UNIVERSIDADE FEDERAL DO NORTE DO TOCANTINS
CENTRO DE CIÊNCIAS INTEGRADAS
CURSO DE LICENCIATURA EM MATEMÁTICA

ELIAS BEZERRA DA SILVA TELES

NOVO CRITÉRIO DE DIVISIBILIDADE POR PRIMOS: UMA INTERFACE ENTRE ÁLGEBRA E TEORIA DOS NÚMEROS

Araguaína-TO
2023

ELIAS BEZERA DA SILVA TELES

NOVO CRITÉRIO DE DIVISIBILIDADE POR PRIMOS: UMA INTERFACE ENTRE ÁLGEBRA E TEORIA DOS NÚMEROS

Monografia apresentada ao curso de Licenciatura em Matemática da Universidade Federal do Norte do Tocantins – Centro de Ciências Integradas, como requisito parcial para obtenção do título de Licenciado em Matemática.

Orientador: Prof. Dr. José Carlos de Oliveira Junior

Araguaína-TO

2023

Dados Internacionais de Catalogação na Publicação (CIP)
Sistema de Bibliotecas da Universidade Federal do Tocantins

B574n Bezerra da Silva Teles, Elias.
NOVO CRITÉRIO DE DIVISIBILIDADE POR PRIMOS: UMA INTERFACE ENTRE ÁLGEBRA E TEORIA DOS NÚMEROS. / Elias Bezerra da Silva Teles. – Araguaína, TO, 2023.
78 f.

Monografia Graduação - Universidade Federal do Tocantins – Câmpus Universitário de Araguaína - Curso de Matemática, 2023.
Orientador: José Carlos de Oliveira Junior

1. Números primos. 2. Álgebra. 3. Divisibilidade. 4. Critério de Divisibilidade. I. Título

CDD 510

Elaborado pelo sistema de geração automática de ficha catalográfica da UFT com os dados fornecidos pelo(a) autor(a).

ELIAS BEZERRA DA SILVA TELES

NOVO CRITÉRIO DE DIVISIBILIDADE POR PRIMOS: UMA INTERFACE ENTRE ÁLGEBRA E TEORIA DOS NÚMEROS

Monografia apresentada ao curso de Licenciatura em Matemática da Universidade Federal do Norte do Tocantins – Centro de Ciências Integradas, como requisito parcial para obtenção do título de Licenciado em Matemática.

Orientador: Prof. Dr. José Carlos de Oliveira Junior

Data de aprovação: 13 / 12 / 2023

Banca Examinadora

Documento assinado digitalmente
gov.br JOSE CARLOS DE OLIVEIRA JUNIOR
Data: 19/12/2023 20:55:58-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. José Carlos de Oliveira Junior, UFNT – Orientador

Documento assinado digitalmente
gov.br RAIMUNDO CAVALCANTE MARANHAO NETO
Data: 19/12/2023 07:36:26-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. Raimundo Cavalcante Maranhão Neto, UFNT– Examinador

Documento assinado digitalmente
gov.br ROGERIO DOS SANTOS CARNEIRO
Data: 18/12/2023 21:27:42-0300
Verifique em https://validar.iti.gov.br

Prof. Dr. Rogerio dos Santos Carneiro, UFNT – Examinador

Araguaína-TO

2023

Ser é ser percebido. (George Berkley)

AGRADECIMENTOS

Primeiramente, agradecer a Deus por chegar até aqui e por me ajudar a me tornar a pessoa que sou hoje. Em segundo lugar, agradecer à UFNT pela oportunidade de realizar este curso. Agradeço também à minha família por todo o apoio, em especial ao meu pai, Augustinho Conceição Teles, e à minha mãe, Maria Bezerra da Silva Teles. Muito obrigado por tudo que fizeram e que continuam fazendo por mim. Quero expressar minha gratidão à minha companheira de vida, Taynna Fernandes Jesus Antônio, por estar sempre ao meu lado, me incentivando.

Agradecer aos professores do curso de Matemática por todos os ensinamentos e por todo o apoio nos vários momentos de incertezas e frustrações no decorrer da jornada. Em especial, agradeço ao meu orientador, Prof. Dr. José Carlos de Oliveira Junior, por sempre acreditar no melhor que seus alunos podem oferecer, e ao Prof. Dr. Raimundo Cavalcante Maranhão Neto por ser o responsável pela origem da ideia que desencadeou essa pesquisa.

Agradecer também ao Prof. Dr. Sinval de Oliveira, Prof. Dr. Rogério dos Santos Carneiro e ao Prof. Dr. Jamur Andre Venturin. Quero expressar que são excelentes profissionais e que estão sempre dispostos a ajudar seus alunos. No geral, deixo aqui meus sinceros agradecimentos a todos os professores do curso de Licenciatura em Matemática da Universidade Federal do Norte do Tocantins (UFNT). Vocês são engrenagens cruciais e são responsáveis pelo curso ser considerado o melhor na Unidade Cimba.

Para finalizar, agradeço a todos os amigos e a todas as pessoas que conheci ao longo do curso e que de alguma forma influenciaram positivamente meu trajeto. Acredito que o ser humano não chega a lugar nenhum sem boas amizades e boas influências; abandonar isso, para mim, significa decretar falência na vida. Nesse sentido gostaria de expressar minha sincera gratidão a três amigos em especial que me ajudaram imensuravelmente nos momentos difíceis e nas dúvidas. Muito obrigado, Guilherme Silva Guida, Rhiel Natham Ribeiro de Souza e Wellyson Junior Sousa Ferreira.

RESUMO

O presente trabalho consiste em uma pesquisa na área da Teoria dos Números com uma interface em Álgebra, tendo como principais áreas de estudo os números primos e a divisibilidade nos inteiros. Inicialmente abordaremos a importância da Matemática pura, evidenciando a evolução e as descobertas que envolvem números primos e a importância que eles possuem para a criptografia. Posteriormente, voltaremos o olhar para resultados que servirão como porta de entrada para o desenvolvimento do principal objetivo deste trabalho que é enunciar e realizar a demonstração de um novo critério de divisibilidade válido para todo e qualquer número primo maior do que ou igual a sete. Esta pesquisa pode ser incorporada à abordagem qualitativa, utilizando métodos de investigação de natureza bibliográfica. A análise dos dados e a fundamentação da pesquisa serão extraídas de livros, dissertações e monografias. Além disso, os resultados da pesquisa, assim como estudos futuros estão dispostos nas considerações finais desta monografia.

Palavras-chaves: Números primos; Álgebra; Divisibilidade; Critério de Divisibilidade.

ABSTRACT

The present work consists of research in the field of Number Theory with an interface in Algebra, focusing on the prime numbers and divisibility in integers as the main areas of study. Initially, we will address the importance of pure Mathematics, highlighting the evolution and discoveries related to prime numbers and their significance in cryptography. Subsequently, we will turn our attention to results that will serve as a gateway to the development of the main objective of this work, which is to state and demonstrate a new divisibility criterion valid for any prime number greater than or equal to seven. This research can be incorporated into a qualitative approach, using methods of bibliographic investigation. The data analysis and research foundation will be drawn from books, dissertations, and monographs. Additionally, the research results, as well as future studies, are presented in the concluding remarks of this monograph.

Keywords: Prime numbers; Algebra; Divisibility; Divisibility Criterion.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SÍMBOLOS

$\mathbb{Z}$	Inteiros
$\mathbb{R}$	Reais
$\mathbb{N}$	Naturais
$\mathbb{C}$	Complexos
$\equiv$	Congruência
mod	Módulo
$\%$	Porcentagem
log	Logaritmo
$\sum$	Somatório
$\pi(n)$	Função de Euler, contagem de primos menores do que ou iguais a n
$\zeta(s)$	Função Zeta aplicada nos complexos
$\zeta(\sigma)$	Função Zeta aplicada nos reais
$\Longrightarrow$	Implica que
$\Leftrightarrow$	Se, e somente se,
$\leq$	Menor do que ou igual a
$\geq$	Maior do que ou igual a
$\mid$	É divisor de
$\nmid$	Não é divisor de

SUMÁRIO

1 INTRODUÇÃO

A teoria dos números e a álgebra são dois ramos fundamentais da matemática que desempenham papéis vitais na compreensão das propriedades dos números primos, bem como na resolução de problemas relacionados à divisibilidade e à estrutura dos números inteiros. Este trabalho, surge da busca por uma compreensão mais profunda da relação entre primos maiores ou iguais a 7 e das implicações práticas que essa conexão pode oferecer.

A matemática, em sua pureza e abstração, tem sido o caminho do conhecimento humano, revelando padrões e relações que sustentam o nosso mundo. No âmbito da matemática, os números primos, aqueles inteiros indivisíveis por qualquer outro além de 1 e eles mesmos, têm desafiado a mente humana ao longo dos séculos. Sua misteriosa distribuição, sua aparente aleatoriedade e sua importância na criptografia moderna tornam os números primos um campo de estudo fascinante e de extrema importância.

Nesse contexto, a divisibilidade por primos desempenha um papel central, uma vez que serve como um elo entre os números primos e a álgebra, revelando conexões profundas com a teoria dos números. Enquanto critérios de divisibilidade por primos menores, como 2 e 3, são bem compreendidos e amplamente utilizados, a extensão desse conhecimento para primos maiores ou iguais a 7 é uma área menos explorada.

É aqui que entra o cerne deste trabalho, pois ele estabelece uma interface entre a álgebra e a teoria dos números, ao desenvolver um critério de divisibilidade específico para primos maiores. Essa iniciativa não só amplia a compreensão desses primos, mas também promete facilitar a tarefa de verificar algumas divisibilidades, tornando-as acessível e, além disso, de fácil compreensão.

A justificativa para este trabalho decorre da importância intrínseca dos números primos e da necessidade de desenvolver critérios de divisibilidade mais abrangentes e eficazes. Pois, como já foi dito, enquanto a divisibilidade por 2, 3 e 5 é bem conhecida, primos maiores ou iguais a 7 muitas vezes desafiam uma análise direta de divisibilidade. A existência de um novo critério específico para esses primos pode revelar conexões surpreendentes entre eles e, ao mesmo tempo, servir como uma ferramenta valiosa para verificar se um número é primo ou não.

Este trabalho tem como objetivo principal formular e realizar a demonstração algébrica de um novo critério de divisibilidade por primos. Esse critério representa uma

inovação no campo da teoria dos números e tem o potencial de simplificar significativamente o processo de verificação da divisibilidade por primos maiores do que ou iguais a 7 (vale ressaltar que foram realizadas pesquisas para verificar a existência de estudos que envolvam o critério e, até a data de escrita deste trabalho, não foram encontrados possíveis estudos).

Outro objetivo deste trabalho é demonstrar a importância da matemática pura no contexto do desenvolvimento da sociedade. Buscamos destacar como a matemática pura, em sua forma mais abstrata, desempenha um papel fundamental na nossa compreensão do mundo e na solução de problemas que vão além das aplicações diretas. Além disso, realizaremos uma retrospectiva histórica, analisando os estudos, descobertas e formulações relacionadas aos números primos ao longo da história. Destacaremos a importância desses números não apenas como objetos matemáticos fascinantes, mas também como elementos essenciais na criptografia e, por conseguinte, na proteção de dados em escala global. Esses objetivos coletivos guiam nossa pesquisa e buscam contribuir para o avanço do conhecimento matemático e sua relevância na sociedade contemporânea.

Considerando o objetivo principal desta pesquisa, esta assume, inicialmente, um caráter exploratório, uma vez que

> [...] tem como finalidade proporcionar mais informações sobre o assunto que vamos investigar, possibilitando sua definição e seu delineamento, isto é, facilitar a delimitação do tema da pesquisa; orientar a fixação dos objetivos e a formulação das hipóteses ou descobrir um novo tipo de enfoque para o assunto. Assume, em geral, as formas de pesquisas bibliográficas e estudos de caso. (PRODANOV; FREITAS, 2013, p. 51-52).

A metodologia adotada é uma pesquisa qualitativa denominada revisão bibliográfica. Este estudo consiste em um compilado de análise de artigos, livros, dissertações e trabalhos de conclusão de curso no campo da teoria dos números, álgebra e da divisibilidade. Além disso, utilizaremos o método hipotético-dedutivo.

> O método hipotético-dedutivo inicia-se com um problema ou uma lacuna no conhecimento científico, passando pela formulação de hipóteses e por um processo de inferência dedutiva, o qual testa a predição da ocorrência de fenômenos abrangidos pela referida hipótese. (PRODANOV; FREITAS, 2013, p.32).

Karl Popper definiu o método hipotético-dedutivo a partir de críticas à indução, conforme expresso em sua obra "A lógica da investigação científica," que foi publicada em 1935 (GIL, 2008).

Uma das contribuições significativas deste trabalho é a introdução de um novo critério de divisibilidade por primos. Este critério não apenas verifica se um número é divisível ou não por um número primo específico, mas também permite a determinação do resultado (quociente) da divisão (caso a divisibilidade ocorra). Essa abordagem simplificada torna o critério acessível e valioso, não apenas para pessoas que tenham contato mais profundo com a Matemática, mas também para professores e alunos da educação básica. A utilização deste critério pode aprimorar a compreensão das características dos números primos, bem como fortalecer o conhecimento sobre múltiplos e divisores.

Ao final do trabalho (ver anexo A), será disponibilizado um código em HTML com a programação básica do algoritmo, fornecendo as respostas em cada passo. Dessa maneira, o leitor poderá copiar e colar o código em algum site que suporte à programação HTML. Além disso, será disponibilizado outro resultado decorrente do critério (ver anexo B), acompanhado por uma breve explicação e alguns exemplos numéricos.

Este trabalho está organizado da seguinte forma: No Capítulo 2, será abordada a importância que a Matemática desempenha na sociedade, focando especificamente na Matemática pura. Mostraremos as áreas de principais influências e como ela se encaixa na sociedade com o passar do tempo. No Capítulo 3, abordaremos um pouco sobre o mistério que envolve os números primos, explorando a definição e os principais autores que desenvolveram trabalhos e realizaram descobertas sobre esses números. No Capítulo 4, será destacada a importância desses magníficos números na computação, sendo o principal elemento na construção do modelo de criptografia mais utilizado globalmente. Além disso, abordaremos o impacto que a solução de um dos problemas matemáticos mais complexos teria nesse modelo de criptografia. Logo em seguida, no Capítulo 5, iniciam-se os estudos sobre o conteúdo que está intimamente ligado ao principal objetivo desta monografia. Nesse capítulo, serão abordados os múltiplos e as principais propriedades de divisibilidade nos inteiros. Posteriormente, no Capítulo 6, será mostrada a origem do tema desta monografia. Além disso, neste momento, entramos no foco do trabalho, começando com exemplos do que vem a ser um critério de divisibilidade e, em seguida, a demonstração de

alguns critérios mais amplamente conhecidos. Por fim, no Capítulo 7, daremos início às explicações do funcionamento do critério e por que ele é válido apenas para primos com terminações específicas. Além disso, formularemos algumas definições que servirão como suporte para a demonstração do critério. Logo em seguida, no mesmo capítulo, será explanada a demonstração seguida de algumas particularidades e alguns exemplos numéricos.

2 A IMPORTÂNCIA DA MATEMÁTICA PURA

Esta pesquisa tem como base uma área da Matemática que, por muitas vezes, é subjugada e menosprezada por pessoas que ainda não entenderam que o processo de evolução da humanidade se deu primordialmente em decorrência de estudos e aplicações de resultados provenientes dela. Além disso, são poucos os indivíduos que se arriscam a adentrar em estudos, pesquisas e o desenvolvimento de dissertações que estejam relacionadas a essa área de pesquisa. Nesse contexto, este capítulo tem como objetivo principal mostrar a importância da Matemática pura.

É impossível falar de Matemática pura e não ressaltar sua beleza e importância. No entanto, essa beleza que ela possui não é algo fácil e simples de perceber, pelo simples motivo de que é preciso muito esforço e dedicação para se demonstrar algo, por exemplo. E é justamente aqui que chegamos ao ponto chave da questão: a beleza sobre a qual falamos nessa área da Matemática não está compreendida apenas em algo superficial, mas sim no desenrolar, na estruturação, na ordem lógica, nos cálculos envolvidos e, por fim, no resultado obtido.

Em uma entrevista concedida à jornalista Cecília Manzoni e publicada no site do IMPA (Instituto de Matemática Pura e Aplicada) em 17 de junho de 2022, o carioca e pesquisador do IMPA, Arthur Ávila, diz que “A Matemática tem essa opacidade; sua beleza só se revela a quem a explora mais a fundo”. Isso se dá justamente pelo fato mencionado acima, de que a Matemática requer tempo e dedicação para que seus mistérios (opacidade) sejam desvendados e sua beleza se mostre.

Outro ponto importante a destacar é a resiliência que os modelos e as provas matemáticas possuem com o passar do tempo. São imutáveis e têm o poder de serem, de certa forma, eternos, desde que demonstrados corretamente. Para efeito de comparação, se comparado com outros modelos não provenientes da demonstração matemática, como, por exemplo, a linguística, que, por sua vez, sofre mutações com o decorrer do tempo.

Por fim, a Matemática pura desempenha um papel fundamental no desenvolvimento da nossa compreensão do mundo e na evolução da sociedade. Embora muitas vezes possa parecer bastante abstrata e distante das aplicações práticas imediatas, a Matemática pura foi e continua sendo essencial para o desenvolvimento da humanidade de um modo geral.

Com base nisso, o cerne desse trabalho foi fundamentado nessa área da Matemática. Espera-se que ele sirva como implementação ou aplicação em alguma área da Tecnologia, por exemplo, para aprimorar algum algoritmo de divisibilidade que busca números primos, contribuindo, assim, de alguma forma com a teoria dos números.

Deste modo, a seguir, serão listados exemplos em que a Matemática pura possui extrema importância.

2.1 Base do Conhecimento Fundamental

A Matemática pura é a base sobre a qual a Matemática aplicada e outras disciplinas científicas são construídas. Por exemplo, modelos físicos e químicos são desenvolvidos a partir de conceitos da Matemática pura. Ela envolve a investigação de conceitos abstratos, relações e estruturas matemáticas, que podem mais tarde encontrar aplicações práticas em diversas áreas.

2.2 Desenvolvimento de Teorias

A Matemática pura frequentemente leva ao desenvolvimento de teorias matemáticas profundas. Essas teorias não apenas podem ter implicações práticas surpreendentes, mas também influenciar outras áreas da Matemática e até mesmo inspirar avanços científicos em outras disciplinas.

2.3 Inovação e Avanço Tecnológico

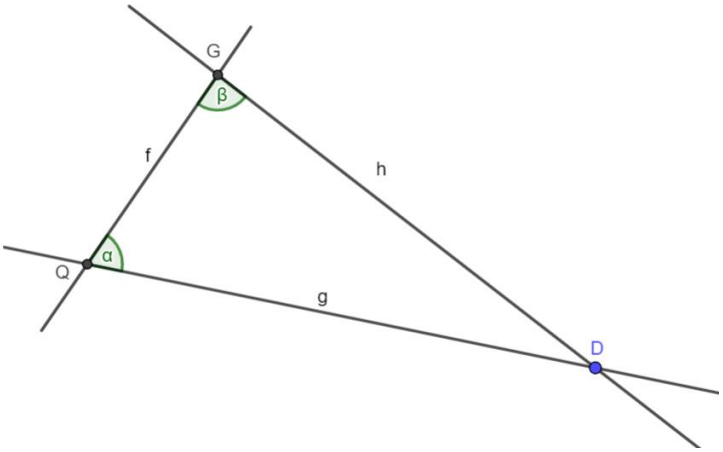
O leitor provavelmente possui algum equipamento eletrônico, como um celular, uma televisão, uma caixa de som, ou até mesmo um automóvel ou uma motocicleta. Todos esses objetos têm algo em comum: desde sua construção até seu funcionamento, só foram possíveis graças aos resultados obtidos a partir da estruturação de modelos matemáticos. Muitos avanços tecnológicos, mesmo aqueles que podem parecer distantes da Matemática pura, têm suas raízes nessa disciplina. As teorias matemáticas puras podem, com o tempo, ser aplicadas a problemas do mundo real, impulsionando a inovação em campos como ciência da computação, engenharia, física e biologia.

Um exemplo que pode ser citado no que diz respeito às aplicações de teorias e resultados no nosso cotidiano teve início com Euclides de Alexandria (300 a.C.), mais especificamente com seu 5º postulado que trata das retas paralelas e afirma o seguinte:

> E, caso uma reta, caindo sobre duas retas, faça os ângulos interiores e do mesmo lado menores do que dois retos, sendo prolongadas as duas retas, ilimitadamente, encontrarem-se no lado no qual estão os menores do que dois retos. (BICUDO, 2009, p.98).

O postulado acima pode ser representado como mostra a Figura 1 a seguir.

