UNIVERSIDADE ESTADUAL DO MARANHÃO – UEMA
PRÓ-REITORIA DE PÓS-GRADUAÇÃO – PPG

PROFMAT

PROGRAMA DE MESTRADO PROFISSIONAL EM MATEMÁTICA EM REDE NACIONAL/PROFMAT

MARLON MAIKO BARROS MARTINS

TESTES DE PRIMALIDADE:
dos métodos tradicionais aos computacionais

São Luís
2021

MARLON MAIKO BARROS MARTINS

TESTES DE PRIMALIDADE:
dos métodos tradicionais aos computacionais

Dissertação apresentada ao Programa de Mestrado em Matemática em Rede Nacional (PROFMAT) da Universidade Estadual do Maranhão (UEMA), como requisito parcial para obtenção do título de Mestre em Matemática.

Orientador: Prof. Dr. Raimundo José Barbosa Brandão.

São Luís

2021

Martins, Marlon Maiko Barros.
Testes de primalidade: dos m¶todos tradicionais aos computacionais / Marlon Maiko Barros Martins. ¯ S² o Luºs, 2021.

86 f.

Disserta´² o (Mestrado Profissional) ¯ Curso de Matem®tica em Rede Nacional, Universidade Estadual do Maranh² o, 2021.

Orientador: Prof. Dr. Raimundo Jos¶ Barbosa Brand² o.

1.Testes de primalidade. 2.Nßmeros primos. 3.Era Pr¶-computacional. 4.Era Computacional. 5.Algoritmo Computacional. I.Tºtulo.

CDU: 511

Elaborado por Giselle Fraz² o Tavares - CRB 13/665

MARLON MAIKO BARROS MARTINS

TESTES DE PRIMALIDADE:

dos métodos tradicionais aos computacionais

Dissertação apresentada ao Programa de Mestrado em Matemática em Rede Nacional (PROFMAT) da Universidade Estadual do Maranhão (UEMA), como requisito parcial para obtenção do título de Mestre em Matemática.

Aprovada em: 26/08/2021

BANCA EXAMINADORA

Prof. Dr. Raimundo José Barbosa Brandão (orientador)
Universidade Estadual do Maranhão (UEMA)

Prof. Dr. Marlon César Oliveira Santos (examinador interno)
Universidade Estadual do Maranhão (UEMA)

Prof.ª Dra. Liamara Scortegagna (examinadora externa)
Universidade Federal de Juiz de Fora (UFJF)

Dedico este trabalho ao meu filho Marlon Lorenzo de Oliveira Martins, por sua vinda ao mundo ter servido de reavivamento e fortalecimento de minhas ações de trabalho e estudo.

AGRADECIMENTOS

Aos meus honrados pais, Rafael Bispo Martins e Beatriz de Araújo Barros, pelo apoio constante e estrutura de estudo que me ofertaram ao longo de minha vida;

À minha querida esposa, Ida Valéria Nunes de Oliveira, pelo apoio constante em meus estudos e compreensão nos momentos de distanciamento necessário ao alcance de minhas metas estudantis;

Aos meus amados filhos, Iasmim Rafaele de Oliveira Martins e Marlon Lorenzo de Oliveira Martins, pela companhia e alegrias obtidas dos felizes momentos convividos;

Ao Prof. Dr. João Coelho Silva Filho, pela sua incansável luta na Coordenação do Programa de Mestrado Profissional em Matemática em Rede Nacional (PROFMAT-UEMA), em prol do bom desenvolvimento e constante aprimoramento do programa;

Ao corpo administrativo do PROFMAT-UEMA, em especial à Annanda Crystina Chagas Santos, pelo seu empenho e prestatividade no atendimento das demandas dos alunos;

Ao Prof. Dr. Raimundo José Barbosa Brandão, pela sua eficiente orientação e disponibilização de atenção em todos os momentos necessários, atributos estes indispensáveis para a produção e conclusão da presente pesquisa;

Ao corpo diretivo, docente e administrativo da Universidade Estadual do Maranhão (UEMA), pela firme e competente atuação durante a execução de cada etapa do PROFMAT;

Aos meus companheiros de mestrado, pelos bons momentos vividos e pela cooperação nos estudos que, mesmo em face ao momento pandêmico vivido durante a disseminação do coronavírus (SARS-COV-2), entre os anos de 2020 e 2021, não deixaram de manter a coesão e companheirismo no transcurso do PROFMAT;

E a todos aqueles que, de alguma forma, colaboraram com a realização do curso e com a concretização do presente trabalho.

“Um problema da teoria dos números é tão atemporal quanto uma verdadeira obra de arte”.

David Hilbert

RESUMO

O presente estudo teve como finalidade apresentar alguns dos principais testes de primalidade desenvolvidos ao longo da história, com detalhamento de suas características gerais, custos computacionais, tempos de execução, dentre outros aspectos. A metodologia utilizada foi a pesquisa bibliográfica e o objetivo geral consistiu em analisar o funcionamento dos testes de primalidade desde sua concepção mais simples até os modernos mecanismos de localização de números primos. A dissertação do assunto modulou-se na apresentação dos primos, abordando conceitos básicos, quantidade destes e fórmulas para sua localização. Estudou-se, ainda, os aspectos básicos dos testes de primalidade, em seguida comparou-se as capacidades humanas com as computacionais e então apontou-se características necessárias para sua classificação. Os testes foram divididos em dois grupos, conforme duas grandes eras: a pré-computacional e a computacional. A análise dos testes incluiu aspectos como tempo de execução, grau de determinação e tipo de número testado. Por fim, tratou-se das principais aplicações dos testes de primalidade no campo da criptografia. Por efeito da análise dos resultados, inferiu-se que os testes de primalidade constituem um relevante método de localização de primos, cuja evolução resultou em algoritmos mais ágeis e eficientes, apoiados no grande avanço computacional das últimas décadas, com tendência ao desenvolvimento contínuo e produção de formas de identificar primos cada vez mais hábeis.

Palavras-chave: Testes de Primalidade. Números Primos. Era Pré-computacional. Era Computacional. Algoritmo Computacional.

ABSTRACT

The present study aimed to introduce some of the main primality tests developed throughout history, with details of their general characteristics, computational costs, execution times, among other aspects. The methodology used was bibliographical research and the general objective was to analyze the functioning of primality tests from their simplest conception to modern mechanisms of location of prime numbers. The dissertation of the subject was modulated in the presentation of primes, presenting basic concepts, quantity of these and formulas for their location. The basic aspects of primality tests were also studied, then human and computational capacities were compared and the characteristics necessary for their classification were pointed out. The tests were divided into two groups, according to two major eras: pre-computational and computational. The analysis of the tests included aspects such as runtime, degree of determination, and type of number tested. Finally, were presented the main applications of primality tests in the field of cryptography. In reason of the analysis of the results, it was inferred that primality tests constitute a relevant method of primes locating, whose evolution resulted in more agile and efficient algorithms, supported by the great computational advance of recent decades, with a tendency to continuous development and production of ways to identify increasingly skilled primes.

Keywords: Primality Tests. Prime Numbers. Pre-Computational Age. Computational Age. Computational Algorithm.

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO

Os números, quando concebidos em sua forma mais comum, remontam à ideia de contagem, um raciocínio natural para quem inicia seu processo de aprendizado em matemática. Na medida que o conhecimento se expande, o indivíduo passa a perceber que o ato de contar pode ser realizado de diversas formas, como o natural raciocínio de agrupar elementos de um conjunto para computar a quantidade destes de maneira mais ágil.

A atividade de juntar membros de um grupo para dar maior celeridade à sua contagem pode parecer relativamente simples, entretanto a ação inversa, em diversos casos, é, contrariamente, complexa. Dessa maneira, para conjuntos com grandes quantidades de elementos, a tarefa de encontrar todos os subconjuntos de mesmo tamanho que dividem exatamente aqueles pode representar um ato bem complicado, especialmente quando não se dispõe de ferramentas adequadas.

Neste raciocínio, destacamos os números primos, um tipo peculiar de conjunto que não pode ser repartido em grupos menores, com exceção do unitário e daqueles com iguais números de elementos, ou seja, só podem ser divididos por um e por eles mesmos.

Logo, diante da necessidade de apresentar e esclarecer o funcionamento dos métodos de localização de primos, realizamos o presente estudo, por meio de pesquisa bibliográfica, apoiado nos avanços obtidos no estudo destes números ao longo da história, o qual buscará identificar os testes de primalidade já desenvolvidos e analisar o desempenho destes, desde sua concepção mais simples até suas formas mais aprimoradas.

O trabalho buscou apresentar as propriedades dos primos e sua forma de localização; analisar os resultados de pesquisas sobre estes números e suas implicações na produção de métodos para sua localização; esclarecer as características de funcionamento dos testes de primalidade, bem como sua evolução; detalhar aspectos básicos dos algoritmos de localização de primos; apresentar testes de primalidade desenvolvidos ao longo da história; discorrer sobre os modernos processos computacionais voltados à procura de primos cada vez maiores e, por fim, exibir as principais aplicações dos testes de primalidade.

O trabalho estruturou-se primeiramente na apresentação dos números primos, com sua conceituação, propriedades e teoremas. Posteriormente, foram apontadas algumas formas de localizá-los e exibir determinadas fórmulas e funções geradoras destes números.

No intuito de detalhar os testes de primalidade, adotou-se uma apresentação por meio de uma linha histórica, delineando sua evolução deste a época da antiga Grécia até os tempos dos modernos computadores, com abordagem aos sofisticados conceitos matemáticos.

Detalhou-se características básicas dos testes de primalidade, expondo sua evolução de acordo com a capacidade do ser humano e da máquina. Destacou-se, também, seus custos computacionais e sua classificação de acordo com a garantia de identificação de primos.

Abordou-se diversos testes atrelados à linha evolutiva do progresso tecnológico. Neste sentido, reunimos alguns dos principais testes apresentados ao longo da história, a saber: a *Divisão por Tentativa*, o *Crivo de Eratóstenes*, o *Teste de Fermat*, o *Teste de Proth*, o *Teste de Pépin*, o *Teste de Lucas-Lehmer* e o *Crivo de Sundaram*, todos da era pré-computacional. Em seguida, expusemos os testes modernos da época computacional, entre eles o *Teste de Solovay-Strassen*, o *Teste de Miller-Rabin* e o *Teste AKS*, além de outros métodos computacionais também recentes, como o *Teste de Baillie – PSW*, o *Teste APR* e o *Teste ECPP (Eliptic Curve Primality Proving*).

Por fim, discorremos sobre as principais aplicações encontradas para os testes de primalidade atuais, que se apoiam no fato da difícil tarefa de fatoração continuar sendo um desafio para os estudiosos da contemporaneidade.

2 PROCEDIMENTOS METODOLÓGICOS

O processo de compreensão conceitual e procedimental para identificar números primos representa um grande desafio no ramo da Teoria dos Números. Quem inicia o estudo dos números primos precisa compreender suas características e saber identificar detalhes da matéria, aprofundando-se em aritmética, de forma a explorar argumentações, demonstrações, provas e usos específicos.

Da antiguidade ao mundo moderno, foram muitos os estudos buscando testes que comprovem a primalidade de um número natural. Após a seleção dos testes de primalidade a serem investigados, escolheu-se o tema deste trabalho, seguido pelo levantamento bibliográfico por meio de leituras de livros, artigos físicos e online, periódicos, dentre outros.

Este trabalho modulou-se em obras de autores renomados, como Coutinho e Ribenboim, que tratam de testes de primalidade sob diversos pontos de vista, como os métodos com uso de exponenciação, necessidade ou não de fatoração, algoritmos determinísticos e não determinísticos etc. Representa também uma continuidade das pesquisas com temas direcionados à localização de primos, encontradas em bancos de trabalhos acadêmicos, incluindo o repositório de dissertações do PROFMAT.

A metodologia utilizada foi a pesquisa bibliográfica, que representa uma etapa essencial de todo trabalho científico e exerce grande influência nas fases de uma investigação, ao passo que fundamenta teoricamente o objeto de estudo.

A pesquisa bibliográfica, na visão de Fonseca (2002):

> É feita a partir do levantamento de referências teóricas já analisadas, e publicadas por meios escritos e eletrônicos, como livros, artigos científicos, páginas de web sites. Qualquer trabalho científico inicia-se com uma pesquisa bibliográfica, que permite ao pesquisador conhecer o que já se estudou sobre o assunto. Existem, porém, pesquisas científicas que se baseiam unicamente na pesquisa bibliográfica, procurando referências teóricas publicadas com o objetivo de recolher informações ou conhecimentos prévios sobre o problema a respeito do qual se procura a resposta (FONSECA, 2002, p. 32).

A fim de garantir uma sólida base referencial, procurou-se fazer um levantamento de literatura de autores reconhecidos na temática, tanto no cenário nacional quanto internacional. Nas consultas de publicações na internet, fez-se uma seleção criteriosa de dissertações, revistas, teses, livros digitalizados, dentre outros. Para assegurar a qualidade da pesquisa bibliográfica, as teses e dissertações foram buscadas no banco de dados da Coordenação de Aperfeiçoamento de Pessoal de

Nível Superior (CAPES), no sítio eletrônico do PROFMAT, na Biblioteca Digital Brasileira de Teses e Dissertações (BDTD), entre outros.

3 SOBRE OS NÚMEROS PRIMOS

3.1 Números naturais

A fim de estudar detalhadamente os primos e os métodos para sua localização, vamos conhecer um pouco sobre o conjunto dos naturais. A aparente simplicidade destes números pode esconder importantes questões com elevados níveis de complexidade. Nesse sentido, destacamos o estudo da Teoria dos Números que, resumidamente, discorre acerca da propriedade dos números inteiros positivos. Sobre essa matéria, Stewart (2014) relata que:

> Os números naturais 1, 2, 3, 4, 5... são claros, sem enfeites. Pode haver algo mais simples? Mas o exterior de simplicidade esconde profundezas ocultas, e muitas das mais desconcertantes questões em matemática abordam as propriedades aparentemente diretas dos números inteiros. Essa área é conhecida como *teoria dos números*, e acaba se mostrando difícil exatamente porque seus ingredientes são tão básicos (STEWART, 2014, p. 88).

O conjunto dos números naturais é intuitivamente um dos conceitos mais triviais do estudo da matemática. Associados à ideia de contagem, estes algarismos proporcionam uma imediata noção de quantidade ao relacionar os elementos deste conjunto com os objetos quantificados. Vejamos sua representação:

$$\mathbb{N} = \{1,2,3,4,5, \dots\}$$

O conjunto dos naturais foi caracterizado com precisão no início do século passado, conforme exposto por Lima (2013, p. 23): “Decorridos muitos milênios, podemos hoje descrever concisa e precisamente o conjunto $\mathbb{N}$ dos números naturais, valendo-nos da notável síntese feita pelo matemático italiano Giuseppe Peano no limiar do século 20”.

Assistamos, agora, os quatro axiomas de Peano:

1. Seja n um número natural, então n possui um único sucessor;
2. Dados m e n naturais, se $n \neq m$, então o sucessor de n é diferente do sucessor de m;
3. O número natural m, representado por 1, é o único natural que não é sucessor de nenhum outro;
4. Dado o conjunto A, com $A \subset \mathbb{N}$. Se $1 \in A$ e se o sucessor de todo elemento de A pertence a A, então $A = \mathbb{N}$.

O *axioma da indução,* largamente utilizado em demonstrações, é baseado no quarto axioma de Peano. Este método é capaz de provar que no conjunto dos números naturais estão definidas as operações de adição e multiplicação, ou seja, para a e b naturais, temos $(a, b) \mapsto a + b$ e $(a, b) \mapsto a \cdot b$.

As operações de adição e multiplicação possuem as seguintes propriedades, também provadas pelo axioma da indução[1]:

1. Comutatividade: se a e b são números naturais, então $a + b = b + a$ e $a \cdot b = b \cdot a$

2. Associatividade: se a, b e c são números naturais, então $a + (b + c) = (a + b) + a$ e $a \cdot (b \cdot c) = (a \cdot b) \cdot c$

3. Distributividade: se a, b e c são números naturais, então $a \cdot (b + c) = a \cdot b + a \cdot c$

4. Lei de Corte para Adição: se a, b e c são números naturais e $a + b = c + b$, então $a = c$

5. Lei de Corte para Adição: se a, b e c são números naturais e $a + b = c + b$, então $a = c$

Outra importante propriedade do conjunto dos números naturais é a relação de ordem, assim definida: dados a e b naturais, diz-se que $a \leq b$ (a é menor do que ou igual a b) para indicar que existe um c natural, tal que $b = a + c$.

A partir desta relação, verifica-se as propriedades a seguir, provadas mais uma vez com ou auxílio do axioma da indução:

1. Tricotomia: para a e b naturais, somente uma das possibilidades é verdadeira:

$$a < b$$

$$b < a$$

$$a = b$$

2. Transitividade da Relação de Ordem: sejam a, b e c naturais, se $a < b$ e $b < c$, então $a < c$

3. Monotonicidade: sejam a, b e c naturais, se $a < b$, então $a + c < b + c$ e $a \cdot c < b \cdot c$

4. Lei de Corte para Desigualdades:

[1] As demonstrações podem ser verificadas no capítulo 2 da obra de Lima (2013).

4.1. Se a, b e c são números naturais e $a + c < b + c$ então $a < b$

4.2. Se a, b e c são números naturais e $a \cdot c < b \cdot c$ então $a < b$

5. Princípio da Boa Ordenação: dado um conjunto não vazio $X \subset \mathbb{N}$. Todo conjunto X possui um menor elemento.

3.2 Conceitos iniciais sobre primos

No conjunto dos números naturais, um importante conjunto é notadamente importante, os números primos, representantes da base de formação dos demais elementos. Um número primo é aquele que só pode ser dividido por um e por si mesmo, conforme destacado por Hefez (2014, p. 140), ao definir que:

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

Se um natural $n > 1$ não é *primo,* dizemos que n é *composto*. A partir da definição de primo, um resultado básico, mas não menos importante, é o lema exposto abaixo:

Lema 1. Todo número par maior que 2 é composto.

Demonstração. Se n é um número par, então pode ser escrito na forma $2k$, com $k \in \mathbb{N}$, como n é maior que 2, então $n > 2 \Rightarrow 2k > 2 \Rightarrow k > 1$, então $2k$ possui no mínimo os divisores 1, 2 e $2k$, logo, por definição, é composto.

Os primos são costumeiramente chamados de *átomos da aritmética*, já que representam o seu sustentáculo, posto que a construção dos números naturais depende de fatores primários. Sautoy (2007) relata que este fato, há milênios, foi provado pelos gregos, conforme trecho a seguir:

> Os gregos da Antiguidade [...] descobriram, no quarto século a.C., a capacidade dos primos de servir como blocos de construção para todos os números. Eles perceberam que todo número podia ser gerado pela multiplicação de números primos. Embora os gregos acreditassem erroneamente que fogo, ar, água e terra fossem os elementos constitutivos da matéria, foram precisos ao identificar os átomos da aritmética (SAUTOY, 2007, p. 31).

Este pensamento nos leva a um dos mais importantes resultados da Teoria dos Números, o Teorema Fundamental da Aritmética, que afirma o seguinte:

Teorema 1. Todo número inteiro maior do que 1 é escrito de forma única (com exceção da ordem dos fatores) como um produto de fatores primos.

