, além disso, os divisores* $1 \leq d < 16$ *de* 16 *são* $1, 2, 4$ *e* 8*, portanto,*

$$5^1 \equiv 5 \not\equiv 1 \mod 17; \quad 5^2 \equiv 8 \not\equiv 1 \mod 17; \quad 5^4 \equiv 13 \not\equiv 1 \mod 17;$$
$$5^8 \equiv 16 \not\equiv 1 \mod 17.$$

Logo, pelo Teste 6 *o número* 17 *é primo. Observe que foram reduzidas* 11 *congruências na sua verificação.*

Podemos constatar que o Teste 6 de primalidade realmente reduz consideravelmente a quantidade de congruências necessárias para a verificação da primalidade do inteiro $m > 1$. Os demais comentários a respeito do Teste 5 são válidos para o Teste 6.

Em 1967 os matemáticos J. Brillhart e J. Selfridge desenvolveram um excelente aperfeiçoamento no Teste de Lucas refinado, conforme baseado na página 38 de [29], obtendo o seguinte teste de primalidade que será nomeado de Teste LBS, em homenagem à E. Lucas, J. Brillhart e J. Selfridge.

Teorema 2.46. *(Teste 7: LBS) Seja o inteiro* $m > 1$*. Então,* m *é primo se, e somente se, para cada um dos fatores primos* p *de* $m-1$*, existe um inteiro* $1 \leq a_p < m$*, tal que:*

i) $a_p^{m-1} \equiv 1 \mod m$*;*

ii) $a_p^{\frac{m-1}{p}} \not\equiv 1 \mod m$*.*

Demonstração. Seja o inteiro $m > 1$. Suponha que $(m-1) \nmid \varphi(m)$, portanto, existe um número primo p tal que $p^r \mid (m-1)$ e $p^r \nmid \varphi(m)$ para algum expoente inteiro $r \geq 1$. Associado ao número primo p que divide $m-1$, suponha que existe um inteiro $1 \leq a_p < m$ tal que as condições $i)$ e $ii)$ sejam satisfeitas, assim, pela condição $i)$ e pelo Teorema 2.32 temos que $ord_m a_p \mid (m-1)$, dessa forma, existe $k \in \mathbb{Z}$ tal que $m - 1 = k \,.\, ord_m a_p$, portanto, temos que $p^r \mid (k \,.\, ord_m a_p)$, ou seja, existe $t \in \mathbb{Z}$ tal que $t \,.\, p^r = k \,.\, ord_m a_p$, assim, $t \,.\, p^{r-1} = \dfrac{k \,.\, ord_m a_p}{p}$, logo, obtemos que $p^{r-1} \mid \left(\dfrac{k \,.\, ord_m a_p}{p}\right)$.

Agora, como $a_p^{\frac{m-1}{p}} \not\equiv 1 \mod m$, na condição $ii)$, pelo Teorema 2.32 obtemos que $ord_m a_p \nmid \left(\dfrac{m-1}{p}\right)$, ou seja, $ord_m a_p \nmid \left(\dfrac{k \,.\, ord_m a_p}{p}\right)$, consequentemente, para todo $t' \in \mathbb{Z}$ temos que $t' \,.\, ord_m a_p \neq \dfrac{k \,.\, ord_m a_p}{p}$, o que ocorre se, e somente se, $\dfrac{k}{p} \notin \mathbb{Z}$, logo, $p \nmid k$, como também $p^r \nmid k$, porém, como visto anteriormente, $p^r \mid (k \,.\, ord_m a_p)$, portanto, pelo Lema 1.17, concluímos que $p^r \mid ord_m a_p$.

Assim, pelo Corolário 2.33 temos que $ord_m a_p \mid \varphi(m)$, mas como $p^r \mid ord_m a_p$, pelo Lema 1.10, obtemos que $p^r \mid \varphi(m)$, o que é um absurdo pela hipótese inicial de $p^r \nmid \varphi(m)$. Logo, temos que $p^r \mid \varphi(m)$.

Como o número primo p foi assumido genericamente, concluímos que para cada primo p tal que $p^r \mid (m-1)$ com $r \geq 1$, também ocorre que $p^r \mid \varphi(m)$, ou seja, obtemos que $(m-1) \mid \varphi(m)$, mas como $\varphi(m) \leq m-1$, concluímos que $\varphi(m) = m-1$, logo, m é um número primo. Reciprocamente, pelo Teorema 2.37, se m é um número primo então sempre existe pelo menos um inteiro $1 \leq a_p < m$, não necessariamente distinto, associado a cada um dos fatores primos p de $m-1$ tal que $ord_m a_p = m-1$, logo, as condições $i)$ e $ii)$ são satisfeitas. □

Dentre o Teste de Lucas (Teste 5), Teste de Lucas refinado (Teste 6) e o Teste LBS (Teste 7), o Teste LBS é o mais utilizado nas bibliografias sobre os números primos e testes de primalidade.

O Teste 7 de primalidade possui uma versatilidade muito grande comparado com os demais testes apresentados que envolvem congruências. Primeiramente, se $m > 3$ é um inteiro ímpar, o Teste 7 necessita de uma quantidade menor de congruências módulo m, quando comparado com o Teste 6, já que o Teste 7 considera, na condição $ii)$, uma congruência para cada um dos números primos $p \mid (m-1)$, enquanto que o Teste 6 considera, na condição $ii')$, uma congruência para cada um dos divisores $1 \leq d < m-1$ de $m-1$, o qual possui uma quantidade maior de verificações quando $m-1$ é divisível por mais de dois números primos, não necessariamente distintos, ou quando é divisível por exatamente dois números primos, não necessariamente distintos, nesse último caso, a verificação teórica de $d = 1$ no Teste 6 é dispensada no Teste 7.

Por conseguinte, o principal diferencial do Teste 7 é, quando satisfeita a condição $i)$, não depender da existência de uma mesma base $1 \leq a < m$ que satisfaz a condição $ii)$ para todo divisor primo p de $m-1$, ou seja, enquanto o Teste 6 depende da determinação de uma mesma base $1 \leq a < m$ tal que $a^d \not\equiv 1 \mod m$ para todo $d \mid (m-1)$ com $1 \leq d < m-1$, no Teste 7 é possível determinar uma base $1 \leq a_p < m$, desde que a base a_p satisfaça a condição $i)$, tal que $a_p^{\frac{m-1}{p}} \not\equiv 1 \mod m$ para cada um dos números primos $p \mid (m-1)$, ou seja, o número primo $p \mid (m-1)$ pode ter uma base a_p associada enquanto que o número primo $p' \mid (m-1)$ pode ter uma base $a_{p'} \neq a_p$ associada. Obviamente as bases podem ser todas iguais, contudo, diferente do Teste 5 e do Teste 6, no Teste 7 não existe a necessidade dessa condição ser satisfeita.

