UNIVERSIDADE FEDERAL DO PARÁ
PRÓ-REITORIA DE PESQUISA E PÓS-GRADUAÇÃO
MESTRADO PROFISSIONAL EM MATEMÁTICA
PROFMAT

MANOEL MESSIAS DE SOUSA JUNIOR

UM TESTE DE PRIMALIDADE: UMA ABORDAGEM ERATOSTÉLICA E EUCLIDIANA, APLICAÇÃO PARA O ENSINO BÁSICO E SUPERIOR.

ABAETETUBA

2024

MANOEL MESSIAS DE SOUSA JUNIOR

UM TESTE DE PRIMALIDADE: UMA ABORDAGEM ERATOSTÉLICA E EUCLIDIANA, APLICAÇÃO PARA O ENSINO BÁSICO E SUPERIOR.

Dissertação apresentada ao Curso de Mestrado Profissional em Matemática - PROFMAT do Programa de Pós-Graduação em Matemática do Centro de Ciências da Universidade Federal de Abaetetuba-PA, como requisito parcial à obtenção do título de mestre em Matemática. Área de Concentração: Matemática

Orientador: Prof. Dr. José Francisco da Silva costa

ABAETETUBA

2024

FICHA CATALOGRÁFICA

Dados Internacionais de Catalogação na Publicação (CIP) de acordo com ISBD
Sistema de Bibliotecas da Universidade Federal do Pará
Gerada automaticamente pelo módulo Ficat, mediante os dados fornecidos pelo(a) autor(a)

S725t Sousa Junior, Manoel Messias de.
Um teste de primalidade: uma abordagem eratostélica e euclidiana, aplicação para o ensino básico e superior. / Manoel Messias de Sousa Junior. — 2024.
83 f. : il.

Orientador(a): Prof. Dr. José Francisco da Silva Costa
Dissertação (Mestrado) - Universidade Federal do Pará, Campus Universitário de Abaetetuba, Programa de Pós-Graduação em Matemática em Rede Nacional, Abaetetuba, 2024.

1. Números primos. 2. Teste . 3. Ensino básico . 4. Aplicações. . I. Título.

CDD 510

MANOEL MESSIAS DE SOUSA JUNIOR

UM TESTE DE PRIMALIDADE: UMA ABORDAGEM ERATOSTÉLICA E EUCLIDIANA, APLICAÇÃO PARA O ENSINO BÁSICO E SUPERIOR.

Dissertação apresentada ao Curso de Mestrado Profissional em Matemática - PROFMAT do Programa de Pós-Graduação em Matemática do Centro de Ciências da Universidade Federal de Abaetetuba-PA, como requisito parcial à obtenção do título de mestre em Matemática. Área de Concentração: Matemática.

Orientador: Prof. Dr. José Francisco da Silva Costa

Aprovada:

BANCA EXAMINADORA

_____

Prof. Dr. José Francisco da Silva Costa (Orientador)
Universidade Federal de Abaetetuba-PA (UFPA)

_____

Prof. Dr. Júlio Roberto Soares da Silva.
Membro externo-PROFMAT

_____

Prof. Dr. Antonio Maia de Jesus Chaves Neto
Membro externo-ICEN-UFPA

_____

Prof. Dr. Wilson Rodrigues Oliveira
Membro externo-FACET

_____

Prof. Dr. Sebastião Martins Siqueira Cordeiro
Membro interno-PROFMAT

A Deus, por guiar os meus caminhos, minhas decisões, minhas viagens de ida e vinda, por iluminar meus estudos e provas. Aos meus pais Manoel e Fátima, a minha esposa Rosana, meus filhos Nícolas e Miguel, a minha irmã Nárgila e seu esposo Renato, a meus sogros Nely e Raimundo, a minha irmã Áila e minhas cunhadas Regiane e Rayssa, enfim, a toda minha família pelo apoio.

AGRADECIMENTOS

A Deus, que nas horas mais difíceis concedeu forças que permitiram a conclusão deste trabalho.

Aos meus pais Manoel e Fátima pelo apoio, incentivo e dedicação que contribuíram para que eu pudesse buscar os caminhos da realização e felicidade.

À minha esposa Rosana pelo apoio, acordando todas as sextas-feiras, de madrugada, sem medir esforços, cuidando de nossos filhos Nícolas e Miguel enquanto eu estudava, e pelas orações.

A minha irmã Nárgila e seu esposo Renato pelo apoio em sua residência, na dormida, na alimentação, que Deus abençoe grandemente suas vidas.

Aos meus sogros Nely e seu Raimundo pelo apoio em sua residência e pelas orações.

As minhas cunhadas Regiane e Rayssa por ajudarem sua irmã Rosana (minha esposa) enquanto eu estava estudando.

A todos os meus familiares que me incentivaram e apoiaram.

A todos os professores por proporcionarem o meu aperfeiçoamento para a minha formação profissional que é a matemática e através desta formação fazer a diferença na vida dos alunos e da sociedade como um todo.

Ao Prof. Dr. Francisco por me orientar neste trabalho, durante a elaboração com esclarecimentos, correções e sugestões, e por demonstrar compreensão e paciência.

Ao Prof. Dr. Manuel por sua coparticipação no trabalho na área da programação e como ex-coordenador do PROFMAT em 2023, pela maneira acolhedora com que sempre tratou os alunos e pela grande ajuda no curso e na minha formação.

Ao Prof. Dr. Sebastião pela sua presente atuação como atual coordenador do programa.

Por fim, todos que, direta ou indiretamente, contribuíram para a realização e conclusão deste sonho o meu muito obrigado.

RESUMO

Esta dissertação visa compreender **a** relevância do teste de primalidade para uma abordagem eratostélica e euclidiana com ênfase em aplicação para o ensino básico e superior**.** O fundamento teórico é desenvolvido a partir de método dedutivo baseado em definição de números primo e composto, a saber os testes de primalidade de Eratóstenes, Wilson e outros como comparativo para a nova abordagem de primalidade, além das propriedades existentes que facilita o processo algébrico. Enfatizam-se com a temática a criação dos números naturais, sua lei de formação e sua correlação com o mundo real e a tecnológico. Baseando-se neste aspecto, verificam-se algumas aplicações de primalidade conforme as habilidades e competências da BNCC, buscando ampliar o conhecimento do pressuposto teórico à luz de um processo de ensino compreensível a partir de uma metodologia que não distancie o aluno da real aplicabilidade de primalidade. O resultado da pesquisa aponta que a teoria de primalidade tem grande utilidade na área da matemática e da tecnologia no que diz respeito a criptografia através do auxílio computacional o que permite enumerar uma sequência de números primos que obedeça ao teste de primalidade numa abordagem eratostélica e euclidiana além de abrir um leque de aplicações necessárias para um melhor entendimento ao ensino básico. Conclui-se a pesquisa considerando que apesar das abstrações da teoria dos números e do extenso formalismo matemático, com axiomas e teoremas, pode-se direcionar a busca por caminhos que ofereçam aplicabilidade no campo da matemática, tecnologia e de outras ciências para proporcionar ao aluno uma aprendizagem significativa de primalidade e aplicações relacionadas ao seu cotidiano

Palavras-Chave: Números Primos, Teste, ensino básico e aplicações.

ABSTRACT

This dissertation aims to understand the relevance of the primality test for an eratostélica e euclidean approach with emphasis on application for basic and higher education. The theoretical foundation is developed from a deductive method based on the definition of prime and composite numbers, namely the primality tests of Eratosthenes, Wilson and others as a comparative for a new approach to primality, in addition to the existing properties that facilitate the algebrian process. Emphasis is placed on the creation of two natural numbers, their training lei and their correlation with the real and technological world. Based on this aspect, we verify some applications of primality according to the skills and competencies of BNCC, seeking to expand the knowledge of the theoretical presupposition in light of a comprehensive teaching process based on a methodology that does not distance or away from the real applicability of primality. The result of the research suggests that the theory of primality has great utility in the area of mathematics and technology, not that it respects cryptography through computational aid or that it allows enumerating a sequence of prime numbers that obeys the test of primality in an eratostelic and Euclidean approach. In addition to opening a list of necessary applications for a better understanding of the basics. The research is concluded considering that despite the abstractions of the theory of numbers and extensive mathematical formalism, with axioms and theorems, the search can be directed along paths that offer applicability in the field of mathematics, technology and other sciences to provide students with a significant learning of primalities and applications related to your daily life

Keywords: Prime Numbers, Test, basic instructions and applications.

SUMÁRIO

CAPÍTULO 1 CONSIDERAÇÕES PRELIMINARES SOBRE PRIMALIDADE

1.1 INTRODUÇÃO

A História mostra o quanto a humanidade evoluiu através da ciência, pois foi a partir do acervo de conhecimentos que a humanidade passou a mudar a forma de sobrivência ((JAQUES, 1959). Na matemática a partir do surgimento dos números naturais positivos (DEWEY, 1980), e inteiros negativos (PORTOLAN, 2017) à contagem de animais, a comercialização de mercadorias, a demarcação de áreas, a contagem do tempo e outros[1]

Além destes números citados surgiram outros como os racionais (BOYER, 1974), os irracionais (BOYER, 1974; CAJORI ,2007), os reais (BONGIOVANNI, 2005) e os complexos (ROSA, 1998, p. 41), para solucionar problemas que não seriam ´possíveis com os naturais e inteiros negativos. Apesar do surgimento dos números reais e complexos, considera-se como destaque neste texto dissertativo, os números naturais primos que foram estudados na Escola Pitagórica, por volta de 530 a.C. e referendado por Euclides em seu livro "Os Elementos" em 300 a.C., por volta de 500d.C., foram estudados em outras partes do mundo (ALEX, 2022).

Atualmente, os números primos pode ser aplicado em recursos tecnológicos e computacionais que é a criptografia na confiabilidade das informações e do armazenamento de dados[2]. A descobertas de números primos se tornou algo valioso e importante à criptografia e com o avanço da tecnologia na sua capacidade lógica de processamento de dados, com as técnicas de programação e os testes de primalidade onde esses números passaram a serem encontrados com maior facilidade (CAMARGO RIZEL, 2014).

Tratando-se da teoria dos números primos tendo em vista o contexto da sua relevância e aplicabilidade, este trabalho apresenta o seguinte objetivo geral citado a subseção a seguir.

1.2 OBJETIVO GERAL

Mostrar um teste de primalidade a partir de uma abordagem Eratostélica e Euclidiana com aplicação para o ensino básico e superior**.**

Neste caso o interesse é compreender a técnica matemática do teste para o caso da raiz quadrada usando o fatorial e o MDC do número dado e o fatorial. Neste primeiro teste, será possível identificar a existência de um numero primo. A segunda técnica matemática consiste

[1] (https://www.todamateria.com.br/historia-dos-numeros-origem-e-evolucao-dos-numeros/).
[2] (Aritmética, Coleção PROFMAT, SBM, ano 2012, unidade 23, pag. 2) .

em usar a expressão do arranjo $A_{2k,k}$ ∀ k inteiro positivo. E dessa maneira, será possível mostrar, novamente a existência do surgimento de uma sequência de números primos num intervalo dado por [$(2k-1)^2$, $(2k+1)^2$ -1]) onde k possui a seguinte restrição $k \geq 1$.

É importante salientar que as duas técnicas a serem desenvolvidas neste trabalho se constituem em teorias inovadoras não encontrados na literatura. No entanto, para verificar a potencialidade da obtenção de números primos pelas duas técnicas supracitadas, desenvolvem-se alguns outros testes conhecidos na literatura, a saber, Wilson (HEFEZ, 2016) , Fermat (COUTINHO, 2015), Lucas-Lehmer (BRUCE, 1993), AKS correspondente ao pequeno teorema de Fermat (COUTINHO,2015; AGAWAL, KAYAL, SAXENA, 2006; BRUNO, 2002), Divisões Sucessivas ou Teorema de Eratóstenes (HEFEZ, 2012.), Solovay-Strassen (Solovay; Strassen, 1978) e Miller-Rabin (RIBENBOIM, 2014). Portanto, para verificar a veracidade dos testes de primalidade inovadores, procura-se fazer uma comparação entre as duas técnicas e os testes encontrados na literatura.

Outra questão de interesse consiste em aplicar os testes primalidades com ênfases nas aplicações voltadas para o ensino básico, pois de nada vale uma teoria sem a sua relevância em problemas que elucidam fenômenos ou soluções de problemas que podem contribuir nos avanços tecnológicos e computacionais. Assim sendo, temas como métodos de contagem, raiz quadrada, multiplicidade de números e MDC são temas inerentes a esse grau de estudo. Assim sendo, é possível aplicar essas técnicas para que o aluno do ensino básico conheça como obter números primos abrangendo os conhecimentos teóricos e práticos de primalidade.

Para melhor alcançar o objetivo geral, entrelaçam-se os seguintes objetivos específicos,

1.2.1 Objetivo específicos

- Compreender a História dos números e dos números primos, as biografias de Eratóstenes X Euclides
- Mostrar os números naturais e suas operações, inteiros, primos, compostos e divibilidade
- Verificar o crivo de Erastóstenes , equações diofantinas lineares e os testes de primalidades

Para melhor desenvolver este trabalho, resolve-se seguir o seguinte roteiro de apresentação.

No capítulo 2 traz como tema central a Histórias dos Números e dos Números Primos, As Biografias de Erastótenes X Euclides, abrangendo como subtópicos, Histórias dos Números nas civilizações antigas; o desenvolvimento matemático pelos filósofos enfatizando os filósofos Tales, Pitágoras e Platão; história do número primo; Eratóstenes e Euclides, fazendo uma abordagem dos filósofos Eratóstenes, Euclides e o problema das fórmulas geradoras de números primos.

No **capítulo 3,** aborda-se como tema o estudo dos números primos segundo a BNCC e as habilidades e competência para o ensino básico, trazendo como base de subtópicos, habilidade e competências para o ensino básico; estudo dos números primos e o Crivo de Eratóstenes segunndo a BNCC e aplicações de números primos no ensino básico segundo A BNCC

No **Capítulo 4,** aborda como temática central os números naturais e suas operações, inteiros, primos, compostos e divibilidade e trazendo como subtópicos, números naturais e operações com ênfases em operações definidas no conjunto dos naturais, operação de Adição de e Multiplicação; a ordenação nos números naturais; números primos e números compostos; divisibilidade e suas proposições; Máximo Divisor Comum.