Demonstração. Dado um número natural n maior do que 1, se n for primo, não há o que se provar. Se n for composto e $m_1 > 1$ for o menor fator positivo de n, portanto primo, então ele pode ser decomposto em $n = m_1 \cdot a_1$. Se a_1 for primo, a prova estará completa, se for composto, então ele possui m_2 como menor fator positivo primo, assim $a_1 = m_2 \cdot a_2$, logo $n = m_1 \cdot m_2 \cdot a_2$. Mantendo o raciocínio e sabendo que n possui um número de fatores finitos, temos $n = m_1 \cdot m_2 \cdot m_3 \cdot m_4 \cdot \ldots \cdot m_n$, e como estes fatores não são essencialmente distintos, representamos n como $n = {m_1}^{k_1} \cdot {m_2}^{k_2} \cdot {m_3}^{k_3} \cdot {m_4}^{k_4} \cdot \ldots \cdot {m_n}^{k_n}$, logo n é formado por um produto de fatores primos.

Quanto à unicidade, podemos prová-la por indução, da seguinte maneira: para $n = 2$, prova-se claramente a unicidade. Supondo sua validade para inteiros maiores que 1 e menores que n, vamos provar sua validade para valores iguais à n. Se n é primo, a prova se verifica claramente. Se n é composto, consideremos que tenha duas fatorações, a saber, $n = m_1 \cdot m_2 \cdot m_3 \cdot m_4 \cdot \ldots \cdot m_q = r_1 \cdot r_2 \cdot r_3 \cdot r_4 \cdot \ldots \cdot r_s$, com m_q e r_s primos. Devemos provar que $q = s$ e que $m_i = r_j$ são iguais, um a um. Como $m_1 | r_1 \cdot r_2 \cdot r_3 \cdot r_4 \cdot \ldots \cdot r_s$, então $m_1 | r_j$. Sem perda de generalidade, iremos supor $m_1 | r_1$. Como m_1 e r_1 são primos, então $m_1 = r_1$. Reordenando os termos, temos $m_2 \cdot m_3 \cdot m_4 \cdot \ldots \cdot m_q = r_2 \cdot r_3 \cdot r_4 \cdot \ldots \cdot r_s$. Visto que $1 < m_2 \cdot m_3 \cdot m_4 \cdot \ldots \cdot m_q < n$, então a hipótese demonstra que $q = s$ e que, um a um, $m_n = r_s$.

Conforme afirmado por Hefez (2005, p.82), “do ponto de vista da estrutura multiplicativa dos naturais, os números primos são os mais simples e ao mesmo tempo são suficientes para gerar todos os números naturais”. Dessa forma, se percebe a importância destes números, uma vez que são a base de formação na construção dos naturais e, portanto, servem de estudo na concepção de outros conjuntos numéricos.

3.3 Números primos e sua infinitude

Ao longo dos anos, muito se descobriu acerca dos primos, como o fato de sua quantidade ser infinita, provado por Euclides em sua obra *Os Elementos*, segundo narrado por Boyer (1974, p. 84), que nos apresenta a Proposição 20: “números primos são mais do que qualquer quantidade fixada de números primos. Isto é, Euclides dá aqui a prova elementar bem conhecida do fato que há infinitos números primos.” A prova apresentada por Euclides, para esta notável descoberta, foi a seguinte:

Proposição 1. Os números primos são infinitos.

Demonstração. Vamos considerar que o número de primos seja finito. Temos, portanto a seguinte sequência de primos: $n_1, n_2, n_3, n_4, \dots, n_r$. Seja, agora, o número $N = n_1 \cdot n_2 \cdot n_3 \cdot n_4 \cdot \dots \cdot n_r + 1$. Se N for primo, então evidentemente não pertence ao conjunto dos elementos da sequência considerada, pois supomos existir apenas r deles. Agora, se N for composto, considerando o Teorema Fundamental da Aritmética, então N possui como um de seus fatores um elemento do conjunto $\{n_1, n_2, n_3, n_4, \dots, n_r\}$, porém 1 não pode ser dividido por nenhum deles. Em ambos os casos a suposição se mostra falsa, logo existe um número primo maior que n_r.

Posteriormente, outras demonstrações foram apresentadas sobre a infinitude dos números primos. Exibiremos uma formulada por Leonhard Euler[2], para a qual precisaremos apresentar, primeiramente, dois importantes resultados.

Lema 2. A série harmônica

$$\sum_{n=1}^{\infty}\left(\frac{1}{n}\right) = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots + \frac{1}{n} + \cdots \qquad (1)$$

é divergente.

Sua primeira demonstração foi dada pelo francês Nicole Oresme (1325-1382), que através do agrupamento dos termos da série (1), comparou-a com outra série, a fim de se chegar ao resultado (ÁVILA, 1995), conforme apresentação a seguir:

Demonstração (Lema 2). Seja a série

$$\sum_{n=1}^{\infty}(a_n) = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} + \frac{1}{9} \dots + \frac{1}{n} + \cdots \qquad (2)$$

Com $a_n = 1/n$,

Apesar da série parecer convergente, afinal

$$\lim_{x\to\infty}\frac{1}{x} = 0$$

[2] Matemático suíço que viveu entre os anos de 1707 e 1783. Foi autor de diversos trabalhos matemáticos e realizou importantes estudos a respeito da Teoria dos Números, incluindo os números primos, sobre os quais fez descobertas que influenciaram grandes avanços no estudo destes (BOYLER, 1974).

Vamos demonstrar que é divergente,

Dada a série

$$\sum b_m = 1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{4} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \cdots \quad (3)$$

Na qual cada termo é formado a partir da seguinte relação:

$b_1 = a_1$, $b_2 = a_2$, $b_3 = a_4$, $b_4 = a_4$, $b_5 = a_8$, $b_6 = a_8$, $b_7 = a_8$, $b_8 = a_8$,

Mantendo esse raciocínio indefinidamente, temos:

$$\sum b_n = 1 + \frac{1}{2} + \left(\frac{1}{4} + \frac{1}{4}\right) + \left(\frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8}\right) + \cdots = 1 + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \cdots \quad (4)$$

Como $b_n = a_m$, para $n = m$ e $b_n < a_m$, para $n \neq m$, temos

$$\sum b_n < \sum_{n=1}^{\infty} \left(\frac{1}{a_n}\right)$$

Como $\sum b_n$ é claramente divergente, conclui-se que $\sum_{n=1}^{\infty} \left(\frac{1}{a_n}\right)$ também é divergente. Logo a série harmônica é divergente.

Agora, vamos provar o segundo resultado.

Seja um número primo p, então

$$\frac{1}{p} < 1$$

Dada, agora, a série geométrica – soma dos termos de uma progressão geométrica – cuja razão é $1/p$ e primeiro termo é 1, temos:

$$\sum_{n=0}^{\infty} \frac{1}{p^n} = \frac{1}{1 - \frac{1}{p}} \quad (5)$$

De forma análoga, seja q outro primo, com $q \neq p$, temos

$$\sum_{n=0}^{\infty} \frac{1}{q^n} = \frac{1}{1 - \frac{1}{q}} \quad (6)$$

Assim, multiplicando os membros de (5) por (7), respectivamente, temos

$$\sum_{n=0}^{\infty}\frac{1}{p^n}\cdot\sum_{n=0}^{\infty}\frac{1}{q^n}=\left(\frac{1}{1-\frac{1}{p}}\right)\left(\frac{1}{1-\frac{1}{q}}\right)$$

$$\left(1+\frac{1}{p}+\frac{1}{p^2}+\frac{1}{p^3}+\cdots+\frac{1}{p^n}+\cdots\right)\left(1+\frac{1}{q}+\frac{1}{q^2}+\frac{1}{q^3}+\cdots+\frac{1}{q^n}+\cdots\right)=\left(\frac{1}{1-\frac{1}{p}}\right)\left(\frac{1}{1-\frac{1}{q}}\right)$$

$$1+\frac{1}{p}+\frac{1}{q}+\frac{1}{pq}+\frac{1}{p^2}+\frac{1}{p^2}+\cdots=\left(\frac{1}{1-\frac{1}{p}}\right)\left(\frac{1}{1-\frac{1}{q}}\right) \qquad (7)$$

Daí, sobrevém o seguinte fato:

O primeiro membro representa a soma de todas as formas possíveis dos inversos de $p^a q^b$, com $a \geq 0\ e\ b \geq 0$, os quais, pelo Teorema Fundamental da Aritmética, são contados uma única vez, a menos da ordem dos fatores.

Por fim, apresentaremos a prova de Euler sobre a infinidade dos números primos.

Demonstração (Proposição 1). Vamos supor que $p_1, p_2, p_3, p_4, \ldots, p_r$ sejam todos os números primos, em número finito, e considerar a seguintes igualdades

$$\sum_{n=0}^{\infty}\frac{1}{p_1^n}=\frac{1}{1-\frac{1}{p_1}}$$

$$\sum_{n=0}^{\infty}\frac{1}{p_2^n}=\frac{1}{1-\frac{1}{p_2}}$$

$$\vdots$$

$$\sum_{n=0}^{\infty}\frac{1}{p_r^n}=\frac{1}{1-\frac{1}{p_r}}$$

Para $i = 1, 2, 3, \ldots, r$

Agora, multiplicando os respectivos membros das igualdades formadas para todos os r, obtemos

$$\prod_{i=1}^{r}\left(\sum_{n=0}^{\infty}\frac{1}{p_i^n}\right)=\prod_{i=1}^{r}\left(\frac{1}{1-\frac{1}{p_i}}\right) \quad (8)$$

De onde conclui-se, pelo resultado (7) e pelo Teorema Fundamental da Aritmética, que o primeiro membro é composto pela soma dos inversos de todos os números naturais.

Deste modo, pelo resultado (1) e como a ordem dos termos não alterará o resultado, já que todos são positivos, resulta que o primeiro membro é divergente, logo, é infinito, contudo, o segundo membro é finito, um absurdo.

Conclui-se, portanto, que os números primos são infinitos.

3.4 Fórmulas para números primos

A notabilidade dos números primos reside, em grande parte, na sua localização imprevisível, ou seja, na cadeia de sucessão de números naturais, e por não ter sido encontrada, ainda, uma forma precisa de se identificar indefinidamente o próximo primo. Esta lacuna na compreensão destes números fora constatada há séculos, conforme percebido nas palavras de Euler, comentadas por Sautoy (2007):

> Porém, até para o grande Euler foi difícil encontrar uma fórmula simples que gerasse todos os primos. Em 1751, ele escreveu que "há alguns mistérios nos quais a mente humana jamais penetrará. Para nos convencermos desse fato, basta fitarmos as tabelas de primos e perceberemos que ali não reina qualquer ordem ou regra". Parece paradoxal que os objetos fundamentais sobre os quais construímos nosso organizado mundo matemático se comportem de maneira tão irregular e imprevisível (SAUTOY, 2007, p. 55).

Na tentativa de localizar primos, foram propostas algumas fórmulas capazes de identificá-los, como a de Pierre de Fermat[3], que, erroneamente, foi admitida por seu autor como capaz de encontrar infinitos primos. Os *Números de Fermat,* provenientes da fórmula $F_n = 2^{2^n} + 1$, de fato são primos para valores de $n = 0,\ n = 1,\ n = 2,\ n = 3\ e\ n = 4$, contudo, ela falha para $n = 5$, dado que este valor representa um número composto, pois $F_5 = 4.294.967.297 = 641 \cdot 6.700.417$, fato provado, em 1732 por Euler (HEFEZ, 2005).

[3] Jurista e pesquisador matemático que viveu entre os anos de 1601 e 1665. Fermat, assim como Euler, realizou importantes pesquisas em diversas áreas da matemática, contudo foi na Teoria dos Números que deixou sua maior influência (STEWART, 2014).

Aliada à capacidade desta ferramenta de encontrar números primos para os primeiros quatro valores de n, existe a frustração de nunca ter sido encontrado outros além destes, pois, atualmente, o maior primo conhecido gerado pela fórmula de Fermat é $F_4 = 65537$ (RIBENBOIM, 2014).

Outra forma de localizar primos também foi considerada pelo francês Marin Mersenne (1588-1648), que propôs números na forma $2^m - 1$, com m primo, capazes de gerar primos, como ocorre com $m = 2$, $m = 3$ e $m = 5$, contudo isso não ocorre indefinidamente, já que, por exemplo, para $m = 11$, obtêm-se $2047 = 89 \cdot 23$. Portanto, define-se como *Número de Mersenne* números na forma $M_q = 2^q - 1$, no qual q é primo. Se M_q for primo, então será denominado *Primo de Mersenne.*

Diversos primos de Mersenne já foram identificados, contudo ainda não se têm provas sobre sua infinidade. Os maiores primos já localizados são de Mersenne e detém o recorde do maior primo conhecido, registrado em janeiro de 2019, o qual bateu seu antecessor, que também era do mesmo tipo. O número pode ser escrito como $2^{82589933} - 1$, com 24.862.048 dígitos (IMPA, 2019).

As tentativas de localizar primos por intermédio de fórmulas não findaram com Fermat e Mersenne. Alguns grandes estudiosos propuseram métodos para se chegar àqueles, como Euler, que apresentou o seguinte teorema:

Seja a função $f: \mathbb{Z}_+ \to \mathbb{Z}$, definida por $f(x) = x^2 + x + 41$. Se $0 < x < 39$, então f assumirá valores primos.

De fato, para $x = 0, 1, 2, 3, 4, \ldots, 39$, temos, respectivamente, $f(x) = 41, 43, 47, 53, 61, \ldots, 1601$, os quais são primos. A função falha para $x = 40$, pois $f(40) = 1681 = 41^2$.

Polinômios da forma $x^2 + x + q$, onde q é um número primo, possui como melhor resultado o de Euler, apresentado anteriormente, em termos de quantidades de valores primos iniciais sucessivos (RIBENBOIM, 2014).

3.5 Outras funções sobre os números primos

Os esforços voltados à procura de funções definidoras de primos ainda não revelaram resultados proeminentes, no entanto um tipo especial de função tem mostrado grande progresso. A função $\pi(x)$, que representa a quantidade de números

primos entre 1 e x, tem sido estudada há séculos, desde a inovadora forma de lidar com os primos, iniciada pelo matemático alemão Carl Friedrich Gauss.

Gauss estimou que a quantidade de primos entre 1 e x seria $x/\log x$ e posteriormente refinou-a por meio da função.

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

Em seguida, a partir desta ideia, desenvolveu-se o *Teorema dos Números Primos*.

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

No qual o limite entre o quociente de $\pi(x)$ e $x/\ln x$, quando x tende ao infinito, é 1, ou seja, $\pi(x)$ tende a se aproximar de $x/\ln x$ à medida que o valor de x aumenta. Este teorema foi provado por Jacques Hadamard[4] e Charles de La Vallée Poussin[5], de forma independente, em 1896 (MOREIRA, MARTINEZ, 2010).

Outro importante resultado relacionado aos números primos foi revelado pelo estudo da função zeta (ζ), representada pela letra grega que leva seu nome. Euler foi um dos primeiros a apresentar importantes aspectos dessa função, a qual recebe a designação de *Função Zeta de Euler (*D'AMBROSIO, 2008).

A função $\zeta: \mathbb{R} \to \mathbb{R}$, é definida por:

$$\zeta(x) = 1 + \frac{1}{2^x} + \frac{1}{3^x} + \frac{1}{4^x} + \cdots + \frac{1}{n^x} + \cdots = \sum_{n=1}^{\infty} \frac{1}{n^x} \qquad (9)$$

Os primeiros registros do desenvolvimento destas somas infinitas vêm da época dos gregos, na qual Pitágoras descobriu uma relação harmônica entre as notas musicais e os números 1, $1/2$, $1/3$ e $1/4$ (SAUTOY, 2007).

---

[4] Jacques Hadamard (1865-1963) foi um matemático francês cujo resultado mais conhecido é a prova do Teorema dos Números Primos, apresentada em 1896, paralelamente à demonstrada por Vallée Poussin, no mesmo ano (O'CONNOR, ROBERTSON, 2003).

[5] Charles Jean Gustave Nicolas Baron de la Vallée Poussin (1866-1962) foi um matemático belga, mais conhecido por sua obra principal, Curso de Análise, e por sua prova do Teorema dos Números Primos, apresentada em 1896, que também foi provada por Hadamard, no mesmo ano, mas de forma independente (O'CONNOR, ROBERTSON, 2001).

Para $x = 1$, provou-se por (1) que a função tende ao infinito, contudo o mesmo não ocorre para valores acima de 1, fato observado por Euler. Este matemático também mostrou que para $x = 2$, ela converge para $\pi^2/6$ e, de forma generalizada, que para todo $x > 1$, a série $\sum_{n=1}^{\infty} \frac{1}{n^x}$ é convergente (RIBENBOIM, 2014).

Ainda sobre a função ζ, Euler também percebeu uma notável conexão entre esta e os números primos, ao verificar a seguinte relação entre aquela soma e o produto exposto abaixo.

$$\zeta(x) = \prod_{p\ primo} \left(\frac{1}{1 - p^{-x}}\right) \tag{10}$$

Para $x > 1$, denomina-se *Produto de Euler.*

Este produto surge a partir da expansão das seguintes séries:

Dada a série geométrica

$$\sum_{n=0}^{\infty} \frac{1}{p^{nx}}$$

Com p primo e $x > 1$. Temos, portanto

$$\sum_{n=0}^{\infty} \frac{1}{2^{nx}} = 1 + \frac{1}{2^x} + \frac{1}{2^{2x}} + \frac{1}{2^{3x}} + \cdots + \frac{1}{2^{nx}} + \cdots = \frac{1}{1 - 2^{-x}}$$

$$\sum_{n=0}^{\infty} \frac{1}{3^{nx}} = 1 + \frac{1}{3^x} + \frac{1}{3^{2x}} + \frac{1}{3^{3x}} + \cdots + \frac{1}{3^{nx}} + \cdots = \frac{1}{1 - 3^{-x}}$$

$$\sum_{n=0}^{\infty} \frac{1}{5^{nx}} = 1 + \frac{1}{5^x} + \frac{1}{5^{2x}} + \frac{1}{5^{3x}} + \cdots + \frac{1}{5^{nx}} + \cdots = \frac{1}{1 - 5^{-x}}$$

$$\vdots$$

$$\sum_{n=0}^{\infty} \frac{1}{p^{nx}} = 1 + \frac{1}{p^x} + \frac{1}{p^{2x}} + \frac{1}{p^{3x}} + \cdots + \frac{1}{p^{nx}} + \cdots = \frac{1}{1 - p^{-x}}$$

$$\vdots$$

Dessa forma, por (8) e pelo Teorema Fundamental da Aritmética, tem-se, através do produto dos primeiros membros de cada uma das igualdades anteriores, a

soma do inverso da enésima potência de todos os números naturais, que igualada ao produto do último membro das respectivas igualdades, obtém-se

$$1+\frac{1}{2^x}+\frac{1}{3^x}+\frac{1}{4^x}+\cdots+\frac{1}{n^x}+\cdots=\left(\frac{1}{1-2^{-x}}\right)\left(\frac{1}{1-3^{-x}}\right)\left(\frac{1}{1-5^{-x}}\right)\cdot\ldots\cdot\left(\frac{1}{1-p^{-x}}\right)\cdot\ldots\Rightarrow$$

$$\sum_{n=1}^{\infty}\frac{1}{n^x}=\prod_{p\ primo}\left(\frac{1}{1-p^{-x}}\right)\Rightarrow$$

$$\zeta(x)=\prod_{p\ primo}\left(\frac{1}{1-p^{-x}}\right) \tag{11}$$

Por fim, obtemos o produto de Euler, para $x>1$, o qual evidenciou que a função ζ relaciona-se com os números primos, percebidos em cada um dos fatores do produto formado.