Exemplo 2.47. *Vamos verificar se o número* 5 *é primo. Observe que* 2 *é o único fator primo distinto de* 4*, assim, assumindo* $a_2 = 2$ *temos que* $2^4 \equiv 1 \mod 5$*, agora basta testar a congruência com o expoente* $\frac{4}{2} = 2$*, assim,* $2^2 \equiv 4 \not\equiv 1 \mod 5$*. Logo, pelo Teste* 7 *o*

número 5 *é primo.*

Exemplo 2.48. *Vamos verificar se o número* 17 *é primo. Observe que* 2 *é o único fator primo distinto de* 16*, assim, assumindo* $a_2 = 5$ *temos que* $5^{16} \equiv 1 \mod 17$*, agora basta testar a congruência com o expoente* $\frac{16}{2} = 8$*, assim,* $5^8 \equiv 16 \not\equiv 1 \mod 17$*. Logo, pelo Teste* 7 *o número* 17 *é primo.*

Exemplo 2.49. *Vamos verificar se o número* 11 *é primo. Observe que os fatores primos distintos de* 10 *são* 2 *e* 5*, assim, assumindo* $a_2 = 6$ *temos que* $6^{10} \equiv 1 \mod 11$*, além disso, é necessário testar a congruência com o expoente* $\frac{10}{2} = 5$*, portanto, temos que* $6^5 \equiv 10 \not\equiv 1 \mod 11$*. Agora, assumindo* $a_5 = 7$ *temos que* $7^{10} \equiv 1 \mod 11$*, além disso, é necessário testar a congruência com o expoente* $\frac{10}{5} = 2$*, assim,* $7^2 \equiv 5 \not\equiv 1 \mod 11$*.*

Logo, pelo Teste 7 *o número* 11 *é primo. Observe que poderíamos ter assumido* $a_5 = 2$*, assim,* $2^2 \equiv 4 \not\equiv 1 \mod 11$*, mas foi preferível ilustrar a versatilidade do Teste* 7*.*

No próximo exemplo desenvolveremos o Teste 7 com um pouco mais de detalhes sobre a sua execução.

Exemplo 2.50. *Vamos verificar se o número* 127 *é primo. Observe que os fatores primos distintos de* 126 *são* 2*,* 3 *e* 7*, assim, assumindo* $a_2 = 2$ *temos que* $2^{126} \equiv 1 \mod 127$*, além disso, é necessário testar a congruência com o expoente* $\frac{126}{2} = 63$*, portanto, temos que* $2^{63} \equiv 1 \mod 127$*, o que viola a condição necessária, logo, precisamos considerar outra base para* a_2*. Assumindo* $a_2 = 3$ *temos que* $3^{126} \equiv 1 \mod 127$*, além disso, para o expoente* $\frac{126}{2} = 63$*, obtemos agora que* $3^{63} \equiv 126 \not\equiv 1 \mod 127$*.*

Agora, assumindo $a_3 = 2$ *temos que* $2^{126} \equiv 1 \mod 127$ *conforme já verificado, além disso, é necessário testar a congruência com o expoente* $\frac{126}{3} = 42$*, assim, temos que* $2^{42} \equiv 1 \mod 127$*, o que viola a condição necessária, logo, precisamos considerar outra base para* a_3*. Assumindo* $a_3 = 3$ *temos que* $3^{126} \equiv 1 \mod 127$ *conforme já verificado, além disso, para o expoente* $\frac{126}{3} = 42$*, obtemos agora que* $3^{42} \equiv 107 \not\equiv 1 \mod 127$*.*

Por fim, assumindo $a_7 = 2$ *temos que* $2^{126} \equiv 1 \mod 127$ *conforme já verificado, além disso, é necessário testar a congruência com o expoente* $\frac{126}{7} = 18$*, assim,* $2^{18} \equiv 16 \not\equiv 1 \mod 127$*.*

Logo, pelo Teste 7 *o número* 127 *é primo.*

Dessa forma, considerando um inteiro $m > 1$ grande, no Teste 6 se verificássemos uma grande quantidade de congruências, conforme os divisores $d \mid (m-1)$ com $1 \leq d < m-1$ para uma determinada base $1 \leq a < m$, porém, em determinado momento no desenvolvimento do Teste 6 encontrássemos um divisor $1 \leq d' < m-1$ de $m-1$ que contradiz a condição ii'), todas as congruências que já foram verificadas para

os outros divisores d de $m-1$ estarão depreciadas e será necessário determinar outra base $1 \leq a' < m$, para verificar todas as congruências novamente.

O Teste 7 elimina esse prejuízo na execução do Teste 6 ou do Teste 5, pois como a base $1 \leq a_p < m$ depende do número primo $p \mid (m-1)$, uma vez verificada a condição $i)$ e $ii)$ do Teste 7 para a base a_p, essas congruências permanecem validadas, não importando se a base a_p contradizer a condição $ii)$ do Teste 7 para algum outro número primo $p' \mid (m-1)$, poder-se-ia considerar outra base $1 \leq a_{p'} < m$ para o número primo p' sem depreciar as congruências que já foram obtidas.

Em resumo, somente faz sentido aplicar um teste de primalidade para inteiros m ímpares, caso esse número for "pequeno", em geral, o Crivo de Eratóstenes é o mais indicado para testar o inteiro m. Se o inteiro ímpar m for "grande", recomenda-se primeiramente testar se $a^{m-1} \equiv 1 \mod m$ para algumas bases $1 < a < m$, quanto mais bases forem testadas, mais fácil é determinar se m é composto, evitando nesse caso, a execução de testes de primalidade mais complexos, os quais são reservados apenas aos casos em que a suspeita do inteiro m ser primo for respaldada por várias bases $1 < a < m$ satisfazendo $a^{m-1} \equiv 1 \mod m$.

Observação 2.51. *Quando dizemos, nesse contexto, que um número é "pequeno"ou "grande", a magnitude desses adjetivos é dada pela capacidade computacional disponível no momento da execução dos testes de primalidade.*

Inicialmente, testar a congruência $2^{m-1} \equiv 1 \mod m$ é um excelente começo, de fato, entre 1 e 10^9 existem apenas 5597 pseudoprimos de Fermat na base 2, contra 50847534 números primos ([10], página 106), o que mostra como os pseudoprimos de Fermat são escassos, pelo menos, consideravelmente mais escassos que os números primos.

Se testarmos também a congruência $3^{m-1} \equiv 1 \mod m$, além da congruência $2^{m-1} \equiv 1 \mod m$, aumentamos consideravelmente a probabilidade de estarmos testando um número primo, de fato, entre 1 e 10^9 existem apenas 1272 pseudoprimos de Fermat na base 2 que também é um pseudoprimo de Fermat na base 3, logo, com a verificação da congruência para uma única base a mais, eliminamos 4325 pseudoprimos de Fermat ([10], página 106).