Figura 1- Representação do 5° postulado



Fonte: Elaboração do autor.

Esse postulado, por cerca de 2000 anos, foi motivo de várias tentativas frustradas de matemáticos que não conseguiram demonstrá-lo, inclusive o próprio Euclides e vários outros após ele. Isso foi considerado um escândalo geométrico naquela época. Além disso, Karl Friedrich Gauss (1777-1855), considerado por muitos como um príncipe da Matemática, chegou a desenvolver uma geometria que buscava negar o postulado de Euclides, através de uma contradição que, no entanto, não se realizou.

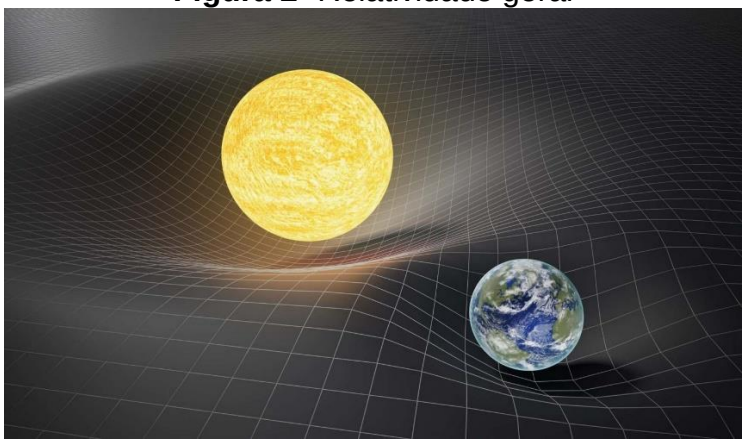
Dessa maneira, somente em 1829, com Nicolai Lobachevsky (1792 - 1856) veio à tona com a publicação de uma geometria que se diferenciava da euclidiana, a qual conhecemos hoje como geometria não-euclidiana.

Mas enfim, o que isso tem a ver com aplicação e avanço tecnológico? Para responder a essa pergunta, é preciso ter em mente quem foi Albert Einstein (1879-

1955) e entender que, entre as várias contribuições que ele deixou para a humanidade, uma se destaca entre todas as outras. É através dela que o homem foi capaz de compreender uma pequena parte de como o universo se comporta. Estamos falando da relatividade geral; essa teoria tem suas bases apoiadas na geometria hiperbólica.

Observe a seguir uma representação da teoria da relatividade geral de Einstein que descreve a deformação que corpos massivos causam no tecido do espaço, como mostra a Figura 2.

Figura 2- Relatividade geral



Fonte: Brasil Escola, 2023
Disponível em: https://brasilescola.uol.com.br/fisica/teoria-relatividade-geral.htm.Acesso em:29/08/2023

Por fim, foi graças à Teoria da Relatividade Geral de Einstein que vários equipamentos tecnológicos puderam ser criados. Um exemplo bem simples a ser citado é o GPS (Global Positioning System), algo que nos dias atuais se torna indispensável. Portanto, na próxima vez que for utilizar um GPS, lembre-se de que ele surgiu implicitamente em 300 a.C. com um postulado. Sendo assim, isso é uma prova incontestável de que os modelos matemáticos, a Matemática pura, mesmo que demorem, em algum momento irão fazer parte do cotidiano da humanidade.

2.4 Treinar a Mente

O estudo da Matemática pura é uma maneira valiosa de desenvolver habilidades analíticas, de resolução de problemas e de raciocínio lógico. Ela ensina a pensar de forma abstrata, a desenvolver argumentos rigorosos e a trabalhar com

conceitos complexos, habilidades que são transferíveis para muitos outros aspectos da vida e do cotidiano, ou seja, a Matemática auxilia no desenvolvimento do indivíduo em outras áreas, isso se deve ao do fato de que, o conhecimento obtido e a maneira utilizada na resolução podem ser adaptados e servirem como base para o desdobramento de outras questões.

2.5 Interdisciplinaridade

A Matemática pura muitas vezes leva a descobertas inesperadas e conexões entre diferentes áreas da Matemática e outras disciplinas, como, por exemplo, a Física e a Química. Essas conexões podem ser responsáveis por novas maneiras de abordar problemas e podem servir como inspiração para o surgimento de colaborações interdisciplinares prósperas.

2.6 Criação de Novos Campos

A exploração de ideias matemáticas puras pode levar à criação de novos campos de estudo. Por exemplo, a topologia algébrica, que inicialmente era uma área da Matemática pura, acabou sendo usada para resolver problemas na física teórica e dessa forma, mais uma vez, a Matemática se mostrou eficiente e essencial.

2.7 Desafios Intelectuais

A Matemática pura é repleta de desafios intelectuais complexos e problemas não resolvidos. Resolver esses problemas não apenas contribui para o avanço do conhecimento humano, mas também oferece satisfação intelectual e um senso de realização para aqueles que os desvendarem.

Um exemplo bem claro desses desafios intelectuais que podem ser mencionados são os problemas matemáticos do Prêmio Millennium, que consiste em 6 problemas matemáticos propostos pelo Instituto CMI (Clay Mathematics Institute), o qual oferece 1 milhão de dólares pela resolução de cada problema. Os problemas do Millennium são:

2.7.1 Conjectura de Birch e Swinnerton-Dyer

Esta conjectura está relacionada com o número de pontos racionais em uma curva elíptica e sua ligação com a ordem do grupo de pontos racionais. É uma questão central na teoria dos números e tem aplicações em criptografia, teoria dos números, entre outros. A conjectura permanece sem solução, embora tenham sido feitos progressos significativos na compreensão de casos especiais. A conjetura pode ser enunciada de forma simplificada da seguinte maneira: *Se E é uma curva elíptica definida sobre os números racionais, então o número de pontos racionais em E (ou seja, soluções racionais para a equação da curva elíptica) está relacionado com a ordem do grupo de Mordell-Weil de E.*

2.7.2 Conjectura de Hodge

Esta conjectura diz respeito à geometria algébrica e à estrutura das soluções de sistemas de equações algébricas. Ela prevê a relação entre a topologia do conjunto de soluções e equações algébricas. Embora seja conhecida em certos casos, permanece em aberto de forma geral, especialmente em dimensões mais altas. A Conjectura de Hodge sugere que a cohomologia de De Rham pode ser decomposta em uma soma direta de subespaços vetoriais, cada um correspondente a uma classe de cohomologia de Hodge. De forma simplificada, podemos escrever:

$$H^*_{DR}(X) \cong \oplus_{p,q} H^{p,q}(X)$$

onde $H^*_{DR}(X)$ representa a cohomologia de De Rham da variedade X e $\oplus_{p,q} H^{p,q}(X)$ representa a soma direta dos termos da cohomologia de Hodge de X.

2.7.3 Equação de Navier-Stokes

Essa equação descreve o comportamento do fluxo de fluidos e é de extrema importância na física e engenharia. Apesar de seu papel fundamental, provar a existência, unicidade e comportamento das soluções para essa equação é um problema em aberto de longa data. A forma geral da equação de Navier-Stokes para o escoamento incompressível (densidade constante) em três dimensões é dada por:

$$\frac{\partial u}{\partial t} + (u \cdot \nabla)u = -\frac{1}{\rho}\nabla p + \nu\nabla^2 u + f\nabla \cdot u = 0$$

Onde:

- u é o vetor de velocidade do fluido em relação ao tempo e ao espaço.
- t é o tempo.
- p é a pressão no fluido.
- ρ é a densidade do fluido.
- ν é a viscosidade cinemática do fluido.
- ∇ é o operador nabla, que representa o gradiente.
- ∇^2 é o operador laplaciano, que representa a divergência do gradiente.
- f representa as forças externas aplicadas ao fluido.

2.7.4 Problema P vs NP

O problema P vs NP é uma questão fundamental na ciência da computação que pergunta se, quando é fácil verificar se uma solução para um problema está correta (P), também é fácil encontrar essa solução (NP). Em outras palavras, ele investiga se a capacidade de verificar soluções é equivalente à capacidade de encontrá-las rapidamente. Por exemplo, se alguém foi encarregado de verificar se o número $3.586.591$ é primo ou composto, provavelmente será uma tarefa árdua, no entanto, se ele tiver conhecimento de que o número é produto entre 1.747 e 2.053, a verificação seria imediata.

2.7.5 Hipótese de Riemann

O teorema dos números primos determina a distribuição média dos números primos. A hipótese de Riemann fala sobre a desvio dessa média. Formulada no artigo de Riemann de 1859, ela afirma que todos os zeros "não óbvios" da função zeta são números complexos com parte real ½, que também é denominada como reta crítica da função zeta de Riemann. A função zeta de Riemann é definida pela seguinte série infinita:

$$\zeta(s) = 1^{-s} + 2^{-s} + 3^{-s} + 4^{-s} + \cdots$$

A hipótese afirma que todos os zeros não triviais (ou seja, que não são zeros esperados devido aos números inteiros negativos) desta função têm parte real igual a

$1/2$. De forma mais precisa, se $\zeta(s) = 0$, então s deve ser da forma $s = a + bi$, onde *a* é ½ e *b* é um número real.

2.7.6 Yang-Mills e o gap de massa

Esse problema surge na teoria quântica de campos, especialmente no contexto da força forte entre partículas elementares. A conjectura sugere a existência de um 'gap de massa', o que significa que certas partículas adquirem massa através de interações. Embora a evidência experimental e simulações apoiem essa ideia, uma prova matemática rigorosa ainda está faltando.

3 RETROSPECTIVA HISTÓRICA SOBRE OS NÚMEROS PRIMOS

Neste capítulo, será apresentada uma retrospectiva histórica acerca do estudo dos números primos, com enfoque nos principais resultados obtidos ao longo do tempo. Destacaremos grandes nomes da Matemática e suas contribuições nesta área, além de abordarmos a definição do que é um número primo. Para concluir, discutiremos a importância deste tema na criptografia.

3.1 Um Segredo Resistente a Revelação

Segundo Abud e Pitta (2014), Pitágoras (570-500 a.C.) estabeleceu uma escola na região que hoje corresponde à Itália, conhecida como a Ordem Pitagórica, com o objetivo de compartilhar suas ideias com as classes que detinham o poder. Essas pessoas eram iniciadas nos profundos mistérios numéricos da organização. Os pitagóricos, como eram conhecidos, dedicaram uma quantidade significativa de tempo e atenção aos números primos. Muitos problemas relacionados à teoria dos números, propostos por eles, ainda permanecem sem solução satisfatória, apesar dos esforços de notáveis matemáticos ao longo dos anos.

Nesse contexto, torna-se interessante entender que a Teoria dos Números é considerada a área de estudo da Matemática que se dedica a entender principalmente o comportamento dos números inteiros ($\mathbb{Z}$) e as relações entre eles. Ela aborda temas de extrema importância, como divisibilidade, congruências e números primos.

Qualquer pessoa que de alguma forma tenha tido contato mais profundo com a Matemática já deve ter se deparado com os números primos e conhecido sua fama, pois, para estar entre os 6 problemas restantes do Prêmio Millennium, é preciso apresentar um nível de dificuldade elevado e, o mais importante, o impacto que a resolução desse problema causaria na sociedade que conhecemos.

Não é de se estranhar que a Hipótese de Riemann (que envolve a conjectura dos primos), citada acima, é considerada um dos problemas mais difíceis. Isso porque os números primos parecem se negar a mostrar seu segredo e de alguma forma se esquivam de qualquer fórmula que possa representá-los. (SAUTOY, 2007).

Essa fama dos números primos já é antiga como vimos no primeiro parágrafo desse tópico, no entanto, foi no adentrar do século $\boldsymbol{XX}$ que ela se consolidou e virou obsessão de muitos matemáticos. Tudo teve início quando o matemático alemão

David Hilbert (1862-1943) em uma palestra no Congresso Internacional de Matemáticos, realizado em Paris, na França, diante de vários cientistas que se fazia presente, apresentou 23 problemas que segundo ele revolucionária a Matemática conhecida: "Quem de nós não gostaria de levantar o véu que esconde o futuro, vislumbrando os próximos avanços da nossa ciência e os segredos do seu desenvolvimento nos séculos que virão?" (SAUTOY, 2007, p. 06).

Dentre os 23 problemas propostos por Hilbert, um dentre todos os outros se destacava, o oitavo da lista. O seu impacto foi tamanho que certa vez perguntaram para Hilbert: "E se, como Barba-Ruiva, você pudesse acordar após 500 anos, o que faria?" Hilbert respondeu: "Eu lhe perguntaria": Alguém conseguiu provar a hipótese de Riemann? " (SAUTOY, 2007, p. 07).

Dessa maneira, a impossibilidade de conseguir encontrar um padrão ou uma fórmula que represente todos os primos faz com que várias outras conjecturas se tornem impossíveis de serem demonstradas, pois as mesmas dependem da resolução da questão anterior.

Logo, nesse momento, vamos adentrar em um dos maiores mistérios do mundo da Matemática, mistério esse que fez grandes nomes da Matemática se debruçarem em estudos na tentativa de desvendá-lo.

3.2 Definição e Principais Autores

Vamos admitir aqui alguma familiaridade do leitor com os conceitos iniciais da Teoria dos Números, como divisor, resto e quociente.

Definição 1: *Dado um número* $\boldsymbol{n} \in \mathbb{Z}$ *, com* $\boldsymbol{n} > \mathbf{0}$ *e* $\boldsymbol{n} \neq \mathbf{1}$ *dizemos que* $\boldsymbol{n}$ *é um número primo se possuir apenas dois divisores positivos distintos, sendo eles* $\mathbf{1}$ *e* $\boldsymbol{n}$*.*

Os números inteiros maiores do que 1 que não são primos, isto é, que não possuem apenas o 1 e eles mesmos como divisores positivos, são chamados de números compostos.

Definição 2: *Um número* $\boldsymbol{b} \in \mathbb{Z}$ *com* $\boldsymbol{b}$ *maior do que 1 é dito composto se não for um número primo, ou seja, se* $\boldsymbol{b}$ *possuir no mínimo três divisores distintos positivos.*

Note que as duas definições apresentadas são muito simples de serem compreendidas, no entanto, apesar dessa simplicidade, é estranho pensar que isso esconde o maior segredo da Matemática atualmente. Tiramos como reflexão que é muito fácil formular problemas elementares que estejam ligados a esses números,

difícil é provar. Isso mostra o quanto a Teoria dos números é bela e ao mesmo tempo de uma complexidade inimaginável.

Veja os exemplos a seguir para compreender melhor as definições acima.

Exemplo 1: O número 7, por exemplo, é um número primo, pois ou únicos divisores positivos de 7 são: 1 e 7.

Podemos representar o conjunto de divisores positivos de 7 por:

$$\mathrm{D}(7)=\{1;7\}$$

Em contrapartida, vamos verificar outro número no exemplo a seguir.

Exemplo 2: O número 8 não pode ser considerado um número primo, pois ele possui mais do que dois divisores positivos. O conjunto que representa todos os divisores positivos de 8 é:

$$\mathrm{D}(8)=\{1;2;4;8\}$$

É importante salientar que, quando queremos saber se um número é ou não é divisor de outro número, basta olharmos se o resto é ou não igual a 0.

Exemplo 3: O número 8 pode ser dividido por 5?

Vamos efetuar essa divisão a seguir.

$$\mathbf{8} = (\mathbf{1} \times \mathbf{5}) + \mathbf{3}$$

A partir do resultado obtido, tiramos como conclusão de que $\mathbf{8}$ não pode ser dividido por 5, logo, 8 não é múltiplo de 5, pois o resto não é igual a 0.

Exemplo 4: O número 65 é divisível por 13?

Aqui já caímos na situação que nos interessa, pois:

$$\mathbf{65} = \mathbf{5} \times \mathbf{13} + \mathbf{0}$$

Nesse caso, obtivemos como quociente um número inteiro e resto 0, logo, é possível afirmar que 65 é múltiplo de 13 e, portanto,13 é divisor de 65.

Matematicamente, escrevemos que $\boldsymbol{M}$ é divisível por $\boldsymbol{Q}$ como:

$$\boldsymbol{Q}|\boldsymbol{M} \iff \boldsymbol{M} = \boldsymbol{XQ} + \mathbf{0} \text{ , com } \boldsymbol{X} \in \mathbb{Z}$$

Conclui-se que “M ser divisível por Q” implica em “Q ser divisor de M” ($\boldsymbol{Q}|\boldsymbol{M}$), e escreve-se $\boldsymbol{Q} \nmid \boldsymbol{M}$ para dizer que $\boldsymbol{Q}$ não é divisor de $\boldsymbol{M}$, ou seja, $\boldsymbol{M}$ não pode ser escrito como $\boldsymbol{M} = \boldsymbol{XQ} + \mathbf{0}$ para $\boldsymbol{X} \in \mathbb{Z}$, logo, $\boldsymbol{M}$ não é múltiplo de $\boldsymbol{Q}$.

Esse tema sobre divisores será trabalhado com mais ênfase quando formos trabalhar com divisibilidade no conjunto dos inteiros.

Para iniciar nossa viagem pelo tempo, começaremos com uma pergunta: você já parou para pensar no porquê os números primos são chamados de “primos”? Surgiu

do nada? Para responder essa pergunta, iniciaremos com um dos matemáticos mais intrigantes e misteriosos que se tem conhecimento.

3.2.1 Pitágoras de Samos

Você provavelmente ao longo de sua jornada educacional com certeza já teve contato com o famoso Teorema de Pitágoras (se aplica no triângulo retângulo), no entanto, apesar desse resultado ser o mais famoso de Pitágoras, não foi sua única contribuição para a Matemática. Os “números primos”, como conhecemos hoje foi pensado muito provavelmente por Pitágoras por volta dos anos 530 a.C. e ao contrário do que se pensa, essa expressão não tem ligação alguma com algum tipo de “grau de familiaridade”, mas sim com o termo “primário” (SILVEIRA,2001).

A escola pitagórica citada acima prestava devoção ao número 1 (em grego: *monad*) que, para eles, era considerado a unidade fundamental, o bloco que constrói outros blocos, em resumo, a *origem*. Em contrapartida, todos os restantes que eram gerados pela *origem* eram denominados números (em grego: *arithmós*).

Vamos encarar essa diferenciação como o berço do surgimento desse mistério. E nesse momento você deve estar se perguntando: Mas por quê? Vamos lá; logo depois desse acontecido, Pitágoras percebeu que existiam dois tipos de números, os *protoi arithmói* que eram os números primários ou primos (esses números não podiam ser gerados via multiplicação por outro número, a não ser via próprio número e a *origem*) e os *deuterói arithmói* que eram números secundários que, ao contrário dos *protoi arithmói,* poderiam ser gerados por outros números, como por exemplo, $\mathbf{4} = \mathbf{2} \times \mathbf{2}$ e $\mathbf{20} = \mathbf{5} \times \mathbf{4}$.

Logo, ao final de todo o processo, o que conhecemos hoje como conjunto dos naturais foi dividido em três classes: *monad, protoi arithmói e os deuterói arithmói*.

Logo adiante, vamos falar um pouco sobre Euclides de Alexandria e será possível perceber uma influência dessas formulações dos pitagóricos para a famosa obra dos Elementos de Euclides e o TFA (Teorema Fundamental da Aritmética).

3.2.2 Erastóstenes

Eratóstenes (276-194 a.C.) foi um brilhante matemático de seu tempo, além de poeta, linguista e astrônomo. É considerado por muitos como o pai da geografia pelo fato de ter determinado com precisão o perímetro da terra. Por seus cálculos, a Terra possuía $\mathbf{40.000}\ \boldsymbol{km}$ de perímetro, e os cálculos feitos nos dias atuais, com equipamentos altamente precisos, revelam que a Terra possui $\mathbf{40.075,017}\ \boldsymbol{km}$, ou seja, Eratóstenes errou por $\mathbf{0,18}\%$. Levando em consideração as limitações e as poucas ferramentas que ele possuía, essa margem de erro pode ser desconsiderada.

No entanto, daremos enfoque em seu lado como matemático, mais precisamente em sua contribuição para os números primos, pois ele foi responsável pela primeira ferramenta capaz de encontrar números primos até um certo $\boldsymbol{n}$, chamada de o Crivo de Eratóstenes. Esse método ainda pode ser utilizado até os dias atuais, todavia torna-se de difícil manuseio caso $\boldsymbol{n}$ seja muito grande.

O crivo consiste basicamente em encontrar um primo da lista em ordem crescente e, a partir dessa identificação, inicia-se o processo de eliminação de números múltiplos do primo identificado. Agora, para uma melhor compreensão do funcionamento do crivo de Eratóstenes, imagine que você queira determinar todos os números primos até 50. Para isso, apresentamos a tabela 1 a seguir que lista todos os inteiros de 2 até 50.

Tabela 1- Inteiros de 2 a 50

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

Fonte: Elaboração do autor.