Em 1859, Bernard Riemann[6] publicou um artigo intitulado *Sobre o número de primos menores do que uma dada grandeza*, no qual realiza uma abordagem inovadora sobre os números primos. Ao examinar a função ζ, ele a considerou como definida no campo dos complexos, resultando na designação de *Função Zeta de Riemann.*

Riemann percebeu que os zeros desta função estavam relacionados com os números primos. Verifiquemos a função de Riemann, representada por.

$$R(x)=\sum_{n=1}^{\infty}\frac{\mu(n)}{n}Li\left(\sqrt[n]{x}\right)$$

Na qual $\mu(n)$ é a *função de Möbius,* $\mu\colon\mathbb{N}\to\{-1,0,1\}$, definida como:

$$\mu(n)=\begin{cases}1, se\ n=1;\\ (-1)^p, se\ n\ \text{é}\ produto\ de\ p\ fatores\ primos\ distintos;\\ 0, se\ n\ tem\ um\ fator\ quadrado.\end{cases}$$

[6] Georg Friedrich Bernhard Riemann foi um matemático alemão que viveu entre os anos de 1826 e 1866. Suas obras influenciaram significativamente a Geometria, Análise e Teoria dos Números. Seus trabalhos sobre Geometria Diferencial e Análise Matemática serviram de base para relevantes estudos em diversas áreas da ciência, como a física moderna. É de sua autoria o trabalho sobre primos que exerceu forte impacto na forma de pensar desses números, o *On the number of primes less than a given magnitude* (*Sobre o número de primos menores do que uma dada grandeza),* publicado em 1859. Esta obra serviu como principal referência para o prova do a dos Números Primos e como revelação de um dos problemas mais importantes em Teoria dos Números, a Hipótese de Riemann (O'CONNOR e ROBERTSON, 1998).

A função R aproxima significativamente o resultado de $R(x)$ ao valor de $\pi(x)$. Através desta nova função, Riemann estimou com grande aproximação o resultado da contagem dos primos até um dado número, refinando expressivamente os valores encontrados pela função de Gauss, conforme dados da tabela a seguir:

Tabela 1 – Comparação entre as funções $Li(x)$ e $R(x)$ ao serem relacionadas com os valores de $\pi(x)$

x	$\pi(x)$	$Li(x) - \pi(x)$	$R(x) - \pi(x)$
10^8	5 761 455	754	97
10^9	50 847 534	1 701	-79
10^{10}	455 052 511	3 104	-1 828
10^{11}	4 118 054 813	11 588	-2 318
10^{12}	37 607 912 018	38 263	-1 476
10^{13}	346 065 536 839	108 971	-5 773
10^{14}	3 204 941 750 802	314 890	-19 200
10^{15}	29 844 570 422 669	1 052 619	73 218
10^{16}	279 238 341 033 925	3 214 632	327 052
10^{17}	2 623 557 157 654 233	7 956 589	-598 255
10^{18}	24 739 954 287 740 860	21 949 555	-3 501 366
10^{19}	234 057 667 276 344 607	99 877 775	23 884 333
10^{20}	2 220 819 602 560 918 840	222 744 643	-4 891 825
10^{21}	21 127 269 486 018 731 928	597 394 254	-86 432 204
10^{22}	201 467 286 689 315 906 290	1 932 355 208	-127 132 665

Fonte: (RIBENBOIM, 2014)

Apesar desta ampla aproximação, a fórmula de Riemann ainda continha erros, entretanto os números complexos, para os quais a função zeta resultava em zero, poderiam corrigi-los, os chamados *zeros da função zeta*, conforme observado nas palavras de Sautoy (2007):

> Riemann fez a descoberta fascinante de que o modo de corrigir sua estimativa dos números de primos estava codificado nas diferentes alturas dessas ondas. A função $R(N)$ lhe dava uma contagem razoavelmente boa do número de primos até N. Porém, ele descobriu que, ao acrescentar a essa estimativa a altura de cada onda sobre o número N, poderia obter o número exato de primos. O erro era completamente eliminado. Assim, Riemann descobriu o Cálice Sagrado que Gauss havia buscado: a fórmula exata para contar o número de primos até N (SAUTOY, 2007, p. 101).

As ondas supramencionadas caracterizam-se pela posição de cada zero da função zeta. A expressão de $\pi(x)$ em relação à $R(x)$, com o termo de erro de aproximação, pode ser verificada a seguir.

$$\pi(x) = R(x) - \sum_{\rho} R(x^{\rho})$$

Cuja somação estende-se a todos os zeros ρ não-triviais[7] da função zeta, contados com sua devida multiplicidade (RIBENBOIM, 2014).

Riemann conjecturou que todos os zeros não-triviais estavam na mesma linha, ou seja, sobre $\mathrm{Re}(s) = \frac{1}{2}$, portanto, da forma $\rho = \frac{1}{2} + it$. Esta é a conhecida *Hipótese de Riemann*, problema não provado até os dias atuais.

[7] A função zeta possui zeros simples nos pontos $-2, -4, -6, \ldots$, os chamados *zeros triviais,* e os zeros no domínio crítico, definido como o conjunto dos números complexos s tais que $0 \leq \mathrm{Re}(s) \leq 1$, os chamados *zeros não-triviais* (RIBENBOIM, 2014).

4 EVOLUÇÃO DOS TESTES DE PRIMALIDADE

Como já salientado, identificar números primos pode ser um trabalho excessivamente difícil, uma vez que é preciso fazer sucessivas divisões até concluir que não é possível encontrar fatores menores diferentes da unidade, o que implicaria na certeza de ser primo. Ante a relutante incapacidade de encontrar primos, indefinidamente, através de fórmulas, adotou-se, de milênios atrás até os dias atuais, métodos capazes de identificar estes números, os conhecidos *testes de primalidade*, através dos quais adquiriu-se mecanismos facilitadores que reduziu os árduos trabalhos de divisões contínuas. Estes testes podem ser definidos como algoritmos capazes de definir um número como primo ou composto a partir de uma sequência de ações prefixadas.

Na medida em que o conhecimento sobre os primos evoluiu, os testes de primalidade também foram aprimorados. Nesta perspectiva, podemos inseri-los em dois grandes momentos da história, o primeiro anterior ao advento do computador moderno e o segundo a partir da criação deste. Desta forma, este estudo trata dos testes desde suas formas tradicionais até os métodos computacionais.

4.1 Era pré-computacional

Uma forma trivial de testar a primalidade de um número é através da realização de divisões sucessivas, por meio das quais busca-se verificar a existência de fatores primos menor que o número em teste. Quando não encontrados, teremos um primo, caso contrário, estaremos diante de um composto.

Ocorre que o método descrito, apesar de funcionar eficientemente para números relativamente pequenos, torna-se bastante dispendioso à medida que a contagem aumenta. A quantidade de divisões necessárias para um número acima da casa dos milhares, por exemplo, já seria uma tarefa árdua para cálculos sem uso de máquinas modernas.

O desenvolvimento da aritmética tornou possível a simplificação de tarefas de contagem, graças a descobertas como o lema descrito abaixo, revelado por Eratóstenes[8], matemático grego do século III a.C.

Lema 3. Seja $n \in \mathbb{N}$, se n não é um número primo, então n possui um fator primo $p \leq \sqrt{n}$.

Demonstração. Seja a um número composto, então $a = a_1 \cdot a_2$, no qual $1 < a_1 < a$ e $1 < a_2 < a$. Sem perder a generalidade, suporemos que $a_1 \leq a_2$. Como

$$a_1 \cdot a_2 = a \Rightarrow \sqrt{a_1} \cdot \sqrt{a_2} = \sqrt{a}$$

Então

$$a_1 \leq a_2 \Rightarrow \sqrt{a_1} \leq \sqrt{a_2}$$

Multiplicando ambos os membros das desigualdades por $\sqrt{a_1}$, temos

$$\sqrt{a_1} \cdot \sqrt{a_1} \leq \sqrt{a_2} \cdot \sqrt{a_1}$$

E como $\sqrt{a_2} \cdot \sqrt{a_1} = \sqrt{a}$, então

$$\sqrt{a_1} \cdot \sqrt{a_1} \leq \sqrt{a_2} \cdot \sqrt{a_1} \Rightarrow a_1 \leq \sqrt{a}$$

Agora, pelo Teorema Fundamental da Aritmética, a_1 possui pelo menos um fator primo p e como $a_1 \leq \sqrt{a}$, então $p \leq \sqrt{a}$. Desse modo, como p é fator primo de a_1, então p também é fator primo de a, já que a_1 é fator de a, provando-se, assim, o lema.

À vista disso, no método supracitado, para verificar a primalidade de determinado número, não é necessário realizar divisões sucessivas até este, basta selecionar possíveis fatores até a raiz quadrada do valor.

Estes conhecimentos tornaram possível a idealização de um dos métodos clássicos mais conhecidos quanto a identificação de primos, o *Crivo de*

[8] Eratóstenes de Cirene foi um matemático grego que nasceu em Cirene, Norte da África, atualmente Shahhat, na Líbia. Viveu entre os anos de 276 a. C. e 194 a.C. Este estudioso ficou famoso por seu trabalho sobre números primos e por medir o diâmetro do planeta Terra (O'CONNOR e ROBERTSON, 1999).

Eratóstenes[9], que através de um raciocínio simples, mas eficaz, é capaz de gerar rapidamente tabelas destes números.

Um dos resultados cruciais sobre os primos que serviu de base para um sólido desenvolvimento do conhecimento acerca destes números foi o *Pequeno Teorema de Ferma*t, revelado no século XVII por aquele que leva o seu nome. Referido teorema diz o seguinte:

Teorema 2. Seja $a \in \mathbb{Z}$ e p um número primo, tem-se que p divide $a^p - a$.

Demonstração. Para $p = 2$, temos $a^2 - a = a(a-1)$, cujo resultado é par, logo é divisível por 2. Agora provaremos para p ímpar. Como para $a < 0$ e p ímpar temos $a^p - a < 0$, então basta provar para $a \geq 0$. Por indução sobre a, temos que $a = 0$ implica em $a^2 - a = 0$, que é divisível por p. Supondo, agora, verdadeiro para $a = k$, temos $k^p - k$ divisível por p. Vamos provar que para $k+1$ também é verdadeiro. Assim, através do desenvolvimento do binômio, temos

$$(k+1)^p - (k+1) = \binom{p}{0}k^p + \binom{p}{1}k^{p-1} + \cdots + \binom{p}{p-1}k^{p-1} + \binom{p}{p}k^0 - (k+1)$$

$$= k^p + \binom{p}{1}k^{p-1} + \cdots + \binom{p}{p-1}k^{p-1} + 1 - (k+1)$$

$$= k^p - k + \binom{p}{1}k^{p-1} + \cdots + \binom{p}{p-1}k^{p-1} \qquad (12)$$

Como $\binom{p}{1}k^{p-1} + \cdots + \binom{p}{p-1}k^{p-1}$ é divisível por p (demonstração no apêndice) e, por hipótese de indução, $k^p - k$ também é divisível por p, segue que (12) é divisível por p, logo, para $k+1$, é verdadeiro, provando-se o teorema.

Uma importante aplicação do Pequeno Teorema de Fermat é o seu uso na verificação de primos, cujos estudos serviram de base para a formulação de diversos testes de primalidade como o Teste de Lucas, Teste de Brillhart e Selfridge, Teste de Pepin, entre outros (RIBENBOIM, 2014).

[9] Método criado por Eratóstenes para localizar primos (será estudado detalhadamente no capítulo 5).

Outros conceitos foram de suma importância para o desenvolvimento de testes de primalidade por intermédio do avanço da aritmética, especialmente a ideia de *congruência*, que é definida por Hefez (2014, p. 192) como “uma das noções mais fecundas da aritmética, introduzida por Gauss no seu livro *Disquisitiones Arithmeticae,* de 1801. Trata-se da realização de uma aritmética com os restos da divisão euclidiana por um número fixado.”

A partir dessa nova abordagem matemática, novas perspectivas foram projetadas e avanços significativos foram alcançados no campo da Teoria dos Números, notadamente no conjunto dos números primos. A grande importância da aritmética modular pode ser percebida nas palavras de Sautoy (2007), que comparou suas propriedades ao funcionamento de uma calculadora-relógio:

> O potencial e a velocidade da calculadora-relógio se tornam evidentes no momento em que Gauss deseja calcular o valor de $7 \times 7 \times 7$. Em vez de multiplicar novamente 49 por 7, Gauss pode simplesmente multiplicar a última resposta (que era 1) por 7, obtendo o resultado 7. Assim, sem ter que calcular o valor de $7 \times 7 \times 7$ (que vem a ser 343), ele sabia, com pouco esforço, que o resultado deixaria resto 7 ao ser dividido por 12. A força da calculadora foi revelada quando Gauss passou a explorar grandes números situados além de seu alcance computacional. Embora não tivesse a menor ideia do valor de 7^{99}, sua calculadora-relógio lhe dizia que o número deixava resto 7 ao ser dividido por 12 (SAUTOY, 2007, p. 29).

Em geral, dizemos que os inteiros a e b são congruentes módulo m, com m natural, se os restos da divisão euclidiana de a e b por m são iguais. Em termos simbólicos, temos:

$$a \equiv b \bmod m, m \in \mathbb{N}, a \in \mathbb{Z}, b \in \mathbb{Z}$$

As aplicações dessa nova aritmética são inúmeras, dado que através de seus conceitos e propriedades, por exemplo, é possível provar que determinado número de Mersenne não é primo, que alguns números de Fermat não são primos, além de estabelecer critérios de divisibilidade por certos números. Isso mostra que o conceito de congruência revelou novas formas de testar a primalidade

4.2 Era computacional

A humanidade, nos últimos séculos, evoluiu tecnologicamente com grande celeridade, como jamais cresceu ao longo de sua história. Grande parte

desse acentuado desenvolvimento se deve ao advento e aperfeiçoamento dos computadores.

As máquinas tornaram-se uma realidade inevitável, dado o constante crescimento científico e sua consequente aplicação em invenções e aprimoramento de instrumentos. Desde o período renascentista, uma forte tendência voltada ao desenvolvimento intelectual se instalou nas sociedades ocidentais, em conformidade com o trecho a seguir:

> [...] O Renascimento deu um extraordinário salto para diante. Nunca uma civilização dera tão grande lugar à pintura e à música, nem erguera ao céu tão altas cúpulas, nem elevara ao nível da alta literatura tantas línguas nacionais encerradas em tão exíguo espaço. Nunca no passado da Humanidade tinham surgido tantas invenções em tão pouco tempo. Pois o renascimento foi, especialmente, progresso técnico; deu ao homem do Ocidente maior domínio sobre um mundo mais bem conhecido. Ensinou-lhe a atravessar os oceanos, a fabricar ferro fundido, a servir-se das armas de fogo, a contar as horas com um motor, a imprimir, a utilizar dia a dia a letra de câmbio e o seguro marítimo (DELUMEAU, 1984, p. 23).

A partir desse período, uma efervescente busca por descobertas no campo científico possibilitou o desenvolvimento tecnológico que se estendeu pelos séculos vindouros e estabeleceu uma nova era da humanidade. Concomitante ao movimento de expansão da ciência, nasceram as máquinas e, dentre estas, destacamos as capazes de realizar operações matemáticas e transpor os obstáculos presentes na limitação de cálculos mentais.

As primeiras máquinas voltadas à realização de operações aritméticas foram as calculadoras mecânicas, cujo funcionamento permitiu ao homem executar cálculos – que na época levavam várias horas – em apenas poucos comandos. Este tipo de funcionamento representou os primórdios dos conceitos do computador moderno. Vejamos o entendimento de Wazlawick (2016) sobre o tema:

> Os séculos XVII, XVIII e XIX viram o surgimento e aperfeiçoamento das calculadoras mecânicas. A partir de trabalhos inovadores como os de Schickard, Pascal e Leibniz, máquinas capazes de realizar as quatro operações aritméticas com o simples girar de uma alavanca se tornaram realidade. Essas máquinas, bem como o tear mecânico, que usava cartões perfurados já no início do século XIX, foram fundamentais para a concepção posterior dos computadores de propósito geral – ou seja, máquinas programáveis para executar qualquer função computável e não apenas as quatro operações. Esse mesmo período também testemunhou o desenvolvimento da aritmética binária e o surgimento dos primeiros

> computadores humanos, ou seja, pessoas cuja profissão era executar cálculos repetitivos à mão (WAZLAWICK, 2016, p. 27).

Nota-se, deste modo, a tendência em delegar à máquina certas tarefas habitualmente exercidas pelo ser humano. Num momento de grande expansão do conhecimento científico, a matemática também passou por um elevado desenvolvimento entre os séculos XVII e XIX, razão pela qual as máquinas também foram objetos de uso para cálculos.

A partir do desenvolvimento constante dos instrumentos de calcular, não demorou até que os computadores surgissem. Através da junção de conceitos preconcebidos de matemática e engenharia, nasceram as primeiras máquinas capazes de executar funções gerais, conforme apresentado a seguir:

> O século XIX viu surgir o primeiro projeto de computador de propósito universal: a Máquina Analítica de Charles Babbage. Neste século também se consolidaram as calculadoras mecânicas baseadas em engrenagens, que passaram a ser bastante utilizadas em empresas e organizações. Pesquisas iniciais com dispositivos elétricos como os relês, permitiram que ao final desse século as primeiras máquinas somadoras ou contadoras com base eletromecânica fossem construídas por Hermann Hollerith. Não menos importante, durante o século XIX ocorreram avanços nas ciências da Lógica e Matemática, devido principalmente a Boole, Frege, dentre outros que lançaram os fundamentos teóricos para a Ciência da Computação a nascer no início do século XX com trabalhos como o de Turing (WAZLAWICK, 2016, p. 53).

Com o surgimento do computador eletrônico, a matemática alcançou novos patamares, por intermédio da resolução de extensos cálculos, antes inalcançáveis pela mente humana. Valores de complexas funções puderam ser conhecidos graças a essa importante invenção.

Alguns clássicos artifícios utilizados na facilitação de cálculos matemáticos e resolução de problemas, como a tábua de logaritmos[10], deram lugar ao poder de processamento dos computadores eletrônicos. Assim, temos a descrição de Boyer (1974) sobre a vastidão da utilidade destas máquinas:

> Os computadores hoje tornaram-se tão vastos e intrincados que ultrapassam os sonhos de Babbage, que viveu um século antes de seu

[10] Tabela com correspondência entre os valores de $\log_a x$ e a^x, para valores de x definidos em determinado intervalo e com base $a = 10$, geralmente. Devido às propriedades operatórias dos logaritmos, estas tabelas eram utilizadas para transformar multiplicações em somas, simplificando a realização de cálculos complexos.

> advento. Problemas que estavam desesperadoramente além das capacidades dos matemáticos de eras anteriores recentemente foram resolvidos com a ajuda dos computadores de alta velocidade. Se, como Kepler disse, a invenção dos logaritmos duplicou a vida de um astrônomo, quanto mais o computador eletrônico expandiu as carreiras de cientistas e matemáticos (BOYER, 1974, p. 456).

Os tradicionais métodos de localização de primos tinham, em sua maioria, funcionamento baseado em sucessivas divisões que, com a elevação dos números testados, tornavam os trabalhos operacionais excessivamente difíceis. Com a cooperação das máquinas de calcular, essas tarefas foram demasiadamente facilitadas.

Dentre as inúmeras possibilidades trazidas pelo computador eletrônico no campo matemático, destacamos a utilização de algoritmos especialmente elaborados para a localização de números primos. Uma das grandes vantagens do poder computacional destes novos equipamentos foi sua capacidade de processar numerosas operações matemáticas de elevada complexidade que naturalmente seriam de difícil resolução pelo ser humano.