Em contrapartida, se m satisfazer a congruência $a^{m-1} \equiv 1 \mod m$ para muitas bases $1 < a < m$, maior é a probabilidade de que o inteiro m seja primo. Mas mesmo com uma boa probabilidade da primalidade de m, não podemos afirmar que m é primo, pois existem os números de Carmichael, que são um problema para os testes de primalidade baseados no Pequeno Teorema de Fermat. Felizmente, os números de Carmichael são muito raros, de fato, entre 1 e 10^9 existem apenas 646 números de Carmichael ([10], página 110).

Logo, testar o Pequeno Teorema de Fermat para algumas bases $1 < a < m$ é uma boa estimativa probabilística para a primalidade do inteiro ímpar m. Para confirmar se um inteiro m é primo, satisfeito o Pequeno Teorema de Fermat para muitas bases, recomenda-se utilizar o Teste LBS.

Exemplo 2.52. *Vamos verificar se o número* 4294967297 *é primo. Observe que* $2^{4294967296} \equiv 1 \mod 4294967297$*, contudo, se testarmos mais uma base, obtemos que* $3^{4294967296} \equiv 3029026160 \not\equiv 1 \mod 4294967297$*. Logo,* 4294967297 *não é primo.*

Existem outros testes clássicos de primalidade, como os testes que são baseados no Teorema de Pocklington, veja página 39 de [29], e os testes que são baseados em sucessão de Lucas, veja página 41 e página 60 de [29]. Testes de primalidade específicos para os números de Fermat e os números de Mersenne também foram desenvolvidos, veja páginas 68 e 74, respectivamente, de [29].

Também existem testes de primalidade bastante sofisticados, como o Teste AKS desenvolvido por M. Agrawal, N. Kayal e N. Saxena, veja página 340 de [20]. Infelizmente esses testes fogem do escopo e espaço do presente trabalho, contudo, espera-se com os testes de primalidade acima apresentados, cumprir o objetivo de introduzir satisfatoriamente a percepção da diversidade e complexidade dos testes de primalidade.

Capítulo 3

No presente capítulo serão indicadas 11 atividades envolvendo os números primos que podem ser aplicadas no Ensino Fundamental II. No geral, um estudo mais aprofundado sobre os números primos ocorre no 6^{o} ano, contudo, as presentes atividades podem ser também utilizadas oportunamente nos demais anos do ensino fundamental. O tempo estipulado para cada atividade é de uma aula.

3.1 Atividade: desafio dos primos.

Objetivo da atividade: Identificar números primos; Desenvolver a habilidade de adição; Desenvolver o raciocínio lógico.
Conteúdos relacionados: Números primos; Lógica matemática.
Materiais: Fichas numeradas de 1 a 10.
Participantes: Um jogador.
Descrição da atividade:

Esta atividade pode ser encontrada em [3]. Neste jogo são utilizadas fichas numeradas de 1 a 10, o objetivo do jogo é dispor as fichas em um formato circular tal que a soma das fichas adjacentes seja um número primo, conforme imagem abaixo:

Figura 2: Ilustração do jogo.
Fonte: Página 2 de [3].

Existem várias maneiras de obter uma solução para o jogo, abaixo é apresentada uma das possibilidades:

Figura 3: Uma das soluções do jogo.
Fonte: Página 3 de [3].

É importante que o professor proporcione aos alunos as situações para perceberem as condições que os números adjacentes precisam satisfazer para que a soma seja um número primo, são elas:

1) Os números adjacentes não podem ser ambos pares, pois assim a soma será um número par maior que 2, isto é, não será um número primo;

2) Os números adjacentes não podem ser ambos ímpares, pois assim a soma será um número par maior que 2, isto é, não será um número primo;

3) Os números adjacentes devem ser de paridade oposta, ou seja, um número ímpar e um número par, assim a soma será um número ímpar, podendo neste caso ser primo.

O jogo acaba quando a solução for encontrada. Se o professor desejar é possível organizar competições entre os alunos para ver quem soluciona o jogo mais rapidamente.

3.2 Atividade: jogo de Crisson.

Objetivo da atividade: Identificar números primos; Desenvolver a habilidade de adição, subtração, multiplicação e divisão.

Conteúdos relacionados: Números primos; As quatro operações básicas.
Materiais: Folha sulfite com exemplares do jogo; lápis e borracha.
Participantes: Um jogador.
Descrição da atividade:

Esta atividade pode ser encontrada na página 69 de [11]. Neste jogo é entregue um exemplar, conforme imagem, para cada um dos alunos:

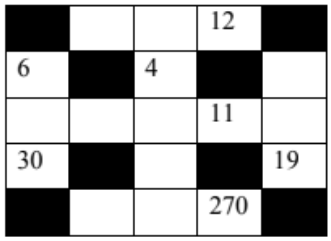


Figura 4: Exemplo da atividade.
Fonte: Página 69 de [11].

Os espaços em branco devem ser preenchidos com números seguindo as seguintes regras:

- Nas linhas, seguindo da esquerda para a direita, deve-se adicionar os dois números e o próximo será a soma desses;
- Nas linhas, seguindo da direita para a esquerda, deve-se subtrair os dois números e o próximo será a diferença desses;
- Nas colunas, seguindo de cima para baixo, deve-se multiplicar os dois números e o próximo será o produto desses;
- Nas colunas, seguindo de baixo para cima, deve-se dividir os dois números e o próximo será o quociente desses.

Desenvolvendo essas etapas, obtemos como resultado:

	10	2	12	
6		4		1
5	3	8	11	19
30		32		19
	14	256	270	

Figura 5: Exemplo da atividade resolvido.
Fonte: Página 69 de [11].

Para concluir a atividade, solicita-se para os alunos encontrarem os números primos que estão listados e destacá-los. Seguem mais dois exemplares para aplicação:

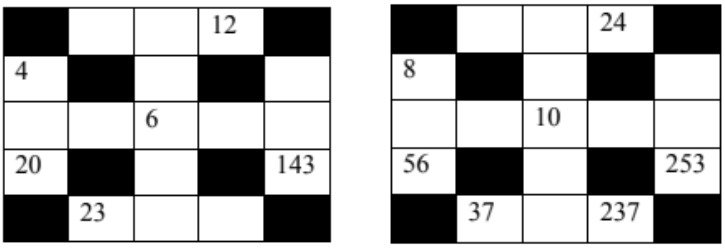


Figura 6: Exemplos da atividade.
Fonte: Páginas 69 e 70 de [11].