Veremos agora como Eratóstenes pensou para conseguir todos os primos dessa sequência.

i) O primeiro primo da lista é 2, logo cortaremos todos os múltiplos de 2 ($> \mathbf{2}$). 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50.

ii) O 3 é primo, corta-se todos os múltiplos de 3 ($> \mathbf{3}$) (observe que restam apenas múltiplos ímpares).
9, 15, 21, 27, 33, 39, 45.

iii) O 5 é primo, corta-se todos os múltiplos de 5 ($> \mathbf{5}$) (observe que só restam os múltiplos que possuem fatores primos $\geq \mathbf{5}$).
25, 35.

iv) O 7 é primo, corta-se todos os múltiplos de 7 ($> \mathbf{7}$) (observe que os múltiplos de 7 que são múltiplos de 2, 3 e 5 já foram retirados).
49.
Chegamos ao final com os números: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43 e 47.

Mas por que não continuamos e fizemos para o 11? Ou para o 13? O processo se encerra no momento que você passa para o próximo número primo da lista e não encontra nenhum múltiplo dele. Observe na lista final que, se fôssemos cortar os múltiplos de 11 (próximo primo), não encontraríamos nenhum, pois, os múltiplos de 11 ($> \mathbf{11}$) entre 2 e 50 são:22,33,44. Veja que dois deles são múltiplos de 2 e o outro é múltiplo de 3. O mesmo acontece para os múltiplos de 13 ($> \mathbf{13}$) que são: 26 e 39.

O crivo pode ser interpretado da seguinte maneira: Um número $\boldsymbol{A}$ só vai ser primo se não existir nenhum primo que é divisor de $\boldsymbol{A}$ no intervalo $[\mathbf{1}; \boldsymbol{A} - \mathbf{1}]$, ou seja, como o processo de corte ocorre da esquerda para a direita, para $\boldsymbol{A}$ ser um número primo, obrigatoriamente ele não deve ser identificado como composto e como ele não foi identificado como múltiplo de nenhum outro primo antes dele, isso significa que ele só pode ser primo. Para um melhor entendimento, observe os exemplos a seguir.

Exemplo 5: 21 é primo ou composto?

Pelo crivo, para 21 ser primo, ele obrigatoriamente não deve ser divisível por nenhum outro número primo entre $[\mathbf{1}; \mathbf{21} - \mathbf{1}]$. Vamos verificar se isso ocorre identificando os primos entre 1 e 20 que são: 2,3,5,7,11,13,17 e 19. Agora é possível notar que 21 é múltiplo de 3 (3 é um número primo), logo, 21 é composto.

Exemplo 6: 73 é primo ou composto?

Pela mesma linha de raciocínio do exemplo anterior, vamos verificar se 73 pode ser dividido por algum número primo entre $\mathbf{2}$ e $\mathbf{72}$. Os primos dessa sequência são: 2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67 e 71. Note que nenhum dos números primos da sequência é divisor de $\mathbf{73}$, logo, ele só pode ser primo.

A limitação do crivo ocorre caso o número que venha a ser verificado for muito grande, pois, se pararmos para pensar, os números primos ocorrem em uma frequência bem menor do que compostos. Vamos verificar se isso é verdade? Imagine a sequência de números que vai de 2 até 300. Podemos pressupor uma aproximação da porcentagem de primos ou compostos nessa sequência? Sim! Aplicando o crivo, segue que:

- Retirando os pares maiores que 2 (149 números)

4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28, 30, 32, 34, 36, 38, 40, 42, 44, 46, 48, 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 72, 74, 76, 78, 80, 82, 84, 86, 88, 90, 92, 94, 96, 98, 100, 102, 104, 106, 108, 110, 112, 114, 116, 118, 120, 122, 124, 126, 128, 130, 132, 134, 136, 138, 140, 142, 144, 146, 148, 150, 152, 154, 156, 158, 160, 162, 164, 166, 168, 170, 172, 174, 176, 178, 180, 182, 184, 186, 188, 190, 192, 194, 196, 198, 200, 202, 204, 206, 208, 210, 212, 214, 216, 218, 220, 222, 224, 226, 228, 230, 232, 234, 236, 238, 240, 242, 246, 248, 250, 252, 254, 256, 258, 260, 262, 264, 266, 268, 270, 272, 274, 276, 278, 280, 282, 284, 286, 288, 290, 292, 294, 296, 298, 300.

-Retirando ímpares múltiplos de 3 (49 números)

9, 15, 21, 27, 33, 39, 45, 51, 57, 63, 69, 75, 81, 87, 93, 99, 105, 111, 117, 123, 129, 135, 141, 147, 153, 159, 165, 171, 177, 183, 189, 195, 201, 207, 213, 219, 225, 231, 237, 243, 249, 255, 261, 267, 273, 279, 285, 291, 297.

- Retirando múltiplos de 5 (19 números)

25, 35, 55, 65, 85, 95, 115, 125, 145, 155, 175, 185, 205, 215, 235, 245, 265, 275, 295.

-Retirando múltiplos de 7 (10 números)

49, 77, 91, 119, 133, 161, 203, 217, 259, 287.

-Retirando múltiplos de 11 (5 números)

121, 143, 187, 209, 253,

-Retirando múltiplos de 13 (4 números)

169, 221, 247, 299

-Retirando múltiplos de 17 (1 número)

289.

Analisando a situação inicial que envolvia 299 números e aplicando o crivo, tivemos um total de: 149+49+19+10+5+4+1=237 números compostos e somente 62 números primos que são: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151,

157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241, 251, 257, 263, 269, 271, 277, 281, 283, 293. Representando em porcentagem, a quantidade de primos existentes entre 2 e 300, chegamos a aproximadamente $\mathbf{20,73}\%$ e isso pode servir como justificativa para a limitação do crivo, pois, conforme o número a ser verificado aumente, a chance de ele ser composto é maior do que a de ele ser primo.

Para um melhor esclarecimento, a frequência que primos ocorrem entre $\mathbf{2}$ e $\mathbf{500}$ é $\mathbf{17,43}\%$ que representa $\mathbf{87}$ dos $\mathbf{499}$ números e a quantidade de primos entre $\mathbf{2}$ e $\mathbf{1000}$ é exatamente $\mathbf{168}$ números que representa $\mathbf{16,81}\%$ do total de 999 números (em todos os exemplos o número $\mathbf{1}$ é desconsiderado pois não é considerado um número primo e nem composto).

Buscar explicações para responder questões ligadas a números primos é sempre complexo, no entanto, em alguns casos, podemos cogitar algumas suposições que tentam nos dar um norte para o problema.

Por exemplo, para responder essa questão da chance de um número extremamente grande ser composto ao invés de primo podemos pensar no seguinte argumento: quanto maior for o número, maior serão as chances de ele ser múltiplo dos outros compostos ou primos antes dele, e se avançarmos mais ainda, o novo número pensado possui uma maior quantidade de números antecessores a ele do que o anterior, inclusive, o novo número pode ser múltiplo do anterior que havíamos pensado já que ele pode ser muito maior do que o mesmo.

Nessa direção, um resultado muito interessante na Teoria dos números é chamado "*O deserto de números primos",* que nos mostra a existência de longas sequências de números inteiros positivos consecutivos, a qual não possui nenhum número primo. Outro ponto a ser destacado é que é possível construir uma sequência com a quantidade desejada de números que se queira, por exemplo, com $\mathbf{36, 70, 140}$, $\mathbf{2584}$ ou $\mathbf{4054785484}$ números consecutivos tais que nenhum termo é primo.

Até esse momento, o leitor já deve saber a diferença entre um número primo e um composto e, para compreendermos o resultado citado no parágrafo acima, devemos saber que todo número inteiro fatorial pode ser dividido por todos os outros que entraram no processo multiplicativo até chegar no número fatorial, ou seja, $\boldsymbol{p}!$ pode ser dividido por $\mathbf{1, 2, 3, 4, 5, 6}, \ldots\ldots, (\boldsymbol{p}-\mathbf{2}), (\boldsymbol{p}-\mathbf{1})$ e por $\boldsymbol{p}$. Vamos tomar como exemplo o $\mathbf{7}! = \mathbf{7} \times \mathbf{6} \times \mathbf{5} \times \mathbf{4} \times \mathbf{3} \times \mathbf{2} \times \mathbf{1} = \mathbf{5040}$, agora observe que $\mathbf{5040}$ é divisível

por todos os números que foram multiplicados para obtê-lo e daqui tiramos como conclusão que todo $\boldsymbol{p}!$ com $\boldsymbol{p} > \mathbf{2}$ é um número composto (portanto, não primo). Para finalizar, devemos entender que, dados dois números inteiros positivos múltiplos de $\boldsymbol{a}$, a soma desses dois inteiros também será um múltiplo de $\boldsymbol{a}$.

Segue que, sendo $\boldsymbol{L}$ e $\boldsymbol{M}$ os inteiros com $\boldsymbol{L} = \boldsymbol{a} \times \boldsymbol{b}$ e $\boldsymbol{M} = \boldsymbol{a} \times \boldsymbol{c}$ teremos:

$$\boldsymbol{L} + \boldsymbol{M} = \boldsymbol{a} \times (\boldsymbol{b} + \boldsymbol{c})$$

Agora, seja $\boldsymbol{p} > \mathbf{2}$ um inteiro e considere a sequência de $\boldsymbol{p}$ números consecutivos:

$$\boldsymbol{p}! + \mathbf{2}, \boldsymbol{p}! + \mathbf{3}, \boldsymbol{p}! + \mathbf{4}, \boldsymbol{p}! + \mathbf{5}, \ldots\ldots, \boldsymbol{p}! + \boldsymbol{p}$$

Observe que a sequência é formada apenas por números compostos consecutivos, já que $\boldsymbol{p}!$ é divisível por $\mathbf{1}, \mathbf{2}, \mathbf{3}, \mathbf{4}, \mathbf{5}, \mathbf{6}, \ldots\ldots, (\boldsymbol{p} - \mathbf{2}), (\boldsymbol{p} - \mathbf{1})$ e $\boldsymbol{p}$ e dessa maneira, $\boldsymbol{p}! + \mathbf{2}$ é divisível por 2, $\boldsymbol{p}! + \mathbf{3}$ é divisível por 3, $\boldsymbol{p}! + \mathbf{4}$ é divisível por 4, $\boldsymbol{p}! + \mathbf{5}$ é divisível por 5, até chegarmos que $\boldsymbol{p}! + \boldsymbol{p}$ é divisível por $\boldsymbol{p}$. Assumindo um valor para $\boldsymbol{p} = \mathbf{8}$, por exemplo, segue que $\mathbf{8}! = \mathbf{40320}$ e

$$\mathbf{8}! + \mathbf{2}, \mathbf{8}! + \mathbf{3}, \mathbf{8}! + \mathbf{4}, \mathbf{8}! + \mathbf{5}, \mathbf{8}! + \mathbf{6}, \mathbf{8}! + \mathbf{7}, \mathbf{8}! + \mathbf{8}$$
$$= \mathbf{40322}, \mathbf{40323}, \mathbf{40324}, \mathbf{40325}, \mathbf{40326}, \mathbf{40327}, \mathbf{40328}$$

é uma sequência formada inteiramente por $\mathbf{7} = \boldsymbol{p} - \mathbf{1}$ números compostos. Observe que a quantidade de números da sequência é sempre uma unidade abaixo do valor escolhido para $\boldsymbol{p}$, pois é necessário excluir o $\boldsymbol{p}! + \mathbf{1}$, uma vez que não se sabe a natureza desse número (primo ou composto). Se quisermos, por exemplo, 1 milhão de números inteiros consecutivos compostos, basta escolhermos $\boldsymbol{p} = \mathbf{1.000.001}$ e construirmos a lista $\boldsymbol{p}! + \mathbf{2}, \boldsymbol{p}! + \mathbf{3}, \ldots, \boldsymbol{p}! + \boldsymbol{p}$. Logo, tiramos como conclusão que, ao avançarmos no conjunto dos naturais, torna-se cada vez mais difícil encontrar um número primo, pois os desertos vão ficando cada vez maiores à medida que o número tomado aumenta.

3.2.3 Euclides de Alexandria

Falar de Matemática e não citar Euclides de Alexandria é praticamente um pecado, visto que ele foi um matemático sem igual, que dispensa apresentações, um dos maiores gênios que a humanidade já possuiu. Feliz foi aquele que teve o prazer de estar ao seu lado.

Euclides foi um dos matemáticos mais importantes da Grécia e ganhou destaque por sua famosa obra "Os Elementos", que até os dias atuais serve como base para o ensino da Matemática, principalmente no que diz respeito à Geometria Plana. A obra é constituída por um total de 13 livros nos quais ele trabalhou com vários temas, incluindo Geometria Plana, Teoria dos Números, Teoria das Proporções e Geometria no Espaço.

Se pararmos para pensar, tudo no universo é constituído pela menor parte possível! Não existe algo (matéria) que não satisfaça essa afirmação. Isso implica que tudo que existe no universo possui algo em comum: todas as coisas são formadas por diferentes tipos de átomos, mesmo que com características diferentes, são todos átomos. Fazendo uma analogia com a Matemática, você perceberá que o universo divide essa particularidade com os números, e Euclides foi o primeiro a perceber isso.

Como já foi citado anteriormente, Pitágoras definiu que existiam dois tipos de números (arithmós), os *Protói arithmói* (números primos) e os *Deuterói arithmói* (números secundários) e segundo eles os números secundários poderiam ser formados via multiplicação por outros números, como por exemplo, $\mathbf{136 = 68 \times 2}$ e $\mathbf{30 = 15 \times 2}$. Euclides foi um pouco mais além e chegou a uma conclusão de que todos os números positivos, com exceção do 1, podem ser representados via multiplicação por fatores primos e esse é um dos resultados mais importantes da Teoria dos Números e é conhecido como TFA (Teorema Fundamental da Aritmética), ou seja, na verdade o $\mathbf{136 = 2 \times 2 \times 2 \times 17}$ e $\mathbf{30 = 2 \times 3 \times 5}$.

Chegamos à conclusão de que, igualmente ao universo, os números também possuem uma espécie de átomo, os números primos. É importante destacar que, apesar de Euclides ter sido o primeiro a pensar no TFA, ele só foi demonstrado completamente por Gauss em 1801 na obra *Disquisitiones Arithmeticae.*

Teorema 1 *(Teorema Fundamental da Aritmética): Seja* $\boldsymbol{n \geq 2}$ *um número natural. Podemos escrever* $\boldsymbol{n}$ *de uma única forma como um produto de primos* (MARTINEZ et al., s.d).

Não estando satisfeito, Euclides foi o primeiro a demonstrar a infinidade dos números primos através de uma forma de demonstração conhecida hoje como: Demonstração por contradição (redução ao absurdo). Esse tipo de demonstração consiste em negar ou assumir como verdade o que se pretende demonstrar e chegar a um resultado oposto ao que foi assumido.

3.2.3.1 Infinitude dos primos e a demonstração de Euclides

Teorema 2: *Os números primos ocorrem infinitamente.*

Demonstração: Para fazer a demonstração, Euclides supôs que a quantidade de números primos é finita e determinou um que seria o maior de todos, vamos nos referir a ele como $\boldsymbol{M_P}$ (maior primo) e o conjunto de todos os números primos $\boldsymbol{C_P}$ (conjunto de todos os primos). Teríamos:

$$\boldsymbol{C_P = (2, 3, 5, 7, \ldots., M_P)}$$

A partir desse conjunto, é possível construir um novo número maior do que todos dentro dele e teríamos $\boldsymbol{N}$ (novo número) como:

$$\boldsymbol{N = 2 \times 3 \times 5 \times 7 \times \ldots \times M_P + 1}$$

O número 1 foi somado estrategicamente para que $\boldsymbol{N}$ não seja divisível por nenhum primo do conjunto, ou seja, a divisão de $\boldsymbol{N}$ por qualquer primo do conjunto sempre deixará resto 1.

Chegamos à conclusão de que $\boldsymbol{N}$ pode ser primo ou composto e se ele for primo, temos a contradição e a demonstração estará concluída, pois inicialmente foi tomado que $\boldsymbol{M_P}$ seria o maior primo e $\boldsymbol{N > M_P}$. Em contrapartida, se $\boldsymbol{N}$ for composto, pelo TFA, ele pode ser representado por fatores primos, no entanto, $\boldsymbol{N}$ não é divisível por nenhum outro primo do conjunto, logo, existem números primos que são fatores de $\boldsymbol{N}$ e são maiores que $\boldsymbol{M_P}$ e chegamos a uma contradição novamente. Desse modo, fica demonstrado que os números primos ocorrem infinitamente.■

Observe os exemplos a seguir para compreender numericamente a demonstração.

Exemplo 7: Vamos supor que o maior número primo seja $\boldsymbol{M_P = 11}$. Logo;

$$\boldsymbol{C_P = (2, 3, 5, 7, 11)}$$

$$\boldsymbol{N = 2 \times 3 \times 5 \times 7 \times 11 + 1}$$

$$\Downarrow$$

$$\boldsymbol{N = 2311}.$$

Como vimos acima, $\boldsymbol{N}$ não é divisível por nenhum primo de $\boldsymbol{C_P}$.Isso significa que ele pode ser primo ou composto e de fato $\boldsymbol{2311}$ é um número primo e $\boldsymbol{2311 > 11}$.

Exemplo 8: Supondo que o maior primo seja $\boldsymbol{M_P = 13}$. Logo;

$$\boldsymbol{C_P = (2, 3, 5, 7, 11, 13)}$$

$$\boldsymbol{N = 2 \times 3 \times 5 \times 7 \times 11 \times 13 + 1}$$

$$\Downarrow$$

$$\boldsymbol{N = 30031}$$

Pela mesma linha de raciocínio, só existem duas possibilidades para $\boldsymbol{N}$, ser primo ou composto e, nesse caso, $\boldsymbol{30031}$ não é um número primo, porém, pelo TFA ele pode ser representado por fatores primos e esses fatores não pertencem a $\boldsymbol{C_P = (2, 3, 5, 7, 11, 13)}$, pois, $\boldsymbol{30031}$ não é múltiplo de nenhum primo do conjunto. Os fatores primos de $\boldsymbol{30031 = 59 \times 509}$ e percebemos que $\boldsymbol{59 > 13}$ assim como $\boldsymbol{509 > 13}$.

3.2.4 Marin Mersenne

Marin Mersenne (1588-1648) foi, na verdade, um padre que se formou em um colégio jesuíta. No entanto, desde muito cedo demonstrou grande interesse pelos estudos em áreas científicas, com destaque para a Matemática. Mersenne chegou a expressar sua insatisfação devido à ausência de lugares onde estudiosos pudessem se reunir para debater descobertas.

> Mersenne lamentava o facto de não existir na altura uma organização formal onde os estudiosos da época se pudessem encontrar regularmente para trocar e discutir ideias e descobertas. Assim, disponibilizou o seu próprio quarto no convento Minim para que se pudessem encontrar estudiosos da época, dando origem aos primeiros encontros regulares de matemáticos que decorreram continuamente desde 1635 até à morte de Mersenne em 1648. (COSTA, 2015 p.50)

Mersenne ficou bastante conhecido por trocar correspondências com outros pesquisadores da época na tentativa de estimular o desenvolvimento científico.

Como já foi mencionado anteriormente, os números primos parecem se esquivar de qualquer expressão que tente representa-los, nesse sentido, “Até os dias atuais não se conhece uma fórmula simples para gerar grandes números primos. Porém existem fórmulas que geram famílias interessantes de números primos” (MOREIRA; SALDANHA, 2008 p.41). Um exemplo de expressão que é capaz de gerar números primos interessantes e grandes foi desenvolvida justamente por Mer
senne, que se dedicou ao estudo dos números primos, mas especificamente na busca por uma expressão que pudesse representar apenas números primos e chegou na seguinte expressão:

$$\boldsymbol{M_n = 2^n - 1}$$

e definiu que se $\boldsymbol{2^n - 1}$ for primo, então $\boldsymbol{n}$ também será primo, no entanto, o contrário nem sempre é verdade, ou seja, partindo do fato de $\boldsymbol{n}$ ser primo não se pode afirmar que $\boldsymbol{M_n}$ será um número primo.

Antes de morrer, ele publicou um trabalho que demonstrava o poder de sua expressão no qual ele afirma que para $\boldsymbol{n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127\ e\ 257}$, $\boldsymbol{M_n}$ será primo e $\boldsymbol{M_n}$ seria composto para todos os primos menores que 257 diferentes dos da lista. No entanto, tempos depois, foi constatado por alguns matemáticos que Mersenne cometeu algumas falhas pois foi verificado que $\boldsymbol{M_{67}}$ e $\boldsymbol{M_{257}}$ na verdade são compostos e $\boldsymbol{M_{61}}$, $\boldsymbol{M_{89}}$ e $\boldsymbol{M_{107}}$ que não estavam na lista eram primos.