No **Capítulo 5,** procura-se abordar o Crivo de Eratóstenes, equações diofantinas lineares e os testes de primalidades; trazendo como subtópico, o crivo de Eratóstenes; equações diofantinas lineares; congruência; decomposição de um número fatorial em potência de números primos; Análise Combinatória; testes de primalidades com ênfases nos de Wilson, de Fermat, de Lucas-Lehmer, AKS; Divisões Sucessivas (Teorema de Eratóstenes); Solovay-Strassen e Miller-Rabin

No **Capítulo 6** tem como temática central, Contribuição Referente Aos Números Primos com os subtópicos, Sequências numéricas e funções; Subsequências, a somação e funções geradoras de primos; teste de primalidade; equações diofantinas; congruência; sequência importante e relação importante, Conclusão e Referências

CAPITULO 2

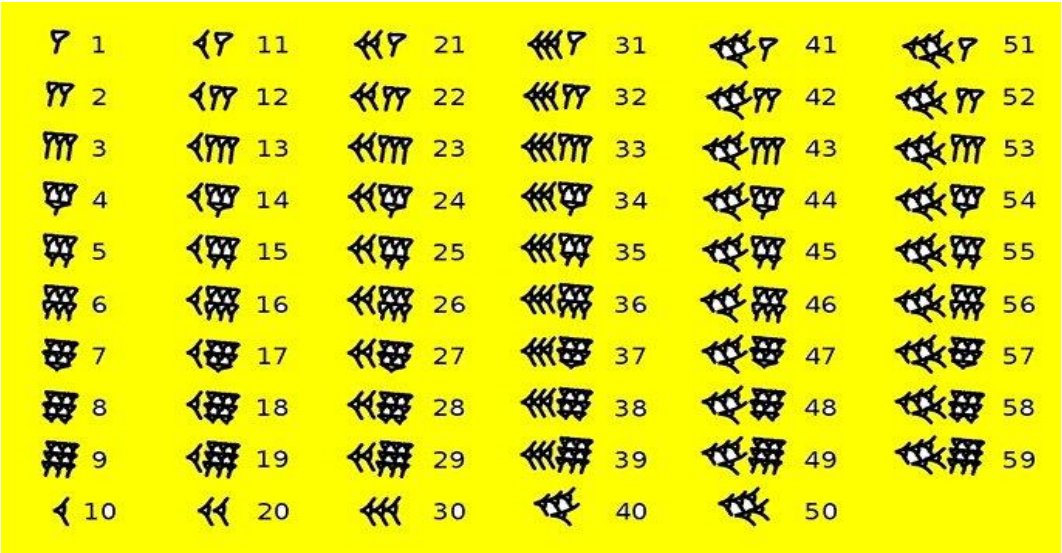
HISTÓRIAS DOS NÚMEROS E DOS NÚMEROS PRIMOS, AS BIOGRAFIAS DE ERASTÓTENES X EUCLIDES

2.1 HISTÓRIAS DOS NÚMEROS NAS CIVILIZAÇÕES ANTIGAS

Há mais de 30 mil anos o homem precisou se organizar para sobreviver, surgindo a necessidade de contar objetos e animais e com o passar do tempo, as pessoas foram vivendo em grupos maiores, as tribos, e cada uma delas desenvolveu um modo de contar. À medida que as aldeias se transformaram em cidades e essas em Impérios, o comércio entre os povos cresceu e houve necessidade de criar registros mais precisos. Um exemplo disso foi a civilização da Babilônia, que construíram um império de 1792 a. C.- 539 a. C., no território que corresponde aproximadamente ao Irã e ao Iraque atuais. (Darela, Coan Cardoso, Camilo da Rosa, 2011)

Os números babilônicos eram escritos de maneira cuneiforme (o símbolo" a cunha" era um instrumento pontiagudo) (figura 1)

Figura 1: Números babilônicos e sua correspondência com os algarismos indo-arábicos



Fonte: (https://www.todamateria.com.br/historia-dos-numeros-origem-e-evolucao-dos-numeros/

Enquanto os Babilônios usavam símbolos para suas representações numéricas, os Romanos por sua vez, recorreram às letras para representar os números como segue: I -1, IV-4, V-5, X-10, L-50, C-100, M-1000,....

Enfim, a simbologia hoje predominante são os algarismos indo-arábicos que foram criados pelos Hindus e divulgados pelo mundo pelos árabes (Darela, Coan Cardoso, Camilo da Rosa, 2011, p. 58-69). Não esquecendo dos algarismos romanos que ainda são usados para capítulos de livros e para datas (anos) em séculos. O zero foi um dos últimos algarismos a ser criado e isto ocorreu porque ele não representava uma quantidade de alguma coisa e sim a ausência de valor (Darela, Coan Cardoso, Camilo da Rosa, 2011, p. 55-58).

Por exemplo, os romanos, deixavam em aberto; os babilônicos, deixando as colunas de cálculo em branco. Foram os hindus, no século VII, influenciados pelo sistema de numeração babilônico, que deram um nome para o espaço em branco deixado na coluna de cálculos: "sunya", que significa "vazio" ou "lacuna". A palavra foi traduzida ao árabe como "siphr" e passou para o latim como "zephirum", dando origem ao vocábulo zero, em português[3].

2.2. O DESENVOLVIMENTO MATEMÁTICO PELOS FILÓSOFOS

2.2.1 Tales, Pitágoras e Platão.

Com todo conhecimento deixado pelos antigos povos obtido através da história, Tales de Mileto (640-546 A.C.) ao retornar do Egito de seus estudos e pesquisas, agregada ao conhecimento grego da época, a matemática começou a tomar novos rumos. Em seguida, foram Pitágoras de Samos (580-500 A.C.) e sua escola (que durou vários séculos) que se incumbiram de desenvolver e difundir o conhecimento matemático pela Grécia e seus domínios.

Um outro grande filósofo que influenciou na matemática da sua época foi Platão (429-348 A.C.), apesar de não ser matemático, nela via um imprescindível treinamento para o filósofo, destacando a metodologia axiomático-dedutiva a ser adotada em todos os campos da ciência. Assim, por volta de 300 A.C., nasce um tratado que se tornaria um dos marcos mais importantes da matemática, Os Elementos de Euclides. Este acordo composto por treze livros, abrange de forma organizada a maior parte do conhecimento matemático da época.

[3] https://www.todamateria.com.br/historia-dos-numeros-origem-e-evolucao-dos-numeros/

2.2.2 Euclides, Diofanto de Alexandria e Pierre de Fermat

Euclides não desenvolveu muito conhecimento, mas constituiu um padrão de organização e de rigidez na Matemática nunca antes alcançado, sendo um exemplo a ser seguido nos séculos que se sucederam. Dos 13(treze) livros de Os Elementos, 10(dez) falam sobre geometria e 3(três) sobre aritmética. Nos livros VII, VIII e IX de aritmética, Euclides cria a teoria dos números naturais, sempre com um olhar geométrico, como por exemplo: um número elevado a primeira potência representa segmento e um número elevado ao quadrado indica área. No Livro VII são definidos os conceitos de Máximo Divisor Comum (MDC), de Divisibilidade, de Mínimo Múltiplo Comum (MMC), de Número Primo, de Número Perfeito e outros.

No mesmo exemplar é apresentado, também, a divisão de um número natural por outro com a definição do resto da operação, chamada divisão euclidiana. Euclides estabelece o algoritmo mais hábil, que ainda hoje é usado, para o cálculo do Máximo Divisor Comum (MDC) de dois números inteiros, chamado de Algoritmo de Euclides. Nos acervos VIII e IX, respectivamente, são estudadas propriedades de sequências de números em progressão geométrica e a quantidade de números primos que supera qualquer número dado, ou seja, existem infinitos números primos. Euclides também prova que todo número natural se escreve de forma única como produto de números primos, resultado hoje chamado de Teorema Fundamental da Aritmética. Também, foi provado o resultado que dá uma condição necessária para que um número natural seja perfeito.

Depois de Euclides, no decorrer da história, a aritmética parou por cerca de 500 anos, mas retornou com os trabalhos de Diofanto de Alexandria, que viveu por volta de 250 D.C.. A obra dele foi chamada de Aritmética e escrita em 13(treze) volumes, infelizmente apenas 7(sete) volumes chegaram até nós. Este foi o primeiro tratado de álgebra até hoje conhecido e diferente de outras abordagens de cunho mais geométrico como os livros os elementos. Diofanto foi além, era totalmente algébrico, sua literatura era diferente da linguagem ou interpretação geométrica de todos os seus predecessores. A maioria dos problemas estudados por Diofanto em Aritmética visava encontrar soluções em números racionais, muitas das vezes contentando-se em descobrir apenas uma solução, de equações algébricas com uma ou várias variáveis[4].

Regiomanto traduziu para o latim, no ano de 1575, o tratado Aritmética de Diofanto e em 1621, Bachet de Méziriac, publicou numa edição francesa que se tornaria protagonista de

[4] Aritmética, Coleção PROFMAT, SBM, ano 2012, unidade 2, pag. 10, 11, 12.

uma das mais ricas histórias de toda a Matemática. Neste período, entre os séculos XIII e XV, ocorre o renascimento da aritmética com a obra do jurista francês Pierre de Fermat (1601-1665).

Na época, era comum os matemáticos não divulgarem as demonstrações das respostas que encontravam, lançando estas como desafio para outros. Os resultados de Fermat foram divulgados por meio de sua carta, principalmente com o padre Marin Mersenne, que desempenhava o papel de divulgador da Matemática. Numa de suas cartas de 1640, Fermat enunciou o seu Pequeno Teorema, falando que não escreveria a demonstração por ser longa demais.

2.3 HISTÓRIA DO NÚMERO PRIMO

Os números primos são analisados desde o período de antigos matemáticos, na Grécia, até os dias atuais pelos filósofos Euclides, Eratóstenes, Fermat, Euler, Wilson, Gauss e outros. Suas propriedades e aplicações encantam muitos estudiosos e esses números receberam esse nome devido aos gregos, que dividiam os números em primários e secundários e os romanos traduziram a palavra grega para primeiro, que em latim é primus.

Com isso os pitagóricos começaram a observar que existiam dois tipos de números, os números primos e os números compostos. Os números primos são números que não podem ser gerados pela multiplicação de dois ou mais números, por exemplo, 2, 3, 5, 7, 11, 13, 17, 19 e outros. Já os números compostos ou secundários são números que podem ser gerados a partir de outros números, ou seja, os números primos.

> Os números primos são a matéria prima na formação de todos os demais números. Sendo assim, são eles objetos de estudos ininterruptos desde os primórdios. Entretanto, os números primos guardam segredos que por vezes nos parecem intransponíveis, sendo considerados por alguns como o assunto mais misterioso já estudado pelos matemáticos. No início do Século XX, David Hilbert, professor da Universidade de Göttingen e um dos maiores matemáticos da época, proferiu uma palestra no Congresso Internacional de Matemáticos, realizado em agosto de 1900, na Sorbone. Em sua palestra, Hilbert falou sobre o desconhecido, sobre os desafios da matemática no século que se iniciava. Ele desafiou a plateia de ilustres matemáticos com uma lista de 23 problemas, que segundo ele, ditariam o futuro das pesquisas matemáticas. Muitos desses problemas encontraram resposta ao longo das décadas seguintes, porém, o oitavo problema, até hoje não foi solucionado. Trata-se de provar a Hipótese de Riemann,.(ARY CAMARGO RIZEL,2014,pág.6)

De acordo com, Ary Camargo Rizel, em sua dissertação NÚMEROS PRIMOS, na pagina 6 no ano de 2014, mostrou os desafios deixados por grandes pensadores para a nossa geração, conjecturas essas que se resolvidas irão impulsionar a humanidade a uma nova era de avanços na área da teoria dos números, na área tecnológica da cripitografia, na engenharia, etc.

> Notícias sobre a última descoberta do maior número primo conhecido são recorrentes. Marcus du SAUTOY, em A Música dos Números Primos – A História de Um Problema não Resolvido na Matemática **(**DU SAUTOY, 2007), se refere a um recorte de jornal guardado com muito cuidado pela matemática Julia Robinson e intitulado ENCONTRADO O MAIOR NÚMERO, que nos mostra que, "mesmo na década de 1930, até as descobertas incorretas chegavam às notícias". Entretanto, diversas provas de que existe uma infinidade de números primos já foram formuladas. A mais ilustre é a demonstração de Euclides, que a mais de 2.300 anos demonstrou que os números primos são infinitos, em uma demonstração considerada uma das mais belas e elegantes em toda a matemática. Esta demonstração consta dos Elementos de Euclides que foram escritos por volta de 300 a.C (ARY CAMARGO RIZEL,2014, pág.11)

De acordo com, Ary Camargo Rizel, em sua dissertação NÚMEROS PRIMOS, na página 11 no ano de 2014, descobertas de números primos se tornou algo valioso e importante para a criptografia e com o avanço da tecnologia na sua capacidade lógica de processamento de dados e com as técnicas de programação e os testes de primalidade, esses números passaram a serem encontrados com maior facilidade. Mas ainda se tem necessidade de uma função que os defina na sua infinitude.

Existem muitos teoremas que são utilizados até hoje como base para muitos resultados em Teoria dos Números e de métodos para testes de primalidade. Será feita uma breve introdução sobre os números naturais, os números inteiros, os números compostos, os números primos, divisibilidade e outros, temas fundamentais para o estudo da primalidade.

2. 4 ERATÓSTENES E EUCLIDES

2.4.1 Eratóstenes

Nasceu na cidade de Cirene, antiga colônia grega na atual Líbia, em 276 a.C.; morreu aos 82 anos na cidade de Alexandria (Egito) em 194 a.C[5] (Apêndice 1) ; foi um importante geógrafo, matemático, astrônomo e filósofo pré-socrático. É considerado o pai da Geografia na Antiguidade, em função dos importantes estudos sobre as medições da Terra que realizou. Foi um dos principais cientistas e pensadores da Grécia Antiga.

[5] (https://www.suapesquisa.com/quemfoi/eratostenes.htm)

Quadro 1: Datas importantes de contribuições de Erastóstenes

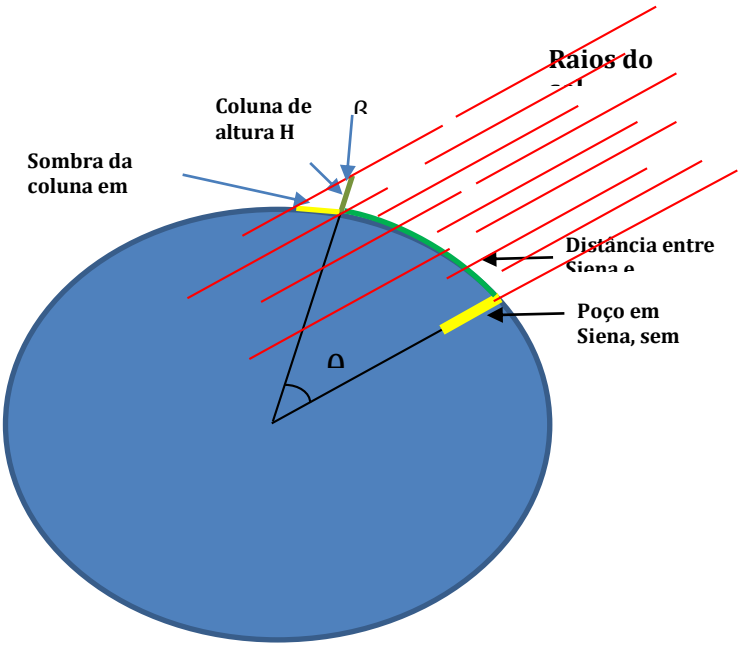
Data	Fatos e contribuições
276 a.C. até sua morte	Viveu e estudou durante sua juventude na cidade de Atenas (Grécia) e a convite do faraó Ptolomeu III do Egito foi o bibliotecário-chefe de Alexandria, a mais importante da Antiguidade e Exerceu este cargo e nesse período foi professor do filho do faraó Ptolomeu III.(BOYER, 1974)
Por volta de 240 a.C	O desenvolvimento de um método matemático para medir as dimensões da Terra (American Physical Society, 2006).
Criada em 255 a.C	É considerado o inventor da Esfera Armilar (astrolábio esférico), que é uma espécie de esfera celeste que serve para mostrar o movimento das estrelas ao redor do Sol e do planeta Terra.
De 275 a 194 a.C	Criador do Crivo de Eratóstenes, método (algoritmo) prático para encontrar números primos dentre os naturais. (BOYER, 1974, p. 117)
Variando entre 246 a 206 a.C	Elaborou um mapa de todas as terras emersas dentro de um quadriculado geográfico.(ROLLER ,2010)

Fonte: Da própria autoria

Erastóstenes deixou várias contribuições durante sua vida que podem ser verificadas no quadro 1 e uma delas foi O desenvolvimento de um método matemático para medir as dimensões da terra datado por volta de 240 a. C. Este fato foi observado através das sombras projetadas por pedestais verticais localizadas nas cidades de Siena e Alexandria.

Ao verificar documentos na biblioteca de Alexandria, Eratóstenes observou que, no solstício de verão, as paredes dos poços localizados na cidade de Siena não projetavam sombra no fundo dos poços, ou seja, os feixes de luz passavam paralelo as paredes. Porém, na mesma data e horário, esse fenômeno não acontecia em Alexandria. Admitindo que os raios solares incidiam paralelamente na Terra, levantou-se a hipótese de que a superfície da Terra deveria possuir uma curvatura, como mostrado na figura 2.

Figura 2: Ilustração representando as duas cidades citadas no texto, Siena e Alexandria, distantes entre si de 5000 estádios.



Fonte: Da própria autoria

Motivado pelas ideias de formas perfeitas e simétricas, elementos comuns nos estudos científicos na Grécia antiga (TB DE OLIVEIRA, 2016). Eratóstenes propôs que o planeta teria uma forma esférica, e então elaborou um experimento para medir o seu diâmetro e consequentemente seu raio.

O trabalho de Eratóstenes consistia em obter uma relação de proporção entre a circunferência da Terra e a distância entre as duas cidades. Para resolver este problema, fez-se necessário medir a distância entre Siena e Alexandria, que deu um valor de cerca de 5.000 estádios (ROBERT, 1980). No decorrer da análise matemática, ele mediu a sombra das colunas ou hastes verticais ao meio-dia, em cada cidade, e verificou através das relações existentes da época que o ângulo α (alfa) mediria, aproximadamente, 7,2 graus. Estas relações são: os feixes de retas paralelas com uma reta transversal (I) e o triângulo retângulo pelas razões trigonométricas em específico a tangente (II).