3.3 Atividade: descobrindo a senha.

Objetivo da atividade: Identificar números primos; Desenvolver a habilidade de fatoração.
Conteúdos relacionados: Números primos; Fatoração.
Materiais: Folha sulfite; Lápis ou caneta; Calculadora.
Participantes: Grupos de jogadores.
Descrição da atividade:

Esta atividade pode ser encontrada na página 66 de [11]. Divide-se os alunos em equipes, o objetivo do jogo é que cada equipe consiga desvendar uma senha que permite acessar uma mensagem secreta. Esse jogo pode ser realizado com um computador, onde a senha protege um arquivo com a mensagem, contudo, o professor também pode ser o portador da mensagem que será entregue somente há quem possuir a senha.

As mensagens devem ser desenvolvidas pelo professor, assim como as senhas que serão os algarismos de alguns números primos organizados em ordem crescente. Cada senha diferente corresponde a uma mensagem diferente e as equipes têm apenas uma tentativa para desvendar cada senha, podendo ser estipulado um tempo se o professor preferir. Ganha o jogo a equipe que conseguir decifrar o maior número de senhas.

Para cada senha será entregue uma pista, que é um número natural n tal que $n = p_1 \times p_2 \times ... \times p_r$; com p_i número primo para $i = 1, 2, ..., r$; onde a equipe buscará decompor o número n em fatores primos e descobrir a senha, organizando os fatores primos em ordem crescente.

Exemplo 3.1. *Se a pista é o número* 187*, usando a decomposição em fatores primos,*

temos que $187 = 11 \times 17$. *Portanto, a senha é formada pela sequência de algarismos* 1117.

Exemplo 3.2. *Se a pista é o número* 2024, *usando a decomposição em fatores primos, temos que* $2024 = 2 \times 2 \times 2 \times 11 \times 23$. *Portanto, a senha é formada pela sequência de algarismos* 2221123.

3.4 Atividade: mensagem secreta.

Objetivo da atividade: Identificar números primos; Desenvolver o raciocínio lógico.
Conteúdos relacionados: Números primos. Criptografia.
Materiais: Folha sulfite; Lápis ou caneta; Calculadora.
Participantes: Grupos de jogadores.
Descrição da atividade:

Nesta atividade é apresentada a seguinte tabela aos alunos, que constitui a cifra que será utilizada:

A	B	C	D	E	F	G	H	I	J	K	L	M
2	3	5	7	11	13	17	19	23	29	31	37	41
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
43	47	53	59	61	67	71	73	79	83	83	97	101

Figura 7: tabela para a cifra.
Fonte: Arquivo pessoal do autor.

Com a tabela acima os alunos podem criptografar e descriptografar mensagens de maneira simples, por exemplo, é entregue a seguinte mensagem criptografada: 24127111412712352132675234 32; quando os alunos descriptografarem essa mensagem obterão a frase: a matemática fascina.

O professor pode organizar várias mensagens para que os alunos descriptografem e criptografem. Em certas ocasiões os alunos podem ter dúvidas, por exemplo, se 23 corresponde à I ou à AB, mas compete ao aluno manter o sentido da frase, assim, ele saberá durante a descriptografia, através do sentido da frase, quais as letras que os números se referem.

Para saber mais sobre criptografia e verificar outras atividades, veja [27].

3.5 Atividade: teste de primalidade.

Objetivo da atividade: Identificar números primos; Compreender o funcionamento do teste de primalidade.
Conteúdos relacionados: Números primos e compostos; Divisão; Raiz quadrada.
Materiais: Folha sulfite ou caderno; Lápis ou caneta; Calculadora.
Participantes: Um jogador.
Descrição da atividade:

Para esta atividade, após o professor explicar o teste de primalidade, conforme abordado no Teorema 2.4, o professor deve solicitar para os alunos produzirem um fluxograma, conforme a imagem abaixo:

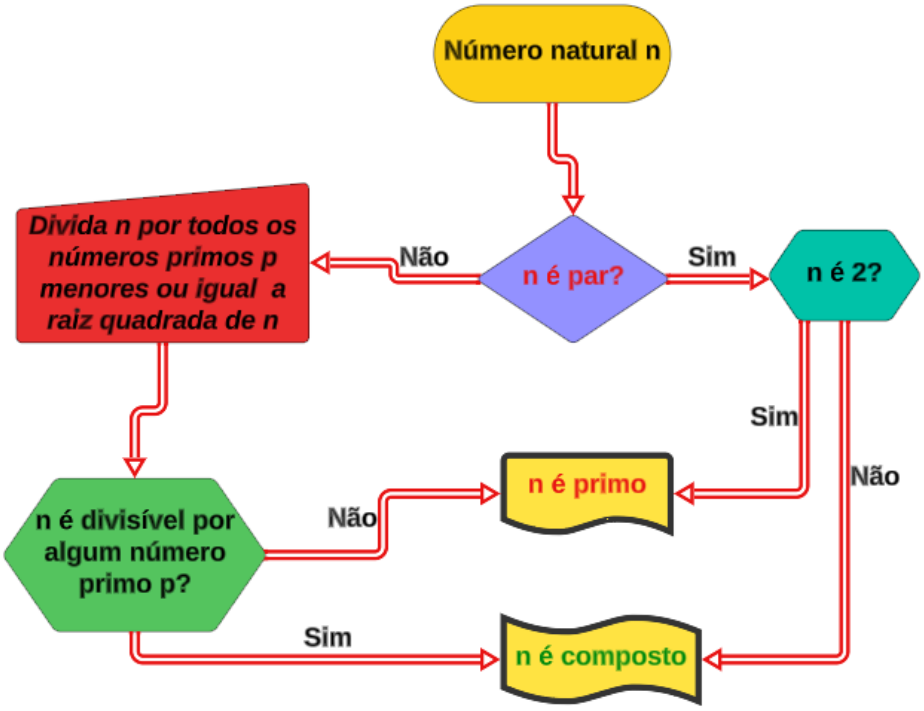


Figura 8: Fluxograma.
Fonte: Arquivo pessoal do autor.

Com posse do fluxograma os alunos executam os comandos do teste de primalidade para determinados números naturais n, conforme os exemplos abaixo.

Exemplo 3.3.

* ***Entrada:*** *número natural* 18*;*

* *É par? Sim;*

* *É 2? Não;*

* ***Saída:*** 18 *é composto.*

Exemplo 3.4.

* ***Entrada:*** *número natural* 37*;*

* *É par? Não;*

* *Quais os números primos menores ou igual a sua raiz quadrada?* 2, 3 *e* 5*;*

* *Algum número primo da etapa anterior divide o número? Não;*

* ***Saída:*** 37 *é primo.*

Exemplo 3.5.