Atualmente, a verificação de números extremamente grandes é feita através de computadores, o que nos faz refletir sobre como Mersenne chegou à conclusão de que $\boldsymbol{M_{127}}$ é primo, por exemplo, pois se trata de um número extremamente grande. Para termos uma ideia da complexidade desse número, vamos pegar um $\boldsymbol{n = 23}$ e aplicar a expressão. Logo:

$$\boldsymbol{M_{23} = 2^{23} - 1}$$
$$\boldsymbol{= (2^{20} \times 2^3) - 1}$$
$$\boldsymbol{= (1048576 \times 8) - 1}$$
$$\boldsymbol{= 8388608 - 1}$$
$$\boldsymbol{= 8388607}$$

Observe que 127 é mais que cinco vezes maior do que 23, então;

$$\boldsymbol{M_{127} = (2^{115} \times 2^{12}) - 1}$$
$$\boldsymbol{M_{127} = (8388608^5 \times 2^{12}) - 1}$$
$$\boldsymbol{M_{127} = 8388608^5 \times 4096 - 1}$$
$$\boldsymbol{M_{127} = 170141183460469231731687303715884105727}$$

Se levarmos em consideração que, na época em que Mersenne afirmou que esse número é primo, ele não tinha à sua disposição muitas ferramentas tecnológicas, essa afirmação se torna algo extraordinariamente fantástico e nos mostra que a Matemática é uma ciência que se, manuseada corretamente, é capaz de fazer coisas realmente admiráveis.

3.2.5 Johann Carl Friedrich Gauss

Considerado por muitos como o Príncipe da Matemática, Gauss foi um matemático alemão nascido em 1777 e fez contribuições em diversas áreas da Matemática, inclusive na Teoria dos Números.

Gauss percebeu que, apesar de grandes matemáticos se debruçarem em estudos e pesquisas na tentativa de encontrar uma fórmula que representasse a lista de números primos, o problema parecia impossível nessa perspectiva. Dessa forma, Gauss adotou outra estratégia: ao invés de procurar uma fórmula que representasse esses números, ele se empenhou em estudar a distribuição deles. Tudo começou em 1792, quando ele tinha 15 anos de idade. Pouco tempo depois, recebeu de presente um livro de logaritmos e, ao final do livro, havia uma lista de números primos em anexo. Como qualquer pessoa que tenha contato e certa intimidade com números, ele foi cativado pela curiosidade de entendê-los (SAUTOY,2007). Graças a esse anexo, ele percebeu que, apesar de serem temas aparentemente distintos matematicamente, ainda assim eles tinham uma ligação. Gauss confirmou essa ligação como um bom matemático, através de vários cálculos.

A estratégia utilizada por Gauss foi verificar a quantidade de números primos existentes em intervalos diferentes, por exemplo, a quantidade de primos entre 1 e 100, entre 1 e 1.000 e assim sucessivamente. Para generalizar, se considerássemos o número $\boldsymbol{N}$, existiria alguma maneira de verificar a provável quantidade de primos entre 1 e $\boldsymbol{N}$? Escolhendo $\boldsymbol{N = 100}$, a quantidade de primos entre 1 e 100 é igual 25, concluímos que se escolhêssemos um número aleatório desse intervalo, a chance de ele ser primo está na razão de $\frac{\mathbf{1}}{\mathbf{4}}$ (25%).

No entanto, Gauss foi mais afundo e verificou como essa proporção se comporta caso o intervalo tomado aumente, por exemplo, entre 1 e 1.000 existem 168 números primos o que implica em aproximadamente $\frac{\mathbf{1}}{\mathbf{6}}$ de números primos, ou $\mathbf{16,6666}\ldots\%$.

Não podemos esquecer que ele já estava munido de uma tabela com milhares de números primos. Portanto, essa verificação da quantidade de primos foi facilitada. No entanto, para Gauss, a quantidade de primos era apenas o início. O que ele realmente buscava era um padrão à medida que o intervalo aumentasse, e ele obteve êxito em sua procura, acabou descobrindo uma regularidade fascinante (vale ressaltar

que encontrar padrões em qualquer assunto que envolva números primos dificilmente acontece, e quando acontece, prová-los se torna uma tarefa árdua).

A Tabela 2 a seguir, nos mostra a quantidade de primos existentes entre 1 e $\boldsymbol{10^a}$ (potências de dez) e a média entre um número primo e outro no decorrer de cada potência de dez.

Tabela 2- Quantidade de primos entre 1 e $\boldsymbol{N}$

N	Primos entre 1 e N (chamado de $\pi(N)$)	**Média entre primos**
10^1	4	**2,5**
10^2	25	**4**
10^3	168	**6**
10^4	1229	**8,1**
10^5	9592	**10,4**
10^6	78498	**12,7**
10^7	664579	**15**
10^8	5761455	**17,4**
10^9	50847534	**19,7**
10^{10}	455052511	**22**

Fonte: Elaboração do autor

Agora, observe atentamente a coluna que indica a média entre primos, propositalmente destacada em negrito. Consegue notar um padrão? Se observarmos cuidadosamente, poderemos perceber que a medida em que $\boldsymbol{N}$ aumenta, a diferença entre as médias tende a $\boldsymbol{2,3}$ e dessa forma, Gauss constatou que os números primos estão ligados com logaritmos em que a base não é uma potência de 10.

> A descoberta de Gauss foi o fato de que os primos podem ser contados usando-se logaritmos cuja base é um número especial, chamado $\boldsymbol{e}$, que, com 12 casas decimais, tem o valor de $\boldsymbol{2.718\,281\,828\,459}\ldots$ (da mesma forma que $\boldsymbol{\pi}$, esse número possui uma expansão decimal infinita sem padrões repetitivos). O número $\boldsymbol{e}$ é tão importante quanto $\boldsymbol{\pi}$, ocorrendo em toda parte no mundo matemático. É por isso que os logaritmos na base $\boldsymbol{e}$ são chamados "naturais". (SAUTOY, 2007, p.72)

Dessa forma, Gauss chegou na seguinte conjectura: "entre os números 1 a $\boldsymbol{N}$, aproximadamente 1 em cada $\boldsymbol{\log(N)}$ será primo (onde $\boldsymbol{\log(N)}$ denota o logaritmo de $\boldsymbol{N}$ na base $\boldsymbol{e}$)" (SAUTOY, 2007, p.72). Assim, ele concluiu que poderia estimar uma aproximação para a quantidade de primos entre 1 e $\boldsymbol{N}$ da seguinte maneira:

$$\boldsymbol{\pi(N) \sim \frac{N}{\log(N)}}$$

onde $\boldsymbol{\pi(N)}$ representa a quantidade de primos entre 1 e $\boldsymbol{N}$. Vale ressaltar que $\boldsymbol{\pi}$ não deve ser interpretado em seu valor real, $\boldsymbol{3,1415}\ldots$ Devemos pensar nele apenas como algo que foi usado para dar nome a essa nova contagem de primos, por exemplo, $\boldsymbol{\pi(100) = 25}$, $\boldsymbol{\pi(1000) = 168}$ e assim segue-se tomando $\boldsymbol{N = 10^a}$.

3.2.6 Georg Friedrich Bernhard Riemann

Em Souza (2022), Georg Friedrich Bernhard Riemann, o discípulo mais brilhante de Gauss, nascido na Alemanha em 1826, da mesma forma que Gauss, demonstrou um grande interesse pelos números primos quando leu sobre eles em um livro. Foi em 1859 que o mesmo fez uma descoberta notável que se tornaria a mais significativa para a teoria dos números primos e também esconderia um dos maiores mistérios da rainha das Matemáticas (Teoria dos Números).

A Hipótese de Riemann teve início quando ele estudou a função $\boldsymbol{\zeta}$ (zeta) de Euler que é representada por:

$$\boldsymbol{\zeta(\sigma) = \sum_{n=1}^{\infty} \frac{1}{n^{\sigma}} \ \text{com } \sigma > 1}$$

Euler trabalhava com a função zeta aplicada aos números $\mathbb{R}$ (reais), Riemann por outro lado, utilizou a função zeta aplicada aos números $\mathbb{C}$ (complexos) e dessa forma, ficou conhecida como função Zeta de Riemann. Riemann deu a seguinte definição para a função.

Definição 3*: A função Zeta de Riemann ζ é definida para uma variável complexa s pela seguinte série* (THOMÉ,s.d, p.3).

$$\boldsymbol{\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^{s}}}$$

Riemann identifica, nesse momento, uma regularidade na disposição de todos os zeros não triviais que residem na reta crítica $\boldsymbol{Re(s) = \frac{1}{2}}$ com $\boldsymbol{s} \in \mathbb{C}$ e $\boldsymbol{n} \in \mathbb{N}$ (LIMA, 2022, p.27). Além disso, Riemann adicionou em sua hipótese que os zeros não triviais de sua função são da forma $\boldsymbol{z = \frac{1}{2} + i\mu}$ com $\boldsymbol{\mu} \in \mathbb{R}$.

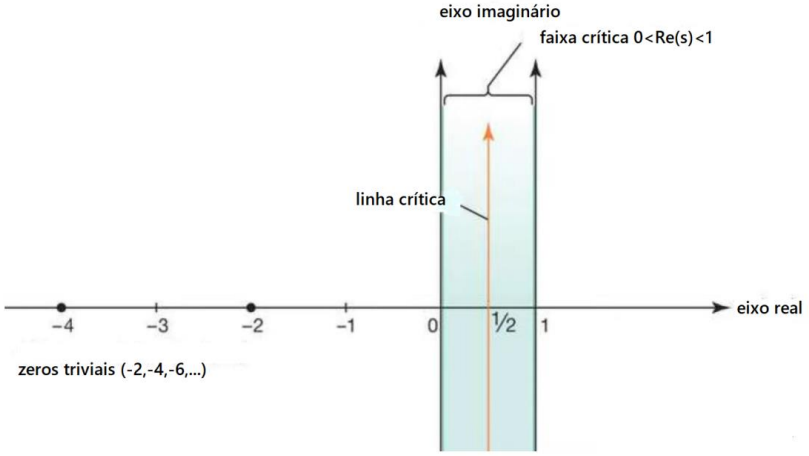
Hipótese de Riemann: *Todos os zeros não triviais da função $\boldsymbol{\zeta(s)}$ pertencem à reta crítica. (FRITSCHE; SUGUIMOTO, 2015).*

Através de cálculos computacionais, já foram encontradas incontáveis quantidades de raízes sobre a reta crítica, no entanto, isso não adianta muita coisa,

pois, algo só é considerado como uma verdade absoluta, matematicamente falando, a partir do momento em que se é demonstrado.

Observe a figura 3 a seguir que nos dá uma ideia de como é interpretada graficamente a Hipótese de Riemann.

Figura 3- Representação gráfica da Hipótese de Riemann



Fonte: LIMA, HERONILZA SILVA, 2022, p.28)

4 NÚMEROS PRIMOS E CRIPTOGRAFIA

Um dos primeiros exemplos históricos de criptografia remonta aos tempos do Imperador Júlio César, que a utilizava para se comunicar com seus soldados em campanhas pela Europa. Esse método de criptografia consistia na substituição de cada letra por outra localizada a uma certa quantidade de casas à frente no alfabeto. Esse processo ficou conhecido como cifra de César (MOLINARI, 2016).

Hoje em dia, o algoritmo de criptografia mais reconhecido globalmente é o RSA. Este método de proteção de dados foi desenvolvido em 1978 por um grupo de estudantes do Instituto de Tecnologia de Massachusetts (MIT), composto por R.L. Rivest, A. Shamir e L. Adleman.

A implementação do método RSA envolve duas coisas fundamentais: dois números primos, geralmente denominados $\boldsymbol{p}$ e $\boldsymbol{q}$. Ao usar o método RSA para criptografar uma mensagem, é suficiente conhecer o produto desses dois números primos, que chamaremos de $\boldsymbol{n}$. No entanto, para decodificar a mensagem, é necessário ter acesso tanto a $\boldsymbol{p}$ quanto a $\boldsymbol{q}$. Portanto, o sistema de chave do RSA é essencialmente constituído pelo número $\boldsymbol{n = pq}$, que é a chave pública compartilhada com todos, e pelas chaves de decodificação privadas, que são justamente os números primos escolhidos. (COUTINHO, 2001).

Se pararmos para pensar, o sistema RSA tem um funcionamento aparentemente simples: dois números primos e o produto desses dois números. No entanto, a complexidade se deve ao fato de que os números primos escolhidos são extremamente grandes e o produto resultante ainda maior. Dessa forma, o sistema RSA garante uma segurança bastante confiável, uma vez que fatorar o produto de dois números primos imensos seria uma tarefa impossível ou que demandaria um tempo suficientemente grande (LIMA, 2022).

Para compreendermos melhor como funciona esse modelo de criptografia, vamos introduzir a definição de congruência modular.

Definição 4*: Congruência Módulo n. de acordo com IEZZI (2003):*

Consideremos $\boldsymbol{a}$ *e* $\boldsymbol{b} \in \mathbb{Z}$ *quaisquer e* $\boldsymbol{n}$ *um outro inteiro positivo. Dizemos que* $\boldsymbol{a}$ *é côngruo a* $\boldsymbol{b}$ *módulo* $\boldsymbol{n}$*, se e somente se,* $\boldsymbol{n}|(\boldsymbol{a}-\boldsymbol{b})$*, ou seja,* $(\boldsymbol{a}-\boldsymbol{b}) = \boldsymbol{nq}$*, com* $\boldsymbol{q} \in \mathbb{Z}$*. Utilizaremos a seguinte notação para expressar essa relação:*

$$\boldsymbol{a \equiv b (mod\ n)}$$

Mas enfim o que significa $\boldsymbol{a \equiv b(mod\ n)}$? Essa relação nos mostra que a divisão de $\boldsymbol{a}$ por $\boldsymbol{n}$ e de $\boldsymbol{b}$ por $\boldsymbol{n}$ deixam restos iguais. Para entendermos melhor, vamos relacionar a congruência com algo que nos deparamos constantemente no dia a dia.

Sabemos que um dia terrestre possui aproximadamente 24h, no entanto, os relógios só possuem um ciclo com 12h. Utilizando congruência modulo $\boldsymbol{n}$, como saber que 14h na verdade significa duas da tarde? Para isso, vamos considerar $\boldsymbol{a = 14}$ e $\boldsymbol{n = 12}$. Teremos

$$\boldsymbol{14 \equiv b(mod\ 12) \Leftrightarrow n|(14 - b)}$$

Para encontrarmos $\boldsymbol{b}$, basta dividir $\boldsymbol{a}$ por $\boldsymbol{n}$, dessa forma, segue que:

$$\boldsymbol{\frac{a}{n} = \frac{14}{12} \Leftrightarrow 14 = 12 \times 1 + 2}$$

e percebemos que o resto da divisão é $\boldsymbol{2}$. Concluímos que $\boldsymbol{14 \equiv 2(mod 12)}$, pois, $\boldsymbol{b = 2}$ satisfaz a condição $\boldsymbol{n|(14 - b)}$ e daí tiramos que 14h na verdade significa duas horas.

Nesse momento, vamos codificar e decodificar uma mensagem com 3 letras utilizando o sistema RSA. Vejamos para a palavra “SEU” e segue que os códigos para pré-codificação estão representados na tabela 3 a seguir.

Tabela 3- Códigos para pré-codificação

A	**B**	**C**	**D**	**E**	**F**	**G**	**H**	**I**	**J**	**K**	**L**	**M**
10	11	12	13	14	15	16	17	18	19	20	21	22
N	**O**	**P**	**Q**	**R**	**S**	**T**	**U**	**V**	**W**	**X**	**Y**	**Z**
23	24	25	26	27	28	29	30	31	32	33	34	35

Fonte: Elaboração do autor

Agora, nesse momento, assim como fazia Júlio Cesar, vamos codificar a mensagem “SEU” tomando como base a Tabela 3, obtendo o código a seguir:

SEU: 281430

Por fim, escolhemos dois números primos aleatórios que serão a chave para decodificar a mensagem.

$$\boldsymbol{p = 5 \text{ e } q = 7}$$

Como já temos a chave privada, podemos criar a chave pública apenas multiplicando os dois números escolhidos, dessa forma teremos:

Chave de codificação: $\boldsymbol{n = p \times q = 35}$

Para iniciar a codificação utilizaremos a relação $\boldsymbol{v^g \equiv b\big(mod(n)\big)}$, onde $\boldsymbol{g}$ é um dos números primos escolhidos para criar a chave pública, nesse caso utilizaremos $\boldsymbol{g = 7}$ e $\boldsymbol{v}$ são os números de dois algarismos decorrentes da pré-codificação.

Logo, para obtermos a mensagem criptografada é necessário resolver as seguintes operações:

$$\boldsymbol{28^7 \equiv b(mod\ 35)}$$

$$\Downarrow$$

$$\boldsymbol{b = 7}$$

$$\boldsymbol{14^7 \equiv b(mod\ 35)}$$

$$\Downarrow$$

$$\boldsymbol{b = 14}$$

$$\boldsymbol{30^7 \equiv b(mod\ 35)}$$

$$\Downarrow$$

$$\boldsymbol{b = 30}$$

por fim, a mensagem final é $\boldsymbol{71430}$.

A regra para a decodificação no método RSA é semelhante à codificação, mas requer o conhecimento das chaves privadas. Enquanto na codificação usamos a chave pública (o número $\boldsymbol{n}$) para criptografar a mensagem, na decodificação utilizaremos as chaves privadas (os números $\boldsymbol{p}$ e $\boldsymbol{q}$) para decodificar a mensagem e revelar seu verdadeiro conteúdo.

Para decodificar a mensagem é necessária uma chave de decodificação $(\boldsymbol{n, d})$, onde $\boldsymbol{d}$ é obtido pela relação:

$$\boldsymbol{g \times d \equiv 1 mod\big((p-1)(q-1)\big)}$$

Substituindo teremos:

$$\boldsymbol{7 \times d \equiv 1(mod\ 24)}$$

$$\Downarrow$$

$$\boldsymbol{d = 7}$$

pois $\boldsymbol{49 \equiv 1 mod(24)}$.

Observe que, nesse momento, a segurança do sistema RSA se mostra, pois como alguém vai conseguir uma chave de decodificação $(\boldsymbol{n, d})$ sem conhecer $\boldsymbol{g}$? Vale lembrar que esse exemplo é meramente ilustrativo, pois fatorar o 35 é algo

extremamente fácil. No entanto, como já foi dito, o sistema RSA utiliza números primos com uma grande quantidade de dígitos.

Agora, utilizaremos a relação $\boldsymbol{b^d \equiv v(mod\ n)}$ para decodificar a mensagem, onde $\boldsymbol{v}$ é a mensagem pré-codificada que se pretende.

Segue que:

$$\boldsymbol{7^7 \equiv v(mod\ 35)}$$
$$\Downarrow$$
$$\boldsymbol{v = 28}$$
$$\boldsymbol{14^7 \equiv v(mod\ 35)}$$
$$\Downarrow$$
$$\boldsymbol{v = 14}$$
$$\boldsymbol{30^7 \equiv v(mod\ 35)}$$
$$\Downarrow$$
$$\boldsymbol{v = 30}$$

Logo, a mensagem é 281430, e agora basta olhar na Tabela 3 para finalizar a decodificação, retornando à palavra 'SEU' como resultado.

4.1 Hipótese de Riemann e o Impacto no Modelo RSA

Como já mencionado anteriormente, a Hipótese de Riemann é um grande problema em aberto na Matemática, revelando um conhecimento avançado no estudo da distribuição infinita dos números primos. No entanto, ela também está relacionada a algo reconhecido como uma preocupação global e de importância gigantesca: a segurança na rede (internet) e, em termos gerais, o sigilo de dados.

Atualmente, todo tipo de ação realizada em meio virtual exige uma confirmação. Por exemplo, uma compra online exigirá que você forneça o número do cartão de crédito, ou até mesmo no momento em que precisamos digitar a senha para entrar no aplicativo do banco. Enfim, são incontáveis as situações em que é necessário lidar com dados/informações sigilosas. No entanto, graças à criptografia, esses dados podem ser mascarados, como vimos anteriormente, sendo a forma mais utilizada desse processo a criptografia RSA.

Mas qual seria o impacto que uma demonstração da Hipótese de Riemann traria para esse sistema? Uma prova de que realmente todos os zeros não triviais da

função Zeta estão distribuídos na reta crítica $\mathbf{1/2}$ seria o suficiente para possibilitar o aprimoramento de uma fórmula que busca números primos no infinito. Entretanto, é precisamente nesta abordagem que reside a ameaça à segurança do modelo de criptografia RSA, como já vimos anteriormente: a chave $\boldsymbol{n}$ é pública e é um número extremamente grande. Apesar disso, se conseguirmos fatorar esse número, torna-se trivial determinar os valores de $\boldsymbol{p}$ e $\boldsymbol{q}$, que são os números primos que compõem as chaves privadas. Portanto, a capacidade de fatorar $\boldsymbol{n}$ implica na quebra do código (OKUMURA,2014).