Assim, pela figura 1, tem-se, pela relação (I), que:

$$\alpha = \beta, \tag{1}$$

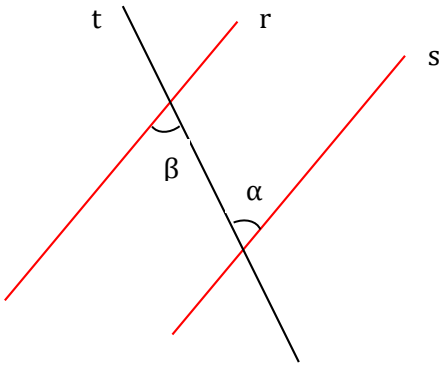
E, pela relação (II), fica:

$$\alpha = arctg\left(\frac{S}{H}\right), \tag{2}$$

Relação I

Duas retas paralelas que são os raios solares (r) e a coluna que está na cidade de Siena (s), a transversal que é a haste que fica na cidade de Alexandria (t) como mostra a figura (figura 3)

Figura 3: Representação gráfica entre um feixe de retas concorrentes em dois pontos



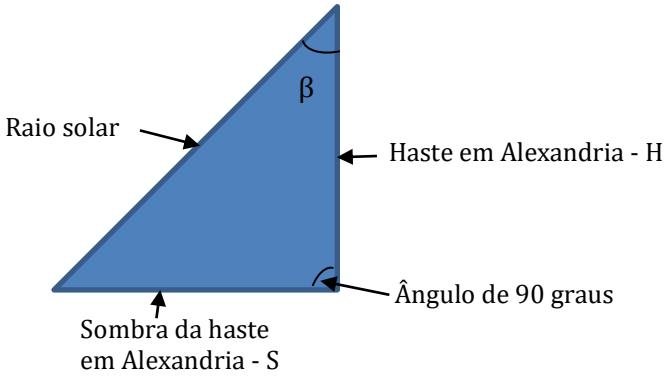
Fonte: Da própria autoria

Pela regra dos ângulos alternos internos $\beta = \alpha$

Relação II

Pelo triangulo retângulo definido pela haste e sua sombra, na cidade de Alexandria, com os raios solares (figura 4)

Figura 4: Representação gráfica de um triângulo retângulo mostrando as denominações da hipotenusa do raio solar.



Fonte: Da própria autoria

Pela definição de razão trigonométrica no triângulo retângulo relacionado a divisão de dois catetos tem-se uma constante chamada tangente referente ao ângulo proposto. Assim, tangente de β será igual a "sombra da haste em Alexandria - S" pela "haste em Alexandria - H".

$$Tg\ \beta\ =\ \frac{S}{H}$$

$$B\ =\ arctg\ (\frac{S}{H})$$

Como definido na relação I,

$$\alpha\ =\ arctg\ (\frac{S}{H})$$

Portanto, o comprimento do planeta terra será calculado pela relação (3):

$$\frac{\boldsymbol{\alpha}}{360} = \frac{D}{C'}, \tag{3}$$

A variável α (alfa) e β (beta) representado pela relação $\beta\ =\ \alpha\ =\ arctg\ (\frac{S}{H})$, onde S é a sombra da haste e H a altura desta. A sigla D é o valor da distância entre a cidade de Siena e Alexandria em estádios E "C" o comprimento do planeta terra em estádios e depois em quilômetros. Substituindo os valores α = 7,2º e D = 5000 estádios na relação (3), tem-se:

$$\frac{\mathbf{7,2}}{360} = \frac{5000}{C}$$

$$C = \frac{5000x360}{7{,}2}$$

$$C = \frac{1.800.000}{7{,}2}$$

$$C\ =\ 250.000\ estádios$$

Como na época 1km era igual a 6,3 estádios, pela regra de três simples, tem-se a relação;

$$\frac{1km}{x} = \frac{6{,}3\ estádios}{250.000\ estádios}$$

$$x = \frac{250.000x1}{6{,}3}$$

$$x\ =\ 39.682{,}54\ km$$

Desta forma estimou-se o comprimento da circunferência da Terra em 39.682,54 quilômetros (ANTONIOS, 2006).). Assim, percebe-se o quanto a ciência produzida no passado ajudou a humanidade a se aprimorar. Isto é notado pelo simples fato que os valores atuais para o comprimento da terra que é de 40.076 quilômetros de comprimento com relação a do passado definido por Eratóstenes de 39.682,54. (NASA, 2021)).

2.4.2 Euclides

Euclides[6] é chamado o pai da Geometria e matemático de Alexandria, no Egito. Escreveu o livro "Elementos de Euclides" e foi professor de Matemática na Escola Real de Alexandria. Ele teria vivido entre 325 a 265 a.C, em pleno florescimento da cultura helenística, quando Alexandria era o centro do saber da época. Muito antes de Euclides, a geometria já era assunto no Egito e era usada para medir terrenos e projetar pirâmides (Darela, Coan Cardoso, Camilo da Rosa, 2011, p. 123; (EUCLIDES, 2009, p.42). Tão famosa era a geometria egípcia, que matemáticos gregos como Tales de Mileto e Pitágoras, iam ao Egito para ver o que havia de novo em matéria de linhas e ângulos. (EVES ,2004).

Embora sejam poucas as informações sobre a vida de Euclides no quadro 2 será mostrado alguns fatos importantes de sua vida.

Quadro 2 : Datas importantes de contribuições de Euclides

Data	Fatos e contribuições
Por volta de 300 a.C	Fundou a Escola Real de Alexandria, no reinado de Ptolomeu I(De 306-283 a.C), fazendo desta o centro mundial do compasso e do esquadro. (EUCLIDES, 2009, p.43)
Por volta de 300 a.C	**Os Elementos**, com 13 volumes, que constitui um dos mais notáveis compêndios de matemática de todos os tempos e foi adotado como livro básico por gregos e romanos durante toda a Idade Média e até o Renascimento. (DARELA, COAN CARDOSO, CAMILO DA ROSA, 2011, p. 123-127)
Por volta de 300 a.C	Deixou trabalhos extensos sobre óptica, acústica, consonância, o livro das divisões, dissonância e outras. EUCLIDES, 2009, p.45
Por volta de 300 a.C	Dos ensinamentos de Euclides dependiam o estudo da mecânica, do som, da luz, da navegação, da ciência atômica, da Biologia, da medicina, enfim de vários ramos da ciência e da tecnologia (EVES ,2004).

Fonte: Da própria autoria

De acordo com BERTRAND (2019), a obra "Elementos" foi considerada, por excelência, o acervo mais importante para o estudo da geometria. Euclides é com razão chamado "o pai da Geometria". Nos livros, ele reuniu em um sistema coerente e compreensível, tudo o que se sabia sobre matemática em seu tempo, sabendo que já existiam pergaminhos teorizados ou obras feitas por Tales, Pitágoras, Platão e dos gregos e egípcios que o precederam.

[6] (https://www.ebiografia.com/euclides/)

Mas, coube a Euclides o mérito de apresentar uma sistematização dos conhecimentos geométricos dos antigos com grande clareza e o encadeamento lógico dos teoremas.

Todos os fragmentos surgiram da necessidade prática do uso da aritmética, geometria plana, teoria das proporções e geometria sólida. Sua contribuição não consistiu na solução de novos problemas de geometria, mas na ordenação de todos os métodos conhecidos, formando um sistema que permitia combinar todos os fatos desenvolvidos, para descobrir e provar novas ideias (HEATH, 1908).

2.5 O PROBLEMA DAS FÓRMULAS GERADORAS DE NÚMEROS PRIMOS

Um outro problema cuja solução é procurada pelos matemáticos a muito tempo é a determinação de fórmulas geradoras de números primos. Fermat morreu com a convicção de que a expressão

$$N = 2^{2^n} + 1, \tag{1}$$

sempre geraria um número primo, mas admitindo que não tinha condições de prová-la rigorosamente. Esta expressão produz números primos para n = 0; 1; 2; 3 e 4, mas a crença de Fermat revelou-se posteriormente falsa com a apresentação de uma fatoração dada por (1) por Leonhard Euler. Este foi o mais importante matemático do século XVIII e que provou todos os resultados de Fermat, exceto a expressão dada por (2)

$$X^3 + Y^3 = Z^3 \text{ e } X^4 + Y^4 = Z^4 , \tag{2}$$

provado por Fermat[7].

Outro estudioso dos números primos foi Mersenne, assim denominados em homenagem ao padre Marin Mersenne, contemporâneo de Fermat, e que exerceu um papel importante na propagação do conhecimento, principalmente da matemática, de seu tempo, através de sua comunicação e relacionamento com os maiores cientistas da época. A expressão definida por (3),

$$Mp = 2^p - 1, \tag{3}$$

onde p é um número primo. No intervalo $2 \leq p \leq 5000$ os números de Mersenne que são primos ou primos de Mersenne, correspondem aos seguintes valores de p: 2, 3, 5, 7, 13, 19, 31, 61, 89, 107, 127, 521, 607, 1 279, 2 203, 2 281, 3 217, 4 253 e 4 423. Até o atual momento,

[7] Aritmética, Coleção PROFMAT, SBM, ano 2012, unidade 13, pag. 6, 7.

o maior primo de Mersenne conhecido é $M_{43112609}$, descoberto em agosto de 2008 e que possui no sistema decimal 12 978 189 dígitos.

Existe um famoso e profundo teorema sobre números primos em progressões aritméticas, devido ao grande matemático do século XIX, J. P. G. Lejeune Dirichlet., cujo enunciado é:

"Em uma PA de números naturais, com primeiro termo e razão primos entre si, existem infinitos números primos".

Na progressão aritmética

$$(3, 7, 11, 15, ..., 4n + 3) \quad (4)$$

existem infinitos números primos[8]. Leonhard Euler (1707-1783) um gênio na sua época, em 1727, começa a sua carreira profissional, assumindo uma posição como físico na nova Academia de São Petersburgo, na Rússia. Foi nesse período que escreveu sua grande obra em Aritmética. Um de seus primeiros grandes sucessos em matemática foi calcular, em 1735, o valor exato da soma infinita da sequência (5),

$$N = 1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{9} + \frac{1}{16} + \cdots + \frac{1}{n^2} = \frac{\pi^2}{6} \quad (5)$$

Cálculos numéricos indicavam que o valor aproximado desta soma era 8/5, ficando em aberto, por cerca de um século. Euler surpreendeu provando que a soma da série era $\pi^2/6$. Euler produziu muitos resultados matemáticos ao longo de sua vida científica, que só cessou com a sua morte. Ele escreveu sobre os mais variados assuntos, tais como, teoria das funções, cálculo diferencial e integral, números complexos, acústica, música, teoria dos números, teoria das partições e mecânica, entre muitos outros, ocupando, indiscutivelmente, um lugar entre os maiores matemáticos de todos os tempos[9].

Outro matemático chamado Gauss introduziu uma das noções mais fecundas da aritmética, no seu livro Disquisitiones Arithmetica no ano de 1801. Trata-se da realização de uma aritmética com os restos da divisão euclidiana por um número fixado chamada de congruência. Também, Euler e Wilson contribuíram nessa nova abordagem[10]. Enfim, grandes pensadores que deixaram grandes legados para a humanidade como assim definido baixo por Abramo Hefez (ano, pag), no livro Elementos da Aritmética, na página iii,

> A Aritmética, como usualmente é chamada a parte elementar da Teoria dos Números,

[8] Aritmética, Coleção PROFMAT, SBM, ano 2012, unidade 15, pag. 2, 3, 4.

[9] Aritmética, Coleção PROFMAT, SBM, ano 2012, unidade 17, pag. 8, 9.

[10] Aritmética, Coleção PROFMAT, SBM, ano 2012, unidade 18, pag. 2.

> teve como principal marco inicial a obra *Os Elementos*, de Euclides (aprox. 300 AC), encontrando o seu auge nos trabalhos de Pierre de Fermat (1601-1665) e Leonhard Euler (1707-1783), o que a levou a se tornar um dos principais pilares da Matemática. A partir do início do século 19, graças à obra de Cari Friedrich Gauss (1777-1855), a Aritmética transforma-se em Teoria dos Números e começa a ter um desenvolvimento extraordinário. Estes são os quatro principais protagonistas da história. (Nome, ano e pag)

De acordo com, Abramo Hefez, no livro Elementos da Aritmética, na página iii,

> A Gauss deve-se a fecunda ideia, entre muitas outras, de efetuar a fatoração de números naturais em anéis de números algébricos. Esta ideia foi grandemente desenvolvida nos trabalhos de Ernsí Kummer, Richard Dedekind e Leopold ronecker, iniciando o que se chama atualmente a Teoria Algébrica dos Números. Por outro lado, com os trabalhos de Lejeune Dirichlet e Bernhard Riemann, também no século 19, foram utilizadas técnicas de Análise Real e Complexa para se compreender melhor a distribuição dos números primos, iniciando, assim, uma outra maneira de se tratar os problemas da Aritmética, a Teoria Analítica dos números. Hoje, há uma terceira abordagem, a Geometria Aritmética, cujos métodos são tomados da Geometria Algébrica e cujos precursores foram Emil Artin, Helmut Hasse, Louis Joel Mordell e André Weil. Esta última abordagem tem se mostrado extremamente fecunda, permitindo provar profundos teoremas em Teoria dos Números, e culminando com a publicação, em 1995, da demonstração, por Andrew Wiles, do chamado Último Teorema de Fermat.

Novos matemáticos do século XIX aprofundaram o estudo através das técnicas de Análise Real e Complexa para se compreender melhor os números primos. Hoje novas ideias sugiram com Emil Artin, Helmut Hasse, Louis Joel Mordell e André Weil, usando um método da Geometria Algébrica, para o estudo da Geometria Aritmética a qual ajudou na resolução de muitos problemas em Teoria dos Números.

No decorrer da história de todos esses estudiosos da matemática e suas teorias é necessário colocar dois em evidência que são Eratóstenes e Euclides. Eles criaram dois teoremas importantes na teoria dos números. O primeiro definiu um teorema chamado Crivo de Eratóstenes que encontra números primos em meio aos números naturais. O segundo criou o te

CAPÍTULO 3

ESTUDO DOS NÚMEROS PRIMOS SEGUNNDO A BNCC E AS HABILIDADES E COMPETÊNCIA PARA O ENSINO BÁSICO

3.1 HABILIDADE E COMPETÊNCIAS PARA O ENSINO BÁSICO

As 10(dez) Competências Gerais da Base Nacional Comum Curricular acompanham o desenvolvimento dos alunos desde a Educação Infantil até o Ensino Médio, como mostra o quadro 3.

Quadro 3: As competências e habilidade descritivas na promoção por uma educação de qualidade.

As competências	Habilidades e metas
Conhecimento	Valorizar e utilizar os conhecimentos historicamente construídos sobre o mundo físico, social, cultural e digital para entender e explicar a realidade, continuar aprendendo e colaborar para a construção de uma sociedade justa, democrática e inclusiva.
Pensamento científico, crítico e criativo	Exercitar a curiosidade intelectual e recorrer à abordagem própria das ciências, incluindo a investigação, a reflexão, a análise crítica, a imaginação e a criatividade, para investigar causas, elaborar e testar hipóteses, formular e resolver problemas e criar soluções (inclusive tecnológicas) com base nos conhecimentos das diferentes áreas.
Repertório cultural	Valorizar e fruir as diversas manifestações artísticas e culturais, das locais às mundiais, e também participar de práticas diversificadas da produção artístico-cultural.
Comunicação	Utilizar diferentes linguagens – verbal (oral ou visual-motora, como Libras, e escrita), corporal, visual, sonora e digital –, bem como conhecimentos das linguagens artística, matemática e científica, para se expressar e partilhar informações, experiências, ideias e sentimentos em diferentes contextos, além de produzir sentidos que levem ao entendimento mútuo.
Cultura digital	Compreender, utilizar e criar tecnologias digitais de informação e comunicação de forma crítica, significativa, reflexiva e ética nas diversas práticas sociais (incluindo as escolares) para se comunicar, acessar e disseminar informações, produzir conhecimentos, resolver problemas e exercer protagonismo e autoria na vida pessoal e coletiva.
Trabalho e projeto de vida	Valorizar a diversidade de saberes e vivências culturais, apropriar-se de conhecimentos e experiências que lhe possibilitem entender as relações próprias do mundo do trabalho e fazer escolhas alinhadas ao exercício da cidadania e ao seu projeto de vida, com liberdade, autonomia, consciência crítica e responsabilidade.
Argumentação	Argumentar com base em fatos, dados e informações confiáveis, para formular, negociar e defender ideias, pontos de vista e decisões comuns que respeitem e promovam os direitos humanos, a consciência socioambiental e o consumo responsável em âmbito local, regional e global, com posicionamento ético em relação ao cuidado de si mesmo, dos outros e do planeta.
Autoconhecimento e autocuidado	Conhecer-se, apreciar-se e cuidar de sua saúde física e emocional, compreendendo- se na diversidade humana e reconhecendo suas emoções e as dos outros, com autocrítica e capacidade para lidar com elas.
Empatia e cooperação	Exercitar a empatia, o diálogo, a resolução de conflitos e a cooperação, fazendo-se respeitar e promovendo o respeito ao outro e aos direitos humanos, com acolhimento e valorização da

	diversidade de indivíduos e de grupos sociais, seus saberes, suas identidades, suas culturas e suas potencialidades, sem preconceitos de qualquer natureza.
. Responsabilidade e cidadania	Agir pessoal e coletivamente com autonomia, responsabilidade, flexibilidade, resiliência e determinação, tomando decisões com base em princípios éticos, democráticos, inclusivos, sustentáveis e solidários.