* ***Entrada:*** *número natural* 51*;*

* *É par? Não;*

* *Quais os números primos menores ou igual a sua raiz quadrada?* 2, 3, 5 *e* 7*;*

* *Algum número primo da etapa anterior divide o número? Sim, o* 3*;*

* ***Saída:*** 51 *é composto.*

Uma atividade semelhante pode ser encontrada na página 85 de [28].

3.6 Atividade: jogo batalha naval com primos.

Objetivo da atividade: Identificar números primos; Compreender o sistema de localização ortogonal; Desenvolver o processo de fatoração em números primos.
Conteúdos relacionados: Números primos; Coordenadas ortogonais; Fatoração.
Materiais: Folhas do jogo; Lápis ou caneta.
Participantes: Dois jogadores.
Descrição da atividade:

Esta atividade é jogada em duplas e consiste em determinar a localização dos combatentes adversários e fazer com que o ataque seja eficiente através da determinação de certo número, escolhido pelo oponente, como primo, a unidade ou composto, neste

último caso indicando os fatores primos do número. Inicialmente, cada aluno recebe uma folha conforme imagem:

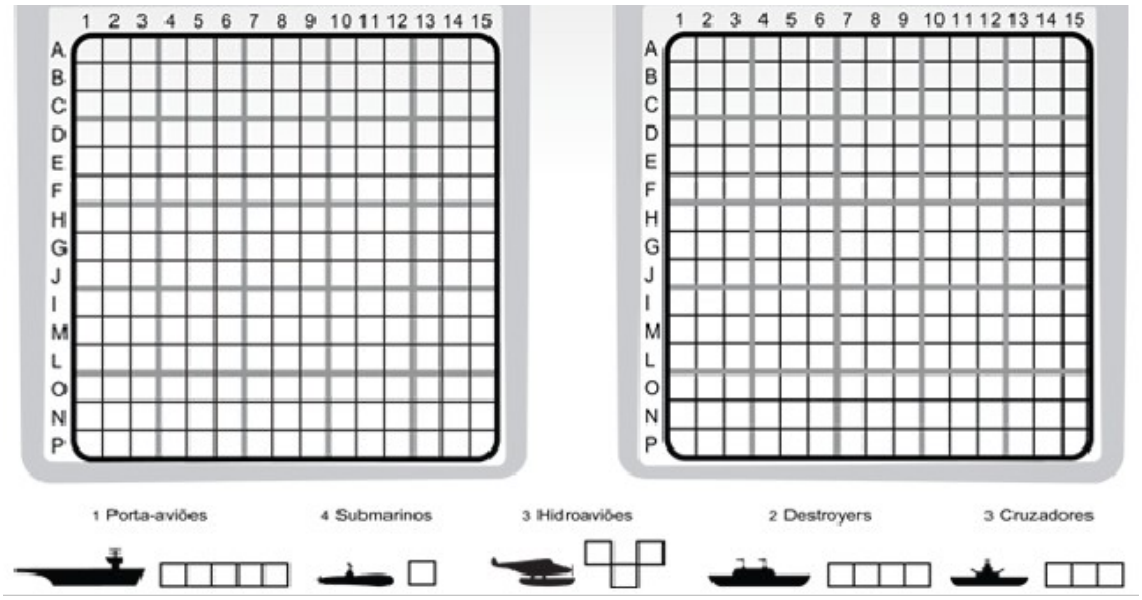


Figura 9: impressão para o jogo.
Fonte: https://www.researchgate.net/figure/Figura-1-Tabuleiro-de-Batalha-Naval-Fonte-wwwbleckimcom_fig1_294106402

Conforme a quantidade de quadradinhos necessários para cada um dos combatentes, os alunos organizarão a localização dos seus combatentes no seu tabuleiro, a quantidade de combatentes fica à critério do professor, por exemplo, 1 porta-aviões, 4 submarinos, 3 hidroaviões, 2 destroyers e 3 cruzadores.

Após localizar os seus combatentes, para cada coordenada ocupada, seguindo o sistema de coordenadas (número, letra), o aluno irá atribuir um número de 1 a 100 em cada coordenada ocupada, este número será a defesa contra os ataques inimigos. Assim, quando o aluno oponente acertar uma coordenada, por exemplo, $(7, D)$, o aluno dirá qual é o número que está na localização e o seu oponente terá que dizer se este número é a unidade, um número primo ou um número composto, nesse último caso, deverá dizer quais são os fatores primos do número.

Se o aluno oponente acertar a resposta, o seu combatente será atingido e destruído naquela coordenada, caso contrário, se o aluno oponente errar a resposta, o ataque foi repelido, isto é, o seu combatente permanece intacto, por exemplo, para $(7, D)$ o número é 62, assim o oponente terá sucesso no ataque se responder que o número é composto com fatores primos 2 e 31. O mesmo segue para ambos os alunos e vence quem conseguir destruir toda a frota inimiga.

Cabe ao professor fornecer as explicações complementares necessárias. Uma atividade similar, mas jogada online, pode ser encontrada em [31].

3.7 Atividade: jogo amarelinha dos primos.

Objetivo da atividade: Identificar números primos; Lógica matemática.
Conteúdos relacionados: Números primos; Lógica matemática.
Materiais: Folha sulfite com o jogo; Fichas para o posicionamento do jogador.
Participantes: Dois jogadores.
Descrição da atividade:

Esta atividade também pode ser encontrada na página 74 de [11]. Entrega-se aos alunos a folha do jogo com as fichas que serão utilizadas para marcar a posição de cada jogador, conforme imagem:

Jogador 1 

Jogador 2 

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

Figura 10: Folha para a amarelinha.
Fonte: Página 75 de [11].

Os jogadores partem da casa 1, o primeiro jogador pega uma ficha e coloca sobre um número primo que se localiza, no máximo, 5 casas da casa 1. O segundo jogador pega a ficha e move para um número primo maior do que o primo do primeiro jogador, que também se localiza, no máximo, 5 casas na frente de onde o primeiro jogador colocou a sua ficha.

O primeiro jogador, em seguida, move a ficha para um número primo novamente maior e que se localiza, no máximo, 5 casas na frente do primo do segundo jogador. O perdedor é o primeiro jogador que colocar a ficha em um número composto ou que fique incapaz de mover a ficha, seguindo as regras:

- A ficha não pode ser movida mais de 5 casas na frente;
- A ficha deve ser movida sempre até um número primo;
- A ficha não pode ser movida para trás e não pode ficar no mesmo lugar durante a sua jogada.

Um exemplo desse jogo está na imagem abaixo:

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

Figura 11: Exemplo da amarelinha.
Fonte: Página 74 de [11].

O jogador que dispor a sua ficha na casa 5 sempre ganhará o jogo, esse é um assunto que pode ser trabalhado pelo professor após a aplicação da atividade, indagando os alunos a explicarem esse fato.