Os primeiros desafios dos computadores modernos consistiram na identificação de primos de Mersenne. O professor da Universidade da Califórnia em Berkeley, Raphael Robinson, marido da matemática norte-americana Julia Robinson[11], conseguiu, por intermédio do *Standards Western Automatic Computer* (SWAC), máquina criada por Derrick Lehmer[12], utilizar um algoritmo, de sua autoria, que identificava primos de Mersenne. Os resultados foram alcançados em 1952, quando este computador conseguiu descobrir os primeiros primos além da capacidade de alcance do ser humano, ao apresentar os números $2^{521} - 1$, $2^{607} - 1$ e $2^{2281} - 1$, batendo o recorde, seguidas vezes, de maiores números primos conhecidos naquela época (SAUTOY, 2007).

[11] Matemática norte-americana que viveu entre 1919 e 1985. Tornou-se famosa por ter participado da resolução do décimo problema de Hilbert, que buscava encontrar um algoritmo capaz de determinar a existência de raízes inteiras de uma equação polinomial (SAUTOY, 2007).

[12] Derrick Henry Lehmer (1905-1991) foi um matemático estadunidense que trabalhou em Teoria dos Números e generalizou os Teste Primalidade de Lucas para os primos de Mersenne (O'CONNOR e ROBERTSON, 2002).

De fato, o computador eletrônico possibilitou um gigantesco passo na captura de primos cada vez maiores. Décadas antes do advento desta máquina, em 1876, Lucas[13], através do *Teste de Lucas e Lehmer* – que será estudado mais à frente – provou que o número $2^{127} - 1$, com 39 dígitos, é primo. Este recorde persistiu durante vários anos, até que, a partir de 1951, primos maiores foram apresentados com o auxílio de computadores, como o número $180(2^{127} - 1)^2 + 1$, em 1951, e os números $2^{521} - 1$, $2^{607} - 1$, $2^{1279} - 1$, $2^{2203} - 1$ e $2^{2281} - 1$, todos em 1952, pelo SWAC, ultrapassando a casa dos 680 dígitos (CALDWELL, 2021).

[13] François Édouard Anatole Lucas (1842-1891) foi um matemático francês que se notabilizou por seus estudos sobre Teoria dos Números, Sequência de Fibonacci e Sequência de Lucas, esta última, com nome em sua homenagem. Lucas desenvolveu importantes testes de primalidade, influentes até os dias atuais (O'CONNOR e ROBERTSON, 1996).

5 ASPECTOS BÁSICOS DOS TESTES DE PRIMALIDADE

Em conformidade com o narrado ao longo deste trabalho, os testes de primalidade representam uma notável forma de se identificar números primos, grandemente utilizada ao longo dos anos. Sua evolução seguiu, em muitos aspectos, uma tendência de torná-los ágeis e praticáveis. Neste sentido, apresentamos alguns conceitos importantes relacionados às características dos testes aqui estudados.

5.1 Capacidade mental versus capacidade computacional

Os primeiros testes de primalidade adotavam o esforço mental mínimo como principal diferencial e, para tal fim, apoiavam-se em propriedades aritméticas dos números inteiros para reduzir o trabalho e o tempo de solução.

Com o advento dos computadores, o tempo de cálculo foi comprimido consideravelmente, reduzindo operações, que levavam horas, para apenas poucos segundos. É inquestionável o poder computacional destes instrumentos e seu alcance transcende excessivamente a capacidade humana de realizar cálculos, percebida através da performance atingida pelas primeiras gerações de computadores e que se acentua cada vez mais com as máquinas atuais.

A disparidade entre o poder de cálculo da mente humana e o das máquinas pode ser percebida pela análise de desempenho do precursor dos computadores digitais e eletrônicos, o ENIAC (*Electronic Numerical Integrator and Calculator*), operado entre os anos de 1946 e 1955. Referido computador, além do grande porte físico – possuía 17 mil válvulas, 10 mil capacitores, 70 mil resistores e pesava 30 toneladas – era capaz de realizar 5 mil adições por segundo e, em termos comparativos, um cálculo que levava vinte e quatro horas manualmente era resolvido em menos de trinta segundos (MACHADO e MAIA, 2014).

O campo de desenvolvimento dos computadores esteve em ampla ascensão desde sua criação, de tal modo que a potência dessas máquinas foi

elevada a níveis colossais nas últimas décadas. Segundo a TOP500[14], o computador mais rápido registrado em novembro de 2020 foi o supercomputador japonês Fugaku, instalado no *RIKEN Center for Computational Science* (R-CCS), em Kobe, Japão. Ele possui uma velocidade de 442 petaflops[15], ou seja, é capaz de realizar 442 quatrilhões de cálculos por segundo (STROHMAIER, DONGARRA, *et al.*, 2020). Ao compará-lo com um computador pessoal da ordem de 100 gigaflops, o Fugaku é 4 milhões e 420 mil vezes mais rápido.

Nota-se, portanto, o quanto as máquinas evoluíram e tornaram-se instrumentos fundamentais na pesquisa científica, na qual inclui-se o estudo dos números primos e consequentemente o desenvolvimento de testes de primalidade aptos a identificar primos cada vez maiores.

5.2 Custo de um algoritmo

Os computadores modernos, apesar da grande capacidade de processamento de alguns de seus modelos, possuem limitações práticas concernentes ao uso de algoritmos específicos. A depender da operação, o tempo de resposta pode demandar um tempo de espera inaceitável. Este campo de estudo refere-se ao custo de um algoritmo, ou seja, aos recursos que este precisa para funcionar.

Diversos atributos podem ser avaliados ao se determinar o custo de um algoritmo, porém Cormem (2002, p. 16) salienta que o fator primoridial é o tempo de resposta, ao afirmar que "ocasionalmente, recursos como memória, largura de banda de comunicação ou hardware de computador são a principal preocupação, mas com frequência é o tempo de computação que desejamos medir."

Tempo de resposta, conforme Machado e Maia (2014) é definido como:

> "*Tempo de resposta* é o tempo decorrido entre uma requisição ao sistema ou à aplicação e o instante em que a resposta é exibida. Em sistemas interativos, podemos entender como o tempo decorrido entre a última tecla

[14] Ranking dos 500 supercomputadores de alto desempenho (disponibilizados comercialmente) mais poderosos do mundo. Esta lista é atualizada duas vezes ao ano.
[15] 1 petaflop equivale à 1 quatrilhão de flops, que é a abreviação para o termo computacional "*floating-point operations per second*", que, traduzido, representa a unidade para operações de ponto flutuante por segundo.

> digitada pelo usuário e o início da exibição do resultado no monitor." (MACHADO e MAIA, 2014, p. 173).

Este tempo depende diretamente do número de operações a serem realizadas por um algoritmo, ou seja, quanto maior a quantidade de algarismos de determinado número de entrada X, maior será a quantidade de operações aritméticas a serem executadas.

Isso nos leva a destacar outro importante conceito, o *tamanho da entrada,* naturalmente medido através do número de itens da entrada. Relacionado a este, temos também o já delineado *tempo de execução*, entendido como o número de operações primitivas ou "passos" executados por um algoritmo em determinada entrada (CORMEM, LEISERSON, *et al.*, 2002).

Em termos gerais, o tempo de execução é representado pela soma dos tempos despendidos em cada uma das etapas executadas pelo algoritmo. Com base no tempo necessário de resposta, um algoritmo pode ser classificado como de *tempo polinomial* ou de *tempo exponencial*. Vejamos como Ribemboim (2014) os define:

> O algoritmo é chamado *de tempo polinomial* se existir um polinômio $f(X)$, tal que, para todo N, o tempo necessário para levá-lo ao fim, quando o dado inicial é o número N, é limitado por $f(\log N)$. Se o algoritmo não é a tempo polinomial, mas se o tempo de execução é limitado por $f(N)$, para todo N (onde $f(X)$ é um polinômio), então é ele chamado *de tempo exponencial,* porque $N = e^{\log N}$. Um algoritmo só é economicamente aceitável se for de tempo polinomial (RIBENBOIM, 2014, p. 108, grifo do autor).

Conforme o supramencionado, há um limite de viabilidade econômica para determinados algoritmos e tal barreira está diretamente relacionada ao seu custo. Desta forma, define-se como *aceitáveis* aqueles classificados como de tempo polinomial.

Tratar de tempo polinomial e tempo exponencial nos remete à análise dos termos da função e suas taxas de crescimento. Dada uma função f representada por $f(x) = ax^2 + bx + c$, para o número de entrada x e tempo de execução $f(x)$, quando se eleva indefinidamente o valor de x, os termos bx e c tornam-se praticamente insignificantes, logo, podem ser ignorados no cálculo do tempo, assim como a constante a, uma vez que também se torna desprezível em

relação à taxa de crescimento quando em grandes entradas. Estas análises apoiam-se no fato de que a taxa de crescimento é o fator decisivo no tempo de execução de um algoritmo (CORMEM, LEISERSON, *et al.*, 2002). Em linhas gerais, quanto menor a ordem de crescimento de um algoritmo, mais eficiente este será.

O custo de um algoritmo é comumente avaliado com base no seu tempo de execução, cujas variáveis englobam a quantidade de operações necessárias para a conclusão das tarefas e o período tomado por cada uma destas. Como já citado, utiliza-se uma função f (função de complexidade) para se verificar o tempo de execução de um algoritmo. Stanat e McAllister (1977, apud ZIVIANI 2011, p. 5) definem que "se $f(n)$ é a medida de tempo necessário para executar um algoritmo para um problema de tamanho n, então f é chamada de função de *complexidade de tempo* do algoritmo."

O principal custo de um algoritmo avaliado neste trabalho será o que relaciona o tamanho da entrada dos dados com seu custo de execução, assim, teremos a função de complexidade de tempo atrelada à dimensão dessas informações. Dentre os casos possíveis – melhor, médio e pior – consideraremos o pior caso, uma vez que representará o pior tempo de execução dentre todas as entradas, dessa forma a função f sempre representará o maior o custo de aplicação do algoritmo.

Sabendo-se que o custo de um algoritmo está diretamente ligado ao tamanho da entrada n, então nota-se que esta entrada oferece um forte parâmetro de medida de complexidade do problema, assim, na medida que n cresce, a complexidade de tempo de algoritmo também sobe.

Feofiloff (2019, p. 10) revela que "Para cada *instância*[16] do problema, o algoritmo consome uma quantidade de tempo diferente. Digamos que o algoritmo consome $T(I)$ unidades de tempo para resolver a instância I. A relação entre $T(I)$ e o tamanho de I dá uma medida da eficiência do algoritmo." (grifo nosso).

[16] Compreendida aqui como *caso particular*.

A análise assintótica[17] da função f nos permite observar seu comportamento quando o custo de n se eleva consideravelmente. Knuth (1968, p. 104, apud Ziviani, 2011, p 12) sugeriu a seguinte notação para dominação assintótica.

> Para expressar que $f(n)$ domina assintoticamente $g(n)$, escrevemos $g(n) = O(f(n))$, onde se lê $g(n)$ é da ordem no máximo $f(n)$. Por exemplo, quando dizemos que o tempo de execução $T(n)$ de um programa é $O(n^2)$, isto significa que existem constantes c e m tais que, para valores de n maiores ou iguais a m, $T(n) \leq cn^2$ (KNUTH, 1968, p. 104, apud ZIVIANI, 2011, p. 12).

Simbolicamente, temos

Definição 2. Dadas as funções $g: \mathbb{N} \to \mathbb{R}$ e $f: \mathbb{N} \to \mathbb{R}$. Dizemos que $g(n) = O(f(n))$, ou que g está em f, se existirem constantes inteiras não negativas p e q, tais que $g(n) \leq p \cdot f(n)$, para todo $n \geq q$.

Exemplo. Seja $g(n) = 2n^2 + n + 1$

Então $g(1) = 4$. Assim podemos considerar que $g(n)$ está em $O(n^2)$, pois quando $q = 1$ e $p = 4$ temos

$$2n^2 + n + 1 \leq 4n^2$$

Para $n \geq 1$.

Ressalta-se que a expressão $g(n) = O(f(n))$, apesar do sinal de igualdade, denota que $g(n)$ "está escondido" em $O(f(n))$, ou seja, que $g(n) \leq p \cdot f(n)$, para p e n suficientemente grandes.

Em resumo, com base na Definição 2, o exemplo supra mostra que, na análise assintótica de g, a expressão $2n^2 + n + 1$ se resume a n^2, isto é, no exame de um algoritmo com custo representado por esta função, o termo determinante será n^2.

[17] Segundo Feofiloff (2021), a matemática que se interessa apenas pelos enormes valores de n é chamada *assintótica***.**

5.3 Testes de primalidade determinísticos e não determinísticos

Outro aspecto de capital importância na classificação dos testes de primalidade é a sua capacidade de garantir que determinado número N de entrada é primo ou composto. Dada a natureza e complexidade de cada teste, determinados algoritmos podem não assegurar a primalidade de um número N e retornam como resultado apenas a probabilidade de ser primo.

Temos, portanto, os *Testes Determinísticos de Primalidade* e os *Não Determinísticos*. No primeiro, a entrada de um inteiro positivo n apresenta na saída uma mensagem indicando se n é ou não primo. Desta forma, temos a garantia se n é primo ou composto. Por outro lado, os testes não determinísticos de primalidade garantem apenas que o número é primo com uma certa probabilidade, controlada de acordo com necessidade do usuário (COUTINHO, 2004).

Uma questão que pode ser levantada é a respeito do uso de testes não determinísticos em detrimento da utilização dos determinísticos, já que estes, diferentemente daqueles, trazem como resultado uma resposta garantida sobre a primalidade de um número. A resposta reside em sua eficiência, detalhada nos testes apresentados nesta obra.

5.4 Formas de classificação

Em razão da grande diversidade de características dos testes de primalidade, é possível encontrar várias formas de classificá-los. Ribenboim, em sua obra sobre números primos, classifica estes testes de acordo com os seguintes critérios: testes para números de forma particular ou testes para números genéricos; testes completamente justificados por teoremas ou testes cuja justificativa é baseada em conjecturas e testes determinísticos ou testes probabilísticos (ou de Monte Carlo) (RIBENBOIM, 2014).

Face à linha temporal adotada neste trabalho, a qual discorre sobre a evolução dos testes de primalidade, opta-se por utilizar como critério de classificação os períodos nos quais estão situados cada um, empregando-se como

divisor capital o início do uso computacional, dividindo-os em *métodos clássicos* e *métodos computacionais*.

Esta forma de classificação nos permite esclarecer as características básicas dos algoritmos e as aplicações dos testes de primalidade encontrados por pesquisadores, tão úteis para a organização das sociedades modernas.

6 TESTES CLÁSSICOS

6.1 Divisão por tentativa

Nas séries iniciais do estudo básico, após aprender os conceitos fundamentais sobre os números primos, um estudante pode idealizar, naturalmente, uma simples forma de identificá-los. Através de sucessivas divisões, é possível testar a primalidade de determinado número. O método consiste nas seguintes etapas:

Passo 1. Seleciona-se um número natural n do qual deseja-se testar a primalidade;
Passo 2. Realiza-se divisões sucessivas de n por m, para $1 < m < n$
Passo 3. Dado o seguinte *lema*, já provado nesse trabalho[18]:

Lema. Seja $n \in \mathbb{N}$, se n não é um número primo, então n possui um fator primo $p \leq \sqrt{n}$.

Então a divisão precisa seguir, apenas, até $\sqrt{n}$, ou seja, $1 < m \leq \sqrt{n}$.

Passo 4. Por fim, se n não for divisível por m, tal que $1 < m \leq \sqrt{n}$, então n será um número primo, caso contrário, será um composto.

Este é um típico método baseado na exaustão, logo, apesar do simples raciocínio, a tarefa se tornará excessivamente trabalhosa para números grandes, entretanto, para números relativamente pequenos, é um teste prático e de fácil aplicação que ainda retorna todos os divisores do número testado.

O teste é claramente determinístico, com tempo de execução de $O(\sqrt{n})$, contudo, levando-se em conta sua representação binária para uso computacional[19], sua complexidade é $O(2^{\sqrt{n}})$, portanto, de tempo exponencial, logo de custo computacional impraticável.

[18] Vide Capítulo 3, Item 3.1.
[19] A linguagem binária, atualmente utilizada pelos computadores, representa uma relação lógica entre a álgebra de Boole (matemático britânico do século XIX) e os circuitos eletrônicos, através dos estados lógicos SIM e NÃO para diferentes diferenças de potencial no circuito (COSTA, 2007).

6.2 Crivo de Eratóstenes

Um dos testes de primalidade mais antigos da história é o *Crivo de Eratóstenes*, nome dado em homenagem ao matemático grego Eratóstenes, que viveu entre os anos de 276 e 194 a. C. Como estampado na designação do teste, este método filtra os números colocados a teste – como um crivo – e então obtém como resposta apenas aqueles classificados como primos.

Uma ideia simples, entretanto, eficiente para localizar primos num intervalo pequeno de números. Vejamos como usar este método para obter os números primos de 1 até um certo natural n.

Passo 1. No conjunto $\mathbb{N}$, seleciona-se um subconjunto com todos os naturais até um dado número n;

Passo 2. O número 1, por definição, não é primo, logo deve ser retirado do conjunto;

Passo 3. Deve-se seguir a análise com o próximo da lista, ou seja, o número 2, que é primo, logo deve ser mantido na lista. Em seguida são cortados da lista todos os múltiplos de 2, isto é, os números pares;

Passo 4. A seguir, seleciona-se o próximo número não riscado da lista, o 3, que necessariamente é primo, pois não é múltiplo do número anterior, não cortado. Após isso, corta-se todos os múltiplos de 3 restantes no conjunto;

Passo 5. Pelo mesmo princípio apresentado na Divisão por Tentativa, o passo 4 deve ser seguido até $\sqrt{n}$. Após isso, restarão na lista apenas os números primos.

Para ilustrar, vamos selecionar os primos para $n = 50$. Escreve-se inicialmente os números naturais até 50.

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

Agora, risca-se o 1. Em seguida mantém-se o 2, porém, risca-se todos os múltiplos deste.

~~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~~

Segue-se o mesmo procedimento para o próximo número, que necessariamente é primo. Na nossa relação é o número 3, logo cortam-se todos os seus múltiplos.

~~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~~

O próximo da lista é o número 7, e como este é o número inteiro imediatamente anterior à $\sqrt{50}$, então, será o último número cujos múltiplos serão cortados de nossa relação, assim.

~~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~~

Ao retirarmos os números não riscados de nosso conjunto, teremos todos os números primos até o número 50, a saber:

2,3,5,11,13,17,19,23,29,31,37,41,43,47

Algumas observações importantes podem ser feitas perante o processo anteriormente apresentado. A primeira é o fato de que alguns números da lista

foram riscados mais de uma vez, como o número 15, que foi cortado, primeiramente, por ser múltiplo de 3 e, posteriormente, por ser múltiplo de 5, provocando um trabalho desnecessário.

Este esforço pode ser extinguido da seguinte forma: ao selecionar um número n cujos múltiplos serão riscados da lista, será notado que os seus múltiplos que concomitantemente são múltiplos de um primo anterior da relação já se encontram riscados, portanto basta iniciar o corte a partir de n^2, evitando-se utilizar fatores menores que n, que seguramente já resultaram em eliminações de números da lista. Em suma, a partir de um novo primo n, a exclusão de novos números deverá ser realizada de n^2 em diante, resultando em economia de tempo.

Uma forma generalizada do crivo de Eratóstenes, na qual se ignora a ordem do número a ser selecionado como referência na retirada dos múltiplos, além de englobar qualquer subconjunto de naturais, pode ser descrita conforme detalhamento abaixo.