Fonte:https://sae.digital/base-nacional-comum-curricular-competencias.

Estas competências e suas habilidades demonstram a importância e compromisso por um ensino que tem como finalidade garantir uma educação de qualidade a partir de um processo de ensino e aprendizagem para formação do discente ao longo da educação Básica. Verifica-se naquela tabela que os pontos fundamentais que a escola deve promover e articular junto os professores as condições necessárias à construção de planejamento que esteja pautado nas habilidades e competências de acordo como descrito na BNCC. Dessa maneira o profissional da educação deve seguir uma construção metodológica que vise o desenvolvimento teórico-prático de conteúdos ao ponto que o discente desenvolva um conhecimento que leve em consideração a sua vivencia. Portanto, partindo dessa descrição, os conhecimentos dos campos de experiência e das áreas específicas devem ser mobilizados para a compreensão e explicação da realidade**.**

Sob esse aspecto, torna-se interessante mostrar o que a BNCC esclarece a respeito de como trabalhar com os temas referentes ao MDC, Clivo de Eratóstenes e métodos euclidianos entre outros para determinar a sequência de números primos e os possíveis caminhos para as aplicações. No subtópico a seguir, mostra-se como a BNCC direciona como aplicar as habilidades e competências relacionados aos estudos supracitados e ao mesmo tempo induzir que o aluno adquire motivação, interesse e curiosidade pela teoria dos números primos, sem no entanto, utilizar o tecnicismo e

3.2 ESTUDO DOS NÚMEROS PRIMOS E O CRIVO DE ARASTÓTENES SEGUNNDO A BNCC

A Lei de Diretrizes e Bases da Educação Nacional (LDB, Lei nº 9.394/1996) tem sua total liberdade de nortear os currículos dos sistemas e redes de ensino das Unidades Federativas, assim como estabelecer propostas pedagógicas de todas as escolas públicas e privadas de Educação Infantil, Ensino Fundamental e Ensino Médio, em todo o Brasil. Sob este aspecto, a LDB estabelece conhecimentos, competências e habilidades e principalmente com caráter motivador, interessante e com curiosidade ao ponto de que o conhecimento repassado tenha sentido e significado, principalmente que esteja contido dentro de um contexto social, econômico, fazendo parte de sua vivência e a escola deve promover esse desenvolvimento ao longo da escolaridade básica.

Assim sendo, torna-se interessante que o discente tenha a orientação pautados pelos princípios éticos e políticos em que sejam traçados pelas Diretrizes Curriculares Nacionais enfatizados pela Educação Básica. Em relação ao processo de desenvolvimento que levou a consolidação da BNCC, pode-se considerar que no dia 6 de abril de 2017, a proposta da BNCC foi entregue pelo Ministério da Educação ao Conselho Nacional de Educação (CNE) e tendo em vista a Lei 9131/95 coube ao CNE, como órgão normativo do sistema nacional de educação, fazer a apreciação da proposta da BNCC para a produção de um parecer e de um projeto de resolução que, ao ser homologado pelo Ministro da Educação, se transformou em norma nacional o que iria trazer um benefício significativo para a educação brasileira.

Para prosseguir com o compromisso de articular o desenvolvimento na garantia por uma educação efetivamente séria e de qualidade, o CNE realizou audiências públicas regionais em Manaus, Recife, Florianópolis, São Paulo e Brasília, com caráter exclusivamente consultivo, destinadas a colher subsídios e contribuições para a elaboração da norma instituidora da Base Nacional Comum Curricular deixando claro parâmetros cruciais contidos em habilidade e competências previstos nos diversos conteúdo do ensino básico e fundamental.

Para verificar o quanto a CNE buscou consolidar a base, pode-se considerar nesse contexto que o destaque nas realizações das audiências, resultou em 235 documentos protocolados com contribuições recebidas no âmbito das audiências públicas, além de 283 manifestações orais. Estas audiências não tiveram caráter deliberativo, mas foram essenciais para que os conselheiros tomassem conhecimento das posições e contribuições advindas de diversas entidades e atores da sociedade civil e, deliberando com todo esse esforço ajustes necessários para adequar a proposta da BNCC e que teve a elaboração pelo MEC, que consideraram as necessidades, interesses e pluralidade da educação brasileira. Com base em toda essa tarefa por intermédio da CNE no dia 22 de dezembro de 2017 foi publicada a Resolução CNE/CP nº 2, que institui e orienta a implantação da BNCC a ser respeitada obrigatoriamente ao longo das etapas e respectivas modalidades no âmbito da Educação Básica.

Com base no contexto apresentado, a BNCC estabelece com base no CNE que em geral, nas turmas de 5° e 6° anos do Ensino Fundamental, acontece o ensino de números primos. Segundo as habilidades e competências, aplicam-se que:

3.3 OBJETOS DE APRENDIZAGEM E CONTEÚDOS PROGRAMÁTICOS-BNCC

Para os temas de primalidade destinado ao 6º ano do ensino fundamental com as habilidades e competências segundo a BNCC. O professor precisa articular uma metodologia capaz de promover uma aprendizagem significativa (AUSUBEL, 1982). para o aluno ao ponto de fazer que conheça e saiba diferenciar os números primos conhecendo a diferença entre um número primo de outros números (quadro 4)

Quadro 4: Conteúdo de Matemática para o 6º ano de acordo com a BNCC.

MATEMÁTICA	6º ANO	CONTEÚDOS
EF06MA01 - Comparar, ordenar, ler e escrever números naturais e números racionais cuja representação decimal é finita, fazendo uso da reta numérica. **EF06MA02 -** Reconhecer o sistema de numeração decimal, como o que prevaleceu no mundo ocidental, e destacar semelhanças e diferenças com outros sistemas, de modo a sistematizar suas principais características (base, valor posicional e função do zero), utilizando, inclusive, a composição e decomposição de números naturais e números racionais em sua representação decimal. **EF06MA03 -** resolver e elaborar problemas que envolvam cálculos (mentais ou escritos, exatos ou aproximados) com números naturais, por meio de estratégias variadas, com compreensão dos processos neles envolvidos com e sem uso de calculadora. **EF06MA04 -** construir algoritmo em linguagem natural e representá-lo por fluxograma que indique a resolução de um problema simples (por exemplo, se um número natural qualquer é par). **EF06MA05 -** Classificar números naturais em primos e compostos, estabelecer relações entre números, expressas pelos termos "é múltiplo de", "é divisor de", "é fator de", e estabelecer, por meio de investigações, critérios de divisibilidade por 2, 3, 4, 5, 6, 8, 9, 10, 100 e 1000. **EF06MA06 -** Resolver e elaborar problemas que envolvam as ideias de múltiplo e de divisor. **EF06MA12** - Fazer estimativas de quantidades e aproximar números para múltiplos da potência de 10 mais próxima.	Sistema de numeração decimal: características, leitura, escrita e comparação de números naturais e de números racionais representados na forma decimal. Operações (adição, subtração, multiplicação, Divisão e potenciação) com números naturais. Divisão euclidiana. Fluxograma para determinar a paridade de um número natural. Múltiplos e divisores de um número natural. Aproximação de números para múltiplos de potências de 10 Números primos e compostos.	**Números Naturais (N)** Sistemas de numeração Estruturação e sequências numéricas Representação geométrica dos números naturais **Operações com Números Naturais (N)** Adição e subtração de números naturais Multiplicação e divisão de números naturais Potência de números naturais Múltiplos e divisores Mínimo múltiplos comuns - MMC Máximo divisor comum - MDC Divisibilidade por 2, 3, 4, 5,6, 7, 8, 9 e 10 **Sequências numéricas** Sequências numéricas Pares e ímpares Números primos e compostos

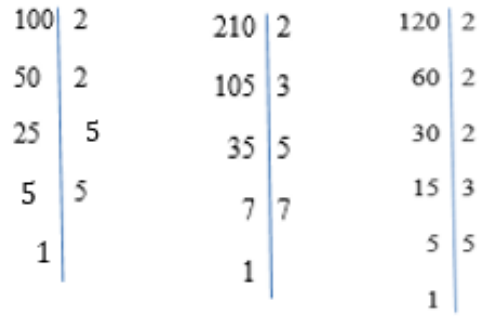
Fonte: Extraído do planejamento da cidade do Rio Grande do Sul.

Exemplo 1

Um estabelecimento de tecidos fabrica retalhos de mesmo comprimento. As três mulheres que executam os cortes necessários, verificaram que três peças restantes tinham as seguintes medidas: 100 cm e 210 cm e 120 cm. Como queriam obter os mesmos comprimentos nos cortes dos tecidos e de maior comprimento possível. Determine a quantidade de cortes e tamanho de cada tecido.

Solução

Deve-se encontrar o MDC entre 100 cm, 210 cm e 120 cm. , esse valor corresponderá à medida do comprimento desejado. Vale ressaltar que o MDC entre os três números deve ser o produto dos números que divide simultaneamente cada tecido. Logo, decompondo os números dados, obtém-se que,



Assim sendo, o MDC (100,120,210) =2. 5=10. Dessa maneira, cada corte terá

$$N_{100} = \frac{100\ cm}{10} = 10\ cm$$

$$N_{120} = \frac{120\ cm}{10} = 12\ cm$$

$$N_{210} = \frac{210\ cm}{10} = 21\ cm$$

E o número total de cortes será 43.

Exemplo 2

Numa escola são escolhidas três salas A, B e C. A sala A possui 30 alunos , sala B 36 e a sala C composta de 24 alunos. Ao final do ano, escola realiza uma integração entre as três salas de aulas, de modo que todas participem ativamente de um grande torneio. As equipes devem conter o mesmo número de alunos com o maior número possível. Determine quantos alunos devem participar de cada equipe e o número possível de equipes.

Solução

O problema consiste em encontrar o MDC entre os números 30, 36 e 24.

18, 30, 24	2
9 ,15, 12	2
9, 15, 6	3
3, 5, 2	2
3, 5 , 1	3
1 , 5, 1	5
1 1 1	

Logo, o MDC (36, 30, 24) =6.

18+30+24=, 72 dividido 6 dar 12. O número de equipes será igual a 12, com 6 participantes cada uma.

Nos dois exemplos dados, verifica-se o quanto o professor pode aplicar os conceitos de MDC de uma maneira contextualizada onde o aluno consegue compreender a importância do conceito a partir de atividades que aguçam e o motiva.

O crivo de Erastóstenes constitui uma sequência de números onde é possível encontrar todos os números primos. No entanto esse conceito de números primos so pode ter um significado para o aluno se houver a contextualização. Nesse caso, antes de aplicar os conceitos de primos, torna-se interessante primeiro compreender o crivo de Erastóstenes ao ponto de saber uma maneira fácil de obter uma quantidade de números primos existentes numa certa sequência de números. Vale salientar, no entanto, que atividade em que o objeto de estudo é o número primo está em consonância com Pensamento científico, crítico e criativo conforme foi visto na tabela (Tabela 1)

2.3 APLICAÇÕES DE NÚMEROS PRIMOS NO ENSINO BÁSICO SEGUNDO A BNCC

Aplicação do novo método em questões problema do dia a dia mostrando como encontrar os números primos com questão contextualizadas.

Exemplo 3: As idades dos alunos

Identificar um número primo requer compreender a definição de sua existência. Esse axioma diz que um número é primo se, somente se, for divisível por 1 e por ele mesmo no livro os elementos. Eratóstenes apresentou um algoritmo que os encontrariam com maior precisão e que foi chamado Crivo de Eratóstenes. Esse método é de simples compreensão e usado no ensino básico, observe no exemplo abaixo seu uso.

O número 41 é primo?

Divida o número 41 por todos os primos abaixo da raíz quadrada de 41. Se não for divisível por nenhum ele será primo. Logo, tem-se: 2, 3 e 5, que não dividem 41 exatamente. Assim 41 é primo.

Usando o método JR, para o mesmo número em análise, tem-se:

mdc([√41]! , 41) = 1 → mdc(6! , 41) = 1 → mdc(720, 41) = 1 → mdc(720-41.17, 41) = 1 → mdc(23, 41) = 1. Como 23 e 41 são primos entre si, logo mdc será 1. Assim, 41 será primo.

Desta forma a tabela abaixo que representa as idades de algumas pessoas, quais dessas idades são números primos, usando o método JR?

Nome	Idade
Nilda	11
Paulo	31
Nargila	51
Aila	43
Nildo	89

Resolução:

Para a idade de:

Nilda: mdc([√11]! , 11) = 1 → mdc(3! , 41) = 1 → mdc(6 , 41) = 1 . Como 6 e 41 são primos entre si, logo 41 é primo.

Paulo: mdc([√31]! , 31) = 1 → mdc(5! , 31) = 1 → mdc(120 , 31) = 1 → mdc(120 – 31.3 , 31) = 1→ mdc(27 , 31) = 1. Como 27 e 31 são primos entre si, logo 31 é primo.

Nargila: mdc([√51]! , 51) = 1 → mdc(7! , 51) = 1 → mdc(5040 , 51) = 1 → mdc(5040 – 51.98 , 51) =

1→ mdc(42 , 51) ≠ 1. Como 42 e 51 não são primos entre si, logo 51 não é primo.

Aila: mdc([√43]! , 43) = 1 → mdc(6! , 43) = 1 → mdc(720 , 43) = 1 → mdc(720 – 43.16 , 43) = 1→ mdc(32 , 43) = 1. Como 32 e 43 são primos entre si, logo 43 é primo.

Nildo: mdc([√89]! , 89) = 1 → mdc(9! , 89) = 1 → mdc(362880 , 89) = 1 → mdc(362880 – 89.4077 , 89) = 1→ mdc(27 , 89) = 1. Como 27 e 89 são primos entre si, logo 89 é primo.

Assim, as idades 11, 31, 43 e 89 são os números primos.

Exemplo 4: A compra de um par de sapatos

A compra de um par de sapatos ou sandália nos dias atuais está definido por uma numeração inteira positiva como por exemplo 10, 12, 13, ..., 26 que são numerações de crianças e 34, 35, 36, 37, 38. 39, 40, ..., 48 são numerações de adultos. Em uma escola de ensino fundamental menor Raimundo fez uma pesquisa e verificou entre as 150 crianças que as numerações encontradas foram 17, 18, 19, 20, 21, 22, 23 e 24. Dentre esses números encontrados quais são os pares de números primos que sua soma dá um número que é quadrado perfeito?

Resolução:

Pelo segundo método JR, tem-se:

$MDC(A'_{\mathbf{2k,k}} ; [(2k-1)^2, (2k+1)^2 -1]) = 1$; para k=2 obtem-se:

$MDC(A'_{\mathbf{4,2}} ; [(2.2-1)^2, (2.2+1)^2 -1]) = 1 \rightarrow MDC(4.3 ; [(3)^2, (5)^2 -1]) = 1 \rightarrow MDC(12 ; [9, 24]) = 1$.