3.8 Atividade: jogo de tabuleiro dos primos.

Objetivo da atividade: Diferenciar números primos e compostos; Desenvolver o raciocínio lógico; Desenvolver o conhecimento sobre os métodos de divisibilidade.
Conteúdos relacionados: Números primos e compostos.
Materiais: Tabuleiro com a folha do jogo; Dado; Peão ou semelhante.
Participantes: Um jogador.
Descrição da atividade:

O jogo é realizado em duplas, cada jogador posiciona o seu peão na "saída"do tabuleiro, decidido quem iniciará o jogo, joga-se o dado e anda o número de casas referente ao valor da face voltada para cima do dado.

O jogador da vez vai dizer se o número presente na casa que o seu peão parou é a unidade, número composto ou número primo, caso a resposta esteja correta o jogador

permanece na posição que está, caso a resposta esteja incorreta o jogador retorna para a posição de origem da jogada.

Cada aluno realiza uma jogada e passa a vez. Vence o jogador que primeiro chegar na marca de "chegada"do tabuleiro.

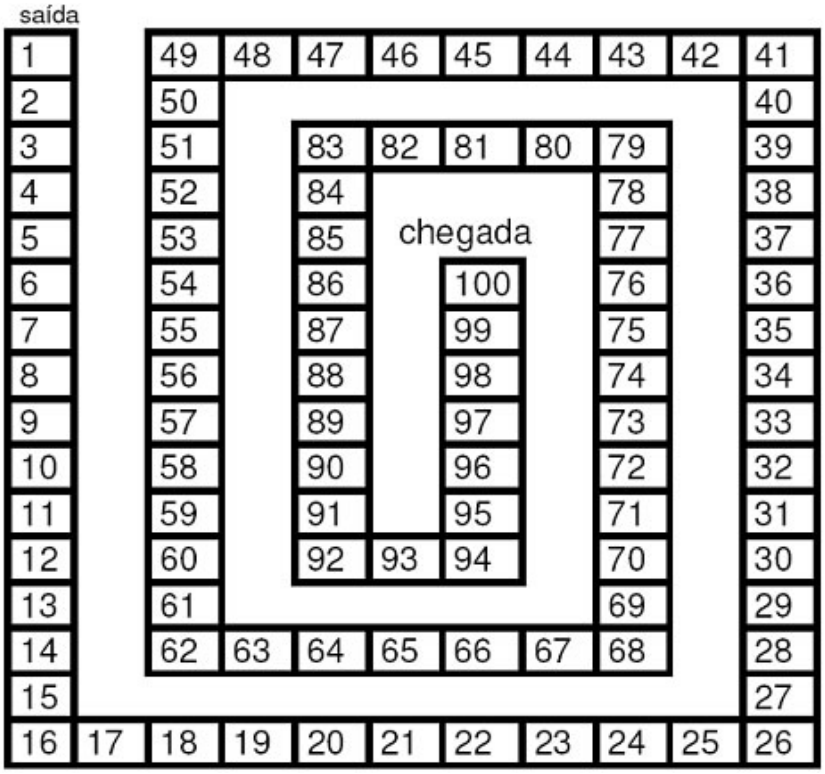


Figura 12: Superfície do tabuleiro.
Fonte: https://br.pinterest.com/pin/661888476457573224/

É possível, caso o professor desejar, organizar campeonatos entre os alunos com este jogo de tabuleiro, motivando os alunos a desenvolverem os seus conhecimentos por meio da competitividade. É preferível que o campeonato ocorra em grupos, igualando o nível dos grupos com uma distribuição adequada dos alunos, assim nenhum aluno fica desmotivado, podendo os alunos com habilidades semelhantes competirem entre si por seus grupos.

Uma atividade similar pode ser encontrada na página 51 de [26].

3.9 Atividade: crivo de Eratóstenes.

Objetivo da atividade: Identificar números primos; Desenvolver a habilidade de divisão e multiplicação; Conhecer um método simples para testar primalidade.

Conteúdos relacionados: Números primos; Fatoração; Multiplicação.
Materiais: Folha sulfite com números; Lápis de colorir.
Participantes: Um jogador.
Descrição da atividade:

Nesta atividade os alunos irão determinar os números primos menores e igual a 100 pelo crivo de Eratóstenes, mas pode-se utilizar outro valor para a atividade.

Cada aluno recebe uma folha com todos os números inteiros positivos menores e igual a 100 e desenvolve-se o método do crivo de Eratóstenes conforme foi descrito no exemplo do teste 1 de primalidade (Teorema 2.4) desse trabalho.

É interessante pedir para os alunos colorirem os números conforme realizam o crivo, escolhendo uma cor para os números primos, outra cor para o número 1, outra cor para os números eliminados na etapa dos múltiplos de 2, outra cor para os números eliminados na etapa dos múltiplos de 3, e assim sucessivamente.

Figura 13: Exemplo da atividade.
Fonte: Arquivo pessoal do autor.

Na atividade da figura acima os números primos foram coloridos de vermelho, a unidade foi colorida de azul (etapa 1), os números eliminados como múltiplos de 2 (etapa 2) foram coloridos de verde, os números eliminados como múltiplos de 3 (etapa 3) foram coloridos de amarelo, os números eliminados como múltiplos de 5 (etapa 4) foram coloridos de marrom e os números eliminados como múltiplos de 7 (etapa 5) foram coloridos de laranja.

Uma atividade similar pode ser encontrada na página 48 de [26].

3.10 Atividade: espiral de Ulam.

Objetivo da atividade: Identificar números primos; Observar conceitos sobre a distribuição dos números primos.
Conteúdos relacionados: Números primos.
Materiais: Folha sulfite; Lápis de colorir.
Participantes: Um jogador.
Descrição da atividade:

Nesta atividade os alunos determinarão os números primos que estão na lista, semelhante ao crivo de Eratóstenes, contudo, pode-se utilizar outro teste de primalidade, como a fatoração de Fermat (Teorema 2.6), contudo, poder-se-ia utilizar o crivo de Erastótenes também, apenas foi sugerido outro teste porque esta atividade não está atrelada ao desenvolvimento de um teste de primalidade específico, sendo a escolha do teste que será utilizado um critério do professor. Inicialmente os alunos recebem uma lista de números dispostos em espiral, conforme imagem abaixo:

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

Figura 14: Lista de números em espiral.
Fonte: Página 69 de [25].

Os alunos devem determinar quais são os números primos da lista e colori-los, conforme imagem abaixo, que apresenta os números primos coloridos de vermelho:

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

Figura 15: Espiral de Ulam.
Fonte: Página 70 de [25].