Passo 1. Seja o conjunto $A = \{n_1, n_2, n_3, \dots, n_m\}$, $A \subset \mathbb{N}$ para o qual deseja-se testar a primalidade dos elementos de A;

Passo 2. Seja n_1 o menor número do conjunto A, verifica-se se n_1 é primo ou composto, adotando-se o seguinte procedimento conforme o respectivo caso;

Caso 1. Se n_1 for composto, então ele é retirado do conjunto, assim como todos os seus múltiplos pertencentes ao conjunto A;

Caso 2. Se n_1 for primo, então ele é mantido no conjunto, contudo todos os seus múltiplos são retirados do conjunto A;

Passo 3. O passo 2 é repetido com o menor elemento de A, a exceção do anteriormente analisado, até que se atinja o maior elemento deste conjunto.

Após conclusão dos passos acima, restarão no conjunto A apenas os números primos.

Uma boa observação do passo 2, nos leva a concluir que o número selecionado como ponto de partida, ou qualquer outro que permaneça no conjunto

A, não necessita ser o menor número de A, todavia, na escolha de um número aleatório como referência para a retirada se seus múltiplos, o processo demandará um maior tempo de execução, visto que eventualmente poderá ser o múltiplo de um número ainda não selecionado, o que acarretará um passo a mais no processo.

O crivo de Eratóstenes é um teste determinístico e de custo exponencial. O'Neill (2008, apud Junior, Neto, 2009, p. 1) relata que "o algoritmo do crivo vai se tornando inapropriado à medida que se aumenta o tamanho de n. O tamanho de n é exponencial no número de dígitos. A complexidade deste algoritmo é $O(n \log \log n)$."

Isto posto, temos um algoritmo de elevado custo, porém, apesar de sua impraticabilidade, o crivo é uma simples forma de se determinar primos em um intervalo pequeno, além de ser alvo de estudos e possuir relevante aplicação na computação.

Atualmente, existem inúmeros dispositivos digitais (computadores, laptops, celulares, tablets etc.) que, por suas características diversas, possuem uma grande variedade de desempenho. Uma forma de avaliar sua performance é através de um ou mais programas.

Um dos mais reconhecidos é o método denominado *benchmark*, que conforme Brookshear (2008, p. 93), "é o processo de comparar o desempenho de máquinas diferentes executando o mesmo programa, conhecido como amostra de teste (benchmark)".

Devido à simplicidade do método, o crivo de Eratóstenes é utilizado como benchmark padrão na avaliação de desempenho de programas de computador, uma vez que dispensa operações com divisão. Vejamos o que Gilbreath (1981, p. 180) fala a respeito das características de um benchmark hábil.

> [...] o benchmark deve ser curto (não mais do que uma página de código-fonte), capaz de acessar uma quantidade considerável de memória, sem realização de multiplicação ou divisão e facilmente codificado em uma variedade de linguagens de alto nível. Finalmente, o benchmark deve realizar algo útil (ou pelo menos reconhecível e verificável) (GILBREATH, 1981, p. 180, tradução nossa).

O programa supra idealizado baseava-se no Crivo de Eratóstenes, pelas peculiaridades já descritas. Em 1980, Gilbreath relatou em seu artigo a criação de um algoritmo do Crivo de Eratóstenes que calculava todos os números primos entre 3 e 16.000 e que, ao contrário de outros métodos, o crivo evitava a divisão e era extremamente rápido, pois usava conhecimento sobre números que podiam ser primos (números pares e múltiplos de primo) (GILBREATH, 1981).

6.3 Teste de Fermat

Como já descrito, Fermat foi um pensador do século XVII que realizou importantes descobertas no campo da Teoria dos Números, dentre elas, destacamos o Pequeno Teorema de Fermat, já apresentado e demonstrado[20]. Vejamos o que a literatura fala a respeito desse importante teorema.

"O teorema tem sido uma grande influência em algoritmos da Teoria dos Números, na medida em que representa a base para alguns dos mais conhecidos algoritmos de testes de primalidade" (AGRAWAL, 2006, tradução nossa).

O Teorema de Fermat também pode ser exibido da seguinte forma.

Teorema 3. Se p é um número primo, então, para todo $a \in \mathbb{Z}$, $a^p \equiv a \bmod \mathrm{p}$.

Quando $p \nmid a$, ou seja, se $(a, p) = 1$[21], pelo Corolário C.8.1, temos

$$a^p \equiv a \bmod \mathrm{p} \Leftrightarrow \frac{a^p}{a} \equiv \frac{a}{a} \bmod \mathrm{p} \Leftrightarrow a^{p-1} \equiv 1 \bmod \mathrm{p}$$

Este resultado, apesar de ter sido proposto por Fermat no ano de 1640, só foi provado em 1736, por Euler, e serviu de base para formulações de diversos testes de primalidade posteriores.

Vejamos, portanto, alguns exemplos de que p primo e $(a, p) = 1$ implica em $a^{p-1} \equiv 1 \bmod p$, para todo a inteiro. Para tanto, adotemos a seguinte forma:

$$P \text{ primo } \Longrightarrow p \mid a^{p-1} - 1, \forall\, a \in \mathbb{Z}$$

[20] Vide Capítulo 4, Item 4.1.
[21] Dados os inteiros a e b, denota-se por (a, b) o máximo divisor comum de a e b.

Como p divide $a^{p-1}-1$, então existe $k \in \mathbb{Z}$, tal que $a^{p-1}-1=kp$. Alguns resultados são apresentados na tabela a seguir, para determinados valores de a e p.

Tabela 2 – Valores de $(a^{p-1}-1)/p$ para alguns primos p

a	p	$a^{p-1}-1$	$k=(a^{p-1}-1)/p$
2	3	3	1
2	5	15	3
2	7	63	9
2	11	1023	93
2	13	4095	315
3	2	2	1
3	5	80	16
3	7	728	104
3	11	59048	5368
3	13	531440	40880
4	3	15	5
4	5	255	51
4	7	4095	585
4	11	1048575	95325

Fonte: Elaborado pelo autor

É importante observar que a utilização do teste para confirmação de primos consiste na utilização da recíproca do Teorema de Fermat, uma vez que desejamos descobrir se determinado número p é primo, contudo, nem todo p que divide $a^{p-1}-1$, para todo a inteiro, é primo.

Vejamos a tabela seguinte com alguns valores de $(a^{p-1}-1)/p$:

Tabela 3 – Valores de $(a^{p-1}-1)/p$ para alguns valores de p composto

a	p	$a^{p-1}-1$	$k=(a^{p-1}-1)/p$
2	9	255	28,33333333
2	15	16383	1092,2
2	21	1048575	49932,14286
2	25	16777215	671088,6
3	4	26	6,5
3	8	2186	273,25
3	10	19682	1968,2
3	14	1594322	113880,1429
4	9	65535	7281,666667
5	8	78124	9765,5
5	10	1953124	195312,4
5	14	1220703124	87193080,29

Fonte: Elaborado pelo autor

À primeira vista, pode parecer que para todo a inteiro e p composto, tem-se que p não divide $a^{p-1}-1$, contudo o composto $p = 561 = 3 \cdot 11 \cdot 17$ é um contraexemplo de que a recíproca do Pequeno Teorema de Fermat nem sempre é verdadeira.

Quando a e p são coprimos, os números compostos p tais que $a^{p-1} \equiv 1 \bmod p$, para todo a, $1 < a < p$, são denominados *Números de Carmichael*[22], cujo menor é $561 = 3 \cdot 11 \cdot 17$ (RIBENBOIM, 2014).

O teste de Fermat consiste na utilização do Pequeno Teorema de Fermat, através do qual adota-se um valor inteiro de a para um determinado número p a ser testado como primo, com $(a, p) = 1$. Estipula-se uma quantidade k de vezes de realização do teste. Se em todas estas, resultar $p \mid a^{p-1} - 1$, então p será retornado como provavelmente primo. Caso contrário, será respondido como seguramente composto. O teste é probabilístico, uma vez que é impossível realizar infinitas tentativas.

O teste é quase perfeito, já que os números de Carmichael são extremamente raros. Há apenas 255 destes menores que 100.000.000, ou seja, somente 0,000255% dos primeiros números naturais são de Carmichael (CORMEM, LEISERSON, *et al.*, 2002).

Segue-se, a partir desta ideia, o conceito de *pseudoprimo*, definidos como prováveis primos que são, na verdade, compostos. Consoante Cadwell (2021), ao se aplicar o Teste de Fermat, em $a^{p-1} \equiv 1 \pmod p$, se o número p testado for primo, então será denominado *provável primo base* a ou apenas *a-PRP* – do inglês, *probable prime base* a) (CALDWELL, 2021).

O teste de Fermat possui larga utilização em criptografia, na medida em que se busca uma rápida localização de chaves criptográficas. Seu tempo de execução é $O(a \log n)$ operações aritméticas para a diferentes bases em a-PRP**.**

[22] Robert Daniel Carmichael (1879-1967), matemático estadunidense com área de atuação em Teoria dos Números. Ficou mais conhecido pelo número que leva seu nome, *número de Carmichael* (O'CONNOR e ROBERTSON, 2010)

6.4 Teste de Proth

Os *Números de Proth*, assim denominados em alusão ao matemático francês François Proth, que viveu no século XIV, são aqueles da forma

$$p = k \cdot 2^n + 1$$

Onde k é um número inteiro ímpar e n é um inteiro positivo tal que $2^n > k$. Os primeiros sete números de Proth são

Para $k = 1$ e $n = 1$, $p = 1 \cdot 2^1 + 1 = 3$

Para $k = 1$ e $n = 2$, $p = 1 \cdot 2^2 + 1 = 5$

Para $k = 1$ e $n = 3$, $p = 1 \cdot 2^3 + 1 = 9$

Para $k = 3$ e $n = 2$, $p = 3 \cdot 2^2 + 1 = 13$

Para $k = 1$ e $n = 4$, $p = 1 \cdot 2^4 + 1 = 17$

Para $k = 3$ e $n = 3$, $p = 3 \cdot 2^3 + 1 = 25$

Para $k = 1$ e $n = 5$, $p = 1 \cdot 2^5 + 1 = 33$

É importante notar que os Números de Fermat $F_n = 2^{2^n} + 1$, já definidos no atual trabalho, são um caso particular dos números de Proth. Quando primos, os números de Proth são denominados *Primos de Proth*.

O *Teste de Primalidade de Proth* é uma consequência direta do *Teorema de Proth*, um teste probabilístico publicado em 1878, cuja descrição pode ser observada logo a seguir.

Teorema 4. Seja $p = k \cdot 2^n + 1$ um número de Proth. Se existe $a \in \mathbb{Z}, a > 1$, tal que

$$a^{\frac{p-1}{2}} \equiv -1 (\mathrm{mod}\, p)$$

Então p é primo.

Demonstração. Adotemos o seguinte resultado, demonstrado na obra de Martinez, Moreira, *et al.*, (2013).

Se $n-1=FR$, com $F>R$ e para todo fator primo q de F existe um $a>1$, tal que $a^{n-1}\equiv 1\ (\mathrm{mod}\ n)$ e $\left(a^{\frac{n-1}{q}}-1,n\right)=1$, então n é primo.

Agora, fazendo $F=2^k$, temos $n=h2^k+1 \Leftrightarrow n-1=h2^k$, como $2^k>h$ e como para todo fator primo q de 2^k $(q=2)$, existe $a>1$ tal que

$$a^{\frac{n-1}{2}}\equiv -1(\mathrm{mod}\ n)\Leftrightarrow\left(a^{\frac{n-1}{2}}\right)^2\equiv(-1)^2(\mathrm{mod}\ n)\Leftrightarrow a^{n-1}\equiv 1(\mathrm{mod}\ n)$$

E como

$$a^{\frac{n-1}{2}}\equiv -1(\mathrm{mod}\ n)\Leftrightarrow n\mid a^{\frac{n-1}{2}}+1$$

Mas n é ímpar maior que 1, logo

$$n\nmid\ a^{\frac{n-1}{2}}+1-2=a^{\frac{n-1}{2}}-1$$

Dessa forma, $(a^{\frac{n-1}{2}}-1,n)=1$

Portanto, n é primo.

O maior primo conhecido antes da era computacional foi de Proth, com 44 dígitos, encontrado em 1951, com a ajuda de uma calculadora mecânica de mesa, conforme descrito por Caldwell (2021): “em 1951, Ferrier encontrou o primo $(2^{148}+1)/17=\ 20988936657440586486151264256610222593863921$”.

Os primos de Proth são frequentes e facilmente verificados, pelos resultados anteriormente apresentados, logo muitos dos maiores primos conhecidos são desse tipo (MARTINEZ, MOREIRA , *et al.*, 2013).

6.5 Teste de Pépin

O *Teste de Pépin* é um teste de primalidade para números de Fermat. O teste leva o nome do matemático francês Jean François Théophile Pépin (1826-1905) e é descrito da seguinte forma

Teorema 5. Seja $F_n=2^{2^n}+1$ (número de Fermat), se $3^{\frac{F_n-1}{2}}\equiv -1\ (\mathrm{mod}\ F_n)$, então F_n é primo.

Demonstração. Seja a seguinte proposição, demonstrada na obra de Martinez, Moreira, *et al.*, (2013).

Dado $n > 1$, se para cada fator primo q de $n-1$ existe um inteiro a_q tal que $a_q^{n-1} \equiv 1 \pmod{n}$ e $a_q^{\frac{n-1}{q}} \not\equiv 1 \pmod{n}$, então n é primo.

Agora, pela proposição destacada, dado $F_n = 2^{2^n} + 1$, que é maior que 1, então $F_n - 1 = 2^{2^n}$, cujo fator primo é 2. Como, pela hipótese, $3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n} \Leftrightarrow \left(3^{\frac{F_n-1}{2}}\right)^2 \equiv (-1)^2 \pmod{F_n} \Leftrightarrow 3^{F_n-1} \equiv 1 \pmod{F_n}$, então existe um inteiro a_q tal que $a_q^{n-1} \equiv 1 \pmod{n}$ e não existe $3^{\frac{F_n-1}{2}}$ congruente à 1 módulo F_n, logo, F_n é primo.

Para exemplificar, vamos aplicar o teste para o número de Fermat com $n = 4$.

Devemos provar que $3^{\frac{F_4-1}{2}} \equiv -1 \pmod{F_4}$. Como $F_4 = 2^{2^4} + 1 = 2^{16} + 1 = 65536 + 1 = 65537$, então $\frac{F_4-1}{2} = 32768$. Mas $3^{32768} \equiv 65536 \equiv -1 (\mathrm{mod}\ 65537)$, então $3^{\frac{F_4-1}{2}} \equiv -1 \pmod{F_4}$, e F_4 é primo.

6.6 Teste de Lucas-Lehmer

O teste a seguir foi apresentado por Lucas em 1876 e aperfeiçoado por Lehmer em 1932. O algoritmo é definido por recorrência e é utilizado para testar a primalidade de números de Mersenne. A chave do teste encontra-se na sequência de inteiros $S_0, S_1, S_2, \ldots$ definida recursivamente como

$$\begin{cases} S_0 = 4 \\ S_n = S_{n-1}^2 - 2 \end{cases}$$

Teste de Lucas-Lehmer. Seja p um número primo positivo. Se $S_{p-2} \equiv 0 \pmod{M_p}$, então o número de Mersenne M_p é primo.

Ou em outras palavras, se M_p divide S_{p-2}, então M_pé primo.

Sua demonstração transcende o conteúdo abordado nesse trabalho, contudo pode ser verificada no trabalho de Coutinho (2004, p. 162), no entanto o teste é de fácil implementação e utilização. Vejamos alguns exemplos.

Para $n = 3$, temos $M_3 = 2^3 - 1 = 7$. Como $S_0 = 4$, então $S_1 = 4^2 - 2 = 14$. Dessa forma, $M_3 \mid S_1$, logo M_3 é primo.

Para $n = 7$, temos $M_7 = 2^7 - 1 = 127$. Devemos achar S_5, então temos

$$S_2 = 14^2 - 2 = 194$$

$$S_3 = 194^2 - 2 = 37.636 - 2 = 37.634$$

$$S_4 = 36634^2 - 2 = 1.416.317.956 - 2 = 1.416.317.954$$

$$S_5 = 1.416.317.954^2 - 2 = 2.005.956.546.822.746.116 - 2$$
$$= 2.005.956.546.822.746.114$$

Como $127 \cdot 15.794.933.439.549.182 = 2.005.956.546.822.746.114$, então $M_7 \mid S_5$ e, portanto, M_7 é primo.

O último exemplo serviu para mostrar que, como a sequência S_n cresce rapidamente, é mais conveniente utilizar operações com módulo M_p. Assim, o Teste de Lucas-Lehmer poderia ser escrito da seguinte forma.

$$\begin{cases} S_0 = 4 \\ S_n \equiv (S_{n-1}^2 - 2) \pmod{M_p} \\ S_{n-2} \equiv 0 \pmod{M_p} \Longrightarrow M_p \text{ é primo} \end{cases}$$

Logo, para $n = 7$ teríamos.

$$S_0 = 4$$

$$S_1 \equiv 14 \pmod{127}$$

$$S_2 \equiv (14^2 - 2) \equiv 194 \equiv 67 \pmod{127}$$

$$S_3 \equiv (67^2 - 2) \equiv 4487 \equiv 42 \pmod{127}$$

$$S_4 \equiv (42^2 - 2) \equiv 1762 \equiv 111 \pmod{127}$$

$$S_5 \equiv (111^2 - 2) \equiv 12319 \equiv 0 \pmod{127}$$

Portanto, como $S_5 \equiv 0 \pmod{M_7}$, M_7 é primo.

O método acima é determinístico de tempo polinomial e seu custo é da ordem de $O(p^2 \log p)$ (COLQUITT e WELSH JR, 1991). Comparado a outros testes, o algoritmo de Lucas-Lehmer é de baixo custo, o que o tem colocado, desde a sua idealização, como um dos principais na descoberta de primos.

Lucas, em 1876, ao aplicar seu próprio teste, descobriu que M_{127} é primo. Com 39 algarismos, este foi o maior primo conhecido até o ano de 1951, quando se iniciou a era dos computadores modernos (RIBENBOIM, 2014).

Na medida que p aumenta, M_p torna-se consideravelmente grande, o que torna os cálculos excessivamente trabalhosos e exaustivos, contudo, com a evolução das máquinas, esta tarefa foi consideravelmente reduzida, conforme se vê na narrativa seguinte.

> A aplicação do teste de LUCAS e LEHMER para investigar a primaridade de M_q quando q é grande, exige cálculos muito longos. Para afrontar esses problemas técnicos, trabalha-se com computadores muito possantes, em equipes. Mas também utilizam-se programas especialmente concebidos. [...] WOLTMAN[23] preparou um programa com janelas e criou o GIMPS ('Great Internet Mersenne Prime Search"). Qualquer um que queira participar no projeto, com seus computadores pessoais, recebe o "software" gratuitamente, uma faixa de primos q a serem investigados bem como acesso de informações sobre o assunto (RIBENBOIM, 2014, p. 76).

Desde 1996, os últimos 15 maiores primos descobertos foram provados pelo programa GIMPS. Até o fechamento deste trabalho (agosto de 2021), o maior primo conhecido é o de Mersenne, $M_{82589933} = 2^{82589933} - 1$, com 24.862.048 de dígitos (CALDWELL, 2021).

6.7 Crivo de Sundaram

Com um método parecido ao Crivo de Eratóstenes, já detalhado nesta pesquisa, apresentaremos agora um sistema de números dispostos em tabela com exclusões e destaque de certos algarismos.

Muitos leitores, provavelmente, estão familiarizados com o "Crivo de Eratóstenes" para filtrar números primos, contudo, em 1934, um jovem estudante

[23] George Woltman, criador e um dos diretores do GIMPS.

indiano chamado Sundaram, propôs uma outra alternativa, chamada Crivo de Sundaram (HONSBERGER, 1970).