Este método define todos os números primos em um determinado intervalo usando o arranjo e o mdc, logo o MDC(12 ; [9, 24]), encontra 11, 13, 17, 19, 23 como números primos. Desta forma os números primos da sequência de números dados 17, 18, 19, 20, 21, 22, 23 e 24 são 17, 19 e 23. Agora fazendo a soma dos pares, fica:

$$17+19 = 36$$

$$17+23 = 40$$

$$19+23 = 42$$

Assim, o único par que satisfaz a condição dada é (17,19) .

Exemplo 5: Senha bancária

Nos dias atuais se faz necessário a proteção das informações pessoais e financeira, por este motivo a criptografia surge para a proteção dos dados, este método se utiliza de números primos para seus códigos, pois são números difíceis de serem descobertos, ou seja, não podem ser fatorados como os números compostos que podem ser escritos de várias formas. Como por exemplo a senha de uma conta bancária que se escolhe de 6 a 8 números aleatórios para a proteção da conta. Assim uma conta que tem um número de 6 dígitos que é primo está bem melhor protegida contra-ataques virtuais, logo qual seria o menor número primo de 6 algarismos?

Resolução

O menor número de 6 algarismos é 100001 que será verificado se é primo, caso contrário continua-se a verificação com o próximo número ímpar de terminação 1, 3, 7 ou 9 até identifica-lo.

Pelo segundo método, tem-se:

$MDC(A'_{\mathbf{316,158}} ; [(2.158-1)^2, (2.158+1)^2 -1]) = 1 \rightarrow MDC(A'_{\mathbf{316,158}} ; [99225, 100489]) = 1$

MDC(316. 315. 314. 313. 312. 311. 310. 309. 308. 307. 306. 305. 304. 303. 302. 301. 300. 299. 298. 297. 296. 295. 294. 293. 292. 291. 290. 289. 288. 287. 286. 285. 284. 283. 282. 281. 280. 279. 278. 277. 276. 275. 274. 273. 272. 271. 270. 269. 268. 267. 266. 265. 264. 263. 262. 261. 260. 259. 258. 257. 256. 255. 254. 253. 251. 250. 249. 248. 247. 246. 245. 244. 243. 242. 241. 240. 239. 238. 237. 236. 235. 234. 233. 232. 231. 230. 229. 228. 227. 226. 225. 224. 223. 222. 221. 220. 219. 218. 217. 216. 215. 214. 213. 212. 211. 210. 209. 208. 207. 206. 205. 204. 203. 202. 201. 200. 199. 198. 197. 196. 195. 194. 193. 192. 191. 190. 189. 188. 187. 186. 185. 184. 183. 182. 181. 180. 179. 178. 177. 176. 175. 174. 173. 172. 171. 170. 169. 168. 167. 166. 165. 164. 163. 162. 161. 160. 159 ; 100001) = 1;

MDC(55248. 70713. 3025. 52024. 17546. 99431. 97515. 11636. 41634. 87346. 48609. 25262. 17143. 24090. 45941. 82534. 33706. 99297. 79143. 73083. 80955. 2596. 52592. 5733. 72105. 51544. 43889. 48978. 66649. 96740. 39088. 93533. 59911. 38061. 27821. 29029. 41523. 65141. 99721. 45100. 1117. 67611. 44418. 31377. 28326. 35103. 51546. 77493. 12781. 57250. 10736. 19445, 100001) = 1;

MDC(12757. 71027. 98881. 73194. 26999. 48279. 70741. 56578. 71214. 50030. 57079. 6921. 42955. 73947. 59785. 81345. 49769. 7733. 22695. 72127. 20732. 89650. 17635. 14234. 4933. 59433, 100001) = 1;

MDC(36443. 5808. 68321. 24354. 34430. 41338. 34650. 59378. 80058, 100001) = 1;

MDC(47597. 79229. 31592, 100001) = 1 ;

MDC(86878, 100001) ≠ 1;

Assim, 100001 não é primo, pois 11 e divisor comum de 86878 e 100001 ao mesmo tempo.

Fazendo para 100003, tem-se:

MDC(316. 315. 314. 313. 312. 311. 310. 309. 308. 307. 306. 305. 304. 303. 302. 301. 300. 299. 298. 297. 296. 295. 294. 293. 292. 291. 290. 289. 288. 287. 286. 285. 284. 283. 282. 281. 280. 279. 278. 277. 276. 275. 274. 273. 272. 271. 270. 269. 268. 267. 266. 265. 264. 263. 262. 261. 260. 259. 258. 257. 256. 255. 254. 253. 251. 250. 249. 248. 247. 246. 245. 244. 243. 242. 241. 240. 239. 238. 237. 236. 235. 234. 233. 232. 231. 230. 229. 228. 227. 226. 225. 224. 223. 222. 221. 220. 219. 218. 217. 216. 215. 214. 213. 212. 211. 210. 209. 208. 207. 206. 205. 204. 203. 202. 201. 200. 199. 198. 197. 196. 195. 194. 193. 192. 191. 190. 189. 188. 187. 186. 185. 184. 183. 182. 181. 180. 179. 178. 177. 176. 175. 174. 173. 172. 171. 170. 169. 168. 167. 166. 165. 164. 163. 162. 161. 160. 159 ; 100003) = 1;

MDC(106119202399453148044205980769478145959013685001230781989715126317605268897173030317908050372671345646366794943000779602534853423659117646611768 0, 100003) = 1;

MDC(871, 100003) = 1

O menor número primo é 100003, pois 871 e 100003 só tem o número 1 como divisor comum.

CAPÍTULO 4: NÚMEROS NATURAIS E SUAS PERAÇÕES, INTEIROS, PRIMOS, COMPOSTOS E DIVIBILIDADE

4.1 NÚMEROS NATURAIS E OPERAÇÕES

Decorridos muitos milênios, pode-se atualmente, descrever resumida e precisamente o conjunto N dos números naturais, síntese feita pelo matemático italiano Giuseppe Peano no limiar do século XX onde considerou que

$$N = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, ... \}$$

N é um conjunto, cujos elementos são chamados números naturais e ele contém os números pares que representa metade de seus elementos e indicado pelo subconjunto P = {0, 2, 4, 6, 8, 10, 12,....} e pelos números ímpares que representa a outra parte e indicado pelo subconjunto

$$I = \{1, 3, 5, 7, 9, 11, 13, ...\}.$$

Quando N está com o asterisco (*) representa a exclusão do zero (0), logo,

$$N^* = \{1, 2, 3, 4, 5, 6, 7, 8, ...\}.$$

A necessidade de apresentar a existência de N reside na palavra sucessor. Intuitivamente, quando n, n' $\in$ N, dizer que n' é o sucessor de n significa que n' vem logo depois de n, não existindo outros números naturais entre n e n'. O termo primitivo sucessor não é definido explicitamente. Seu uso e suas propriedades são regidos por algumas regras, conhecidas como os axiomas de Peano descritos e enunciados como segue,

a) Todo número natural tem um único sucessor;

b) Números naturais diferentes têm sucessores diferentes;

c) Existe um único número natural, chamado um e representado pelo símbolo 1, que não é sucessor de nenhum outro;

d) Seja X um conjunto de números naturais (isto é, X $\subset$ N). Se 1 $\in$ X e se, além disso, o sucessor de todo elemento de X ainda pertence a X, então X = N.

O último dos axiomas de Peano é conhecido como o axioma da indução. Ele é o alicerce de um eficiente método de demonstração de proposições referentes a números naturais. Isto é,

Seja P(n) uma propriedade relativa ao número natural n. Suponha-se que:

a) P(1) é válida;

b) Para todo n $\in$ N, a validez de P(n) implica a validez de P(n'), onde n'é o sucessor de n. Então P(n) é válida qualquer que seja o número natural n.

Com efeito, chamando-se de X o conjunto dos números naturais n para os quais P(n) é

válida, verifica-se que:

1 ∈ X em virtude de (a); e que n ∈ X ⇒ n' ∈ X em virtude de (b). Logo, pelo axioma da indução, conclui-se que X = N.

4.1.1 Operações definidas no conjunto dos naturais

Entre os números naturais existem duas operações fundamentais: a soma e a multiplicação, sendo n, p ∈ N, acontece a operação soma n + p e a operação multiplicação n.p. A operação adição n + p é o número natural que se obtém a partir de n aplicando-se p vezes seguidas a operação de tomar o sucessor. Em particular, n + 1 é o sucessor de n, n + 2 é o sucessor do sucessor de n, etc. Por exemplo, tem-se 2 + 2 = 4 simplesmente porque 4 é o sucessor do sucessor de 2. De agora em diante, o sucessor do número natural n será designado por n + 1.

Quanto ao produto, põe-se n · 1 = n, por definição e, quando p ≠ 1, n.p é a soma de p parcelas iguais a n. Essas ideias intuitivas serão observadas agora no quadro 5 através das operações e suas demonstrações.

Quadro 5: operações de adição e multiplicação e suas demonstrações.

Adição	Seja $n + 1$ o sucessor de n e $n + (p + 1) = (n + p) + 1$ a igualdade que representa a soma de um número n mais o sucessor de p que equivale, por associativa, o sucessor de $n + p$, ou seja, pelo axioma da indução garante que a soma $n + p$ está definida para quaisquer n, p ∈ N.
Multiplicação	Por indução matemática, se n·1 = n e n.(p+1) = n.p + n. Tem-se que multiplicando um número n por 1 não o altera o seu resultado. Se multiplicar todos os números naturais n por p, sabe-se também multiplicá-los por p+1. Assim, basta tomar n(p+1) = n.p + n que garante a operação para todo n e p natural. Por indução, sabemos multiplicar todo n por qualquer p.

Fonte: Da própria autoria

Estas operações gozam das conhecidas propriedades de associatividade, comutatividade, distributividade, elemento neutro e elemento oposto, definida na quadro 6.

Quadro 6: propriedades da adição e multiplicação para quaisquer a, b e c inteiros

ADIÇÃO	
Comutativa	a + b = b + a
Associativa	(a + b) + c = a + (b + c)
Elemento Neutro	a + 0 = 0 + a = a
Elemento Simétrico	a+(-a) = (-a)+a = 0, (-a) simétrico de a
Multiplicação	
Comutativa	a.b = b. a
Associativa	(a.b). c = a. (b. c)
Elemento Neutro	a.1 = 1. a = a
Distributiva	a.(b + c) = a.b + a. c e (a + b). c = a. c + b.c

Fonte: Da própria autoria

4.2 A ORDENAÇÃO NOS NÚMEROS NATURAIS

A descrição do conjunto N dos números naturais finaliza com a relação de ordem m < n. Dados m; n ϵ N, diz-se que m é menor do que n, e escreve-se m < n, para significar que existe algum p ϵ N tal que n = m + p. A relação m < n tem as seguintes propriedades como mostra a quadro 7

Quadro 7: ordenação e propriedades

Ordenação	**Propriedades**
Transitividade	Se m < n e n < p então m < p.
Tricotomia:	Dados m; n ϵ N, vale uma, e somente uma, das alternativas: m = n, m < n ou n < m.
Monotonicidade:	Se m < n então, para qualquer p ϵ N, tem-se m + p < n + p e m.p < n.p.
Boa-ordenação	Todo subconjunto não-vazio X C N possui um menor elemento. Isto significa que existe um elemento $m_o \epsilon$ X que é menor do que todos os demais elementos de X. A boa-ordenação pode muitas vezes substituir com vantagem a indução como método de prova de resultados referentes a números naturais.

Fonte: Da própria autoria

Para uma melhor compreensão de como utilizar essas propriedades, recorre-se em demonstrar e verificar como aplica-las como mostram os exemplos a seguir.

Exemplo 6

Quer-se provar a validez:

Para todo número natural n, da igualdade

$$P(n): 1 + 3 + 5 + \ldots + (2n - 1) = n^2, \quad (1)$$

Usaremos indução.

Para n = 1, P(1) se resume a afirmar que 1 = 1.

Supondo P(n) verdadeira para um certo valor de n, somamos 2n+1 a ambos os membros da igualdade acima, obtendo:

$$1 + 3 + 5 + \ldots + (2n - 1) + (2n + 1) = n^2 + 2n + 1,$$

ou seja,

$$1 + 3 + 5 + \ldots + [2(n + 1) - 1] = (n + 1)^2. \quad (2)$$

Mas esta última igualdade é P(n+1).

Logo P(n) →P(n+1).

Assim, P(n) vale para todo n ϵ N. Podemos então afirmar que a soma dos n primeiros números ímpares é igual ao quadrado de n.

Exemplo 7

Um número natural p, chama-se primo quando não pode ser expresso como produto p = m.n de dois números naturais, a menos que um deles seja igual a 1 (e o outro igual a p); isto equivale a dizer que os fatores m; n não podem ser ambos menores do que p. Um resultado fundamental em Aritmética diz que todo número natural é primo ou é um produto de fatores primos. Provar-se-á essa veracidade pela boa ordenação.

Usa-se a linguagem de conjuntos. Isto é, Seja X o conjunto dos números naturais que são primos ou produtos de fatores primos. Observa-se que se m e n pertencem a X então o produto m.n pertence a X. Seja Y o complementar de X. Assim, Y é o conjunto dos números naturais que não são primos nem são produtos de fatores primos. Pretende-se provar que Y é vazio. Isto será feito por redução ao absurdo (como sempre se dá nas demonstrações por boa-ordenação). Com efeito, se Y não fosse vazio, haveria um menor elemento a ϵ Y. Então todos os números menores do que a pertenceriam a X. Como a não é primo, ter-se-ia:

a = m.n, com m < a e n < a, logo, m ϵ X e n ϵ X. Sendo assim, m.n ϵ X. Mas m.n = a, o que daria a ϵ X, uma contradição[11].

[11] . (Matemática Discreta, Coleção PROFMAT, SBM, ano 2014, unidade 1 pag.4,5,6)

4.3 NÚMEROS INTEIROS

Como os números naturais mostraram-se insuficientes para resolver os problemas do cotidiano. Nos séculos XV e XVI foi desenvolvida uma linguagem padrão para designar perdas, débitos, prejuízos etc. Isto se deu no início do Renascimento com a expansão comercial, que aumentou a circulação de dinheiro, obrigando os comerciantes a expressarem situações envolvendo lucros e prejuízos. A maneira que eles encontraram de resolver tais situações problemas consistia no uso dos símbolos + e –. Surgia um novo conjunto numérico representado pela letra Z (significa: Zahlen: número em alemão), sendo formado pelos números positivos (Naturais) e seus respectivos opostos, podendo ser escrito da seguinte forma:

$$Z = \{...,–3, –2, –1, 0, 1, 2, 3,...\}.$$

Estes números podem ser representados, também, na reta, possuindo sucessor e antecessor bem definidos. A ideia de que todo número natural possui um oposto ou simétrico**,** que é igual a esse número só que negativo, ou seja, estes números estão a mesma distância do zero na reta numerada. Esta definição representa a operação modular de um número, logo $|x| = \pm x$.

Os Matemáticos da época desenvolveram técnicas operatórias capazes de expressar qualquer situação envolvendo números positivos e negativos.

Considerem as operações abaixo:

Operação Soma: (-2) + (-5) = -7 ; (+6) + (+8) = +14.

É a ideia para representar a soma de dois ou mais números que tem o mesmo sinal.

Operação Subtração: (+25) – (+10) = +15 ; (+20) – (+50) = -30 .

É a ideia para representar a diminuição de dois números que tem sinais opostos.

Operação Multiplicação: (+30).(-20) = - 600 ; (-10).(-15) = +150 ; (+30).(+40) = +120.

É a ideia para representar a soma de várias número iguais, sendo ele só positivo ou só negativo, assim definindo a palavra multiplicação ou produto nesta pespequitiva. No geral, nesta operação é usada a tática do jogo de sinal.

Operação Divisão: (+30)/(-10) = - 3 ; (-225)/(-15) = +15 ; (+80)/(+40) = +20.

É a ideia para representar a divisão de um todo em partes iguais. No geral, nesta operação é usada a tática do jogo de sinal.

O conjunto dos números inteiros possui subconjuntos, como o conjunto dos números naturais,

que está contido nos números inteiros, ou o conjunto dos inteiros positivos.

$Z^* = \{\ldots -4, -3, -2, -1, 1, 2, 3, 4 \ldots\}$ (lê-se: conjunto dos números inteiros não nulos).

$Z_+ = \{ 0, 1, 2, 3, 4, 5 ...\}$ (lê-se: conjunto dos números inteiros não negativos). Note que esse conjunto é o dos números naturais, que também é subconjunto dos inteiros.