O professor deve indagar os alunos sobre possíveis padrões, a resposta esperada é que os números primos tendem a se concentrar em diagonais. Para fomentar o debate o professor pode apresentar uma espiral de Ulam mais ampliada, conforme a imagem, que é formada pelos números de 1 a 65025 e está com os números primos coloridos de vermelho:

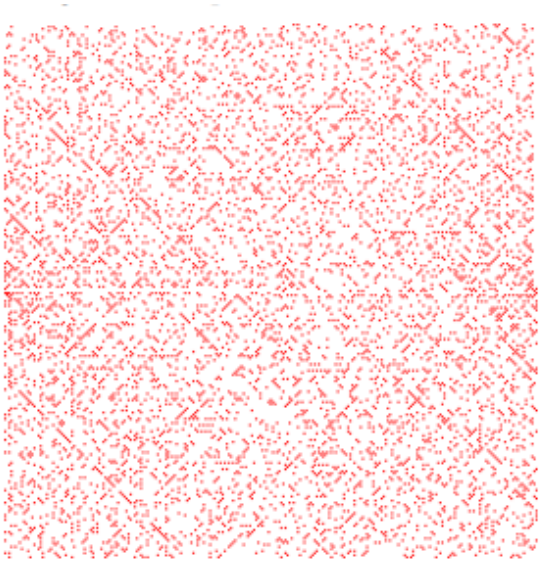


Figura 16: Espiral de Ulam ampliada.
Fonte: Página 70 de [25].

Observação 3.6. *A espiral de Ulam foi descoberta pelo matemático polonês Stanislaw Ulam em 1963, o mesmo constatou, conforme já foi comentado, que os números primos tendem a se concentrar em diagonais e esse padrão se mantêm conforme a espiral é ampliada, contudo, uma explicação para esse fato permanece em aberto.*

Para os alunos é importante o professor comentar sobre como os números primos se distribuem e a dificuldade de determinar o n-ésimo número primo através de um padrão, por mais que esse padrão de distribuição dos números primos seja existente. Para saber mais sobre a espiral de Ulam, veja [25].

3.11 Atividade: infinidade dos números primos.

Objetivo da atividade: Desenvolver o raciocínio lógico-dedutivo para a verificação de argumentos; Desenvolver a habilidade de divisão e multiplicação.
Conteúdos relacionados: Números primos; Lógica; Fatoração; Multiplicação.
Materiais: Feijão, fichas ou semelhante.
Participantes: Um jogador.
Descrição da atividade:

O objetivo desta atividade é mostrar a ideia da demonstração da infinidade dos números primos de Euclides aos alunos de uma maneira mais lúdica.

Com uma quantidade de feijão cada aluno, considera-se que o único número primo conhecido é o 2, então, os alunos selecionam 2 feijões e adicionam 1 feijão. Agora, com os 3 feijões, solicita-se que os alunos busquem dividir os 3 feijões em grupos com 2 unidades cada, os alunos constatarão que é impossível, portanto, pode-se formar apenas um grupo com as 3 unidades, assim, o número 3 é um número primo que era desconhecido.

Por conseguinte, se considera que os números primos conhecidos sejam o 2 e o 3, a sua multiplicação resulta em 6 e os alunos selecionam 6 feijões e adicionam 1 feijão, obtendo 7. Solicita-se aos alunos tentarem dividir os feijões em grupos de 2 unidades e depois em grupos de 3 unidades, eles perceberão que sempre resta 1, então, pede-se para tentarem dividir em grupos iguais com outros valores maiores que 1, eles observarão que não é possível, logo, pode-se formar apenas um grupo com as 7 unidades, conclui-se que 7 é um número primo que não era conhecido.

Para não demandar uma quantidade muito grande de feijões, pode-se solicitar multiplicações específicas entre dois números primos para os alunos, por exemplo, considerando os números primos 2 e 7, que já são conhecidos, multiplicando os primos obtemos 14 e adicionando 1 resulta em 15 feijões selecionados, pede-se para os alunos dividirem os feijões em grupos de 2 unidades e depois em grupos de 7 unidades, eles perceberão que sempre resta 1, então, solicita-se para tentarem dividir na menor quantidade de grupos iguais com outros valores maiores que 1. Os alunos encontrarão 3 grupos com 5 unidades, logo, 5 é um número primo que não era conhecido.

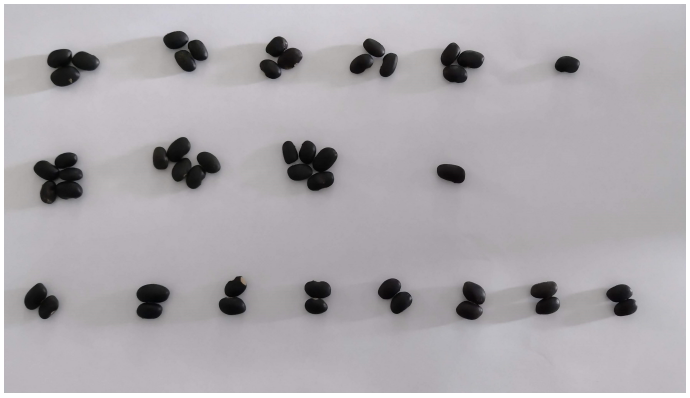


Figura 17: Exemplo da atividade.
Fonte: Arquivo pessoal do autor.

A atividade pode seguir com outros valores, por exemplo, os números primos 2 e 5, e assim sucessivamente. Pode-se solicitar que os alunos anotem os resultados obtidos e posteriormente justifiquem o que está ocorrendo, buscando que deduzam o raciocínio da demonstração da infinidade dos números primos.

Após a realização da atividade, o professor deve indagar os alunos sobre o que ocorreria se multiplicarmos uma quantidade qualquer de números primos conhecidos e adicionarmos 1 unidade, segundo a atividade realizada, os alunos devem responder que seria encontrado um novo número primo. A ideia da demonstração por absurdo é inserida pelo professor e a conclusão da infinidade dos números primos é obtida com a participação dos alunos.

Pretende-se que os alunos percebam que independentemente de quantos números primos considerarmos, se deduzirmos que existe apenas uma quantidade finita instituída, sempre encontraremos, pelo processo apresentado, um número primo que era desconhecido inicialmente.

Essa atividade foi baseada na ilustração apresentada por Marcus du Sautoy no documentário da BBC, a música dos números primos, que pode ser encontrado em [4].

Considerações Finais

Os números primos reservam muitas propriedades interessantes, conjecturas e mistérios que transcendem as breves páginas do presente trabalho.

Existem diversas demonstrações da infinidade dos números primos que não foram, por força maior, apresentadas no primeiro Capítulo do presente trabalho, ainda assim, é possível perceber a diversidade das demonstrações da infinidade dos números primos existentes, essas demonstrações percorrem diversas áreas da matemática e apresentam variados níveis de dificuldade. No artigo de R. Meštrović, publicado em 2023, é apresentado um levantamento com catalogação bibliográfica de 200 diferentes demonstrações da infinidade dos números primos, veja [21].