O método explora o fato de que todo primo a partir do 2 é um número ímpar não composto. Consiste, portanto, na formação de uma tabela de números naturais ímpares compostos dispostos em progressão aritmética, em cada coluna. Ao final, os ímpares que não estiverem na tabela, serão primos.

Consideremos os números ímpares representados por $2m + 1$ e $2n + 1$, com m e n naturais. Assim sendo, poderíamos representar o número ímpar p composto da seguinte maneira: $p = (2m + 1)(2n + 1) = 4mn + 2m + 2n + 1$

A montagem da tabela consiste em organizar seus números $p_{i\times j}$ conforme a disposição das linhas $m_i = i$, com $i \in \mathbb{N}$, e colunas $n_j = j$, com $j \in \mathbb{N}$. Assim, teríamos $p_{i\times j} = 4m_i n_j + 2m_i + 2n_j + 1$. Dessa forma, para a primeira linha e primeira coluna, temos $m_1 = 1$ e $n_1 = 1$ que resultam em $p_{1\times1} = 4 \cdot 1 \cdot 1 + 2 \cdot 1 + 2 \cdot 1 + 1 = 9$; para a segunda linha e primeira coluna, possuímos $m_2 = 2$ e $n_1 = 1$ que resultam em $p_{2\times1} = 4 \cdot 2 \cdot 1 + 2 \cdot 2 + 2 \cdot 1 + 1 = 15$, e assim sucessivamente, até chegarmos na seguinte tabela, para valores de m e n de 1 a 16.

Tabela 4 – Crivo de Sundaram

	n_1	n_2	n_3	n_4	n_5	n_6	n_7	n_8	n_9	n_{10}	n_{11}	n_{12}	n_{13}	n_{14}	n_{15}	n_{16}
m_1	9	15	21	27	33	39	45	51	57	63	69	75	81	87	93	99
m_2	15	25	35	45	55	65	75	85	95	105	115	125	135	145	155	
m_3	21	35	49	63	77	91	105	119	133	147	161	175	189	203		
m_4	27	45	63	81	99	117	135	153	171	189	207	225	243			
m_5	33	55	77	99	121	143	165	187	209	231	253	275				
m_6	39	65	91	117	143	169	195	221	247	273	299					
m_7	45	75	105	135	165	195	225	255	285	315						
m_8	51	85	119	153	187	221	255	289	323							
m_9	57	95	133	171	209	247	285	323								
m_{10}	63	105	147	189	231	273	315									
m_{11}	69	115	161	207	253	299										
m_{12}	75	125	175	225	275											
m_{13}	81	135	189	243												
m_{14}	87	145	203													
m_{15}	93	155														
m_{16}	99															

Fonte: Elaborado pelo autor

A tabela formada pelos números m_i e n_j, com $i = j$, separa os elementos $(2m_{i'} + 1)(2n_{j'} + 1)$ e $(2m_{i''} + 1)(2n_{j''} + 1)$, com $i' = j''$ e $i'' = j'$, e consequentemente $m_{i'} = n_{j''}$ e $m_{i''} = n_{j'}$, logo $(2m_{i'} + 1)(2n_{j'} + 1) = (2m_{i''} + 1)(2n_{j''} + 1)$. A tabela 4 reúne todos os elementos com i variando de 1 a 16 e j de 1 a 16, dos quais, os números formados por m_1 e $n_j, j \in (1{,}16)$, m_2 e $n_j, j \in (1{,}9)$, m_3 e $n_j, j \in (1{,}6)$, m_4 e $n_j, j \in (1{,}5)$ formam todos os números ímpares compostos até 99. Como, com exceção do 1, todo número ímpar não contido na tabela não é composto, então todos os ímpares até 100, não pertencentes àquela, são primos, a saber: 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.

7 TESTES COMPUTACIONAIS

7.1 Teste de Solovay-Strassen

O *Teste de Slovay-Strassen* é um método desenvolvido em 1977 pelo estadunidense Robert Martin Solovay e pelo alemão Volker Strassen. É um teste probabilístico em tempo polinomial do tipo Monte-Carlo. Sobre esta última ferramenta, Weisstein (2021) a define como "qualquer método que resolva um problema por meio da geração adequada de números aleatórios e analise se aquela fração de números obedece determinadas propriedades. O método é útil para obtenção de soluções numéricas para problemas que são muito complicados de resolver analiticamente." (WEISSTEIN, 2021, tradução nossa)

O teste é realizado, basicamente, através de uma seleção aleatória dos dados de entrada que retorna um resultado provavelmente correto. Dado um número de entrada n, a saída será n composto ou n provavelmente primo. Seu funcionamento baseia-se no *Critério de Euler*, que afirma:

Se p é um número ímpar e $a \in \mathbb{Z}$, com a e p coprimos, então

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) (\mathrm{mod}\ p)$$

Onde $\left(\frac{a}{p}\right)$ é o símbolo de Legendre[24], definido, para p primo, como:

$$\begin{cases} 0, & \text{caso } p \text{ divida } a \\ 1, \text{caso } a \text{ seja um resíduo quadrático}^{25} \text{ módulo } p \\ -1, \text{caso } a \text{ não seja um resíduo quadrático módulo } p \end{cases}$$

O critério é demonstrado em Hefez (2014, p. 287).

Para $n \in \mathbb{Z}$, ímpar, temos $\left(\frac{a}{n}\right)$ como resultado do produto dos símbolos de Legendre, definido como símbolo de Jacobi[26], portando representa uma generalização daquele. Sendo p_i cada um dos fatores primos de n, temos

[24] Adrien-Marie Legendre, matemático francês que viveu entre os séculos XVIII e XIX (1752-1833)
[25] Um número $a \in \mathbb{Z}$ é um resíduo quadrático módulo p se existe algum x que satisfaça a equação $x^2 \equiv a\ (\mathrm{mod}\ p)$
[26] Carl Gustav Jakob Jacobi, matemático alemão do século XIX (1804-1851).

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\left(\frac{a}{p_3}\right)\cdot \ldots \cdot \left(\frac{a}{p_n}\right)$$

Como, para todo $a \in \mathbb{Z}$, o critério é verdadeiro, então se, após testados todos os valores do intervalo $(1, n-1)$, o critério for satisfeito, n será primo. Sendo assim, para valores aleatórios de n, a congruência a ser verificada será.

$$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) (\mathrm{mod}\ n)$$

Os passos adotados no algoritmo de Solovay-Strassen são os seguintes.

Passo 1. Selecionar aleatoriamente um número x;

Passo 2. Aplicado o teste, este trará como resposta que x é seguramente composto ou que x é provavelmente primo;

Passo 3. Se x for provavelmente primo, a chance de ser composto é de no máximo $1/2$;

Passo 4. Após n operações, com a permanência da resposta de *provavelmente primo*, a probabilidade de retorno de um pseudoprimo é de no máximo de $(½)^n$. Na medida que n aumenta, o erro se torna desprezível.

Assim como os demais testes probabilísticos, o algoritmo de Solovay-Strassen possuirá maior precisão quanto maior for o número de iterações, logo, pelo exposto, o teste é determinístico para exames com todos os valores de n, contudo, para enormes valores de n, o método é inviável.

Com uso de rápidos algoritmos de exponenciação modular, o custo computacional deste algoritmo é $O(k \cdot log^3 n)$, para k testagens (GEEKSFORGEEKS, 2021).

7.2 Teste de Miller-Rabin

É um teste probabilístico de tempo polinomial também do tipo Monte Carlo, elaborado por Gary Miller e Michael Rabin. É um aprimoramento do teste de Solovay-Strassen, com margem de erro consideravelmente menor. Sobre esse algoritmo, Sautoy (2007, p. 263) relata que “nos anos de 1980, dois matemáticos,

Gary Miller e Michael Rabin, desenvolveram finalmente uma variação que garantiria, após poucos testes, que um número é primo".

O teste é fundamentado no seguinte teorema.

Teorema 6. Se p é um número primo e $x > 1$, tal que $x^2 \equiv 1(\mathrm{mod}\, p)$, então $x \equiv 1 \pmod{p}$ ou $x \equiv (p-1) \pmod{p}$

Demonstração. $x^2 \equiv 1 \pmod{p} \Longrightarrow x^2 - 1 \equiv 0 \pmod{p} \Longrightarrow (x+1)(x-1) \equiv 0 \pmod{p} \Longrightarrow x + 1 \equiv 0 \pmod{p}$ ou $x - 1 \equiv 0 \pmod{p} \Longrightarrow x \equiv -1 \pmod{p}$ ou $x \equiv 1 \pmod{p} \Longrightarrow x \equiv -1 \equiv p - 1 \pmod{p}$ ou $x \equiv 1 \pmod{p} \Longrightarrow x \equiv (p - 1) \pmod{p}$ ou $x \equiv 1 \pmod{p}$

O funcionamento do teste é baseado na seguinte análise:

Dado um número $x \in \mathbb{Z}$, par, podemos escrevê-lo como $x = 2p$, logo, temos dois casos:

I. p ímpar $\Longrightarrow x = 2p_1$
II. p par $\Longrightarrow p_1 = 2p_2$, logo $x = 2 \cdot 2p_2 = 2^2 p_2$

No segundo caso, podemos continuar o processo enquanto p_n for par, com consequente aumento do índice n. À vista disso, p_n diminui até que em dado momento p_n será ímpar, ou seja, $x = 2^n p_n$. Fazendo $p_n = p$, temos $x = 2^n p$.

Sabendo que para todo primo $p > 2$, $p - 1$ é par, teremos $p - 1 = 2^n m$.

Dados p primo e $a \in \mathbb{Z}$, se $p \nmid a$, então $(a, p) = 1$ e, pelo Pequeno Teorema de Fermat, $a^{p-1} \equiv 1 \pmod{p}$, assim $a^{2^n m} \equiv 1 \pmod{p} \Longrightarrow (a^m)^{2^n} \equiv 1 \pmod{p}$. Dessa forma, pela Proposição C.9, $a^m \equiv 1 \pmod{p}$ ou $a^m \equiv -1 \pmod{p}$.

Pelo Teorema C.10, se $p \nmid a$, $a \not\equiv 1 \pmod{p}$, $a \not\equiv -1 \pmod{p}$ e $a^2 \equiv 1 \pmod{p}$, então p é composto.

Agora, utilizando-se destes resultados, podemos testar a primalidade de um número da seguinte forma.

Passo 1. Seleciona-se um número inteiro $n > 2$ ímpar e faz-se $n - 1 = 2^n m$;

Passo 2. Seleciona-se um número inteiro a qualquer, $1 < a < n - 1$, e calcula-se $a^m \bmod n$. Daí, haverá dois casos possíveis.

Caso 1. $a^m \bmod n = 1 \Longrightarrow a^m \equiv 1 \pmod n$ ou $a^m \bmod n = n - 1 \Longrightarrow a^m \equiv (\mathrm{n} - 1) \pmod n \Longrightarrow a^m \equiv -1 \pmod n$. Logo $a^m \equiv \pm 1 \pmod n \Longrightarrow a^{2^n m} \equiv 1 \pmod n$, então $a^{n-1} \equiv 1 \pmod n$ e, portanto, n será primo;

Caso 2. $a^m \bmod n \neq 1$ e $a^m \bmod n \neq n - 1 \Longrightarrow a^m \not\equiv 1 \pmod n$ e $a^m \not\equiv (n - 1) \pmod n \Longrightarrow a^m \not\equiv -1 \pmod n \Longrightarrow a^m \not\equiv \pm 1 \pmod n$. Fazemos, então, $x_1 = (a^m \bmod n)^2 \bmod n$ e teremos as seguintes possibilidades.

I. Se $x_1 = n - 1$, então n será primo
II. Se $x_1 = 1$, então n será composto
III. Se não I ou II não for verdadeiro, faz-se $x_2 = x_1^2 \bmod n$, e verifica-se novamente se I ou II é verdadeiro.

Repete-se este processo até que x_i seja igual a $n - 1$ ou 1.

O teste mostra-se muito eficiente para um número determinado de tentativas, conforme observa-se adiante.

> [...] o algoritmo Miller-Rabin, um exemplo de teste de primalidade *probabilístico*. Dado n, tomamos t valores de a ao acaso no intervalo $1 < a < n$ e verificamos para cada a se n passa no teste de primalidade na base a. Se n for ímpar composto, a probabilidade de que um dado a acuse a não-primalidade de a é maior do que $3/4$ (pelo teorema); assim, a probabilidade de que n escape a t testes é menor do que 4^{-t} (MOREIRA e SALDANHA, 2012, p. 3).

Deste modo, para dado n, após testagem de 75% das bases menores que n, haveria certeza sobre a primalidade de n, contudo, para elevados valores de n, o teste é obviamente custoso.

O teste apresentado neste tópico é uma variação probabilística, devida a Rabin, de um teste determinístico proposto por Miller que dependia da generalização da Hipótese de Riemann. Uma forma de transformar o teste de Miller-Rabin em determinístico é testar todos os valores da base a em um intervalo suficientemente grande. A referida generalização da Hipótese citada implica que o

intervalo de 1 até $2(log\, n)^2$ é o suficiente. Apesar deste algoritmo ser rápido, depende da comprovação de uma conjectura (MARTINEZ, MOREIRA , *et al.*, 2013).

7.3 Teste AKS

No ano de 2002, os pesquisadores indianos Manindra Agrawal, Neeraj Kayal e Nitin Saxena publicaram no trabalho intitulado *PRIMES is in P* um algoritmo determinístico que determina a primalidade de um número em tempo polinomial, um relevante resultado da busca de um teste capaz de tal feito.

O teste é de fácil aplicação e utiliza como base a generalização do Pequeno Teorema de Fermat. O algoritmo fundamenta-se no seguinte lema:

Lema 4. Dado a inteiro, n natural maior que 2 e a e n coprimos, então

$$(x + a)^n \equiv x^n + a \pmod{n} \Leftrightarrow n \text{ é primo}$$

Uma vez que $(x + a)^n$ e $x^n + a$ deixarão o mesmo resto módulo n se divididos por qualquer polinômio, então, em particular, se forem divididos por $x^r - 1$, teremos.

$$(x + a)^n \equiv x^n + a \pmod{x^r - 1, n} \Leftrightarrow n \text{ é primo}$$

Ambos resultados são demonstrados no artigo *PRIMES is in P* (AGRAWAL, 2006) e o último mostra que para verificar a primalidade de n, basta testar a congruência para um determinado valor de r, que no trabalho mencionado representa um número primo no qual $r - 1$ possui um fator primo $q \geq 4\sqrt{r}\log n$, que divide a ordem de n módulo r.

Com este último resultado, a aplicação do teste consiste em selecionar um determinado número n a fim de testar sua primalidade e adotar um determinado valor primo para a e r. Em seguida, após substituição na congruência $(x + a)^n \equiv x^n + a \pmod{x^r - 1, n}$, analisar se os restos da divisão de $(x + a)^n$ e $x^n + a$ por $x^r - 1$ divididos por n são iguais.

Os autores do teste puderam avaliar o tempo de execução deste algoritmo em $(\log n)^{12}$, o qual foi aprimorado e reduzido para $(\log n)^{7,5}$. Por fim, no trabalho intitulado *Primality testing with Gaussian periods*, pode ser verificada uma

redução ainda maior da complexidade do algoritmo para $(\log n)^6$ (RIBENBOIM, 2014).

Face a imensa importância da identificação de primos cada vez maiores, este teste tornou-se um marco na busca por números primários gigantes, fortalecendo ainda mais as operações dependentes destes algarismos, conforme se vê nas palavras de Agrawal, Kayal e Saxena (2004).

> Os números primos são de fundamental importância na matemática em geral, e na Teoria dos Números, em particular. Por isso, é de grande interesse estudar diferentes propriedades de números primos. Há um destaque especial para aquelas propriedades que permitem determinar eficientemente se um número é primo. Tais testes eficientes também são úteis na prática: uma série de protocolos criptográficos precisam de grandes números primos (AGRAWAL, KAYAL e SAXENA, 2004, p. 781, tradução nossa).

7.4 Outros métodos computacionais

Além da relevante descoberta do teste AKS, que rompeu com a barreira da espera de um algoritmo determinístico em tempo polinomial, uma série de estudos avançados foram desenvolvidos com o intuito de aprimorar os métodos de localização de grandes primos. Nesta corrida, muitos outros testes foram apresentados, com resultados e alcances notáveis.

O *Teste de Baillie – PSW*, desenvolvido por Robert Baillie, Carl Pomerance, John Selfridgee e Samuel Wagstaff, é um método que consiste na utilização de um conjunto de algoritmos probabilísticos.

Conforme Weisstein (2021), uma das formas desse algoritmo é a aplicação de um teste de pseudoprimo forte de base 2, para um número n. Se passar, aplica-se o teste de Lucas, com emprego do símbolo de Jacobi. Se n passar neste último, então será considerado provavelmente primo.

O teste possui algo grau de confiabilidade e até a data de fechamento deste trabalho ainda não fora apresentado um número composto que passe no teste. Sobre esse fato, Weisstein (2021) afirma que não há exemplos de números compostos que passem no teste e, em 13 de junho de 2009, Jeff Gilchrist confirmou que não há pseudoprimos Baillie-PSW até 10^{17}.

As linhas de pesquisas sobre testes de primalidade foram desviadas para campos mais avançados da matemática, com uso de conceitos mais complexos. Neste contexto, testes como *APR*, proposto por L. M. Adleman, C. Pomerance e R. S. Rumely, em 1983, surgiram como novas ferramentas de menor custo na identificação de primos.

O teste APR utiliza conceitos avançados de Teoria dos Números, conforme se vê a seguir.

> O teste é rigorosamente justificado e, para isso, foi necessário, pela primeira vez nesse domínio, apelar para resultados difíceis da teoria dos números algébricos; há necessidade de intervenção de cálculos com as raízes da unidade e da lei de reciprocidade geral do símbolo de restos de potências (RIBENBOIM, 2014, p. 111).

Trata-se, então, de conteúdos pouco utilizados em cursos básicos de matemática, úteis, no entanto, em áreas específicas de estudo. Ainda conforme Ribenboim (2014), o teste possui larga vantagem em relação a seus antecessores, como a possibilidade de aplicação a números naturais quaisquer, sem necessidade de determinar fatores primos de $n-1$ ou $n+1$, para um dado n testado. Um exemplo de sua eficiência é a testagem de um número de 247 algarismos em 1987, por Cohen e A.K Lenstra, que levou apenas 15 minutos.

Outro tipo de abordagem na verificação de primos, é a utilização de curvas elípticas[27], desenvolvido em 1986 por A.O.L. Atkin e denominado *ECPP* (*Eliptic Curve Primality Proving*). O teste é realizado em tempo polinomial e pode ser comprovado com rigor. Estima-se que seu custo computacional é da ordem de $O(\log n)^5$ (MORAIN, 2007).

[27] Curvas definidas por equações cúbicas

8 APLICAÇÕES

O que outrora aparentava ter um fim em si mesmo, atualmente o estudo dos números primos possui uma imensa importância na forma de organização do mundo moderno, motivo pelo qual os testes de primalidade ganharam notável destaque ao longo dos últimos séculos.

Além das aplicações já elencadas no bojo deste trabalho, salientamos uma daquelas que podemos considerar de maior proveito na atualidade: a criptografia. Antes de adentramos no assunto, vamos discorrer sobre alguns conceitos relevantes no ramo desta ciência, a começar pelo conceito de criptografia que, conforme (COUTINHO, 2005), é descrita como.