$Z_- = \{\ldots -3, -2, -1, 0\}$ (lê-se: conjunto dos números inteiros não positivos).

$Z^*_+ = \{1, 2, 3, 4, 5 ...\}$(lê-se: conjunto dos números inteiros positivos).

$Z^*_- = \{\ldots -3, -2, -1\}$ (lê-se: conjunto dos números inteiros negativos).

Perceba que todos esses conjuntos são subconjuntos de Z, pois todos os elementos estão contidos no conjunto dos números inteiros[12].

4.4 NÚMEROS PRIMOS E NÚMEROS COMPOSTOS

Um número inteiro positivo p chama-se número primo quando os seus únicos divisores são o número 1 e ele mesmo. Os números 2, 3, 5, 7, 11, 13, 17 e 19 são primos, pois os seus únicos divisores são, o número 1 e ele mesmo. O número 2 é o único número primo par. Assim temos: Um número natural maior do que 1 que só possui como divisores positivos 1 e ele próprio é chamado de número primo.

Dados dois números primos "p e q" e um número inteiro "a" qualquer, decorrem da definição acima os seguintes fatos:

I) Se $p|q$, então $p = q$. De fato, como $p|q$ e sendo q primo, temos que $p = 1$ ou $p = q$. Sendo p primo, tem-se que $p > 1$, o que acarreta $p = q$.

II) Se p não divide a, então $(p, a) = 1$. De fato, se $(p, a) = d$, temos que $d|p$ e $d|a$. Portanto, $d = p$ ou $d = 1$. Mas $d \neq p$, pois p não divide a e, consequentemente, $d = 1$.

Um número maior do que 1 e que não é primo será chamado composto. Portanto, se um número inteiro $n > 1$ é composto, existirá um divisor natural n_1 de n tal que $n_1 \neq 1$ e $n_1 \neq n$. Portanto, existirá um número natural n_2 tal que $n = n_1.n_2$; com $1 < n_1 < n$ e; $1 < n_2 < n$. Por exemplo, 2, 3, 5, 7, 11 e 13 são números primos, enquanto que 4, 6, 8, 9, 10 e 12 são compostos.

Por outro lado, o número composto é aquele que tem mais de dois divisores e pode ser fatorado na forma de produto de potências de números primos, ou seja,

[12] (https://mundoeducacao.uol.com.br/matematica/o-surgimento-dos-numeros-inteiros.htm)

$$N = p_1^k . p_2^r \ldots . p_n^t, \quad (1)$$

onde p_1, p_2 , p_3 , ..., p_n são números primos, e k, r,..., t são os expoentes de números naturais, como por exemplo 6 = 2.3; 8 = 2^3 ; 36 = $2^2.3^2$ e etc.

4.5 DIVISIBILIDADE

Como a divisão de um número inteiro por outro nem sempre é possível, expressa-se esta possibilidade através da relação de divisibilidade.

Quando não existir uma relação de divisibilidade entre dois números inteiros, ainda assim, será possível efetuar uma "divisão com resto pequeno", chamada de divisão euclidiana. Da possibilidade de sempre ser possível efetuar tal divisão é responsável por inúmeras propriedades dos inteiros que será explorada agora.

Dados dois números inteiros a e b, diremos que a divide b, escrevendo a|b, quando existir c ϵ Z tal que b = c.a . Neste caso, diremos também que a é um divisor ou um fator de b ou, ainda, que b é um múltiplo de a.

Observe que a notação a|b não representa nenhuma operação em Z, nem representa uma fração. Trata-se de uma sentença que diz ser verdade que existe c tal que b = c.a . A negação dessa sentença é representada por a$\nmid$b, significando que não existe nenhum número inteiro c tal que b = ca (quadro 8). Portanto, temos que 0 $\nmid$ a, se a $\neq$ 0.

Exemplificando:

1|0 ; -5|-5 ; -1|6 ; 7|-7 ; 3$\nmid$4 ; -5$\nmid$7 ; ....

Quadro 8: Proposições e demonstrações.

Proposição 1	**Demonstração:**
Sejam a; b; c ∈ Z. Tem-se que i) $1\|a$, $a\|a$ e $a\|0$. ii) se $a\|b$ e $b\|c$, então $a\|c$.	(i) Isto decorre das igualdades $a = a.1$, $a = 1.a$ e $0 = 0.a$. (ii) $a\|b$ e $b\|c$ implica que existem f; g ∈ Z, tais que $b = f.a$ e $c = g.b$. Substituindo o valor de b da primeira equação na outra, obtém-se $c = g.b = g.(f.a) = (g.f).a$; o que prova que $a\|c$.
Proposição 2	**Demonstração:**
Se a; b; c; d ∈ Z, então $a\|b$ e $c\|d \rightarrow a.c\|b.d$	Se $a\|b$ e $c\|d$, então existe f; g ∈ Z; $b = f.a$ e $d = g.c$. Portanto, $b.d = (f.g)(a.c)$, logo, $a.c\|b.d$.
Proposição 3	**Demonstração:**
Sejam a; b; c ∈ Z, tais que $a\|(b \pm c)$. Então $a\|b \leftrightarrow a\|c$.	Suponha que $a\|(b + c)$. Logo, existe f ∈ Z tal que $b + c = f.a$. Agora, se $a\|b$, tem-se que existe g ∈ Z tal que $b = g.a$. Juntando as duas igualdades acima, tem-se $g.a + c = f.a$; onde implica que $c = (f - g).a$, logo $a\|c$. A prova da implicação contrária é totalmente análoga. Por outro lado, se $a\|(b - c)$ e $a\|b$, pelo caso anterior, temos $a\|-c$, o que implica que $a\|c$.
Proposição 4	**Demonstração**
Se a; b; c ∈ Z são tais que $a\|b$ e $a\|c$, então $a\|(xb + yc)$, para todo x; y ∈ Z.	Se $a\|b$ e $a\|c$ implicam que existem f; g ∈ Z tais que $b = f.a$ e $c = g.a$. Logo, $x.b + y.c = x.(f.a) + y.(g.a) = (x.f + y.g).a$; o que prova o resultado.
Proposição 5	**Demonstração:**
Dados a; b ∈ N, tem-se que $a\|b \rightarrow a \leq b$.	De fato, se $a\|b$, existe c ∈ Z tal que $b = c.a$. Como $a > 0$ e $b > 0$, segue-se que c ∈ N. Como $1 \leq c$, segue-se que $a \leq ac = b$. Note que a relação de divisibilidade em N é uma relação de ordem, pois i) é reflexiva: Va ∈ N; $a\|a$. (Proposição 1(i)), ii) é transitiva: se $a\|b$ e $b\|c$, então $a\|c$. (Proposição 1(ii)), iii) é anti-simétrica: se $a\|b$ e $b\|a$, então $a = b$. (Segue da **Proposição 5**).
Proposição 6	**Demonstração**

Sejam a; b ϵ Z e n ϵ N. Tem-se que $a - b$ divide $a^n - b^n$.	Será provado isto por indução sobre n. É óbvio que a afirmação é verdade para n = 1, pois $a - b$ divide$a^1 - b^1 = a - b$. Suponha, agora, que $a - b \mid a^n - b^n$. Veja: $a^{n-1} - b^{n-1} = a.a^n - b.a^n + b.a^n - b.b^n = (a - b).a^n + b.(a^n - b^n)$. Como $a - b \mid a - b$ e, por hipótese, $a - b \mid a^n - b^n$, decorre da igualdade acima e da Proposição 4 que $a - b \mid a^{n-1} - b^{n-1}$. Estabelecendo o resultado para todo n ϵ N.
Proposição 7	**Demonstração:**
Sejam a; b ϵ Z e n ϵ N. Tem-se que $a + b$ divide $a^{2n+1} + b^{2n+1}$.	Será provado isto, também, por indução sobre n. A afirmação é, obviamente, verdade para n = 0, pois $a + b$ divide $a^1 + b^1 = a + b$. Suponha, agora, que $a + b \mid a^{2n+1} + b^{2n+1}$. Escreva $a^{2(n+1)+1} + b^{2(n+1)+1}$ $= a^2.a^{2n+1} - b^2.b^{2n+1} + b^2.a^{2n+1} + b^2.b^{2n+1}$ $= (a^2 - b^2).a^{2n+1} + b^2.(a^{2n+1} + b^{2n+1})$. Como $a + b$ divide $a^2 - b^2 = (a + b)(a - b)$ e, por hipótese, $a + b \mid a^{2n+1} + b^{2n+1}$,decorre das igualdades acima e da **Proposição 4** que $a + b \mid a^{2(n+1)+1} + b^{2(n+1)+1}$. Estabelecendo, assim, o resultado para todo n ϵ N.
Proposição 8	**Demonstração:**
Sejam a; b ϵ Z e n ϵ N. Tem-se que $a + b$ divide $a^{2n} - b^{2n}$.	Novamente será usado por indução sobre n. A afirmação é verdadeira para n = 1, pois claramente $a + b$ divide $a^2 - b^2 = (a + b)(a - b)$. Suponha, agora, que $a + b \mid a^{2n} - b^{2n}$. Escreve-se $a^{2(n+1)} - b^{2(n+1)} = a^2.a^{2n} - b^2.b^{2n} + b^2.a^{2n} - b^2.b^{2n}$ $= (a^2 - b^2).a^{2n} + b^2.(a^{2n} - b^{2n})$. Como $a + b \mid a^2 - b^2$ e, por hipótese, $a + b \mid a^{2n} - b^{2n}$, decorre das igualdades acima e da **Proposição 4** que $a + b \mid a^{2(n+1)} - b^{2(n+1)}$. Estabelecendo, desse modo, o resultado para todo n ϵ N.

Fonte: Da própria autoria

4.6 DIVISÃO EUCLIDIANA

Teorema 1

Sejam a e b dois números inteiros com a≠0. Existem dois únicos números inteiros q e r tais que $b = a.q + r$, com $0 \leq r < |a|$.

Demonstração:

Considere o conjunto S = $\{x = b - a.y$; y ϵ Z$\} \cap$ (N U $\{0\}$).

Existência: Pela Propriedade Arquimediana, existe n ϵ Z tal que $n.(-a) > -b$, logo $b - n.a > 0$, o que mostra que S é não vazio. O conjunto S é limitado inferiormente por 0, logo, pelo princípio da boa ordenação, temos que S possui um menor elemento r. Suponhamos então que $r = b - a.q$. Sabemos que $r > 0$.

Vamos mostrar que $r < |a|$. Suponhamos por absurdo que $r > |a|$. Portanto, existe s ϵ N U $\{0\}$ tal que $r = |a| + s$, logo $0 \leq s < r$. Mas isto contradiz o fato de r ser o menor elemento de S, pois $s = b - (q \pm 1).a$ ϵ S, com $s < r$.

Unicidade: Suponha que $b = a.q + r = a.q_0 + r_0$, onde q; q_0; r; r_0 ϵ Z , $0 \leq r < |a|$ e $0 \leq r_0 < |a|$. Assim, temos que $-|a| < -r \leq r_0 - r < |a|$. Logo, $|r_0 - r| < |a|$. Por outro lado, $a(q - q_0) = r_0 - r$, o que implica que $|a|.|q - q_0| = |r_0 - r| < |a|$, o que só é possível se $q = q_0$ e consequentemente, $r = r_0$.

Nas especificações do teorema definido acima, os números q e r são chamados de quociente e de resto da divisão, respectivamente, da divisão de b por a. No caso em que o resto da divisão de b por a é zero, diz-se que a divide b exatamente.

Exemplo 8

O quociente e o resto da divisão de 31 por 5 são q = 6 e r = 1. O quociente e o resto da divisão de -51 por 5 são q = -11 e r = 4.

Corolário 1

Dados dois números naturais a e b com $a > 0$, existe um número inteiro n tal que $n.a \leq b < (n + 1).a$.

Demonstração:

Pela divisão euclidiana, temos que existem q, r ϵ Z com $0 \leq r < a$, univocamente determinados, tais que $b = a.q + r$. Basta agora tomar $n = q$

Exemplo 9

Dado um número inteiro k ϵ Z qualquer, temos duas possibilidades:

i) o resto da divisão de k por 2 é 0, isto é, existe r ϵ N tal que $k = 2r$; ou

ii) o resto da divisão de k por 2 é 1, ou seja, existe r ϵ N tal que $k = 2r + 1$.

Portanto, os números inteiros se dividem em duas partes, a dos números da forma $2r$ para algum r ϵ Z, chamados de números pares, e a dos números da forma $2r + 1$, chamados de números ímpares. A paridade de um número inteiro é o caráter do número ser par ou ímpar.

Exemplo 10

É fácil determinar a paridade da soma e do produto de dois números a partir da paridade dos mesmos. Veja:

$6 + 7 = 13\,;\ 3 + 9 = 12\,;\ 12 + 4 = 16$

$6.7 = 42\,;\ 3\,.9 = 27\,;\ 12.4 = 48$

Mais geralmente, fixado um número natural $p > 2$, pode-se sempre escrever um número qualquer t, de modo único, na forma $t = pq + r$, onde q, r ϵ Z e $0 \leq r < q$.

Por exemplo, todo número inteiro t pode ser escrito em uma, e somente uma, das seguintes formas: $3q, 3q + 1, ou\ 3q + 2, quando\ p = 3$

Ou ainda, todo número inteiro n pode ser escrito em uma, e somente uma, das seguintes formas: $4q, 4q + 1, 4q + 2, ou\ 4q + 3, quando\ p = 4$

4.6.1 Máximo Divisor Comum

Dados dois números inteiros a e b, não simultaneamente nulos, diz-se que o número inteiro d ϵ Z é um divisor comum de a e b se $d|a$ e $d|b$. Por exemplo, os números $\pm 1, \pm 2, \pm 4$ são os divisores comuns de 16 e 20.

Diz-se que um número natural d é um máximo divisor comum (mdc) de a e b, não simultaneamente nulos, se possuir as seguintes propriedades:

i) d é um divisor comum de a e de b, e

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

A condição (ii) acima pode ser reescrita como segue:

ii_0) Se c é um divisor comum de a e b, então $c|d$.

Portanto, se d é o mdc de a e b e como c é um divisor comum desses números, então |c| divide d e, portanto, $c \leq |c| \leq d$. Isto remete que o máximo divisor comum de dois números é o maior dentre todos os divisores comuns desses números.

Assim, se d e d_0 são dois números que satisfazem o máximo divisor comum de um mesmo par de números, então $d \leq d_0$ e $d_0 \leq d$, e, consequentemente, $d = d_0$. Ou seja, o mdc de dois números é único.

O mdc de a e b será denotado por (a, b). Como o mdc de a e b não depende da ordem em que a e b são tomados, temos que $(a, b) = (b, a)$.

Em alguns casos é fácil verificar a existência do mdc.

Por exemplo, se a é um número inteiro não nulo, tem-se:

a) $(0, a) = |a|$;

b) $(1, a) = 1$;

c) $(a, a) = |a|$;

d) $(a, b) = |a|$, se para todo b ϵ Z, temos que $a|b$.

De fato, se $a|b$, temos que |a| é um divisor comum de a e b, e, se c é um divisor comum de a e b, então c divide |a|, o que mostra que $|a| = (a, b)$.

Reciprocamente, se $(a, b) = |a|$, segue-se que |a| divide b, logo $a|b$.

Observe que dados a; b ϵ Z ,não ambos nulos, se existir o $mdc\ (a, b)$ de a e b, então $(a, b) = (-a, b) = (a, -b) = (-a, -b)$.

Assim, Euclides utiliza, essencialmente, o resultado abaixo.

Lema 1(lema de Euclides)

Sejam a; b; n ϵ Z. Se existe $(a; b - na)$, então (a, b) existe e $(a, b) = (a, b - na)$.

Demonstração:

Seja $d = (a, b - na)$. Como $d|a$ e $d|(b - na)$, segue que d divide $b = b - na + na$. Logo, d *é* um divisor comum de a e b. Suponha agora que c seja um divisor comum de a e b. Logo, c um divisor comum de a e $b - na$ e, portanto, $c|d$. Isso prova que $d = (a, b)$.