> De acordo com nossos estudos e pesquisa a hipótesse de Riemann que, na verdade ainda é uma conjectura, se solucionada, pode aperfeiçoar uma fórmula capaz de obter a fatoração da chave pública n presente nas codificações de mensagens criptografas e alcançar as chaves privadas p e q para decodificação de mensagens codificadas pelo modelo de criptografia RSA. (LIMA,2022, p.43)

Portanto, a Hipótese de Riemann, apesar de representar um grande avanço para a área da Teoria dos Números, pode representar um grande perigo no que diz respeito à segurança dos dados e, dessa forma, fazer com que novos modelos de criptografia sejam criados ou implementados para oferecer uma maior proteção.

5 PONTO DE PARTIDA

Nesse momento, vamos dar continuidade ao assunto iniciado no Capítulo 3, Exemplo 4 do Tópico 3.2, de uma forma mais completa, enunciando suas propriedades que estão diretamente relacionadas com a origem deste trabalho.

Falar em divisão é algo comum no dia a dia da sociedade contemporânea. Estamos cercados por divisões em todos os momentos. Por exemplo, o dia é dividido em vinte e quatro horas, uma pizza geralmente é dividida em 8 pedaços, e um ano pode ser dividido em dois semestres, quatro trimestres ou seis bimestres. Enfim, isso se tornou algo tão normal que, por vezes, nem nos damos conta de que estamos utilizando a divisão para realizar algo.

Antes de adentrarmos nesse tema, é essencial ter em mente algo que é fundamental para o bom entendimento do assunto: os múltiplos. Vale ressaltar que, como estamos lidando apenas com números primos positivos, desconsideraremos o conjunto dos números inteiros negativos ao abordarmos múltiplos e divisibilidade.

5.1 Múltiplos de um Número Inteiro

Ao abordarmos esse tema, estamos basicamente nos referindo a características dos números primos e dos números secundários (compostos) apresentadas pelos Pitagóricos, como foi visto no capítulo 3, tópico 3.2.1.

Matematicamente, diz-se que um número inteiro é múltiplo de outro inteiro pela seguinte definição:

Definição 5*: Dados dois números inteiros* $\boldsymbol{p}$ *e* $\boldsymbol{n}$*, nesse caso,* $\boldsymbol{p}$ *será múltiplo de* $\boldsymbol{n}$ *se existir um único inteiro* $\boldsymbol{a}$*, de tal forma que* $\boldsymbol{p}$ *possa ser representado por:*

$$\boldsymbol{p = n \times a}$$

Generalizando, vejamos a definição a seguir.

Definição 6*: Dado o número inteiro positivo* $\boldsymbol{n}$*, o conjunto de todos os múltiplos positivos de* $\boldsymbol{n}$ *é representado por:*

$$\boldsymbol{M(n) = \{0; 1n; 2n; 3n; 4n; \dots \dots \dots\}}$$

Dessa forma, analisando o conjunto acima, percebemos que todos os números que não são múltiplos de $\boldsymbol{n}$ consequentemente estarão entre dois múltiplos

consecutivos de $\boldsymbol{n}$, ou seja, dado o número positivo $\boldsymbol{u}$, com $\boldsymbol{u} \neq \mathbf{0}; \boldsymbol{n}; \mathbf{2}\boldsymbol{n}$; ...., temos que $\boldsymbol{u}$ estará entre um dos conjuntos de múltiplos a seguir.

$$(\mathbf{0} < \boldsymbol{u} < \boldsymbol{n}), (\boldsymbol{n} < \boldsymbol{u} < \mathbf{2}\boldsymbol{n}), (\mathbf{2}\boldsymbol{n} < \boldsymbol{u} < \mathbf{3}\boldsymbol{n}), (\mathbf{3}\boldsymbol{n} < \boldsymbol{u} < \mathbf{4}\boldsymbol{n}), \ldots \ldots \ldots$$

Para um melhor entendimento, vamos considerar $\boldsymbol{n} = \mathbf{7}$, daí temos que:

$$\boldsymbol{M}(\mathbf{7}) = \{\mathbf{0}; \mathbf{7}; \mathbf{14}; \mathbf{21}; \mathbf{28}; \ldots \ldots \ldots\}$$

e seja $\boldsymbol{u} = \mathbf{10}$. Segue que:

$$(\mathbf{7} < \mathbf{10} < \mathbf{14})$$

e dessa forma constatamos que nesse exemplo $\boldsymbol{u}$ está entre $(\boldsymbol{n} < \boldsymbol{u} < \mathbf{2}\boldsymbol{n})$.

Da Definição 5, como $\mathbf{0} \in \mathbb{Z}$ e sabemos que qualquer que seja o número multiplicado por $\mathbf{0}$ será sempre $\mathbf{0}$, ou seja, o número $\mathbf{0}$ é múltiplo de todo e qualquer número inteiro. Esse fato será importante para verificarmos se um número é ou não é múltiplo de um número primo maior do que ou igual a $\mathbf{7}$ na aplicação do critério logo adiante.

5.2 Divisibilidade no Conjunto dos Inteiros

Se tratando de divisão, sabemos que no conjunto dos números inteiros, uma divisão pode ser possível ou não (exata ou não). A partir disso, torna-se extremamente necessário conhecermos divisibilidade no conjunto dos inteiros além de entendermos suas definições e suas propriedades

5.2.1 Definição e propriedades

Definição 7*:* Dados dois números positivos $\boldsymbol{c}, \boldsymbol{d} \in \mathbb{Z}$, diremos que $\boldsymbol{c}$ divide $\boldsymbol{d}$ se existir um número inteiro $\boldsymbol{q}$ de tal forma que $\boldsymbol{d} = \boldsymbol{c}\boldsymbol{q}$.

Dessa definição, dizemos também que $\boldsymbol{c}|\boldsymbol{d}$ ($\boldsymbol{c}$ é divisor de $\boldsymbol{d}$) e por consequência, $\boldsymbol{d}$ é divisível por $\boldsymbol{c}$. Além disso, como vimos no tópico acima, como $\boldsymbol{d}$ pode ser representado por $\boldsymbol{c}\boldsymbol{q}$ com $\boldsymbol{q} \in \mathbb{Z}$, isso implica que $\boldsymbol{d}$ é múltiplo de $\boldsymbol{c}$. Veja os exemplos a seguir.

Exemplo 9: Perceba que $\mathbf{3}|\mathbf{21}$, pois existe um inteiro $\boldsymbol{q} = \mathbf{7}$ tal que $\mathbf{21} = \mathbf{3} \times \mathbf{7}$ e dessa forma percebemos também que $\mathbf{21}$ é múltiplo de $\mathbf{3}$.

Exemplo 10: Agora observe que $\boldsymbol{4 \nmid 19}$ ($\boldsymbol{4}$ não é divisor de $\boldsymbol{19}$), pois o inteiro $\boldsymbol{q}$ não existirá nesse caso, consequentemente $\boldsymbol{19}$ não é múltiplo de 4, porém estará entre dois múltiplos dele. Considerando $\boldsymbol{u = 19}$, temos que:

$$(\boldsymbol{16 < 19 < 20})$$

Da definição anterior, obtém-se as seguintes proposições:

Proposição 1: Dados $\boldsymbol{a}$, $\boldsymbol{b}$ e $\boldsymbol{c}$ inteiros não nulos, segue que:

i) $\boldsymbol{1|a, a|a, 0|a;}$

ii) $\boldsymbol{Se\ a|b\ e\ b|c, então\ a|c}$;

iii) $\boldsymbol{a|b\ e\ c|d \implies ac|bd}$;

iv) $\boldsymbol{a|b\ se, e\ somente\ se, |a|\ divide\ |b|}$;

Demonstraremos $\boldsymbol{ii}$).

Demonstração: Pela definição 7, se $\boldsymbol{a|b\ e\ b|c}$, nesse caso existirão inteiros $\boldsymbol{p}$, $\boldsymbol{m} \in \mathbb{Z}$ de tal forma que:

$$\boldsymbol{b = ap}$$

$$\boldsymbol{c = bm \implies c = (ap)m}$$

Dessa forma, como queremos demonstrar que: se $\boldsymbol{a|b\ e\ b|c \implies a|c}$ e já conhecemos $\boldsymbol{b}$ e $\boldsymbol{c}$, vamos trabalhar com substituições e ao final verificar se existe um inteiro $\boldsymbol{k}$ de tal forma que $\boldsymbol{c = ak}$, em que $\boldsymbol{k = pm}$. Portanto, se $\boldsymbol{a|b\ e\ b|c}$, isso implica que $\boldsymbol{a|c}$, como queríamos mostrar. ■

Proposição 2: Se $\boldsymbol{a, b, c} \in \mathbb{Z}$ de tal forma que $a|b$ e $a|c$, então $\boldsymbol{a|b + c}$.

Demonstração: Pela definição 7, se $\boldsymbol{a|b\ e\ a|c}$, então existem inteiros $\boldsymbol{p}$ e $\boldsymbol{q}$ tais que:

$$\boldsymbol{b = ap}$$

$$\boldsymbol{c = aq}$$

e como queremos provar $\boldsymbol{a|b + c}$, devemos somar as duas expressões. Segue que:

$$\boldsymbol{b + c = ap + aq}$$

que, utilizando a propriedade distributiva, colocando $\boldsymbol{a}$ em evidência, temos que:

$$\boldsymbol{b + c = a(p + q)}$$

de onde concluímos que, se $\boldsymbol{p}$ e $\boldsymbol{q}$ são inteiros, a soma deles resultará em um número inteiro, dessa forma:

$$\boldsymbol{p + q = w, w \in \mathbb{Z}}$$

Logo, podemos reescrever o resultado $\boldsymbol{b + c = a(p + q)}$ como:

$$\boldsymbol{b + c = aw}$$

de onde concluímos que $\boldsymbol{a|b + c}$. ■

Proposição 3: *Se* $\boldsymbol{a, b, c} \in \mathbb{Z}$ *de tal forma que* $\boldsymbol{a|b}$ *e* $\boldsymbol{a|c}$*, então* $\boldsymbol{a|b - c}$

Demonstração: Novamente, pela definição **7**, se $\boldsymbol{a|b}$ *e* $\boldsymbol{a|c}$, então existem inteiros $\boldsymbol{p}$ e $\boldsymbol{q}$ tais que:

$$\boldsymbol{b = ap}$$

$$\boldsymbol{c = aq}$$

Dessa forma, segue que:

$$\boldsymbol{b - c = ap - aq}$$

$$\boldsymbol{= a(p - q)}$$

de onde conclui-se que, como $\boldsymbol{(p - q)} \in \mathbb{Z}$, tem-se

$$\boldsymbol{b - c = al, l = p - q} \in \mathbb{Z}. \quad ■$$

Proposição 4: *Sejam* $\boldsymbol{a, b, c} \in \mathbb{Z}$*. Se* $\boldsymbol{a|b}$ *e* $\boldsymbol{a|c}$*, então* $\boldsymbol{a|(bm + cn)}$*, com* $\boldsymbol{m, n} \in \mathbb{Z}$*.*

Demonstração: Se $\boldsymbol{a|b}$ e $\boldsymbol{a|c}$, então pela Definição 7, segue que existem inteiros $\boldsymbol{g}$ e $\boldsymbol{k}$ de tal forma que:

$$\boldsymbol{b = ag}$$

e

$$\boldsymbol{c = ak}.$$

Logo, considerando os inteiros $\boldsymbol{m}$ e $\boldsymbol{n}$ e multiplicando em ambos respectivamente, temos que:

$$\boldsymbol{bm = (ag)m}$$

$$\boldsymbol{cn = (ak)n}.$$

Agora, como queremos provar que $\boldsymbol{a|(bm + cn)}$, devemos somá-las. Segue que:

$$\boldsymbol{bm + cn = (ag)m + (ak)n}$$

$$\boldsymbol{= agm + akn}$$

$$\boldsymbol{= a(gm + kn)}.$$

Dessa forma, como $\boldsymbol{(gm + kn)} \in \mathbb{Z}$, vamos chamá-lo de $\boldsymbol{w}$. Isso nos leva à conclusão de que $\boldsymbol{a|(bm + cn)}$, pois existe o inteiro $\boldsymbol{w}$ tal que:

$$\boldsymbol{bm + cn = aw}. ■$$

6 GÊNESIS DO TRABALHO

A ideia dessa monografia foi concebida inicialmente após a aplicação de uma prova da disciplina de Álgebra Abstrata no período 2023.1, ministrada pelo Prof. Dr. Raimundo Cavalcante Maranhão Neto, da Universidade Federal do Norte do Tocantins, campus de Araguaína. A questão pedia aos discentes que enunciassem e demonstrassem um critério de divisibilidade por sete. Como se tratava de um número primo, naquele momento, a resolução da questão não foi desenvolvida de forma adequada e esperada pelo professor.

No entanto, a fascinação por buscar padrões numéricos ou algo que tenha sentido lógico matematicamente entrou em cena mais uma vez na busca por uma resposta para a questão. Dias após a prova, como em um estalo, uma das possíveis respostas para a questão (podendo haver inúmeras) se apresentou como algo muito simples de se compreender numericamente.

Por fim, a nova ideia foi apresentada ao orientador desta monografia, que já estava ciente de que o objetivo era realizar uma pesquisa baseada em números primos e em algo que, de certa forma, fosse uma nova formulação. Espantosamente, uma simples ideia trazia consigo uma bagagem repleta de implicações lógicas e matemáticas, sendo prontamente proposta pelo orientador como tema da pesquisa.

O leitor deve estar se perguntando por que o critério é válido apenas para primos maiores do que ou iguais a 7, e isso será explicado no decorrer do desenvolvimento desta monografia.

Mas, afinal, o que vem a ser um critério de divisibilidade?

6.1 O que é um Critério de Divisibilidade?

Analisando o significado da palavra critério, veremos que é um termo utilizado para se referir a um conjunto de regras, princípios, padrões ou diretrizes usados para julgar, avaliar, classificar ou tomar decisões sobre algo. Além disso, os critérios são usados para determinar a qualidade, a adequação ou o valor de algo em relação a um determinado objetivo.

Trazendo para o contexto que pretendemos, podemos dizer que um critério de divisibilidade diz respeito a padrões que determinados números devem possuir para serem divisíveis por outro número, ou seja, podemos dizer que $\boldsymbol{n|a}$ se, e somente se,

$\boldsymbol{a}$ possuir algum padrão ou característica que faça com que ele se encaixe em um dos múltiplos de $\boldsymbol{n}$.

6.2 Alguns Critérios de Divisibilidade

6.2.1 Critério de divisibilidade por 2

Teorema 3: *Dado um número natural qualquer p, ele será divisível por 2 se, e somente se, o último algarismo de p for par*.

Demonstração: Seja *p* um número escrito na base 10, ou seja,

$$\boldsymbol{p = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_2 10^2 + a_1 10^1 + a_0}$$

onde, $\boldsymbol{0 \leq a_i \leq 9}\ \forall\ \boldsymbol{1 \leq i \leq n}$, e $\boldsymbol{n} \in \mathbb{N}$. Agora, note que, de $\boldsymbol{a_n 10^n}$ até $\boldsymbol{a_1 10^1}$ temos o número $\boldsymbol{10}$ como termo comum, logo, podemos reescrever $\boldsymbol{P}$ da seguinte forma:

$$\boldsymbol{p = 10(a_n 10^{n-1} + a_{n-1} 10^{n-2} + \cdots + a_2 10^1 + a_1) + a_0}$$

e agora reescrevemos $\boldsymbol{P}$ como:

$$\boldsymbol{p = Q + a_0}$$

onde $\boldsymbol{Q = 10(a_n 10^{n-1} + a_{n-1} 10^{n-2} + \cdots + a_2 10^1 + a_1)}$. Temos que $\boldsymbol{10 = 2 \times 5}$ e isso significa que $\boldsymbol{2|Q}$, além disso, nessas condições, $\boldsymbol{Q}$ sempre será um número par. Daí, segue que:

$$\boldsymbol{2|P \Leftrightarrow 2|a_0}$$

$$\boldsymbol{\Leftrightarrow\ a_0 = 2t, t\ \in\ \mathbb{Z}}$$

de onde concluímos que $\boldsymbol{a_0}$ deve ser par, ou seja, $\boldsymbol{a_0 \neq 1, 3, 5, 7, 9}$. ■

Exemplo 11: O número $\boldsymbol{854726}$ é divisível por $\boldsymbol{2}$?

Note que, chamando $\boldsymbol{P = 854726}$, temos que ele também pode ser escrito como;

$$\boldsymbol{P = 8 \times 10^5 + 5 \times 10^4 + 4 \times 10^3 + 7 \times 10^2 + 2 \times 10^1 + 6}$$

e vemos facilmente que o último dígito é $\boldsymbol{6}$ que é múltiplo de 2. Logo, $\boldsymbol{2|854726}$.

Exemplo 12: O número $\boldsymbol{3419}$ é divisível por $\boldsymbol{2}$?

Considerando $\boldsymbol{p = 3 \times 10^3 + 4 \times 10^2 + 1 \times 10^1 + 9}$, de onde concluímos que o último dígito é $\boldsymbol{9}$, ou seja, $\boldsymbol{2 \nmid 3419}$.

6.2.2 Critério de divisibilidade por 3

Teorema 4*: Dado* $\boldsymbol{p}$ *um número natural,* $\boldsymbol{p}$ *será divisível por* $\mathbf{3}$ *se, e somente se, a soma dos dígitos de* $\boldsymbol{p}$ *for divisível por* $\mathbf{3}$*.*

Demonstração: Assim como na demonstração acima, vamos considerar $\boldsymbol{P}$ como

$$\boldsymbol{p = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_2 10^2 + a_1 10^1 + a_0}$$

de onde tiramos que a representação decimal de $\boldsymbol{p}$ é $(\boldsymbol{a_n a_{n-1}}\ldots.\ \boldsymbol{a_2 a_1 a_0})$. Agora, note que $\mathbf{9 = 10 - 1}$, ou seja, toda potência de $\boldsymbol{10^n = 999 \ldots . 999 + 1}$, onde o $\mathbf{9}$ se repetirá $\boldsymbol{n}$ vezes. Daí, segue que

$\boldsymbol{p = (a_n 999 \ldots 99 + a_{n-1} 999 \ldots 9 + \cdots + a_2 99 + a_1 9) + (a_n + a_{n-1} + \cdots + a_2 + a_1 + a_0)}$,

e agora, chamaremos $\boldsymbol{D = (a_n 999 \ldots 99 + a_{n-1} 999 \ldots 9 + \cdots + a_2 99 + a_1 9)}$ e dessa forma é possível notar que $\mathbf{3}|\boldsymbol{D}$. Seguindo com a demonstração do critério, vamos supor que $\boldsymbol{p}$ seja divisível por $\mathbf{3}$. Com isso, como sabemos que $\mathbf{3}|\boldsymbol{D}$ e estamos supondo que $\mathbf{3}|\boldsymbol{p}$, pela proposição 3, temos que

$$\mathbf{3}|\boldsymbol{p - D}.$$

No entanto:

$$\boldsymbol{p - D = a_n + a_{n-1} + \cdots + a_2 + a_1 + a_0}$$

que é justamente a soma dos algarismos de $\boldsymbol{p}$. ■

Exemplo 13: Os números $\mathbf{478}$ e $\mathbf{594}$ são divisíveis por $\mathbf{3}$?

Para $\mathbf{478}$ temos que a soma de seus algarismos resulta em $\mathbf{19}$, ou seja, $\mathbf{3} \nmid \mathbf{19}$ e consequentemente $\mathbf{3} \nmid \mathbf{478}$. No entanto, para $\mathbf{594}$ temos que a soma de seus algarismos resulta em $\mathbf{18}$ e, como $\mathbf{3}|\mathbf{18}$, tem-se $\mathbf{3}|\mathbf{594}$.

6.2.3 Critério de divisibilidade por 4

Teorema 5*: Seja* $\boldsymbol{p}$ *um número natural. Então,* $\boldsymbol{p}$ *será divisível por* $\mathbf{4}$ *se, e somente se, a soma de* $\boldsymbol{a_1 10^1 + a_0}$ *for divisível por* $\mathbf{4}$.