> Em grego, *cryptos* significa secreto, oculto. A criptografia estuda os métodos para codificar uma mensagem de modo que só o destinatário legítimo consiga interpretá-la. É a arte dos 'códigos secretos', que todos já praticamos quando criança. O mais simples destes códigos consiste em substituir uma letra pela seguinte; isto é transladar o alfabeto uma casa para adiante. Um código semelhante foi usado por César para comunicar-se com as legiões em combate pela Europa (COUTINHO, 2005, p. 1).

A conceituação e detalhamento supra nos serve de confirmação para a mais basilar importância das comunicações secretas: a confidencialidade. Em diversos tipos de eventos, a troca de mensagens necessita de segurança na transmissão de seu conteúdo, logo, desde tempos remotos, o transmissor e receptor buscam meios de proteger a troca de informações.

Ao se debater sobre a segurança das informações, logo se suscita o método de codificação de mensagens, através do qual o conteúdo destas é cuidadosamente dissimulado por um conjunto de caracteres ou símbolos e, assim, modificado em sua aparência, mas mantido em seu conteúdo.

Um dos métodos mais antigos de codificação de mensagens é a substituição de cada caractere por outro, o qual pode ser entendido pelo interlocutor que saiba quais critérios na escolha do conjunto de símbolos foram utilizados pelo comunicante. Para exemplificar: se alguém codifica uma mensagem escolhendo como novo caractere de cada letra o correspondente da ordem inversa do alfabeto, então, se a mensagem original for PRIMOS, pela tabela seguinte, a palavra codificada será KIRNLH.

Tabela 5 – Códigos de ordem invertida do alfabeto

ORDEM	CARACTERE ORIGINAL	CARACTERE SUBSTITUTO
1°	a	z
2°	b	w
3°	c	y
4°	d	x
5°	e	v
6°	f	u
7°	g	t
8°	h	s
9°	i	r
10°	j	q
11°	k	p
12°	l	o
13°	m	n
14°	n	m
15°	o	l
16°	p	k
17°	q	j
18°	r	i
19°	s	h
20°	t	g
21°	u	f
22°	v	e
23°	x	d
24°	y	c
25°	w	b
26°	z	a

Fonte: Elaborado pelo autor

Esse método de substituição de caracteres por símbolos previamente estabelecidos possui algumas fraquezas, como o fato de cada idioma possuir certa regularidade na formação de suas palavras. Para exemplificar, citamos o fato de que a probabilidade de uso de uma vogal em determinada palavra é maior que o uso de uma consoante, já que estas são em número maior que aquelas. Há também o fato de que letras como m e p são bem mais frequentes em palavras da língua portuguesa do que letras como z e y. Estes e outros fatos correlacionados geram

critérios de formação de palavras que revelam dicas de decodificação, facilitando a descoberta do conteúdo da mensagem.

É importante, também, definir o significado dos termos *codificar* e *decodificar*, que significam, respectivamente, um conjunto de ações necessárias para *encobrir* e *descobrir* uma mensagem, ambas realizadas por usuários autorizados. Neste mesmo sentido, vem à tona o termo *decifrar*, que significa a ação de desvendar o código a fim de interpretar a mensagem.

Inúmeros códigos foram utilizados ao longo dos anos, alguns de alta complexidade, entretanto, com ferramentas adequadas, capazes de serem quebrados e terem suas mensagens reveladas. Um famoso exemplo é o código utilizado pelas forças alemães na segunda Guerra Mundial, com o auxílio da máquina denominada *enigma,* a mais avançada da época, conforme mencionado por Sautoy (2007, p. 241): “o mais avançado método mecânico de codificação era a máquina Enigma”.

Tal ferramenta era tão avançada para a época que a façanha de quebrar seu código foi realizada por instrumentos que executavam ações que transcendiam a capacidade mental. Era a época da exploração da computação e nascia uma das mais importantes cooperações da história: o conhecimento humano e a capacidade de processamento de computadores.

A partir da criação e rápido desenvolvimento dos computadores eletrônicos, códigos antes inacessíveis à compreensão humana, tornaram-se obsoletos ao poder computacional destas máquinas. Desta forma, era necessário a adoção de novos métodos de codificação de mensagens, capazes de reduzir ao máximo a possibilidade de sua quebra, até mesmo pelos computadores.

Foi nesse cenário, aliado à ampliação do mercado financeiro realizado por intermédio da rede mundial de computadores, que surgiram ideias de proteção de mensagens e de segurança das transações comerciais por meios digitais. Destacamos, aqui, os modernos códigos de *chave pública,* detalhados da seguinte forma:

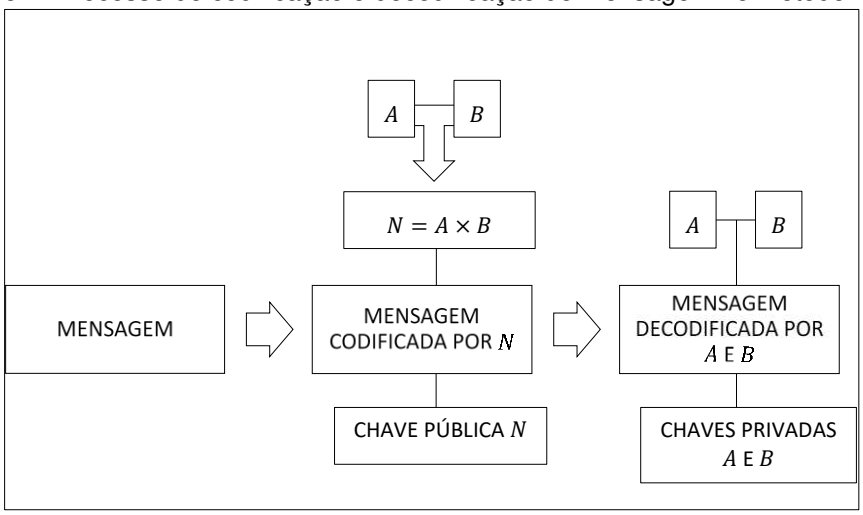
> Esta é uma ideia introduzida em 1976 por W Diffie e M.E. Hellman da Universidade da Califórnia. No código usado por César, se você sabe codificar, então sabe decodificar. Em um código de *chave pública* saber codificar não implica saber decodificar! Isto parece impossível: se sei codificar, para decodificar basta desfazer o que fiz. [...] 'desfazer' o processo de codificação pode não ser tão simples quanto parece (COUTINHO, 2005, p. 3).

Criptografia de Chave Pública pode ser definida, então, como sendo um sistema criptográfico que usa uma chave pública e uma chave privada, das quais, a primeira é de conhecimento amplo e a segunda de domínio apenas do usuário.

Nasce, portanto, o *RSA*, assim denominado por conta de seus criadores, os pesquisadores R. L. Rivest, A. Shamir e L, Adleman, que em 1978 criaram este método de criptografia de chave pública que se tornaria um dos mais importantes das últimas décadas.

O método RSA baseia em conhecimentos sobre primos, pois para sua implementação são necessários dois destes números. Vejamos o processo no diagrama a seguir, para A e B primos.

Quadro 1: Processo de codificação e decodificação de mensagem no método RSA



Fonte: Elaborado pelo autor

Podemos verificar que uma determinada mensagem, na criptografia RSA, é encriptada pela chave pública N, logo de fácil acesso, contudo, para ser decodificada, são necessárias as chaves privadas, representadas pelos fatores primos A e B de N. Fatorar N, quando este é grande, é uma tarefa excessivamente difícil pelos métodos conhecidos atualmente, senão vejamos:

> Decifrar o RSA é *teoricamente* muito simples: o obstáculo é de natureza tecnológica. Usando como chaves de codificação do RSA números muito grandes (de 150 algarismos ou mais), fatorar n, para achar p e q, com os métodos atuais levaria alguns milhares de anos. É disto que depende a segurança do RSA; da ineficiência dos métodos de fatoração atualmente conhecidos (COUTINHO, 2005, p. 4).

Então, para a segurança do RSA, n deve ser bem grande e consequentemente a e b também serão. Neste processo, os fatores primos de n também serão de difícil verificação, conforme estudado no decurso deste trabalho. Extrai-se daqui a elevada importância dos testes de primalidade, fundamentais na localização de primos cada vez maiores e sua utilização em métodos como o RSA.

9 CONCLUSÃO

Após a análise dos testes de primalidade e consumadas as discussões apresentadas no transcurso deste trabalho, pode-se inferir importantes resultados alcançados após aplicação dos métodos pré-selecionados e abordagens das referências empregadas.

Um relevante aspecto acerca dos primos é a possibilidade de encontrar alguns destes por meio de fórmulas. Neste sentido, apresentamos a fórmula proposta por Pierre de Fermat, todavia esta se mostrou verdadeira apenas para alguns valores testados. Outra forma de gerar primos mostrada nesse trabalho foi a proposta apresentada pelo estudioso Mersenne, na forma $2^m - 1$, em que m é primo, a qual é capaz de gerar primos para diversos valores de m. Os maiores primos conhecidos são do tipo idealizado por Mersenne.

Com o mesmo objetivo, porém com uma diferente abordagem, apresentamos a função π de Gauss, desenvolvida durante vários anos até que se demonstrasse o Teorema dos Números Primos, que provou que $\pi(x)$ tende a se aproximar de $x/\ln x$ à medida que o valor de x aumenta. Além desta, outra função de importância na atualidade, é a Função Zeta de Riemann, desenvolvida a partir da Função Zeta de Euler, que mostramos resultar em uma notável conjectura nomeada Hipótese de Riemann. Apesar de ainda não provada, os resultados desta estruturam relevantes testes de primalidade apresentados nos últimos anos.

Os resultados que exibimos sobre os números primos serviram de base para a elaboração daquelas que podemos considerar as principais de formas de localizá-los, os testes de primalidade. Estes algoritmos utilizam como base fatos resultantes de teoremas e propostas de estrutura de primos, para então identificá-los após a realização de uma série de etapas pré-definidas.

Tratamos do estudo dos métodos de localização dos primos de forma cronológica, abordando sua forma mais elementar até as mais sofisticadas, dividindo-os em dois grandes grupos: os testes pré-computacionais e os computacionais. Nessa linha, saímos das formas mais simplórias de buscar primos,

como as divisões sucessivas, até os testes mais complexos, como o APR, demonstrando como se deu esse processo de evolução.

Observou-se que as etapas históricas de evolução dos testes de primalidade foram alicerçadas em diversos fatores, dos quais um mereceu grande destaque: o progresso da tecnologia. Apresentamos a evolução das máquinas e sua conexão com os testes de primalidade. A nível de exemplificação, destacamos a calculadora mecânica de Leibniz e a máquina analítica de Babbage, que evoluíram até culminarem nos computadores modernos, cujas ideias iniciais se fundamentaram nos trabalhos de Turing.

No campo computacional, os importantes aspectos que detalhamos sobre os testes foram o custo de um algoritmo, com destaque para o tempo polinomial e o tempo exponencial, além de abordá-los mediante sua divisão em testes determinísticos e não determinísticos

Os testes discorridos nesse estudo foram iniciados pelos clássicos, incluídos na era pré-computacional. O primeiro foi o de Divisão por Tentativa, seguido pelo Crivo de Eratóstenes, o Teste de Fermat, o teste probabilístico de Proth, o Teste de Pepin, o Teste de Lucas-Lehmer (utilizado frequentemente para testar números de Mersenne M_p) e o crivo de Sundaram.

Em cumprimento ao acompanhamento do processo de evolução dos testes de primalidade, analisamos também os testes da era computacional, iniciando pelo estudo do algoritmo de Solovay-Strassen e seguindo pelo teste probabilístico de Miller-Rabin, acompanhado pela apresentação do inovador teste AKS, de Manindra Agrawal, Neeraj Kayal e Nitin Saxena, divulgado em 2006.

Um pensamento diferente que relacionamos à procura de primos é o uso de mais de um teste de primalidade para um mesmo número. É a forma de abordagem do Teste de Baillie-PSW. Outros testes que mostramos consistem em temas matemáticos avançados, como o APR. Por fim, também foi abordado o teste de algoritmo ECPP (Eliptic Curve Primality Proving), com uso de equações cúbicas.

Apresentamos um método criptográfico que revolucionou as relações financeiras do mundo contemporâneo: a criptografia RSA. Esta ferramenta surgiu a partir de importantes fatos sobre os primos, como o da sua difícil localização para valores elevados e consequente dificuldade de fatoração de grandes números, o que torna os processos financeiros mais seguros.

Os testes apresentados e discorridos neste estudo mostraram a linha evolutiva dos conhecimentos acerca dos primos e os importantes passos dados ao longo dos anos para um conhecimento mais aprofundado destes números. Pode-se verificar as diversas formas de abordagem para se localizar primos, dentre as quais destacamos: a *força bruta* de divisões sucessivas; o uso de crivos (tabelas de números com exclusão de algarismos compostos) para filtrar conjuntos de números naturais e localizar primos; a utilização de teoremas sobre propriedades dos primos e, por fim, a utilização de conceitos avançados em matemática.

Com resultados amplos ou restritos, seguros ou prováveis, rápidos ou demorados, os testes aqui apresentados tiveram como fundamentos descobertas sobre os primos reveladas ao longo dos anos e processos engenhosos de localização destes números, o que nos leva a garantir que essa busca por formas cada vez mais rápidas e confiáveis permanecerá por anos a frente, tornando este trabalho um alicerce para pesquisa futuras, apoiadas nas descobertas a serem reveladas.

REFERÊNCIAS

AGRAWAL, M. Primality tests based on Fermat's little theorem. In: CHAUDHURI , S., et al. **Distributed computing and networking:** 8th International Conference, ICDCN 2006, Guwahati, India, December 27-30, 2006, proceedings. [S.l.]: Springer Science & Business Media, v. 4308, 2006. ISBN 978-3-540-68139-7.

AGRAWAL, M.; KAYAL, N.; SAXENA, N. PRIMES is in P. **Annals of Mathematics**, v. 160, p. 781-793, Setembro 2004. Disponivel em: <https://annals.math.princeton.edu/wp-content/uploads/annals-v160-n2-p12.pdf>. Acesso em: 05 Junho 2021.

ÁVILA, G. A série harmônica e a fórmula de Euler-Maclaurin. **Matemática Universitária,** Rio de Janeiro, n. 19, p. 55-63, Dezembro 1995. Disponivel em: <https://rmu.sbm.org.br/wp-content/uploads/sites/27/2018/03/n19_Artigo05.pdf>. Acesso em: 05 Janeiro 2021.

BOYER, C.. **História da Matemática**. Tradução de Elza F. Gomide. São Paulo: Edgard Blucher, Ed. da Universidade de São Paulo, 1974.

BROOKSHEAR, J. G. **Ciência da Computação [recurso eletrônico]:** uma visão abrangente. Tradução de Cheng Mei Lee. 7. ed. Porto Alegre: Bookman, 2008. ISBN 978-85-7780-314-9. Dados Eletrônicos.

CALDWELL, C. K. Probable Prime. **The Prime Pages**, 2021. Disponivel em: <https://primes.utm.edu/glossary/xpage/PRP.html>. Acesso em: 2 maio 2021.

CALDWELL, C. K. The Largest Known prime by Year: A Brief History. **The Prime Pages**, 2021. Disponivel em: <https://primes.utm.edu/notes/by_year.html>. Acesso em: 19 Janeiro 2021.

COLQUITT, W. N.; WELSH JR, L. A NEW MERSENNE PRIME. **Mathematics of Computation**, 56, n. 194, Abril 1991. 867-870. Disponivel em: <https://www.ams.org/journals/mcom/1991-56-194/S0025-5718-1991-1068823-9/S0025-5718-1991-1068823-9.pdf>. Acesso em: 15 Maio 2021.

CORMEM, T. H. et al. **Algoritmos:** teoria e prática. Tradução de Vanderberg D. de Souza. Rio de Janeiro: Elsevier, 2002. ISBN 85-352-0926-3.

COSTA, R. George Boole. **Brasil Escola**, 2007. Disponivel em: <https://brasilescola.uol.com.br/biografia/george-boole.htm>. Acesso em: 06 abril 2021.

COUTINHO, S. C. **Primalidade em Tempo Polinomial:** uma introdução ao algoritmo AKS. Rio de Janeiro: [s.n.], 2004. Disponivel em: <https://dcc.ufrj.br/~collier/Books/AKS1.pdf>. Acesso em: 10 Fevereiro 2021.

COUTINHO, S. C. **Nùmeros Inteiros e Criptografia RSA**. 2ª. ed. RIo de Janeiro: IMPA, 2005. ISBN 85-244-0124-9.

D'AMBROSIO, U. EULER, UM MATEMÁTICO MULTIFACETADO. **Revista Brasileira de História da Matemática**, [S. l.], Vol. 9, n. 17, p. 13-31, 2020. Disponivel em: <https://www.rbhm.org.br/index.php/RBHM/article/view/167. >. Acesso em: 09 Janeiro 2021.

DELUMEAU, J. **A Civilização do Renascimento**. 4. ed. Lisboa: Editorial Estampa, v. I, 1994. ISBN 972-33-1000-7.

FEOFILOFF,. **Minicurso de Análise de Algoritmos**. São Paulo: [s.n.], 2019. Disponivel em: <https://www.ime.usp.br/~pf/livrinho-AA/>. Acesso em: 05 Abril 2021.

FEOFILOFF,. Comparação assintótica de funções. **IME**, 2021. Disponivel em: <https://www.ime.usp.br/~pf/analise_de_algoritmos/aulas/Oh.html>. Acesso em: 05 abril 2021.

FONSECA, J. J. S. D. **Metodologia da Pesquisa Científica**. Fortaleza: UEC, 2002. Apostila.

GEEKSFORGEEKS. Primality Test | Set 4 (Solovay-Strassen). **GeeksforGeeks**, 19 Maio 2021. Disponivel em: <https://www.geeksforgeeks.org/primality-test-set-4-solovay-strassen/>. Acesso em: 01 Junho 2021.

GILBREATH, J. A High-Level Language Benchmark. **BYTE Magazine Volume 06 Number 09 - Artificial Intelligence**, v. 6, Setembro 1981. Disponivel em: <https://archive.org/details/byte-magazine-1981-09/page/n181/mode/2up?q=criteria+were>. Acesso em: 02 Abril 2021.

HEFEZ, A. **Elementos de Aritmética**. Rio de Janeiro: SBM, 2005. ISBN 85-85818-25-5.

HEFEZ, A. **Aritmética**. 1. ed. Rio de Janeiro: SBM, 2014. ISBN 978-85-85818-92-0. (Coleção PROFMAT;08).

HONSBERGER , ROSS. Sundaram's Sieve. **Ingenuity in Mathematics**, New York, v. 23, 1970. ISSN 0394709233. Disponivel em: <https://archive.org/details/ingenuityinmathe0000hons/page/76/mode/2up>. Acesso em: 15 maio 2021.

IMPA. Instituto de Matemática Pura e Aplicada, 15 Janeiro 2019. Disponivel em: <https://impa.br/noticias/descoberto-numero-primo-com-quase-25-milhoes-de-digitos/>. Acesso em: 02 Janeiro 2021.

JÚNIOR, J. G. D. S.; NETO, L. P. V. **Progração Concorrente e Paralela:** algoritmo paralelo para o Crivo de Eratóstenes. [S.l.]: [s.n.], 2009. Disponivel em: <http://www.inf.puc-rio.br/~noemi/pcp-13/primos.pdf>. Acesso em: 09 abril 2021.

LIMA, E. L. **Números e Funções Reais**. 1ª. ed. RIo de Janeiro: SBM, 2013. ISBN 978-85-85818-81-4.

MACHADO, F. B.; MAIA, L. P. **Arquitetura de sistemas operacionais**. 5. ed. Rio de Janeiro: LTC, 2014. ISBN 978-85-216-2287-1.