Exemplo 11

$d = (8,54) \rightarrow d = (8,54 - 6.8) \rightarrow d = (8,6) \rightarrow d = (6,8) \rightarrow d = (6,8 - 1.6) \rightarrow d = (6,2) \rightarrow d = 2$

Exemplo 12

Dados a, k ϵ N com $a > 1$, tem-se que

$$\left(\frac{a^k - 1}{a - 1}, a - 1\right) = (a - 1, k).$$

A igualdade acima é verificada se $k = 1$, de fato:

$$\left(\frac{a^1 - 1}{a - 1}, a - 1\right) = (a - 1,1).$$

$(1, a - 1) = (a - 1,1)$

Supondo que $k \geq 2$. Chamando de d o primeiro membro da igualdade, tem-se:

d = $(a^{k-1} + a^{k-2} + \cdots + a + 1, a - 1)$

d = $[(a^{k-1} - 1) + (a^{k-2} - 1) + \cdots + (a - 1) + (1 - 1) + k, a - 1]$

Como (a – 1) | $[(a^{k-1} - 1) + (a^{k-2} - 1) + \cdots + (a - 1) + (1 - 1)]$, segue-se que $[(a^{k-1} - 1) + (a^{k-2} - 1) + \cdots + (a - 1) + (1 - 1) = n.(a - 1)$, para algum n ϵ N.

Logo $d = [n.(a - 1) + k, a - 1] = [a - 1, k + n.(a - 1)] = (a - 1, k)$.

Exemplo 13

Determinar os valores de a não negativos e n ϵ N para os quais $a + 1$ divide $a^{4n} + 2$.

Observe, inicialmente que

$a + 1 | a^{4n} + 2 \leftrightarrow (a + 1, a^{4n} + 2) = a + 1$.

Como $a^{4n} + 2 = (a^{2n} - 1) + 3$, e $a + 1 | a^{4n} - 1$,por definição, para todo n ϵ N.

Logo $(a + 1, a^{4n} + 1) = (a + 1, (a^{4n} - 1) + 3) = (a + 1, 3)$.

Portanto, $a + 1 | a^{4n} + 2$, para algum n ϵ N, se, e somente se, $a + 1 = (a + 1; 3)$, o que ocorre se, e somente se, a = 0 ou a = 1 ou a = 2.

4.6.2 Algoritmo de Euclides

O método, chamado de Algoritmo de Euclides, é uma expressão adequada, ou seja, de fácil processamento no ponto de vista computacional e que na atualidade pouco conseguiu-se aperfeiçoá-lo desde sua criação a dois mil anos atrás.

Dados a; b ϵ N, pode-se supor $a \leq b$. Se $a = 1$ ou $a = b$, ou ainda $a|b$, que equivale $(a, b) = a$. Suponha-se, então, que $1 < a < b$ e que a não divide b. Logo, pela divisão euclidiana, pode-se escrever $b = a.q_1 + r_1$, com $0 < r_1 < a$.

Sendo as duas possibilidades:

a) $r_1|a$, logo

$r_1 = (a, r_1) = (a, b - q_1.a) = (a, b)$, ou

b) r_1 não divide a, e, em tal caso, pode-se efetuar a divisão de a por r_1, obtendo $a = r_1 . q_2 + r_2$; com $0 < r_2 < r_1$.

Continuando nessa mesma ideia, tem-se duas possibilidades:

a_1) $r_2|r_1$, logo $r_2 = (r_1, r_2) = (r_1, a - q_2 . r_1) = (r_1, a) = (b - q_1.a, a) = (b, a) = (a, b)$, ou

b_1) r_2 não divide r_1, e, em tal caso, podemos efetuar a divisão de r_1 por r_2, obtendo $r_1 = r_2 . q_3 + r_3$, com $0 < r_3 < r_2$.

Este procedimento não pode continuar indefinidamente, caso fosse tería uma sequência de números naturais infinitos $a > r_1 > r_2 > \ldots\ldots$,que não possui menor elemento, o que não é possível pela Propriedade da Boa Ordenação. Logo, para algum n, tem-se que $r_n|r_{n-1}$, o que implica que $(a, b) = r_n$.

O algoritmo acima pode ser representado de forma mais simples na prática. Observe abaixo como será elucidado:

Inicialmente, efetua-se a divisão $b = a.q_1 + r_1$ e colocando os números envolvidos no seguinte diagrama:

	q_1	
b	a	
r_1		

A seguir, continua-se efetuando a divisão $a = r_1.q_2 + r_2$ e colocando os números envolvidos no diagrama

	q_1	q_2	
b	a	r_1	
r_1	r_2		

Prosseguindo, enquanto for possível, tem-se

	q_1	q_2	q_3	$\cdots$	q_{n-1}	q_n	q_{n+1}
b	a	r_1	r_2	$\cdots$	r_{n-2}	r_{n-1}	$r_n = (a, b)$
r_1	r_2	r_3	r_4	$\cdots$	r_n		

Exemplo 14

Calcule o mdc de 372 e 162.

	2	3	2	1	2
372	162	48	18	12	6
48	18	12	6		

Observe que, no exemplo acima, o Algoritmo de Euclides fornece:

6 = 18 – 1.12

12 = 48 – 2.18

18 = 162 – 3.48

48 = 372 – 2.162

Onde se define que

6 = 18 – 1.12 = 18 – 1.(48 – 2.18) = 3.18 - 48 =

3.(162 – 3.48) - 48 = 3.162 – 10.48 =

3.162 – 10.(372 – 2.162) = 23.162 – 10.372.

Tem-se, que

(372; 162) = 6 = 23.162 + (-10).372 .

Note que através do uso do Algoritmo de Euclides conseguiu-se escrever 6 = (372; 162) como a soma de produtos dos números dados 372 e 162 com seus respectivos quantitativos de repetição, ou seja, **23**.162 + **(-10)**.372 .

CAPÍTULO 5

O CRIVO DE ERATÓSTENES, EQUAÇÕES DIOFANTINAS LINEARES E OS TESTES DE PRIMALIDADES

5.1 O CRIVO DE ERATÓSTENES

A maneira visivelmente mais simples e intuitiva de constatar se um determinado número natural é primo é conhecida como o Crivo de Erastóstenes. Ele era diretor da biblioteca do grande instituto de pesquisa da Grécia Antiga em Alexandria, no século III a.C., foi a primeira pessoa a produzir tabelas de números primos. A técnica por ele utilizada foi bastante simples e intuitiva. Ele escrevia inicialmente os números de 1 a N. Em seguida, escolhia o primeiro primo 2 e eliminava da lista todos os seus múltiplos. Passava, então ao próximo número não eliminado, 3, e eliminava também todos os seus múltiplos. Repetia sucessivamente este método até o maior inteiro inferior a $\sqrt{N}$ e cada novo primo que encontrava gerava um crivo que era utilizado para eliminar os números compostos múltiplos desse crivo.

Os números não primos da relação eram então decompostos da seguinte forma. Seja N um número composto identificado por $N = N_1 * N_2 * ... * N_n$, onde N_1 , N_2 , ..., $N_n < N$. Esse algoritmo fornece a decomposição de N em fatores primos. Esse método pode ser utilizado para gerar tabelas de primos relativamente grandes, porém para valores muito grandes de N, o algoritmo exige muito tempo e cálculos para verificar se é um número primo ou composto. Surge então a necessidade de encontrar um algoritmo eficaz, ou seja, que exija menos tempo e menor custo, para execução.

Por exemplo, vamos elaborar a tabela de todos os números primos inferiores a 81. Escrevem-se todos os números naturais de 2 a 81. Riscam-se, de modo sistemático, todos os números compostos da tabela, seguindo o roteiro abaixo. Risque todos os múltiplos de 2 acima de 2, já que nenhum deles é primo. O segundo número não riscado é 3, que é primo. Risque todos os múltiplos de 3 maiores do que 3 pois esses não são primos. O terceiro número não riscado que aparece é 5, que é primo. Risque todos os múltiplos de 5 maiores do que 5 pois esses não são primos. O quarto número não riscado que ora aparece é 7, que é primo. Risque todos os múltiplos de 7 maiores do que 7 pois esses não são primos. Será necessário prosseguir com este procedimento até chegar a 81? A resposta é não e se baseia no seguinte resultado

devido ao próprio Eratóstenes.

- ✓ Se um número natural n > 1 não é divisível por nenhum número primo tal que $p^2 \leq n$, então ele é primo.

Portanto, a tabela 1 de números de 2 a 81, deve-se ir até alcançar o primo 7, pois o próximo primo é 11, cujo quadrado supera 81(quadro 9)

Quadro 9 : Representação de números por Erastóstenes

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

Fonte: Própria do autor

5.2 EQUAÇÕES DIOFANTINAS LINEARES

O desenvolvimento de vários problemas de aritmética, recaem em equações do tipo

$$a.x + b.y = c, \quad (1)$$

que terão soluções em números inteiros. Tais equações são chamadas equações diofantinas lineares em homenagem a Diofanto de Alexandria (aprox. 300 DC).

Nem sempre estas equações possuem solução. Por exemplo, a equação $8x + 10y = 7$ não possui nenhuma solução x_0, y_0 em números inteiros, caso foce, $8x_0 + 10y_0$ seria par e, portanto, nunca igual a 7.

Assim, serão definidas algumas regras ou proposições para a solução do problema. Como pode ser verificado a seguir,

- ✓ Sejam a,b ϵ Z\{0} e c ϵ Z. A equação a.x + b.y = c admite solução em números inteiros

se, somente se, (a, b)\c .

- ✓ Seja x_o , y_o uma solução da equação $a.x + b.y = c$, onde (a, b) = 1 . Então as soluções x, y em Z da equação são da forma $x = x_0 + t_b$ e $y = y_0 - t_a$; t ϵ Z .

Como por exemplo $2x + 3y = 5$ tem solução pois mdc (2,3) = 1 que divide 5, logo a solução $x_o = 1$ e $y_o = 1$ é uma das soluções da equação. As outra soluções serão do tipo $x = 1 + 3t$ e $y = 1 - 2t$, para todo t ϵ N.

5.3 CONGRUÊNCIA

Apresentaremos uma das noções mais fecundas da aritmética, introduzida por Gauss no seu livro Disquisitiones Arithmetica, de 1801. Trata-se da realização de uma aritmética com os restos da divisão euclidiana por um número fixado.

Seja m um número natural diferente de zero. Diremos que dois números inteiros a e b são congruentes módulo m se os restos de sua divisão euclidiana por m são iguais. Quando os inteiros a e b são congruentes módulo m, escreve-se

$$a \equiv b \ mod \ m \ . \qquad (1)$$

Por exemplo, 21 ≡ 13 mod 2, já que os restos da divisão de 21 e de 13 por 2 são iguais a 1.

Quando a relação (1) for falsa, diremos que a e b não são congruentes, ou que são incongruentes, módulo m. Escreveremos, neste caso,

$$a \not\equiv b \bmod m. \qquad (2)$$

Como o resto da divisão de um número inteiro qualquer por 1 é sempre nulo, temos que $a \equiv b \ mod \ 1$, quaisquer que sejam a; b ϵ Z. Isto torna desinteressante a aritmética dos restos módulo 1. Portanto, doravante, considerar sempre m > 1.

Decorre, imediatamente, da definição que a congruência, módulo um inteiro fixado m, é uma relação de equivalência. Isto será enunciado explicitamente abaixo.

- ✓ Seja m ϵ N. Para todos a; b; c ϵ Z, tem-se que

(i) a ≡ a mod m,

(ii) se a ≡ b mod m, então b ≡ a mod m,

(iii) se a ≡ b mod m e b ≡ c mod m, então a ≡ c mod m.

Exemplo 15

Paulo passou a caminhar todos os dias em duas praças que tinha em sua cidade, a primeira tinha 500 metros de comprimento e a segunda 400 metros. Em um dia ele caminhou 5000 metros. Qual a quantidade máxima de voltas que ele pode fazer na praça de menor comprimento?

Resolução:

Por congruência, tem-se:

$500x \equiv 5000 \bmod 400 \rightarrow x = 10$

A quantidade máxima de voltas será de 10, pois 10. 400 = 4000 e 2. 500 = 1000. Somando dará 5000 metros que foi a caminhada de Paulo.

5.4. TEOREMA DE WILSON

O teorema atribuído a Wilson(1741-1793), mas que, na realidade, foi provado, pela primeira vez, por J.L. Lagrange (1736-1813) é o que está definido abaixo:

- ✓ Se p é um número primo, então $(p - 1)! \equiv -1 \bmod p$

Esta congruência prova se um número N é primo ou não, mas que não é usado para cálculos com N muito grande.

Como por exemplo os números 13 e 15 são primos?

Usando o teorema de Wilson tem-se para p = 13 o resultado:

$(13 – 1)! \equiv -1 \bmod 13 \rightarrow 12! \equiv -1 \bmod 13$. Usando o teorema da decomposição para um número fatorial fica: $12! = 2^{10}.3^5.5^2.7.11 \equiv -1 \bmod 13 \rightarrow (1024-13.78).(243-13.18).(25-13).(77-13.5) \equiv -1 \bmod 13 \rightarrow 10.9.12.12 \equiv -1 \bmod 13 \rightarrow (90-13.6).(144-13.11) \equiv -1 \bmod 13 \rightarrow 12.1 \equiv -1 \bmod 13 \rightarrow 12+1/13 \rightarrow 13/13 = 1$. Assim 13 é primo.

Aplicando o mesmo teorema para p = 15 fica:

$(15 – 1)! \equiv -1 \bmod 15 \rightarrow 14! \equiv -1 \bmod 15$. Usando o teorema da decomposição para um número fatorial tem-se: $14! = 2^{11}.3^5.5^2.7^2.11.13 \equiv -1 \bmod 13 \rightarrow (2048-15.136).(243-15.16).(25-15).(49-15.3).(143-15.9) \equiv -1 \bmod 15 \rightarrow 8.3.10.4.8 \equiv -1 \bmod 15 \rightarrow (240-15.16).(32-15.2) \equiv -1 \bmod 15 \rightarrow 0.2 \equiv -1 \bmod 15 \rightarrow 0+1/15 \rightarrow 1/15 \neq 1$. Assim 15 não é primo.

5.5 DECOMPOSIÇÃO DE UM NÚMERO FATORIAL EM POTÊNCIA DE NÚMEROS PRIMOS

O método que será elucidado aqui foi criado por Euclides para facilitar a fatoração de números fatoriais e responder perguntas como: “Quantos zeros tem esse número?”; “O número 7^3 divide esse número?”.

Para começar a vislumbrar essa ideia será necessário compreender a divisão euclidiana.

Sejam “a, b e c” números naturais e “b e c” diferentes de zero e a relação

$$\left[\frac{\left[\frac{a}{b}\right]}{c}\right] = \left[\frac{a}{b.c}\right] . \quad (1)$$

Essa relação é verdadeira?

A demonstração a seguir verificará essa igualdade. Assim, fica:

Demonstração:

Note que $q_1 = \left[\frac{a}{b}\right]$ e $q_2 = \left[\frac{\left[\frac{a}{b}\right]}{c}\right]$ são funções quocientes que não retorna o resto da divisão e sim o quociente. Assim F(a,b) = [a/b] = q ,para todo a, b e q pertencente aos inteiros.

Sejam $a = b.q_1 + r_1$, para $r_1 \leq b-1$ (I) <=> $\left[\frac{a}{b}\right]$ e $q_1 = c.q_2 + r_2$, para $r_2 \leq c-1$ (II)<=> $\left[\frac{\left[\frac{a}{b}\right]}{c}\right]$;

Substituindo (II) em (I), tem-se:

$a = b.(c.q_2 + r_2) + r_1 = b.c.q_2 + (b.r_2 + r_1)$, para $(b.r_2 + r_1) \leq b.c-1$<=> $\left[\frac{a}{b.c}\right]$

Essas divisões mostram que “a” é dividido pelo produto “b.c” .

A ideia usada nessas divisões é mostrar o quociente que será usado para encontrar o maior expoente de cada fator primo de “n!”. Logo, $E_p(n!)$ será chamado de maior expoente de base “p”, um número primo.