Demonstração: Considerando $\boldsymbol{P = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_2 10^2 + a_1 10^1 + a_0}$, vamos fazer modificações de tal forma que alguma parte de $\boldsymbol{P}$ seja divisível por $\mathbf{4}$. Se *P* tiver apenas 2 algarismos, o resultado é claramente válido. Do contrário, analisando

$\boldsymbol{P}$, é possível notar que $\mathbf{100} \leq \mathbf{10^2}, \ldots, \mathbf{10^{n-1}}, \mathbf{10^n}$ e, dessa maneira, podemos reescrever $\boldsymbol{P}$ como

$$\boldsymbol{P = 10^2(a_n 10^{n-2} + a_{n-1} 10^{n-3} + \cdots + a_2) + a_1 10^1 + a_0}.$$

Agora, devemos observar que $\mathbf{4}|\mathbf{10^2}$, e isso significa que a expressão

$$\mathbf{10^2(a_n 10^{n-2} + a_{n-1} 10^{n-3} + \cdots + a_2)}$$

obrigatoriamente deve ser divisível por $\mathbf{4}$. Chamando $\boldsymbol{D = 10^2(a_n 10^{n-2} + a_{n-1} 10^{n-3} + \cdots + a_2)}$, dessa forma $\boldsymbol{P = D + a_1 10^1 + a_0}$. Pela Proposição 3,

$$\mathbf{4}|\boldsymbol{P - D} \Leftrightarrow \mathbf{4}|\boldsymbol{a_1 10^1 + a_0}$$

$$\Leftrightarrow \boldsymbol{a_1 10^1 + a_0 = 4m, m} \in \mathbb{Z}. \blacksquare$$

Exemplo 14: Os números $\mathbf{1388}$ e $\mathbf{474}$ são divisíveis por $\mathbf{4}$?
Note que os últimos dois dígitos de $\mathbf{1388}$ são $\mathbf{88}$, e $\mathbf{4}|\mathbf{88}$. Portanto, $\mathbf{4}|\mathbf{1388}$. Para $\mathbf{474}$, o pensamento é análogo, no entanto, os últimos dois dígitos de $\mathbf{474}$ é $\mathbf{74}$, e $\mathbf{4} \nmid \mathbf{74}$, e consequentemente $\mathbf{4} \nmid \mathbf{474}$.

6.2.4 Critério de divisibilidade por 5

Teorema 6*: Seja* $\boldsymbol{P}$ *um número natural. Então,* $\boldsymbol{P}$ *será divisível por* $\mathbf{5}$ *se, e somente se,* $\boldsymbol{a_0}$ *for igual a* $\mathbf{5}$ *ou* $\mathbf{0}$*.*

Demonstração: Consideremos $\boldsymbol{P = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_2 10^2 + a_1 10^1 + a_0}$, note que todos os $\boldsymbol{a_i}$ com exceção do $\boldsymbol{a_0}$ estão sendo multiplicados por uma potência de base 10 elevado a um expoente diferente de zero ($\boldsymbol{a_0}$ é multiplicado por $\mathbf{10^0 = 1}$), e como sabemos, $\mathbf{10 = 2 \times 5}$. Tendo isso como base, vamos reescrever $\boldsymbol{P}$ como

$$\boldsymbol{P = 10(a_n 10^{n-1} + a_{n-1} 10^{n-2} + \cdots + a_2 10^1 + a_1) + a_0}.$$

Agora, chamando $\boldsymbol{D = 10(a_n 10^{n-1} + a_{n-1} 10^{n-2} + \cdots + a_2 10^1 + a_1)}$, temos que $\mathbf{5}|\boldsymbol{D}$. Logo, assumindo que $\mathbf{5}|\boldsymbol{P}$ **e** $\mathbf{5}|\mathbf{D}$, pela Proposição 3 segue que:

$$\mathbf{5}|\boldsymbol{P - D}$$

No entanto, isso ocorrera com uma condição:

$$\mathbf{5}|\boldsymbol{P - D} \Leftrightarrow \mathbf{5}|\boldsymbol{a_0}$$

$$\Leftrightarrow \boldsymbol{a_0 = 5m, m} \in \mathbb{Z}. \blacksquare$$

Importante ressaltar que todos os infinitos múltiplos de $\mathbf{5}$ sempre terminam em $\mathbf{0}$ ou $\mathbf{5}$ e dessa forma $\boldsymbol{m}$ pode ser igual a $\mathbf{0}$, uma vez que $\mathbf{0} = \mathbf{5}\boldsymbol{m}$ quando $\boldsymbol{m} = \mathbf{0}$.

Exemplo 15: Os números $\mathbf{1430}$ e $\mathbf{756}$ são divisíveis por $\mathbf{5}$?

Como foi visto acima, $\mathbf{1430}$ tem como último algarismo o número $\mathbf{0}$, logo, $\mathbf{5}|\mathbf{1430}$. Em contrapartida, note que $\mathbf{756}$ tem como último algarismo o $\mathbf{6}$, que é diferente de $\mathbf{0}$ e $\mathbf{5}$, consequentemente $\mathbf{5} \nmid \mathbf{756}$.

Exemplo 16: Dado $\boldsymbol{p} = \mathbf{1} \times \mathbf{3} \times \mathbf{5} \times \ldots \times \mathbf{1177}$. Nessas condições, qual o último algarismo de $\boldsymbol{p}$?

Analisando $\boldsymbol{p}$, podemos concluir que $\boldsymbol{p}$ é um número ímpar, pois é formado por um produto de números ímpares. Agora, concluímos também que $\mathbf{5}|\boldsymbol{p}$, ou seja, $\boldsymbol{p}$ é múltiplo de 5. Dessa maneira, como $\boldsymbol{p}$ é ímpar e é divisível por $\mathbf{5}$, o único algarismo da unidade possível é $\mathbf{5}$.

6.2.5 Critério de divisibilidade por 6

***Teorema 7**: Seja $\boldsymbol{p}$ um número natural. Então, $\boldsymbol{p}$ será divisível por $\mathbf{6}$ se, e somente se, $\mathbf{2}|\boldsymbol{p}$ e $\mathbf{3}|\boldsymbol{p}$ simultaneamente.*

Demonstração: A demonstração desse critério na verdade decorre da união entre o critério de divisibilidade por $\mathbf{2}$ e $\mathbf{3}$, ou seja, para que $\boldsymbol{p}$ seja divisível por $\mathbf{2}$, obrigatoriamente ele deve terminar em $(\mathbf{0}, \mathbf{2}, \mathbf{4}, \mathbf{6}, \mathbf{8})$ e para ser divisível por $\mathbf{3}$ a soma de seus algarismos deve ser um número múltiplo de $\mathbf{3}$. Dessa maneira, concluímos que $\mathbf{6}|\boldsymbol{p}$ apenas nos casos em que $\boldsymbol{p}$ for par e a soma de seus algarismos for um número divisível por 3.■

6.2.6 Critério de divisibilidade por 7

***Teorema 8**: Seja $\boldsymbol{p} = \mathbf{10}\boldsymbol{k} + \boldsymbol{t}$. Então, $\boldsymbol{p}$ será divisível por $\mathbf{7}$ se, e somente se, $\boldsymbol{k} - \mathbf{2}\boldsymbol{t}$ for divisível por $\mathbf{7}$.*

Demonstração: Primeiramente, vamos supor que $\boldsymbol{p}$ seja divisível por 7, com isso, segue que:

$$\mathbf{10}\boldsymbol{k} + \boldsymbol{t} = \mathbf{7}\boldsymbol{n}, \boldsymbol{n} \in \mathbb{Z},$$

agora, note que podemos escrever $\boldsymbol{t}$ estrategicamente como $\boldsymbol{t} = \mathbf{21}\boldsymbol{t} - \mathbf{20}\boldsymbol{t}$. E daí,

$$\mathbf{10}\boldsymbol{k} + \mathbf{21}\boldsymbol{t} - \mathbf{20}\boldsymbol{t} = \mathbf{7}\boldsymbol{n}.$$

Com isso, $\mathbf{10}\boldsymbol{k} - \mathbf{20}\boldsymbol{t} = \mathbf{7}\boldsymbol{n} - \mathbf{21}\boldsymbol{t}$. E como $\mathbf{7}|\mathbf{21}$, então, $\mathbf{7}|\mathbf{7}\boldsymbol{n} - \mathbf{21}\boldsymbol{t}$. Dessa forma,

$$\mathbf{10}\boldsymbol{k} - \mathbf{20}\boldsymbol{t} = \mathbf{7}\boldsymbol{r}, \boldsymbol{r} = \mathbf{7}\boldsymbol{n} - \mathbf{21}\boldsymbol{t}$$

$$\Downarrow$$

$$\mathbf{10}(\boldsymbol{k} - \mathbf{2}\boldsymbol{t}) = \mathbf{7}\boldsymbol{r}$$

Nesse momento, para entendermos que $\boldsymbol{k} - \mathbf{2}\boldsymbol{t} = \mathbf{7}\boldsymbol{g}, \boldsymbol{g} \in \mathbb{Z}$. Segue o seguinte lema:

Lema 1*: Se* $\boldsymbol{s}|\boldsymbol{ab}$ *e* $\boldsymbol{mdc}(\boldsymbol{s}, \boldsymbol{a}) = \mathbf{1}$*, então* $\boldsymbol{s}|\boldsymbol{b}$*.*

Note que, no problema, $\mathbf{7}|\mathbf{10}(\boldsymbol{k} - \mathbf{2}\boldsymbol{t})$, vale que o $\boldsymbol{mdc}(\mathbf{7}, \mathbf{10}) = \mathbf{1}$, ou seja, eles são primos entre si. Isso implica que

$$\mathbf{7}|(\boldsymbol{k} - \mathbf{2}\boldsymbol{t})$$

Agora, vamos supor que $\boldsymbol{k} - \mathbf{2}\boldsymbol{t} = \mathbf{7}\boldsymbol{g}$ e verificar que $\mathbf{10}\boldsymbol{k} + \boldsymbol{t} = \mathbf{7}\boldsymbol{n}$. Segue que:

$$\boldsymbol{k} - \mathbf{2}\boldsymbol{t} = \mathbf{7}\boldsymbol{g}$$

Multiplicando por $\mathbf{10}$ em ambos os lados, temos que $\mathbf{10}\boldsymbol{k} - \mathbf{20}\boldsymbol{t} = \mathbf{7}\boldsymbol{u}, \boldsymbol{u} = \mathbf{10}\boldsymbol{g}$.

Dessa maneira, temos uma relação de igualdade e podemos realizar operações iguais em ambos os lados sem alterar essa relação. O passo a seguir é considerado um artifício algébrico.

$$\mathbf{10}\boldsymbol{k} - \mathbf{20}\boldsymbol{t} + \mathbf{21}\boldsymbol{t} = \mathbf{7}\boldsymbol{u} + \mathbf{21}\boldsymbol{t}$$

Note que, ao somar $\mathbf{21}\boldsymbol{t}$ na equação, não alteramos a igualdade, além disso, $\mathbf{7}|\mathbf{21}$, ou seja, $\mathbf{7}|\mathbf{7}\boldsymbol{u} + \mathbf{21}\boldsymbol{t}$. Onde podemos escrever $\mathbf{7}\boldsymbol{n} = \mathbf{7}\boldsymbol{u} + \mathbf{21}\boldsymbol{t}$ e dessa forma segue que:

$$\boldsymbol{p} = \mathbf{10}\boldsymbol{k} + \boldsymbol{t} = \mathbf{7}\boldsymbol{n}. \blacksquare$$

Exemplo 17: Verifique se $\mathbf{3731}$ é um múltiplo de $\mathbf{7}$.

Pelo critério, devemos olhar o número que representa o algarismo das unidades e multiplicar por $\mathbf{2}$, então,

$$\mathbf{373} - \mathbf{2} \times \mathbf{1}$$

$$= \mathbf{371}$$

Então $\mathbf{3731}$ será múltiplo de 7 apenas se $\mathbf{371}$ o for. No entanto, ainda é complicado dizer se $\mathbf{7}|\mathbf{371}$ e, dessa maneira, aplica-se o critério mais uma vez.

$$\mathbf{37} - \mathbf{2} \times \mathbf{1}$$

$$= \mathbf{35}$$

Como $\mathbf{7}|\mathbf{35}$, podemos concluir que $\mathbf{7}|\mathbf{371}$ assim como $\mathbf{7}|\mathbf{3731}$.

Exemplo 18: Verifique se $\mathbf{93275}$ pode ser escrito como $\mathbf{7}\boldsymbol{n}$.

Note que o exercício não pede para que $\mathbf{93275}$ seja escrito como $\mathbf{7}\boldsymbol{n}$, apenas para verificar se pode ser escrito, ou seja, devemos verificar se $\mathbf{93275}$ é um múltiplo de $\mathbf{7}$ e faremos isso aplicando o critério.

$$\mathbf{9327 - 2 \times 5}$$

$$\mathbf{= 9317}$$

$$\mathbf{931 - 2 \times 7}$$

$$\mathbf{= 917}$$

$$\mathbf{91 - 2 \times 7}$$

$$\mathbf{= 77}$$

Daí, conclui-se que $\mathbf{7|77}$ e isso implica que $\mathbf{7|93275}$, ou seja, $\mathbf{93275 = 7}\boldsymbol{n}$.

7 NOVO CRITÉRIO DE DIVISIBILIDADE POR PRIMOS

Iniciaremos explicando por que o critério é válido para todo e qualquer primo que seja maior ou igual a $\mathbf{7}$. Isso acontece devido ao fato de todo número primo maior ou igual a $\mathbf{7}$ ter apenas quatro terminações (último dígito) possíveis, a saber: $\mathbf{1, 3, 7\ e\ 9}$. Isso porque não pode terminar com um número par (senão seria divisível por 2 e, logo, não seria primo) e nem com o número 5 (senão seria divisível por 5 e, portanto, não seria primo). Sem contar que, para os primos 2 e 5, saber se um número é ou não múltiplo deles é relativamente simples. Essas possíveis quatro terminações possuem uma propriedade interessante.

Ao realizar uma multiplicação, é possível saber antecipadamente qual será o último dígito do resultado? Sim, para isso, basta saber os dígitos finais de ambos os fatores.

Exemplo 19: Qual o último dígito do produto entre $\mathbf{13}$ e $\mathbf{17}$?

Note que os últimos dígitos dos fatores são, respectivamente, $\mathbf{3}$ e $\mathbf{7}$. Daí, o resultado da multiplicação entre $\mathbf{3 \times 7 = 21}$. Com isso, verificamos que o último dígito do resultado é $\mathbf{1}$, ou seja, o dígito final do produto entre $\mathbf{13}$ e $\mathbf{17}$ é $\mathbf{1}$. De fato

$$\mathbf{13 \times 17 = 221}$$

Sabemos que a quantidade de terminações para o último dígito dos infinitos números inteiros é limitada e isso é algo simples de ser percebido, pois, nosso sistema numérico possui apenas dez algarismos distintos, que são eles: $(\mathbf{0, 1, 2, 3, 4, 5, 6, 7, 8, 9})$. Concluímos que, dado um número qualquer $\boldsymbol{n} \in \mathbb{Z}$, as possíveis terminações de $\boldsymbol{n}$ (último dígito) são $(\mathbf{0, 1, 2, 3, 4, 5, 6, 7, 8, 9})$.

Agora, já temos conhecimento de que as únicas terminações possíveis para qualquer primo maior ou igual a $\mathbf{7}$ são $\mathbf{1, 3, 7}$ e $\mathbf{9}$. Também já sabemos como verificar o último dígito do resultado de um produto entre inteiros. Nesse momento, vamos verificar todas as terminações de produtos desses quatro algarismos.

Tabela 04 - Combinação de fatores

$1 \times 0 = 0$	$3 \times 0 = 0$	$7 \times 0 = 0$	$9 \times 0 = 0$
$1 \times 1 = 1$	$\mathbf{3 \times 1 = 3}$	$\mathbf{7 \times 1 = 7}$	$\mathbf{9 \times 1 = 9}$
$1 \times 2 = 2$	$\mathbf{3 \times 2 = 6}$	$\mathbf{7 \times 2 = 14}$	$\mathbf{9 \times 2 = 18}$
$1 \times 3 = 3$	$\mathbf{3 \times 3 = 9}$	$\mathbf{7 \times 3 = 21}$	$\mathbf{9 \times 3 = 27}$
$1 \times 4 = 4$	$\mathbf{3 \times 4 = 12}$	$\mathbf{7 \times 4 = 28}$	$\mathbf{9 \times 4 = 36}$
$1 \times 5 = 5$	$\mathbf{3 \times 5 = 15}$	$\mathbf{7 \times 5 = 35}$	$\mathbf{9 \times 5 = 45}$
$1 \times 6 = 6$	$\mathbf{3 \times 6 = 18}$	$\mathbf{7 \times 6 = 42}$	$\mathbf{9 \times 6 = 54}$
$1 \times 7 = 7$	$\mathbf{3 \times 7 = 21}$	$\mathbf{7 \times 7 = 49}$	$\mathbf{9 \times 7 = 63}$
$1 \times 8 = 8$	$\mathbf{3 \times 8 = 24}$	$\mathbf{7 \times 8 = 56}$	$\mathbf{9 \times 8 = 72}$
$1 \times 9 = 9$	$\mathbf{3 \times 9 = 27}$	$\mathbf{7 \times 9 = 63}$	$\mathbf{9 \times 9 = 81}$

Fonte: Elaboração do autor

É possível tirar alguma afirmação dos dados acima? Perceba que todos os $\mathbf{10}$ produtos de cada coluna possuem todas as terminações possíveis, além disso, sem repetições. Por exemplo, se um número primo $\boldsymbol{p}$ terminar em 7, então sempre é possível escolher de forma única um algarismo *q* entre 0 e 9, inclusive, para o qual o produto $\boldsymbol{pq}$ termine com 4, ou com 5, ou com 9, ou com 0, ou com 2. Basta escolhermos $\boldsymbol{q = 2,\ q = 5, q = 7, q = 0\ e\ q = 6,}$ respectivamente. Isso vale para primos que terminam com 1, 3 e 9 também.

Exemplo 20: Verifique se o número $\mathbf{13}$ é capaz de gerar todas as terminações possíveis de um número.

Para fazer a verificação basta notar que o último algarismo do número $\mathbf{13}$ é $\mathbf{3}$ e, com isso, realizar todas as combinações (produtos) com o último dígito do outro possível fator. Segue que:

$3 \times 0 = 0$	$3 \times 5 = 15$
$3 \times 1 = 3$	$\mathbf{3 \times 6 = 18}$
$3 \times 2 = 6$	$\mathbf{3 \times 7 = 21}$
$3 \times 3 = 9$	$\mathbf{3 \times 8 = 24}$
$3 \times 4 = 12$	$\mathbf{3 \times 9 = 27}$

Concluímos que todo número primo maior ou igual a $\mathbf{7}$ sempre terá infinitos múltiplos com todas as terminações possíveis. Essa conclusão que faz possível o funcionamento do critério que será trabalhado logo abaixo. Antes disso, segue uma importante definição que servirá como suporte para o critério.

Definição 8 *(*$\boldsymbol{M - suporte\ de\ p}$*): Considere* $\boldsymbol{M}$ *um inteiro não negativo qualquer cujo algarismo da unidade seja* $\boldsymbol{m_0}$*. Dado* $\boldsymbol{p \geq 7}$ *um número primo, o* $\boldsymbol{M - suporte\ de\ p}$

será $\boldsymbol{q_{M,p} \in \{0,1,2,3,4,5,6,7,8,9\}}$ *o menor número não negativo tal que* $\boldsymbol{pq_{M,p}}$ *termina com* $\boldsymbol{m_0}$.

Observe que a existência e a unicidade de $\boldsymbol{q_{M,p}}$ são garantidas pela Tabela $\mathbf{04}$ e iremos nos referir a ele como $\boldsymbol{M - suporte\ de\ p}$, ou seja, o número que dará suporte para $\boldsymbol{p}$ de tal forma que o novo múltiplo de $\boldsymbol{p}$ termine com o último algarismo de $\boldsymbol{M}$. Além disso, vale ressaltar que $\boldsymbol{M - suporte\ de\ p}$ é único para cada uma das dez terminações de $\boldsymbol{M}$ e será representado por um dos seguintes algarismos: $(\mathbf{0,1,2,3,4,5,6,7,8,9})$.

Exemplo 21: Se $\boldsymbol{p = 7}$ e $\boldsymbol{M = 293}$, então $\boldsymbol{q_{M,p} = 9}$, pois $\boldsymbol{9 \times 7 = 63}$.

Exemplo 22: Se $\boldsymbol{p = 13}$ e $\boldsymbol{M = 5434}$, então $\boldsymbol{q_{M,p} = 8}$, pois $\boldsymbol{8 \times 13 = 104}$.

Exemplo 23: Se $\boldsymbol{p = 29}$ e $\boldsymbol{M = 1877}$, então $\boldsymbol{q_{M,p} = 3}$, pois $\boldsymbol{3 \times 29 = 87}$.

Exemplo 24: Se $\boldsymbol{p = 31}$ e $\boldsymbol{M = 1419}$, então $\boldsymbol{q_{M,p} = 9}$, pois $\boldsymbol{9 \times 31 = 279}$.