MARTINEZ, F. E. B. et al. **Teoria dos Números:** um passeio com primos e outros números familiares pelo mundo inteiro. [S.l.]: [s.n.], 2013. Disponivel em: <https://edisciplinas.usp.br/pluginfile.php/4576649/mod_resource/content/1/Um%20passeio%20pelos%20primos%20e%20outros%20n%C3%BAmeros%20familiares.pdf>. Acesso em: 02 Maio 2021.

MORAIN, F. Implementing the Asymptotically Fast Version of the Elliptic Curve Primality Proving Algorithm. **Mathematics of Computation**, Providence - Rhode Island - USA, v. v. 76, n. 257, p. 493-505, Janeiro 2007. Disponivel em: <https://www.ams.org/journals/mcom/2007-76-257/S0025-5718-06-01890-4/S0025-5718-06-01890-4.pdf>. Acesso em: 15 Junho 2021.

MOREIRA, C. G. T. D. A.; SALDANHA, N. C. Critérios de Primalidade, Rio de Janeiro, 19 Junho 2012. Disponivel em: <http://klein.sbm.org.br/wp-content/uploads/sites/17/2016/02/criterios-de-primalidade.pdf>. Acesso em: 02 Junho 2021.

MOREIRA, C. G.; MARTINÉZ, F. E. B. Primos gêmeos, primos de Sophie Germain e o Teorema de Brun. **Matemática Universitária**, Rio de Janeiro, n. 48/49, p. 93-101, Junho/Dezembro 2010. Disponivel em: <https://rmu.sbm.org.br/wp-content/uploads/sites/27/2018/03/n48_n49_Artigo06.pdf>. Acesso em: 06 Janeiro 2021.

O'CONNOR, J.; ROBERTSON, E. François Édouard Anatole Lucas. **MacTutor History of Mathematics Archive**, Dezembro 1996. Disponivel em: <https://mathshistory.st-andrews.ac.uk/Biographies/Lucas/>. Acesso em: 18 Janeiro 2021.

O'CONNOR, J.; ROBERTSON, E. Georg Friedrich Bernhard Riemann. **MacTutor History of Mathematics Archive**, Setembro 1998. Disponivel em: <https://mathshistory.st-andrews.ac.uk/Biographies/Riemann/>. Acesso em: 15 Janeiro 2021.

O'CONNOR, J.; ROBERTSON, E. Eratosthenes of Cyrene. **MacTutor History of Mathematics Archive**, Janeiro 1999. Disponivel em: <https://mathshistory.st-andrews.ac.uk/Biographies/Eratosthenes/>. Acesso em: 16 Janeiro 2021.

O'CONNOR, J.; ROBERTSON, E. Charles Jean Gustave Nicolas Baron de la Vallée Poussin. **MacTutor History of Mathematics Archive**, Março 2001. Disponivel em: <https://mathshistory.st-andrews.ac.uk/Biographies/Vallee_Poussin/>. Acesso em: 16 Janeiro 2021.

O'CONNOR, J.; ROBERTSON, E. Derrick Henry Lehmer. **MacTutor History of Mathematics Archive**, Novembro 2002. Disponivel em: <https://mathshistory.st-andrews.ac.uk/Biographies/Lehmer_Derrick/>. Acesso em: 18 Janeiro 2021.

O'CONNOR, J.; ROBERTSON, E. Jacques Salomon Hadamard. **MacTutor History of Mathematics Archive**, Outubro 2003. Disponivel em: <https://mathshistory.st-andrews.ac.uk/Biographies/Hadamard/>. Acesso em: 2015 Janeiro 2021.

O'CONNOR, J.; ROBERTSON, E. Robert Daniel Carmichael. **MacTutor History of Mathematics Archive**, Fevereiro 2010. Disponivel em: <https://mathshistory.st-andrews.ac.uk/Biographies/Carmichael/>. Acesso em: 30 Abril 2021.

RIBENBOIM, P. **Números Primos:** velhos mistérios e novos recordes. 1. ed. Rio de Janeiro: IMPA, 2014. ISBN 978-85-244-0334-7. (Coleção Matemática Universitária).

SANTOS, J. P. D. O. **Introdução à Teoria dos Números**. 3. ed. Rio de Janeiro: IMPA, 2015. ISBN 978-85-244-0142-8.

SAUTOY, M. D. **A Música dos Números Primos:** a história de um problema não resolvido na matemática. Tradução de Diego Alfaro. Rio de Janeiro: Zahar, 2007. ISBN 978-85-378-007-9.

SPENTHOF, R.; SOUZA, J. D. Primos: da aleatoriedade ao padrão. **Revista eletrônica da Sociedade Brasileira de Matemática**, v.1, n.1. Rio de Janeiro, 2013. 12-31. Disponivel em: <http://pmo.sbm.org.br/wp-content/uploads/sites/16/dlm_uploads/2019/03/art2_vol1_2013_SBM_PMO-1.pdf>. Acesso em: 27 Dezembro 2020.

STEWART, I. **Em Busca do Infinito:** uma história da matemática dos primeiros números à teoria do caos. Tradução de George Schlesinger. Edição digital: fevereiro 2014. ed. Rio de Janeiro: Zahar, 2014. ISBN 978-85-378-1193-1. Disponivel em: <https://lelivros.love/book/baixar-livro-em-busca-do-infinito-ian-stewart-em-pdf-epub-e-mobi-ou-ler-online/>. Acesso em: 22 Dezembro 2020.

STROHMAIER, E. et al. TOP500, 2020. Disponivel em: <https://top500.org/lists/top500/2020/11/>. Acesso em: 30 março 2021.

WAZLAWICK, R. S. **HIstória da Computação**. 1. ed. Rio de Janeiro: Elsevier, 2017. ISBN 978-85-352-8545-1.

WEISSTEIN, E. W. Monte Carlo Method. **MathWorld--A Wolfram Web Resource**, 18 Maio 2021. Disponivel em: <https://mathworld.wolfram.com/MonteCarloMethod.html>. Acesso em: 30 maio 2021.

WEISSTEIN, W. Baillie-PSW Primality Test. **MathWorld**, 23 Julho 2021. Disponivel em: <https://mathworld.wolfram.com/Baillie-PSWPrimalityTest.html>. Acesso em: 25 Julho 2021.

ZIVIANI, N. **Projeto de algoritmos:** com implementações em Java e C++. 1. ed. São Paulo: Cengage Learning, 2011. ISBN 978-85-221-0821-3.

APÊNDICE A – MÁXIMO DIVISOR COMUM E DEMONSTRAÇÕES

A.1 Máximo Divisor Comum. Dados a e b inteiros, com $a \neq 0 \; ou \; b \neq 0$, define-se como máximo divisor comum entre a e b, representado por (a, b), o número inteiro d, tal que d é o maior inteiro que divide a e b.

A.2 Teorema. Se $d = (a, b)$, então existem $m, n \in \mathbb{Z}$, tais que $d = ma + nb$.

Demonstração. Dados a e b inteiros e a combinação linear $ma + nb$, com $m, n \in \mathbb{Z}$. Seja, agora, $t = m'a + n'b$ tal que t é o menor inteiro positivo resultante dessa combinação linear. Devemos provar que t divide a e t divide b. Supondo, por absurdo, que $t \nmid a$, então, pela divisão euclidiana, podemos escrever $a = qt + r$, como $0 < r < t$. Dessa maneira, $r = a - qt = a - q(m'a + n'b) = a - qm'a - qn'b = a(1 - qm') + b(-qn')$. Daí, conclui-se que r é uma combinação linear de a e b, pois $1 - q'm$ e $-qn'$ são inteiros, mas $0 < r < t$ e t é o menor inteiro positivo resultante da combinação linear $ma + nb$, portanto é uma contradição, provando que $t \mid a$. Prova-se que $t \mid b$ de forma análoga.

Agora, como $d = (a, b)$, então existem c' e c" inteiros, tais que $a = c'd$ e $b = c"d$, logo $t = m'a + n'b = m'c'd + n'c"d = d(m'c' + n'c")$, portanto $d \mid t$. Como $d > 0 \; e \; t > 0$, então $d \leq t$, mas d não pode ser menor do que t, pois d é o máximo divisor comum entre $a \; e \; b$. Logo $t = d$ e conclui-se que $d = m'a + n'b$.

A.2.1 Corolário. Para todo t inteiro não nulo, temos $(ta, tb) = t(a, b)$

Demonstração. Pelo teorema anterior, $(ta, tb) = mta + ntb$, $m, n \in \mathbb{z}$. Logo temos

$$(ta, tb) = mta + ntb = t(ma + nb) = t(a, b)$$

A.2.2 Corolário. Se $c > 0$, $c \mid a$ e $c \mid b$, então

$$\left(\frac{a}{c}, \frac{b}{c}\right) = \frac{1}{c}(a, b)$$

Demonstração. Como $c \mid a$, então $\frac{a}{c} \in \mathbb{z}$ e como $c \mid b$, então $\frac{b}{c} \in \mathbb{Z}$, logo $a = ck'$ e $b = ck"$, para k', k" inteiros, assim, para $m, n \in \mathbb{z}$, temos

$$\left(\frac{a}{c},\frac{b}{c}\right)=\left(\frac{ck'}{c},\frac{ck"}{c}\right)=(k',k")=mk'+nk"=\frac{mck'}{c}+\frac{nck"}{c}=\frac{ma}{c}+\frac{nb}{c}=\frac{1}{c}(ma+nb)$$

$$=\frac{1}{c}(a,b)$$

A.2.3 Corolário. Se $d=(a,b)$, para a e b inteiros, e $a\neq 0$ ou $b\neq 0$, temos

$$\left(\frac{a}{d},\frac{b}{d}\right)=1$$

Demonstração.

$$\left(\frac{a}{d},\frac{b}{d}\right)=\left(\frac{a}{(a,b)},\frac{b}{(a,b)}\right)$$

Como (a,b) divide a e divide b, então, pelo corolário anterior,

$$\left(\frac{a}{(a,b)},\frac{b}{(a,b)}\right)=\frac{1}{(a,b)}(a,b)=1$$

A.3 Proposição. Dados a, b e c inteiros positivos tais que $a \mid bc$ e $(a,b)=1$, então $a \mid c$.

Demonstração. Como $(a,b)=1$, pelo Teorema A.2, existem m e n inteiros tais que $ax+by=1$. Multiplicando ambos os membros por c, temos $axc+byc=c$. Como $a \mid axc$ e $a \mid byc$, então $a \mid c$.

A.4 Proposição. Se p é um número primo e $p \mid ab$ então $p \mid a$ ou $p \mid b$.

Demonstração. Se $p \mid a$, está provada a proposição. Se $p \nmid a$, então, como p é primo, então $(a,p)=1$, logo, pela Proposição A.3, $p \mid b$.

APÊNDICE B – NÚMEROS PRIMOS E DEMONSTRAÇÕES

B.1 Lema. Dados os números $\binom{p}{k}$, com $0 < k < p$. Se p é primo, então $\binom{p}{k}$ é divisível por p.

Demonstração. Para $k = 1$, temos

$$\binom{p}{1} = p$$

Logo, divisível por p. Vamos verificar, agora, para $1 < k < p$. Como $k! = k(k-1)(k-2) \cdot \ldots \cdot 2 \cdot 1$, então $k!$ divide $p(p-1) \cdot \ldots \cdot (p-k+1)$. Já que $k!$ e p são primos entre si, então $(k!, p) = 1$, logo $k!$ divide $(p-1) \cdot \ldots \cdot (p-k+1)$. Sabendo-se que

$$\binom{p}{k} = p\frac{(p-1) \cdot \ldots \cdot (p-k+1)}{k!}$$

Então p divide $\binom{p}{k}$, concluindo, assim, a demonstração.

ANEXO C – CONGRUÊNCIAS E DEMONSTRAÇÕES

C.1 Proposição. $a \equiv a \bmod m$, para $a \in \mathbb{Z}, m \in \mathbb{N}$

Demonstração. Decorre imediatamente da definição de congruência

C.2 Proposição. Se $a \equiv b \bmod m$, então $b \equiv a \bmod m$

Demonstração. Decorre imediatamente da definição de congruência

C.3 Proposição. Se $a \equiv b \bmod m$ e $b \equiv c \bmod m$, então $a \equiv c \bmod m$

Demonstração. Decorre imediatamente da definição de congruência

C.4 Proposição. Dados a, b e m inteiros, com $m > 1$, então

$$a \equiv b \bmod m \Leftrightarrow m \mid b - a$$

Demonstração. Se $a \equiv b \bmod m$, então o resto da divisão de a por m é igual ao resto da divisão de b por m, assim, para q_1, r_1, q_2 e r_2 inteiros, temos

$$a = q_1 m + r_1 \Longrightarrow r_1 = a - q_1 m$$

$$b = q_2 m + r_2 \Longrightarrow r_2 = b - q_2 m$$

Com $0 \leq r_1 < m$ e $0 \leq r_2 < m$, logo

$$r_1 = r_2 \Longrightarrow a - q_1 m = b - q_2 m \Longrightarrow a - b = q_1 m - q_2 m \Longrightarrow a - b = m(q_1 - q_2)$$
$$= b - a = m(q_2 - q_1)$$

Portanto,

$$m \mid b - a$$

Reciprocamente, se m divide $b - a$, então existe $c \in \mathbb{Z}$, tal que $b - a = cm$. Fazendo $c = q_2 - q_1$, com q_1 e q_2 inteiros, temos $b - a = (q_2 - q_1)m$, então

$$b - a = (q_2 - q_1)m \Longrightarrow b - a = mq_2 - mq_1 \Longrightarrow b - mq_2 = a - mq_1$$

Como $b - mq_2$ é o resto da divisão de b por m e $a - mq_1$ é o resto da divisão de a por m, e são iguais, então, pela definição de congruência, temos

$$a \equiv b \bmod m$$

Assim, conclui-se que

$$a \equiv b \bmod m \Leftrightarrow m \mid b - a$$

C.5 Proposição. $a \equiv b \bmod m$ e $c \equiv d \bmod m \Longrightarrow a + c \equiv b + d \bmod m$

Para a, b, c, d, m inteiros e $m > 1$

Demonstração. Pela proposição anterior, se $a \equiv b \bmod m$, então $m \mid b - a$ e se $c \equiv d \bmod m$, então $m \mid d - c$. Agora, se $m \mid b - a$, então existe $x \in \mathbb{Z}$, tal que

$$b - a = xm \qquad \text{(I)}$$

Anologamente, se $m \mid d - c$, então existe $y \in \mathbb{Z}$, tal que

$$d - c = ym \qquad \text{(II)}$$

Somando-se (I) e (II), temos

$$(b - a) + (d - c) = xm + ym = m(x + y) \Longrightarrow$$

$$(b + d) - (a + c) = m(x + y)$$

Portanto, m divide $(b + d) - (a + c)$ e, pela proposição anterior, conclui-se que

$$a + c \equiv b + d \bmod m$$

C.6 Proposição. $a \equiv b \bmod m \Leftrightarrow a + c \equiv b + c \bmod m$, para a, b, c, m inteiros e $m > 1$

Demonstração. Se $a \equiv b \bmod m$ e, pela Proposição 1, $c \equiv c \bmod m$, temos, pela Proposição 5, o seguinte

$$a + c \equiv b + c \bmod m$$

Agora, se $a + c \equiv b + c \bmod m$, temos

$$a + c \equiv b + c \bmod m \Longrightarrow m \mid (b + c) - (a + c) \Longrightarrow m \mid b - a \Longrightarrow a \equiv b \bmod m$$

Portanto,

$$a \equiv b \bmod m \Leftrightarrow a + c \equiv b + c \bmod m$$

C.7 Proposição. $a \equiv b \bmod m$ e $c \equiv d \bmod m \Longrightarrow ac \equiv bd \bmod m$

Para a, b, c, d, m inteiros e $m > 1$

Demonstração. Como $a \equiv b \bmod m$ e $c \equiv d \bmod m$, então $m \mid b - a$ e $m \mid d - c$, respectivamente. Dessa forma, para x e y inteiros, temos

$$b - a = xm \quad \text{(I)}$$

$$d - c = ym \quad \text{(II)}$$

Agora, multiplicando (I) e (II) por d e a, respectivamente, temos

$$bd - ad = dxm \quad \text{(III)}$$

$$ad - ac = aym \quad \text{(IV)}$$

Somando-se (III) e (IV), obtemos

$$bd - ac = dxm + aym = m(dx + ay)$$

Logo, $m \mid bd - ac$, e, portanto, $ac \equiv bd \bmod m$.

Uma consequência direta da Prosição 6 é o seguinte corolário

C.7.1 Corolário. Dados n natural e a, b inteiros, temos

$$a \equiv b \bmod m \Longrightarrow a^n \equiv b^n \bmod m$$

C.8 Proposição

$$ac \equiv bc \bmod m \Leftrightarrow a \equiv b \, mod \, \frac{m}{(c, m)}$$

Para a, b, c inteiros e m inteiro maior do que 1.

Demonstração. Seja $ac \equiv bc \bmod m$, com $a, b, c \in \mathbb{Z}$ e $m \in \mathbb{Z}$, $m > 1$, então, pela Proposição C.4,

$$ac \equiv bc \bmod m \Leftrightarrow m \mid bc - ac = m \mid c(b - a) \Leftrightarrow \frac{m}{(c, m)} \mid \frac{c}{(c, m)}(b - a)$$

Como, pelo Corolário A.2.3, $\left(\frac{m}{(c,m)}, \frac{c}{(c,m)}\right) = 1$, então $\frac{m}{(c,m)}$ e $\frac{c}{(c,m)}$ são coprimos[28], logo

$$\frac{m}{(c,m)} \mid \frac{c}{(c,m)}(b-a) \Leftrightarrow \frac{m}{(c,m)} \mid b-a$$

E novamente pela Proposição C.4,

$$\frac{m}{(c,m)} \mid b-a \Leftrightarrow a \equiv b \bmod \frac{m}{(c,m)}$$

C.8.1 Corolário. Da Proposição C.8, se $(c,m) = 1$, então

$$ac \equiv bc \bmod m \Leftrightarrow a \equiv b \bmod m$$

C.9 Proposição. Se p é primo, $(p,a) = 1$ e $a^2 \equiv 1 \pmod p$, então $a \equiv 1 \pmod p$ ou $a \equiv -1 \pmod p$.

Demonstração.

$$a^2 \equiv 1 \pmod p \Leftrightarrow p \mid (a^2-1) \Leftrightarrow p \mid (a+1)(a-1)$$

Como p é primo, então $p \mid (a+1)$ ou $p \mid (a-1)$, portanto $a \equiv -1 \pmod p$ ou $a \equiv 1 \pmod p$.

C.10 Teorema. Sejam a e q inteiros, se $q \nmid a$, $a \not\equiv 1 \pmod q$ e $a \not\equiv -1 \pmod q$ e $a^2 \equiv 1 \pmod q$, então q é composto.

Demonstração. Como $a^2 \equiv 1 \pmod q$, então $q \mid (a^2-1)$ que equivale a $q \mid (a+1)(a-1)$. Supondo que q é primo, então, pela proposição anterior, temos $q \mid (a+1)$ ou $q \mid (a-1)$, um absurdo, pois, por hipótese, $a \not\equiv 1 \pmod q$ e $a \not\equiv -1 \pmod q$, isto é, $q \nmid (a-1)$ e $q \nmid (a+1)$, logo q é composto.

[28] Define-se como *coprimos*, dois números inteiros a e b, cujo único divisor positivo comum é 1, isto é, $(a,b) = 1$. Os números a e b também são definidos como *primos entre si*.