Os princípios envolvidos nos clássicos testes de primalidade foram abordados no segundo Capítulo desse trabalho, contudo, os testes apresentados apesar de clássicos e excelentes para introduzir a teoria envolvida nos processos de verificação da primalidade de números inteiros, são testes computacionalmente ultrapassados e pouco eficientes, logo, espera-se que após uma leitura do presente trabalho o leitor interessado investigue os testes de primalidade mais modernos e úteis, como o Teste Probabilístico de Miller-Rabin, veja página 332 de [20], e o Teste AKS, veja página 340 de [20].

Por fim, as atividades apresentadas no terceiro Capítulo se destinam a complementar a teoria através de algumas atividades destinadas à sala de aula, obviamente essa amostra de atividades não extingue as imensas possibilidades existentes para abordar os números primos na educação básica.

Para um aprofundamento sobre o assunto apresentado, uma consulta atenta às referências utilizadas é recomendada. Frases de efeito são destinadas à grandes autores, mas é consenso para todos os matemáticos dedicados ao estudo dos números primos que: os números primos são as partículas de Deus na matemática.

Referências Bibliográficas

[1] AIGNER, M; ZIEGLER, G. *Paul Erdös: as mais belas demonstrações matemáticas*, 5° ed. Berlin: Editora Blucher, 2017.

[2] ALFORD, W; GRANVILLE, A. E. A. There are infinitely many carmichael numbers. *Annals of Mathematics 139* (1994), 703–722.

[3] BARRIENTOS, A. N; VERGARA, C. G. E. A. *Desafio dos Primos*. Portal OBMEP: Quebras cabeças de matemática - Nível de Dificuldade 2. Rio de Janeiro: IMPA, 2020.

[4] BBC. *The Music of the Primes*. Documentário apresentado por Marcus du Sautoy, 2007.

[5] BICUDO, I. *Os elementos - Euclides*, 1 ed. São Paulo: Unesp, 2009.

[6] BRASIL. Base nacional comum curricular (bncc). *Ministério da Educação. Brasília: MEC* (2018).

[7] BUCK, R. Solution to problem 4072. *The American Mathematical Monthly 51* (1944), 409–410.

[8] CINTRA, D. Uma coleção de demonstrações da existência de infinitos primos. *Matemática e Estatística em Foco 6* (2019), 34–43.

[9] COSTA, A. I. *Uma demonstração do teorema fundamental da álgebra*. Dissertação (Mestrado Profissional em Matemática em Rede Nacional), Universidade Federal de São Carlos, São Carlos, 2016.

[10] COUTINHO, S. C. *Números inteiros e criptografia RSA*, 2 ed. Rio de Janeiro: IMPA, 2005.

[11] FARIAS, D. G. *Um estudo do ensino de números primos na Educação Básica*. Dissertação (Mestrado Profissional em Matemática em Rede Nacional), Universidade Federal de Alagoas, Maceió, 2016.

[12] FIGUEIREDO, D. *Números irracionais e transcendentes.*, 3 ed. Rio de Janeiro: SBM, 2002.

[13] FONSECA, R. V. *Teoria dos números*, 1 ed. Belém: UEPA, 2011.

[14] GOMES, O.; SILVA, J. *Estruturas algébricas para licenciatura: introdução à teoria dos números*, 1 ed. Brasília: Ed. do Autor, 2008.

[15] GRANVILLE, A. A panopoly of proofs that there are infinitely many primes. *London Mathematical Society Newsletter 472* (2017), 23–27.

[16] HEFEZ, A. *Aritmética*, 2 ed. Rio de Janeiro: SBM, 2016.

[17] LEITHOLD, L. *Cálculo com Geometria Analítica*, 3 ed., vol. 1 e 2. São Paulo: Harbra Ltda, 1994.

[18] LIMA, E. *Elementos de topologia geral*, 1 ed. Rio de Janeiro: IMPA, 1970.

[19] LIMA, E. *Números e funções reais*, 1 ed. Rio de Janeiro: SBM, 2013.

[20] MARTINEZ, F; MOREIRA, C. E. A. *Teoria dos Números: um passeio com primos e outros números familiares pelo mundo inteiro*, 4 ed. Rio de Janeiro: IMPA, 2015.

[21] MEŠTROVIĆ, R. Euclid's theorem on the infinitude of primes: a historical survey of its 200 proofs (300 bc-2022). *arXiv:1202.3670v4* (2023).

[22] NARKIEWICZ, W. *The development of prime number theory: from Euclid to Hardy and Littlewood*, 1 ed. Berlin: Springer Science, 2000.

[23] NORTHSHIELD, S. A one-line proof of the infinitude of primes. *The American Mathematical Monthly 122* (2015), 466–466.

[24] OLIVEIRA SANTOS, J. P. *Introdução à Teoria dos Números*, 3 ed. Rio de Janeiro: IMPA, 2020.

[25] PEDROZA, P. A. *Distribuição de Números Primos, Padrões Gráficos e a Espiral de Ulam*. Dissertação (Mestrado Profissional em Matemática em Rede Nacional), Universidade Federal Rural de Pernambuco, Recife, 2020.

[26] PEREIRA, A. L. *Números primos e a conjectura de Goldbach*. Dissertação (Mestrado Profissional em Matemática em Rede Nacional), Universidade Federal do ABC, Santo André, 2017.

[27] PEREIRA, R. S. R. *Criptografia: proposta de atividades para o ensino básico.* Dissertação (Mestrado Profissional em Matemática em Rede Nacional), Universidade Estadual de Mato Grosso do Sul, Dourados, 2020.

[28] QUEIROZ, N. *O problema da primalidade: alguns testes e uma proposta de situação de aprendizagem.* Dissertação (Mestrado Profissional em Matemática em Rede Nacional), Universidade Federal de São Carlos, São Carlos, 2021.

[29] RIBENBOIM, P. *Números primos: velhos mistérios e novos recordes*, 1 ed. Rio de Janeiro: IMPA, 2012.

[30] RIEMANN, B. Ueber die anzahl der primzahlen unter einer gegebenen grösse. *Monatsberichte der Berliner Akademie* (1859).

[31] SILVA, R. Jogo matemático batalha naval com números primos. *WebSite: Os fantásticos números primos* (2019).

[32] VIEIRA, L.; FEITOZA, L. E. A. Introdução aos números transcendentes e aos números de liouville. *Professor de Matemática Online 7* (2019), 77–94.

[33] WEGENER, D. Primitive pythagorean triples and the infinitude of primes. *The Fibonacci Quarterly 19* (1981), 449–450.

[34] WHANG, J. Another proof of the infinitude of the prime numbers. *The American Mathematical Monthly 117* (2010), 181–181.