Exemplo 25: Se $\boldsymbol{p = 11}$ e $\boldsymbol{M = 3368}$, então $\boldsymbol{q_{M,p} = 8}$, pois $\boldsymbol{8 \times 11 = 88}$.

Exemplo 26: Se $\boldsymbol{p = 23}$ e $\boldsymbol{M = 5411}$, então $\boldsymbol{q_{M,p} = 7}$, pois $\boldsymbol{7 \times 23 = 161}$.

Exemplo 27: Se $\boldsymbol{p = 17}$ e $\boldsymbol{M = 5688}$, então $\boldsymbol{q_{M,p} = 4}$, pois $\boldsymbol{4 \times 17 = 68}$.

7.1 Demonstração do Critério para Primos $p \geq 7$

Segue a seguinte proposição que servirá como suporte e principal motivo para o funcionamento do critério.

Proposição 5: Seja $\boldsymbol{p \geq 7}$ um número primo e considere $\boldsymbol{M}$ um número não negativo. Se $\boldsymbol{a_0 = m_0}$ são os últimos algarismos de $\boldsymbol{pq_{M,p}}$ e $\boldsymbol{M}$, então $\boldsymbol{10 | M - pq_{M,p}}$.

Demonstração: Seja $\boldsymbol{M = b_v 10^v + \cdots + b_2 10^2 + b_1 10^1 + m_0}$ e $\boldsymbol{pq_{M,p} = a_n 10^n + \cdots + a_2 10^2 + a_1 10^1 + a_0}$. Dessa forma,

$\boldsymbol{M - pq_{M,p} = (b_v 10^v + \cdots + b_2 10^2 + b_1 10^1 + m_0) - (a_n 10^n + \cdots + a_2 10^2 + a_1 10^1 + a_0)}$, e agora colocando $\mathbf{10}$ em evidência, teremos

$$\boldsymbol{M - pq_{M,p} = 10[(b_v 10^{v-1} + \cdots + b_2 10^1 + b_1) - (a_n 10^{n-1} + \cdots + a_2 10^1 + a_1)] + m_0 - a_0}$$

$$\boldsymbol{= 10[(b_v 10^{v-1} + \cdots + b_2 10^1 + b_1) - (a_n 10^{n-1} + \cdots + a_2 10^1 + a_1)]}$$

Com isso concluímos que $\boldsymbol{10 | M - pq_{M,p}}$ se os algarismos da unidade de $\boldsymbol{M}$ e $\boldsymbol{pq_{M,p}}$ forem iguais, o que de fato ocorre pela definição do $\boldsymbol{M - suporte\ de\ p}$. ■

Definição 9: *(Processo de Elias): Sejam* $\boldsymbol{p \geq 7}$ *um número primo e* $\boldsymbol{M}$ *um inteiro positivo. Considere o número inteiro*

$$\boldsymbol{M_1 = \frac{M - pq_{M,p}}{10}}.$$

Note que, pela definição de $\boldsymbol{M - suporte\ de\ p}$ *e pela proposição anterior,* $\boldsymbol{M_1}$ *é com certeza um número inteiro, já que* $\boldsymbol{10|M - pq_{M,p}}$*. Agora, supondo definido o número* $\boldsymbol{M_n}$*, definimos por indução*

$$\boldsymbol{M_{n+1} := \frac{M_n - pq_{M_n,p}}{10}, n \geq 1}.$$

Daí, note que $\boldsymbol{M_1 \geq M_2 \geq M_3 \geq \cdots \geq M_n \geq \cdots, \forall\, n \geq 1}$.

Teorema 9 *(Critério de Divisibilidade de Elias): Sejam* $\boldsymbol{p \geq 7}$ *um número primo e* $\boldsymbol{M}$ *um inteiro positivo. Nas notações da definição de* $\boldsymbol{M - suporte\ de\ p}$ *e do Processo de Elias, vale que:*

$$\boldsymbol{p|M \Leftrightarrow p|M_1}.$$

Demonstração: Se $\boldsymbol{p|M}$, então, pela Definição 7, $\boldsymbol{M = ps, s} \in \mathbb{Z}$. Assim,

$$\boldsymbol{M_1 = \frac{M - pq_{M,p}}{10}}$$
$$\boldsymbol{= \frac{(ps - pq_{M,p})}{10}}$$
$$\boldsymbol{= \frac{p(s - q_{M,p})}{10}}$$

Note que $\boldsymbol{p \geq 7}$ é um número primo, ou seja, da igualdade

$$\boldsymbol{10M_1 = p(s - q_{M,p})}$$

tem-se $\boldsymbol{p|M_1}$ pois $\boldsymbol{10}$ possui fatores primos diferentes de $\boldsymbol{p}$ já que $\boldsymbol{10 = 2 \times 5}$. Reciprocamente, se $\boldsymbol{p|M_1}$, segue que

$$\boldsymbol{M_1 = pa}$$
$$\Downarrow$$
$$\boldsymbol{\frac{M - pq_{M,p}}{10} = pa}$$

que, multiplicando por $\boldsymbol{10}$, torna-se

$$\boldsymbol{M - pq_{M,p} = 10pa}$$
$$\Downarrow$$

$$\boldsymbol{M = 10pa + pq_{M,p}}$$

$$\Downarrow$$

$$\boldsymbol{M = p(10a + q_{M,p})}$$

$$\Downarrow$$

$$\boldsymbol{p|M}. \ \blacksquare$$

Vale ressaltar que o critério de Elias deve ser visto como um processo iterado para sabermos se $\boldsymbol{p}$ divide $\boldsymbol{M}$ ou não. Em outras palavras, se não soubermos se $\boldsymbol{p}$ divide $\boldsymbol{M_1}$, aplicamos novamente o critério, obtendo

$$\boldsymbol{p|M \Leftrightarrow p|M_1 \Leftrightarrow p|M_2} \ldots \boldsymbol{\Leftrightarrow p|M_n},$$

ou seja, esse processo deve ser feito até o momento em que seja possível concluir que $\boldsymbol{p|M_n}$ ou $\boldsymbol{p \nmid M_n}$ para algum $\boldsymbol{n} \in \mathbb{N}$.

A grande questão é: Como saber que, para algum $\boldsymbol{M_n}$, será sempre possível concluir que $\boldsymbol{p|M}$ ou $\boldsymbol{p \nmid M}$? Vamos mostrar que sempre, em algum passo do algoritmo, é possível dizer se $\boldsymbol{M}$ é ou não um múltiplo de $\boldsymbol{p}$.

Sabemos que o primeiro passo do algoritmo é fazer $\boldsymbol{M_1 := \frac{M - pq_{M,p}}{10}}$ e, nesse caso, há cinco alternativas para $\boldsymbol{M_1}$.

I. $\boldsymbol{M_1 < 0}$. Tem-se $\boldsymbol{\frac{M - pq_{M,p}}{10} < 0 \iff M - pq_{M,p} < 0}$ $\qquad (\boldsymbol{1})$

Vamos concluir que $\boldsymbol{M}$ não pode ser múltiplo de $\boldsymbol{p}$. Suponha por absurdo que se escreva $\boldsymbol{M = pk}$ para algum $\boldsymbol{k} \in \mathbb{Z}$. Note que, sendo $\boldsymbol{M > 0}$, tem-se $\boldsymbol{k > 0}$. Assim, de $(\boldsymbol{1})$, segue que

$$\boldsymbol{p(k - q_{M,p}) < 0 \Leftrightarrow k < q_{M,p}}.$$

Isso diz que existe $\boldsymbol{0 < k < q_{M,p} \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}}$ tal que $\boldsymbol{pk}$ tem o mesmo algarismo da unidade de $\boldsymbol{M}$, o que contradiz a minimalidade do $\boldsymbol{M - suporte\ de\ p}$, $\boldsymbol{q_{M,p}}$. Logo, $\boldsymbol{M}$ não é múltiplo de $\boldsymbol{p}$.

II. $\boldsymbol{M_1 = 0}$

Aqui, $\boldsymbol{M = pq_{M,p}}$ e $\boldsymbol{M}$ é múltiplo de $\boldsymbol{p}$.

III. $\boldsymbol{M_1 = p}$

Nesse caso, $\boldsymbol{M = p(10 + q_{M,p})}$ e $\boldsymbol{M}$ é múltiplo de $\boldsymbol{p}$.

IV. $\boldsymbol{0 < M_1 < p}$

Supondo por absurdo novamente que $\boldsymbol{M = pk, k} \in \mathbb{N}$, temos

$$\boldsymbol{0 < \frac{M - pq_{M,p}}{10} < p \iff 0 < p(k - q_{M,p}) < 10p \Leftrightarrow 0 < k - q_{M,p} < 10}.$$

De um lado, $\boldsymbol{k < 10 + q_{M,p} = 1q_{M,p}}$ (1 é o algarismo da dezena e $\boldsymbol{q_{M,p}}$, da unidade), e esse número, é o primeiro inteiro maior do que $\boldsymbol{q_{M,p}}$ que, multiplicado por $\boldsymbol{p}$, tem a mesma terminação de $\boldsymbol{M}$. Como $\boldsymbol{pk = M}$, e $\boldsymbol{k < 1q_{M,p}}$, segue que $\boldsymbol{k = q_{M,p}}$, porém, eles não podem ser iguais em vista de $\boldsymbol{0 < k - q_{M,p}}$. Com isso, chegamos a um absurdo, ou seja, $\boldsymbol{M}$ não é múltiplo de $\boldsymbol{p}$.

Note que, das quatro alternativas anteriores, é possível sabermos se $\boldsymbol{M}$ é ou não múltiplo de $\boldsymbol{p}$, restando apenas uma.

V. $\boldsymbol{M_1 > p}$

Nesse caso, fazemos o passo 2 do critério, definindo

$$\boldsymbol{M_2 = \frac{M_1 - pq_{M_1,p}}{10}}.$$

Nessa nova etapa, todas os quatro passos anteriores são aplicados agora em $\boldsymbol{M_2}$, e substituímos a letra $\boldsymbol{M}$ por $\boldsymbol{M_1}$. Lembrando que o critério deve ser visto como um processo iterado e, diante do processo feito no Teorema 9, tem-se

$$\boldsymbol{p|M \Leftrightarrow p|M_1 \Leftrightarrow p|M_2}$$

E novamente, deve ser verificado se $\boldsymbol{M_2}$ se enquadra em I, II, III ou IV. Caso

$$\boldsymbol{M_2 > p}$$

aplicamos o critério, considerando $\boldsymbol{M_3}$:

$$\boldsymbol{M_3 = \frac{M_2 - pq_{M_2,p}}{10}}.$$

Procedemos assim sucessivamente. Afirmamos que, em algum passo, digamos o passo $\boldsymbol{n + 1} \in \mathbb{N}$, acontece uma das alternativas anteriores. De fato, note que:

$$\begin{aligned}
\boldsymbol{M_{n+1}} &= \boldsymbol{\frac{M_n - pq_{M_n,p}}{10} = \frac{M_n}{10} - \frac{pq_{M_n,p}}{10}} \\
&= \boldsymbol{\frac{\frac{M_{n-1} - pq_{M_{n-1},p}}{10}}{10} - \frac{pq_{M_n,p}}{10}} \\
&= \boldsymbol{\frac{M_{n-1}}{10^2} - \frac{pq_{M_{n-1},p}}{10^2} - \frac{pq_{M_n,p}}{10}} \\
&= \cdots \\
&= \boldsymbol{\frac{M}{10^{n+1}} - \frac{pq_{M,p}}{10^{n+1}} - \cdots - \frac{pq_{M_n,p}}{10}}, \qquad (2)
\end{aligned}$$

de tal forma que

$$\boldsymbol{M_{n+1} \leq \frac{M}{10^{n+1}}, \forall\, n \geq 1}.$$

Portanto, tomando $\boldsymbol{n} \in \mathbb{N}$ grande o bastante, vemos que $\boldsymbol{M_{n+1} < p}$ em algum passo. Concluímos que sempre é possível saber se $\boldsymbol{M}$ é ou não múltiplo de $\boldsymbol{p}$.

Corolário 1*: Sejam* $\boldsymbol{M}$ *um inteiro positivo e* $\boldsymbol{p \geq 7}$ *um número primo. Então,* $\boldsymbol{p|M \Leftrightarrow M_{n+1} = 0}$ *para algum* $\boldsymbol{n \in \mathbb{N} \cup \{0\}}$.

Demonstração: Se $\boldsymbol{M_{n+1} = 0}$ para algum $\boldsymbol{n \in \mathbb{N} \cup \{0\}}$, então $\boldsymbol{M_n = pq_{M,p} \Longrightarrow p|M_n \Longrightarrow p|M}$. Se $\boldsymbol{p|M}$, seja $\boldsymbol{n \in \mathbb{N} \cup \{0\}}$ dado anteriormente de tal forma que $\boldsymbol{M_{n+1} < p}$. Assim, $\boldsymbol{M_{n+1} < 0}$ ou $\boldsymbol{M_{n+1} = 0}$ ou $\boldsymbol{0 < M_{n+1} < p}$. Mas, se $\boldsymbol{M_{n+1} < 0}$ ou $\boldsymbol{0 < M_{n+1} < p}$ ocorresse, teríamos $\boldsymbol{p \nmid M}$ como foi feito nas alternativas colocadas anteriormente, contradizendo nossa hipótese. Logo, $\boldsymbol{M_{n+1} = 0}$, como queríamos mostrar. ■

As considerações anteriores nos fornecem uma informação fundamental dentro do cenário de divisibilidade nos inteiros. Em palavras, o critério de Elias explicita o valor do quociente da divisão se esta for exata.

Corolário 2*: Sejam* $\boldsymbol{M}$ *um inteiro positivo e* $\boldsymbol{p \geq 7}$ *um número primo. Se* $\boldsymbol{M_{n+1} = 0}$ *para algum* $\boldsymbol{n \in \mathbb{N} \cup \{0\}}$ *e* $\boldsymbol{n}$ *é o menor dos elementos com essa propriedade, então*

$$\boldsymbol{\frac{M}{p} = q_{M,p} + 10q_{M_1,p} + \cdots + 10^n q_{M_n,p}.}$$

Em outras palavras, o quociente $\boldsymbol{\frac{M}{p}}$ é formado pelos algarismos $\boldsymbol{q_{M_n,p}, q_{M_{n-1},p}, \ldots, q_{M,p}}$ nessa ordem.

Demonstração: Segue de (2) que

$$\boldsymbol{M_{n+1} = 0 = \frac{M}{10^{n+1}} - \frac{pq_{M,p}}{10^{n+1}} - \cdots - \frac{pq_{M_n,p}}{10}}$$

$$\Leftrightarrow$$

$$\boldsymbol{\frac{M}{10^{n+1}} = \frac{pq_{M,p}}{10^{n+1}} + \frac{pq_{M_1,p}}{10^n} + \cdots + \frac{pq_{M_n,p}}{10}}$$

Agora, multiplicando por $\boldsymbol{10^{n+1}}$, teremos

$$\boldsymbol{M = pq_{M,p} + 10pq_{M_1,p} + \cdots + 10^n pq_{M_n,p}}$$

$$\boldsymbol{M = p(q_{M,p} + 10q_{M_1,p} + \cdots + 10^n q_{M_n,p})}$$

$$\Leftrightarrow$$

$$\boldsymbol{\frac{M}{p} = q_{M,p} + 10q_{M_1,p} + \cdots + 10^n q_{M_n,p}.}$$

A minimalidade do número $\boldsymbol{n}$ é utilizada apenas para que não apareçam números da forma, por exemplo, $\mathbf{000352}$ que seria o número $\mathbf{352}$ na base decimal. ■

Vejamos alguns exemplos numéricos.

Exemplo 28: Verifique se o número $\mathbf{7}$ é divisor de $\mathbf{4172}$. Segue que:

$$\boldsymbol{p = 7}$$

$$\boldsymbol{M = 4172}$$

$$\boldsymbol{0 \leq q_{M,p} \leq 9}$$

Veja que $\boldsymbol{M}$ termina em $\mathbf{2}$, logo, precisamos encontrar um múltiplo de $\mathbf{7}$ terminado em $\mathbf{2}$. Como $\boldsymbol{0 \leq q_{M,p} \leq 9}$ e nesse caso $\boldsymbol{q_{M,p} = 6}$, pois, $\boldsymbol{7 \times 6 = 42}$. Daí,

$$\mathbf{7|4172} \Leftrightarrow \mathbf{7|}\frac{\mathbf{4172 - (7 \times 6)}}{\mathbf{10}}$$

$$\Leftrightarrow \mathbf{7|}\frac{\mathbf{4172 - 42}}{\mathbf{10}}$$

$$\Leftrightarrow \mathbf{7|}\ \frac{\mathbf{4130}}{\mathbf{10}}$$

$$\Leftrightarrow \mathbf{7|413}$$

Agora,

$$\boldsymbol{p = 7}$$

$$\boldsymbol{M_1 = 413}$$

e perceba que $\boldsymbol{M_1}$ termina em $\mathbf{3}$ e nesse caso, $\boldsymbol{q_{M1,p} = 9}$, pois, $\boldsymbol{7 \times 9 = 63}$. Segue que:

$$\mathbf{7|4172} \Leftrightarrow \mathbf{7|413} \Leftrightarrow \mathbf{7|}\frac{\mathbf{413 - 63}}{\mathbf{10}}$$

$$\Leftrightarrow \mathbf{7|}\frac{\mathbf{350}}{\mathbf{10}}$$

$$\Leftrightarrow \mathbf{7|35}$$

Logicamente que já é possível perceber que $\mathbf{7|35}$, no entanto, aplicaremos mais um passo. E nesse caso, $\boldsymbol{M_2 = 35}$ e, consequentemente, $\boldsymbol{q_{M2,p} = 5}$.

$$\mathbf{7|4172} \Leftrightarrow \mathbf{7|413} \Leftrightarrow \mathbf{7|35} \Leftrightarrow \mathbf{7|}\frac{\mathbf{35 - 35}}{\mathbf{10}}$$

$$\Leftrightarrow \mathbf{7|}\frac{\mathbf{0}}{\mathbf{10}}$$

$$\Leftrightarrow \mathbf{7|0}.$$

Com isso, concluímos que de fato $\mathbf{7|4172}$, pois $\boldsymbol{M_3 = 0}$. Além disso, $\frac{\mathbf{4172}}{\mathbf{7}} = \mathbf{596}$.

Exemplo 29: Agora, vamos verificar se $\mathbf{7|4117}$. Segue que:

$$\boldsymbol{p = 7}$$

$$\boldsymbol{M = 4117}$$

$$\boldsymbol{0 \leq q_{M,p} \leq 9}$$

Com isso teremos que $\boldsymbol{q_{M,p} = 1}$ e dessa forma:

$$\boldsymbol{7|4117 \Leftrightarrow 7|\frac{4117 - 7}{10}}$$

$$\boldsymbol{7\left|\frac{4110}{10} \Leftrightarrow 7\right|411}.$$

Seguindo para o segundo passo e tendo em mente que $\boldsymbol{M_1 = 411}$, então $\boldsymbol{q_{M_1,p} = 3}$.

$$\boldsymbol{7|4117 \Leftrightarrow 7|411 \Leftrightarrow 7|\frac{411 - 21}{10}}$$

$$\boldsymbol{\Leftrightarrow 7|\frac{390}{10} \Leftrightarrow 7|39}$$

Agora $\boldsymbol{M_2 = 39}$. Segue que $\boldsymbol{q_{M_2,p} = 7}$.

$$\boldsymbol{7|4117 \Leftrightarrow 7|411 \Leftrightarrow 7|39 \Leftrightarrow 7|\frac{39 - 49}{10}}$$

$$\boldsymbol{\Leftrightarrow 7| - 1}.$$

Perceba que $\boldsymbol{M_3 = -1 < 0}$, ou seja, isso implica que $\boldsymbol{7 \nmid 4117}$. E nessa condição, não é possível determinar o resultado da divisão.

Exemplo 30: Verifique se $\boldsymbol{101|95828194}$

$$\boldsymbol{p = 101}$$

$$\boldsymbol{M = 95828194}$$

$$\boldsymbol{0 \leq q_{M,p} \leq 9}$$

Como $\boldsymbol{M}$ termina em $\boldsymbol{4}$, $\boldsymbol{q_{M,p} = 4}$. Assim,

$$\boldsymbol{101|95828194 \Leftrightarrow 101|\frac{95828194 - 404}{10}}$$

$$\boldsymbol{\Leftrightarrow 101|9582779}$$

Agora, $\boldsymbol{M_1 = 9582779}$ e, então, $\boldsymbol{q_{M_1,p} = 9}$. Logo,

$$\boldsymbol{101|95828194 \Leftrightarrow 101|\ 9582779 \Leftrightarrow 101|\frac{9582779 - 909}{10}}$$

$$\boldsymbol{\Leftrightarrow 101|958187}$$

Nesse caso, $\boldsymbol{M_2 = 958187}$ e $\boldsymbol{q_{M_2,p} = 7}$. Segue que

$$\boldsymbol{101|95828194 \Leftrightarrow 101|9582779 \Leftrightarrow 101|958187 \Leftrightarrow 101|\frac{958187 - 707}{10}}$$

$$\boldsymbol{\Leftrightarrow 101|95748}$$

Temos $\boldsymbol{M_3 = 95748}$ e $\boldsymbol{q_{M_3,p} = 8}$.

$$\boldsymbol{101|95828194 \Leftrightarrow 101|9582779 \Leftrightarrow 101|958187 \Leftrightarrow 101|95748}$$

$$\boldsymbol{\Leftrightarrow 101|\frac{95748 - 808}{10}}$$

$$\boldsymbol{\Leftrightarrow 101|9494}$$

Daí, $\boldsymbol{M_4 = 9494}$ e $\boldsymbol{q_{M_4,p} = 4}$. Então,

$$\boldsymbol{101|95828194 \Leftrightarrow 101|9582779 \Leftrightarrow 101|958187 \Leftrightarrow 101|95748 \Leftrightarrow 101|9494}$$

$$\boldsymbol{\Leftrightarrow 101|\frac{9494 - 404}{10}}$$

$$\boldsymbol{\Leftrightarrow 101|909}$$

Segue que, $\boldsymbol{M_5 = 909}$ e $\boldsymbol{q_{M_5,p} = 9}$.

$$\boldsymbol{101|95828194 \Leftrightarrow 101|9582779 \Leftrightarrow 101|958187 \Leftrightarrow 101|95748 \Leftrightarrow 101|9494}$$

$$\boldsymbol{\Leftrightarrow 101|909 \Leftrightarrow 101|\frac{909 - 909}{10}}$$

$$\boldsymbol{\Leftrightarrow 101|0}$$

Como $\boldsymbol{M_6 = 0}$, concluímos que $\boldsymbol{101|95828194}$. Daí, $\boldsymbol{\frac{95828194}{101} = 948794} = (\boldsymbol{q_{M_5,p}q_{M_4,p}q_{M_3,p}q_{M_2,p}q_{M_1,p}q_{M,p}})$, que foram os $\boldsymbol{M - suportes\ de\ p}$ necessários no processo.

8 CONSIDERAÇÕES FINAIS

Levando em consideração os objetivos deste trabalho, acreditamos que todos foram satisfeitos dentro de suas limitações. Primeiramente, realizamos uma discussão sobre o valor que a Matemática pura possui na sociedade. Logo em seguida, conduzimos uma investigação histórica sobre os principais autores que se debruçaram em estudos com o principal objeto de estudo desta monografia (números primos), bem como a importância destes na criptografia. Posteriormente, voltamos a atenção para temas que serviram como base e inspiração para o principal objetivo da pesquisa.

Em resumo, este TCC introduziu um critério de divisibilidade inovador, proporcionando avanços significativos na compreensão dos números e na aplicação prática da teoria dos números. Além disso, a capacidade de determinar o resultado da divisão (caso seja múltiplo) acrescenta uma camada adicional de utilidade, simplificando o processo de cálculo e proporcionando uma abordagem mais abrangente. Isso destaca a importância e o impacto deste trabalho não apenas na comunidade acadêmica, mas também na educação básica como um todo, considerando que sua simplicidade de aplicação e entendimento o torna relevante para esse nível de ensino.

Novamente, o fato de este critério ser capaz de entregar o resultado da divisão demonstra mais uma vez a importância dessa nova ferramenta. Se compararmos com outros critérios existentes, como por exemplo, critérios de divisibilidade por $\mathbf{2}, \mathbf{3}$ ou $\mathbf{5}$, ele se sobressairá nesse quesito, sendo válido não apenas para qualquer número primo com terminação em $\mathbf{1}, \mathbf{3}, \mathbf{7}$ ou $\mathbf{9}$. Ou seja, o critério é válido para todo e qualquer número inteiro ímpar, diferente de um múltiplo de cinco.

Exemplo: Verifique se $\mathbf{49}|\mathbf{139944}$.

Note que $\mathbf{49}$ é um número composto terminado em $\mathbf{9}$, ou seja, o critério pode ser aplicado. Segue que:

$$\mathbf{49}|\mathbf{139944} \Leftrightarrow \mathbf{49}|\frac{\mathbf{139944} - \mathbf{49} \times \mathbf{6}}{\mathbf{10}}$$

$$\Leftrightarrow \mathbf{49}|\mathbf{13965} \Leftrightarrow \mathbf{49}|\frac{\mathbf{13965} - \mathbf{49} \times \mathbf{5}}{\mathbf{10}}$$

$$\Leftrightarrow \mathbf{49}|\mathbf{1372} \Leftrightarrow \mathbf{49}|\frac{\mathbf{1372} - \mathbf{49} \times \mathbf{8}}{\mathbf{10}}$$

$$\Leftrightarrow \mathbf{49}|\mathbf{98} \Leftrightarrow \mathbf{49}|\frac{\mathbf{98}-\mathbf{49}\times\mathbf{2}}{\mathbf{10}}$$

$$\Leftrightarrow \mathbf{49}|\mathbf{0}$$

Portanto, de fato $\mathbf{49}|\mathbf{139944}$, além disso, o resultado da divisão de $\frac{\mathbf{139944}}{\mathbf{49}} = \mathbf{2856}$.

Outro ponto importantíssimo a ser destacado é o fato de o critério ter sido validado computacionalmente com uma programação em HTML, conforme apresentado nos anexos abaixo. Isso demonstra que a ferramenta possui relevância, apesar de não ser algo astronômico, matematicamente falando.

Concluímos que os critérios de divisibilidade desempenham um papel fundamental na teoria dos números, fornecendo ferramentas cruciais para compreender a estrutura e as propriedades dos números inteiros. Essas regras estabelecem padrões que indicam quando um número é divisível por outro, simplificando a resolução de problemas matemáticos e facilitando a identificação de relações numéricas. Além de seu valor intrínseco na solução de equações e na simplificação de cálculos, os critérios de divisibilidade são essenciais em diversas áreas, incluindo criptografia, fatoração de números e elaboração de algoritmos.

Sua importância transcende a matemática pura, estendendo-se a aplicações práticas em ciência da computação, segurança de dados e diversas disciplinas científicas. Isso destaca o papel crucial desses critérios no avanço do conhecimento e na resolução de problemas do mundo real.

Por fim, vale ressaltar que ainda há muito a ser estudado sobre essa nova ferramenta, como, por exemplo, sua aplicação também para números pares. Além disso, determinar o resto da divisão nos casos em que $\boldsymbol{p} \nmid \boldsymbol{M}$ é um tópico a ser explorado. Isso mostra a gama de possibilidades que esse novo critério disponibilizou.

REFERÊNCIAS

ALVES, Rafael Pimenta. **Um estudo sobre os critérios de divisibilidade**: questionamento sobre a inserção deste como conteúdo a ser abordado no ensino médio.2020.79f. Dissertação (Mestrado Profissional em Matemática) – Universidade Federal do Tocantins, Programa de Pós-Graduação em Matemática, Arraias, 2020. Disponível em: http://hdl.handle.net/11612/2957. Acesso em: 15/09/2023.

AVILA, Artur. **Beleza da matemática 'só se revela a quem a explora a fundo'.** [Entrevista concedida a IMPA] Cecília Manzoni. IMPA, Notícias, 06/2022. Disponível em: https://impa.br/noticias/artur-avila-beleza-da-matematica-so-se-revela-a-quem-a-explora-a-fundo/. Acesso em: 17/08/2023.

BEZERRA, Nazaré. **Teoria dos números**: um curso introdutório. Belém: EditAedi, 2018. E-book (193 p.). Disponível em: http://livroaberto.ufpa.br/jspui/handle/prefix/479. Acesso em: 30/08/2023

CANÁRIO, Cláudia *et al*. **Roteiro de viagem**:o quinto postulado de Euclides. 2000. Disponível em: https://webpages.ciencias.ulisboa.pt/~ommartins/seminario/euclides/index.htm. Acesso em: 17/08/2023.

COSTA, Tito José Minhava Botelho da. **Os números perfeitos e os primos de Mersenne**. 2015. 65 f. Dissertação (Mestrado) - Curso de Matemática, Mestrado em Matemática Para Professores, Universidade de Lisboa, Lisboa, 2015. Disponível em: https://repositorio.ul.pt/bitstream/10451/20623/1/ulfc113672_tm_Tito_Costa.pdf. Acesso em: 13/09/2023.

COUTINHO, S. C. **Números Inteiros e Criptografia RSA** (Série Computação e Matemática). Rio de Janeiro: IMPA, 2001.

DIAS, Léo Amaro de Abreu. **A importância da pesquisa em matemática pura**. UFSC (Universidade Federal de Santa Catarina), Repositório Institucional. 10/2020. Disponível em: https://repositorio.ufsc.br/handle/123456789/216789. Acesso em: 17/08/2023.

FRITSCHE, Willian Cleyson; SUGUIMOTO, Alexandre Shuji. **OS NÚMEROS PRIMOS E A HIPÓTESE DE RIEMANN**. 2015. 9 p. Disponível em: https://www.unicesumar.edu.br/epcc-2015/wp-content/uploads/sites/65/2016/07/willian_cleyson_fritsche_1.pdf. Acesso em: 22/09/2023.

FUSCO, Cristiana Abud da Silva; COELHO, Sônia Pitta. Um pouco da teoria dos números: da antiguidade até os dias atuais. **Ensino da Matemática em Debate**, São Paulo, v. 1, n. 2, p.1-12, 2014. Disponível em: https://revistas.pucsp.br/emd/article/download/21712/15995. Acesso em: 23/08/2023.

GIL, Antônio Carlos. **Métodos e técnicas de pesquisa social**. 6. ed. São Paulo, Atlas, 2008.

IEZZI, Hygino H. Domingues Gelson. **Álgebra Mordena**. 4. ed. São Paulo: Atual Editora, 2003. 371 p.

LIMA, Heronilza Silva. **A hipótese de Riemann e a ameaça a criptografia** / Heronilza Silva Lima. – Goiânia: Trabalho de Conclusão de Curso (Especialização em Matemática) – Instituto Federal de Educação, Ciência e Tecnologia de Goiás, 2022.Disponível em: https://abrir.link/aS0RL. Acesso em:29/09/2023.

MARTINEZ, Fabio E. Brochero. MOREIRA, Carlos Gustavo T. de A. SALDANHA, Nicolau C. TENGAN, Eduardo. **TEORIA DOS NÚMEROS**: um passeio com primos e outros números familiares pelo mundo inteiro. [S.D]. 510 p.

MARTINS, Maria do Carmo. Eratóstenes: um génio do período Helénico!. **Correio dos Açores**, p. 14-14, 2014. Disponível em; https://abrir.link/h86qw. Acesso em:04/09/2023.

MOLINARI, José Royson Aggio. **NÚMEROS PRIMOS E A CRIPTOGRAFIA RSA**. Dissertação (Mestrado) - Curso de Pós-Graduação em Matemática, Setor de Ciências Exatas e Naturais, Universidade Estadual de Ponta Grossa, Ponta Grossa, 2016. 54f. Disponível em: http://tede2.uepg.br/jspui/handle/prefix/1504. Acesso em: 06/10/2023.

MOREIRA, Carlos Gustavo; SALDANHA, Nicolau. **Primos de Mersenne** (e outros primos muito grandes). 3. ed. Rio de Janeiro: IMPA, 2008.

OKUMURA, Mirella Kyio. **Números primo e criptografia RSA**. 2014. 41 f. Dissertação (Doutorado) - Curso de Matemática, Instituto de Ciências Matemáticas e de Computação, Universidade de São Paulo, São Carlos, 2014. Disponível em: https://abrir.link/NMtdu. Acesso em: 01/10/ 2023.

OS ELEMENTOS: Euclides. [S. L.]: Unesp, 2009. 600 p. Tradução e Introdução: Irineu Bicudo.

PRODANOV, C. C.; FREITAS, E. C. **Metodologia do trabalho científico**: métodos e técnicas da pesquisa e do trabalho acadêmico. Novo Hamburgo: Feevale, 2013. Ebook. ISBN 978-85-7717-158-3. Disponível em: https://drive.google.com/file/d/1lp5R-RyTrt6X8UPoq2jJ8gO3UEfM_JJd/view>. Acesso em:11/08/2023.

RANGEL, Ester Silva; BERNARDO, Brasil Leomaques Francisco Silva; SILVA, Taiane Barboza. **NÚMEROS PRIMOS E SUAS CONTRIBUIÇÕES**, Disponível em; http://www.mat.ufcg.edu.br/pet/arquivos/resumos/ii-wmm-taiane-ester.pdf. Acesso em: 13/09/2023.

SAUTOY, Marcus de. **A Música dos Números Primos**: a história de um problema não resolvido na matemática. [S. L.]: Zahar, 2007. 351 p. Tradução de Diego Alfaro.

SILVEIRA, J.F. Porto da. **POR QUE O NOME PRIMO PARA OS NÚMEROS PRIMOS ?** 2001. Elaborada por Universidade Federal do Rio Grande do Sul. Disponível em: http://athena.mat.ufrgs.br/~portosil/histo2.html. Acesso em: 03/09/2023.

SIMÕES, Márcio. **Deserto de números primos**: um erro comum no ensino básico. 2019. Blogue Imaginário Puro. Disponível em: https://imaginariopuro.wordpress.com/2019/05/24/desertos-de-numeros-primos-e-um-erro-comum-no-ensino-basico/. Acesso em: 22/09/2023.

SOUZA, Rhiel Natham Ribeiro de. **INTEIROS QUE SÃO SOMAS DE DOIS QUADRADOS**: uma interface entre primos e congruência modular. 2022. 50 f. TCC (Graduação) - Curso de Matemática, Universidade Federal do Norte do Tocantins, Araguaína, 2022.

THOMÉ, Joao Antonio Francisconi Lubanco. **Uma Breve Introdução à Hipótese de Riemann**. Disponível em: https://abrir.link/1RFvY. Acesso em: 29/09/2023.

ANEXOS

Anexo A - Código em HTML do Critério

Este anexo é um código com a programação do critério provado anteriormente nesta monografia. Sua construção ocorreu com o suporte de inteligência artificial. Espera-se que o leitor copie e cole o código em uma plataforma de teste para códigos em HTML e veja a força do algoritmo.

```
<!DOCTYPE html>
<html>
<head>
    <title>Número Primo e Natural</title>
    <style>
        body {
            font-family: Arial, sans-serif;
            background-color: #f7f7f7;
            text-align: center;
            padding: 20px;
        }

        h2 {
            color: #333;
        }

        input, button {
            padding: 10px;
            margin: 10px;
            border-radius: 5px;
            border: 1px solid #ddd;
        }

        button {
            background-color: #007bff;
            color: white;
            cursor: pointer;
        }

        button:hover {
            background-color: #0056b3;
        }

        #resultado {
            margin-top: 20px;
            text-align: left;
```

```
                    display: inline-block;
                    font-size: 1.2em;
                }
            </style>
        </head>
        <body>
            <h2>Calculadora de Números Primos e Naturais</h2>

            <div>
                <label for="numeroN">Digite um número natural (n):</label><br>
                <input type="number" id="numeroN"><br>
            </div>

            <div>
                <label for="numeroP">Digite um número primo (p) maior ou igual a
7:</label><br>
                <input type="number" id="numeroP"><br>
            </div>

            <button onclick="calcularNumero()">Calcular</button>

            <div id="resultado"></div>

            <script>
            function calcularNumero() {
                    var n = parseInt(document.getElementById("numeroN").value);
                    var p = parseInt(document.getElementById("numeroP").value);

                    if (!isPrime(p) || p < 7 || n < 1) {
                        alert("Certifique-se de que 'n' é um número natural e 'p'
é um primo maior ou igual a 7.");
                        return;
                    }

                    var resultado = "";
                    var passo = 1;
                    while (true) {
                        var h = n % 10;
                        var q = encontrarQ(p, h);

                        var n_i = Math.floor((n - p * q) / 10);
                        resultado += "Passo " + passo + ": n: " + n + ", q: " +
q + ", n_" + passo + ": " + n_i + "<br>";

                        if (n_i <= 0) {
                            break;
                        }

                        n = n_i;
                        passo++;
                    }
```

```
            document.getElementById("resultado").innerHTML = resultado;
        }

        function encontrarQ(p, h) {
            for (var i = 0; i < 10; i++) {
                if ((i * p) % 10 === h) {
                    return i;
                }
            }
            return 0; // Retorna 0 se não encontrar um q adequado
        }

        function isPrime(num) {
            for (var i = 2; i < num; i++)
                if (num % i === 0) return false;
            return num > 1;
        }
    </script>
</body>
</html>
```

Anexo B - Resultado decorrente

Este anexo traz uma breve introdução há um resultado similar ao algoritmo demonstrado nesta monografia. O objetivo é mostrar ao leitor que o processo reverso pode ser utilizado e possui as mesmas propriedades do algoritmo trabalhado. Vale ressaltar que o resultado abaixo não foi demonstrado nesta monografia, contudo, conjecturamos que esse processo possa ser validado pela Proposição 2 já que consiste basicamente em somar múltiplos do primo em questão através de um processo iterado e inverso ao que foi discutido anteriormente.

Suponha que precise ser verificado se $7|881258$, nesse caso, $p = 7$ e $M = 881258$. Como já temos conhecimento, o número 7 possui infinitos múltiplos com todas as terminações para o último dígito possível, ou seja, $(0,1,2,3,4,5,6,7,8,9)$. O processo contrário do critério demonstrado nesta monografia ocorre da seguinte maneira: *Construir M somando múltiplos de p específicos, de tal forma que os algarismos de M e do novo número construído sejam iguais a cada passo*.

Vejamos para o caso anterior. Note que $M = 881258$ termina em 8, logo V (novo número) será

$$V = 4 \times 7 = 28$$

Daí, já temos o último algarismo de M igual ao último algarismo de V. O passo seguinte é igualar o penúltimo algarismo de V com o penúltimo algarismo de M.Para isso, será preciso somar um múltiplo de p que termine em 30 (pois não é permitido alterar os algarismos que já coincidem), e esse número certamente é um múltiplo de p que termina em 3, multiplicado por 10.

$$7 \times 9 = 63$$
$$\Downarrow$$
$$63 \times 10 = 630$$

Dessa forma,

$$V_1 = 28 + 630 = 658$$

O próximo algarismo de M é 2, logo será necessário somar um múltiplo de p que termine em 600, e novamente, esse número é o múltiplo que termina em 6 multiplicado por 100. Segue que

$$7 \times 8 = 56$$
$$\Downarrow$$
$$56 \times 100 = 5600$$
$$\Downarrow$$
$$V_2 = 28 + 630 + 5600 = 6258$$

Perceba que a cada passo, o novo múltiplo a ser somado é multiplicado por uma potência de 10 que aumenta seu expoente em uma unidade a cada passo. Nesse sentido, o próximo múltiplo a ser somado deve terminar com 5000

$$7 \times 5 = 35$$
$$\Downarrow$$
$$35 \times 10^3 = 35000$$
$$\Downarrow$$
$$V_3 = 28 + 630 + 5600 + 35000 = 41258$$

O múltiplo seguinte deverá terminar em 40000, ou seja,

$$7 \times 2 = 14$$
$$\Downarrow$$
$$14 \times 10^4 = 140000$$
$$\Downarrow$$
$$V_4 = 28 + 630 + 5600 + 35000 + 140000 = 181258$$

Por último, o primeiro algarismo de M é 8, nesse caso deve ser somado um múltiplo de p que termine em 700000 já que o primeiro algarismo de V_4 é 1.

$$7 \times 1 = 7$$

$$\Downarrow$$

$$7 \times 10^5 = 700000$$

Portanto

$$V_5 = 28 + 630 + 5600 + 35000 + 140000 + 700000 = 881258$$

Perceba que $V_5 = M$, logo, $7|881258$ e $\frac{881258}{7} = 125894$.

Note que $V_5 = M$, e nesse caso, o processo é encerrado. Caso em um determinado passo V_i, acontecer de $V_i < M$, o processo avança ao próximo passo até que $V_i = M$ ou $V_i > M$. Caso $V_i > M$, o processo é encerrado e se conclui que $p \nmid M$.

Em resumo,

$$V_i = M \Longrightarrow p|M, nesse\ caso\ o\ processo\ \text{é}\ encerrado$$

$$V_i < M, nesse\ caso\ o\ processo\ continua$$

$$V_i > M \Longrightarrow p \nmid M, nesse\ caso\ o\ processo\ \text{é}\ encerrado$$