Essas divisões serão finitas até que “n” seja menor que “p^i “, para todo “i” natural, que implicará $\left[\frac{n}{p^i}\right] = 0$. Assim, define-se:

Teorema 1

$$\mathbf{E_p(n!) = [\frac{n}{p}] + [\frac{n}{p^2}] + [\frac{n}{p^3}]+...+ [\frac{n}{p^i}] = q_1 + q_2 + q_3 +...+q_i = \sum_1^i \frac{n}{p^i}} \quad \mathbf{(2)}$$

Exemplificando:

Fatore o número 10! .

$$E_2(10!) = [\frac{10}{2}] + [\frac{10}{2^2}] + [\frac{10}{2^3}] = 5 + 2 + 1 = 8$$

$$E_3(10!) = [\frac{10}{3}] + [\frac{10}{3^2}] = 3 + 1 = 4$$

$$E_5(10!) = [\frac{10}{5}] = 2$$

$$E_7(10!) = [\frac{10}{7}] = 1$$

$$10! = 2^8.3^4.5^2.7^1$$

Teorema 16

Sejam p, n ϵ N com "p" primo. Se

$$N = n_r.p^r + n_{r-1}.p^{r-1} + ...+ n_1.p^1 + n_0 \quad (3)$$

É a representação p-ádica de n, então:

$$E_p(n!) = \frac{n - (n_0 + n_1 + \cdots + n_r)}{p-1} \quad (4)$$

Exemplificando:

Fatore o número 13!.

Transformando 13 na base 2, tem-se: $\frac{13}{2} = 6 + resto\ 1$; $\frac{6}{2} = 3 + resto\ 0$; $\frac{3}{2} = 1 + resto\ 1$; $13_{10} = 1101_2$. Aplicando $E_p(n!) = \frac{n - (n_0 + n_1 + \cdots + n_r)}{p-1}$, fica: $E_2(13!) = \frac{13 - (1+1+0+1)}{2-1} = 10$.

Transformando 13 na base 3, tem-se: $\frac{13}{3} = 4 + resto\ 1$; $\frac{4}{3} = 1 + resto\ 1$;; $13_{10} = 111_3$. Aplicando $E_p(n!) = \frac{n - (n_0 + n_1 + \cdots + n_r)}{p-1}$, fica: $E_3(13!) = \frac{13 - (1+1+1)}{3-1} = 5$.

Transformando 13 na base 5, tem-se: $\frac{13}{5} = 2 + resto\ 3$; $13_{10} = 23_5$. Aplicando $E_p(n!) = \frac{n - (n_0 + n_1 + \cdots + n_r)}{p-1}$, fica: $E_5(13!) = \frac{13 - (3+2)}{5-1} = 2$.

Transformando 13 na base 7, tem-se: $\frac{13}{7} = 1 + resto\ 6$; $13_{10} = 16_7$. Aplicando $E_p(n!) = \frac{n - (n_0 + n_1 + \cdots + n_r)}{p-1}$, fica: $E_7(13!) = \frac{13 - (1+6)}{7-1} = 1$.

Transformando 13 na base 11, tem-se: $\frac{13}{11} = 1 + resto\ 2$; $13_{10} = 12_{11}$. Aplicando $E_p(n!) =$

$\frac{n-(n_0+n_1+\cdots+n_r)}{p-1}$, fica: $E_{11}(13!) = \frac{13-(1+2)}{11-1} = 1$.

Transformando 13 na base 13, tem-se: $\frac{13}{13} = 1 + resto\ 0$; $13_{10} = 10_{13}$. Aplicando $E_p(n!) = \frac{n-(n_0+n_1+\cdots+n_r)}{p-1}$, fica: $E_{13}(13!) = \frac{13-(1+0)}{13-1} = 1$.

Assim $13! = 2^{10}. 3^5. 5^2.7.11.13$

5.6. ANÁLISE COMBINATÓRIA[13]

O princípio fundamental da contagem é usado na maioria dos problemas relacionados com contagem como por exemplo a escolha de uma roupa para vestir, a quantidade de números de telefones que podem ser definidos, a quantidade de placas de carro que podem ser feitas, etc. É necessário definir uma ferramenta muito usada em problemas de contagem, o fatorial. Este número natural é definido como o produto deste número por todos os seus antecessores. Utilizamos o símbolo "!" para indicar o fatorial de um número.

Exemplo 17

3! = 3.2.1 = 6
7! = 7.6.5.4.3.2.1 = 5 040
10! = 10.9.8.7.6.5.4.3.2.1 = 3 628 800

Casos especiais de fatorial:

O fatorial de 0(zero) que é igual a 1(um): 0! = 1
O fatorial de 1(um) que é igual a 1(um): 1! = 1

5.6.1. Arranjo

No **arranjo**, os agrupamentos dos objetos dependem da ordem e da natureza dos mesmos. Para obter o arranjo simples de **n** elementos tomados, p a p ($p \leq n$), utiliza-se a seguinte expressão:

[13] https://www.todamateria.com.br/analise-combinatoria/

$$A_{n,p} = \frac{n!}{(n-p)!} \quad (1)$$

Exemplo 18

Como exemplo de arranjo, pode-se pensar na escolha para presidente e um vice-presidente de uma empresa, com 30 funcionários. Sendo que o mais votado será o presidente e o segundo mais votado o vice-presidente. Desta forma, de quantas maneiras distintas a escolha poderá ser feita?

Resolução:

Sendo que n = 30 e p = 2 , logo $A_{n,p} = \frac{n!}{(n-p)!} \rightarrow A_{30,2} = \frac{30!}{(30-2)!} = 30.29 = 870$.

Assim, o arranjo pode ser feito de **870** maneiras diferentes.

5.7. TESTES DE PRIMALIDADES

5.7.1 Teste de Wilson

Este teste é determinístico, pois verifica se um número N é primo utilizando a fórmula

$$(N - 1)! \equiv -1 \; mod \; N. \quad (1)$$

Exemplo 19. Verifique se o número 6 é primo ou composto.

Sendo (6-1)! = 5! = 5.4.3.2.1 = 120 ≡ 0 (mod 6).

Portanto, 6 não é um número primo.

Exemplo 20 Verifique se o número 11 é primo ou composto.

Como (11-1)! = 10! = 10.9...2.1, tem-se:

10! = 10.9...2.1 ≡ -1 (mod 11).

Assim, o número 11 é primo.

5.7.2 – Teste de Fermat

Este teste é determinístico, baseia-se no pequeno teorema de Fermat e verifica-se

$$2^N - 1 \equiv 1 \; mod \; N, \quad (2)$$

onde N é o número a ser testado. (Obs.: Nem sempre a congruência, neste caso, será verdade)

Exemplo 21. Verifique se o número 6 é primo ou composto.

Sendo $2^{N-1} \equiv 1 \bmod N$ e N = 6, tem-se: $2^{6-1} \equiv 1 \bmod 6 \rightarrow 2^5 \equiv 1 \bmod 6 \rightarrow 32 \equiv 1 \bmod 6 \rightarrow 32-1= 31$ não é divisível por 6. Portanto, 6 não é um número primo.

Exemplo 22. Verifique se o número 11 é primo ou composto..

Sendo $2^{N-1} \equiv 1 \bmod N$ e N = 11, tem-se: $2^{11-1} \equiv 1 \bmod 11 \rightarrow 2^{10} \equiv 1 \bmod 11 \rightarrow 1024 \equiv 1 \bmod 11 \rightarrow 1024-1= 1023$ é divisível por 11. Portanto, 11 é um número primo.

5.7.3 Teste de Lucas-Lehmer

Este teste é determinístico, utilizado para testar a primalidade de números de Mersenne que são definidos pela expressão

$$N = 2^p - 1, \tag{3}$$

onde p é primo.

Teorema 5.7.3..1. Seja S_k a sequência definida por

$$S_k = (2+\sqrt{3})^{2^k} + (2-\sqrt{3})^{2^k} \tag{4}$$

para k ϵ N. Seja p > 2, $N_p = 2^p - 1$ é primo se, e somente se, S_{p-2} é múltiplo de N_p.

Exemplo 23 Verifique se $N_5 = 2^5 - 1 = 31$ é um número primo.

Tomando S = 4 e atualizando o valor da expressão S ←(S.S - 2) (mod $\mathbf{N_5}$) , (5-2) = 3 vezes:

• S ←(4.4 - 2) (mod 31) = 14

• S ←(14.14 - 2) (mod 31) = 8

• S ←(8.8-2) (mod 31) = 0

Portanto, o número 31 é primo.

Exemplo 24. Determine a primalidade do número $N_{11} = 2^{11} - 1 = 2047$.

Atualizando 11-2 = 9 vezes a expressão S (S.S - 2) (mod N_{11}) tem-se:

• S ←(4.4-2) (mod 2047) = 14

• S ←(14.14-2) (mod 2047) = 194

• S ←(194.194-2) (mod 2047) = 788

• S ←(788.788-2) (mod 2047) = 701

• S ←(701.701-2) (mod 2047) = 119

• S ←(119.119-2) (mod 2047) = 1877

• S ←(1877.1877-2) (mod 2047) = 240

• S ←(240.240-2) (mod 2047) = 282

• S ←(282.282-2) (mod 2047) = 1736

Portanto, o número 2047 não é primo, pois o valor final de S é diferente de 0 (zero).

5.7.4 AKS

Este teste é determinístico, os indianos Manindra Agrawal, Neeraj Kayal e Nitin Saxena, definido pela sigla AKS, é capaz de verificar a primalidade de um número em tempo polinomial.

O algoritmo baseia-se na equação de congruência

$$(x + a)^p \equiv (x^p + a)\ (mod\ p), \tag{5}$$

onde p é primo, é uma generalização do Pequeno Teorema de Fermat.

Teorema 5.7.4.1. Sejam a ϵ Z, n ϵ N, n ≥ 2 e (a, n) = 1. Então n é primo se, e somente se,

$$(x + a)^p \equiv (x^p + a)\ (mod\ p)$$

Exemplo 25. Verifique se o número 31 é primo ou composto.

Executando o teste AKS obtem-se:

(1) 31 não é uma potência;

(2) Para r = 29 tem-se $ord_{29}(31) > (\log_2 31)^2$;

(3) Não existe a ≤ 29 tal que 1 < (a,31) < 31;

(4) 31 > 29, nada pode-se afirmar;

(5) A congruência é verdadeira para todo 1 ≤ a ≤ 29;

(6) Logo, o número 31 é primo.

Exemplo 26. Detemine a primalidade do número 341.

Analisando cada passo do algoritmo AKS tem-se:

(1) 341 não é uma potência;

(2) Para r = 77 tem-se $ord_{77}(341) > (\log_2 341)^2$;

(3) Para a = 11 tem-se 1 < (11,341) = 11 < 341, portanto, 341 é um número composto.

5.7.5 Divisões Sucessivas (Teorema de Eratóstenes)

Este teste é determinístico, o mais simples dos testes de primalidade consiste em dividir um número n por todos os números naturais primos que estiverem na faixa que vai de 2 até √n natural. Se n for divisível por qualquer um deles, então n é um número composto. Caso contrário, é um número primo.

Exemplo 27. Por exemplo, elaborando a tabela de todos os números primos inferiores a 81. Escrevem-se todos os números naturais de 2 a 81. Riscam-se, de modo sistemático, todos os números compostos da tabela, seguindo o roteiro abaixo. Risque todos os múltiplos de 2 acima de 2, já que nenhum deles é primo. O segundo número não riscado é 3, que é primo. Risque todos os múltiplos de 3 maiores do que 3 pois esses não são primos. O terceiro número não riscado que aparece é 5, que é primo. Risque todos os múltiplos de 5 maiores do que 5 pois esses não são primos. O quarto número não riscado que ora aparece é 7, que é primo. Risque todos os múltiplos de 7 maiores do que 7 pois esses não são primos. Será necessário prosseguir com este procedimento até chegar a 81? A resposta é não e se baseia no seguinte resultado devido ao próprio Eratóstenes.

- ✓ Se um número natural n > 1 não é divisível por nenhum número primo tal que $p_2 < n$, então ele é primo.

Portanto, a tabela 1 de números de 2 a 81, deve-se ir até alcançar o primo 7, pois o próximo primo é 11, cujo quadrado supera 81 (quadro 10).

Quadro 10 : Representação de números por Erastóstenes

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

Fonte: Própria do autor

5.7.6 Solovay-Strassen

Este teste é probabilístico, desenvolvido por Robert Martin Solovay e Volker Strassen, este algoritmo permite que dado um número ímpar possamos determinar se o mesmo é um número composto ou provavelmente primo utilizando o Critério de Euler e o Símbolo de Jacobi.

Teorema 5.7.6.1. Seja n um número inteiro ímpar composto, existe um inteiro a tal que (a,n) = 1 e

$$a^{\frac{n-1}{2}} \text{ não é côngruo a } [a/n] \ (mod\ n). \tag{6}$$

Exemplo 28. Verificando se 15 é primo ou composto.

Note que, a = 3;5;6;9;10 e 12 o resultado será COMPOSTO, pois [a/n] = 0. Para outros valores de a tem-se:

• a = 2 → [2/15] = 1 e $2^7 \equiv 8$ (mod 15)

• a = 4 →[4/15] = 1 e $4^7 \equiv 4$ (mod 15)

• a = 7→[7/15] = -1 e $7^7 \equiv 13$ (mod 15)

• a = 8→[8/15] = 1 e $8^7 \equiv 2$ (mod 15)

• a = 11→[11/15] = -1 e $11^7 \equiv 11$ (mod 15)

• a = 13→[13/15] = -1 e $13^7 \equiv 7$ (mod 15)

• a = 14→[14/15] = -1 e $14^7 \equiv 14$ (mod 15)

Assim, o algoritmo retorna PRIMO apenas para a = 14, ou seja, a probabilidade de identificar o número 15 como COMPOSTO é 12/13 ≈ 92,3%.

5.7.7. Miller-Rabin

Este teste é probabilístico, pois usa de um teste probabilístico, com várias iterações, pode fornecer uma alta probabilidade de que esse número seja primo. Este processo nos dá resultados muito precisos, mas há uma pequena chance de erro. No entanto são usados amplamente devido sua eficiência para números muito grandes. Desenvolvido por Gary Lee Miller e Michael Oser Rabin utilizando os conceitos de congruência e o Pequeno Teorema de Fermat.

Teorema 5.7.7.1. Seja n um primo ímpar tal que

$$n - 1 = 2^w . m, \quad (7)$$

onde 2^w é a maior potência de 2 em n-1. Dado a um inteiro tal que (a,n)=1, então $a^m \equiv 1 \pmod n$ ou existe r ϵ {0,1,2,...,w-1} tal que

$$a^{2^r}.m \equiv -1 \ (mod\ n). \quad (8)$$

Exemplo 29. Mostre que n = 1729 é um número composto.

Para n-1 = 1728 = 2^6. 27, então w = 6 e m = 27.

Tomando a = 671 temos:

$671^{27} \equiv 1084 \pmod{1729}$

$671^{27.2} \equiv 1084^2 \equiv 1065 \pmod{1729}$

$671^{27.2.2} \equiv 1065^2 \equiv 1 \pmod{1729}$

Assim, n é declarado composto e o teste termina.

CAPÍTULO 6

CONTRIBUIÇÕES REFERENTE AOS NÚMEROS PRIMOS

6.1 SEQUÊNCIAS NUMÉRICAS E FUNÇÕES

Os números primos representam a essência dos números compostos e base para a criptografia da era digital. A função 2n - 1 representa a sequência de todos os números ímpares para todo n ϵ Z que são {... -13, -11, -9, -7, -5, -3, -1, 1, 3, 5, 7, 9, 11, 13, ...} e que contém todos os números primos impares {3,5,7,11,13,17,19,23,29,31,37,41, ...}.

Também pode-se observar que as funções 6n + 1 e 6n -1 possuem sequências numéricas que são, respectivamente, {7, 13, 19, 25, 31, 37, 43, 49, 55, 61, 67, ...} e {5, 11, 17, 23, 29, 35, 41, 47, 53, 59, 65, ...} e dessa maneira se verifica que todos os números nelas formados tem a terminação 1, 3, 5, 7, 9 para todo n ϵ N. Estas sequências unidas possuem em sua estrutura todos os números primos começando pelo número 5.

Os números primos possuem na casa das unidades os algarismos 1, 3, 7 e 9 e como não existe ainda uma função que defina a sequência dos números primos proponho oito funções que definem oito sequências com as terminações 1, 3, 7 e 9 para todo n ϵ N.

As funções são:

(I) 30n -19 e (II) 30n +1 para as sequências de números que termina com o algarismo 1;

(III) 30n -7 e (IV) 30n -17 para as sequências de números que termina com o algarismo 3;

(V) 30n -13 e (VI) 30n -23 para as sequências de números que termina com o algarismo 7;

(VII) 30n -1 e (VIII) 30n -11 para as sequências de números que termina com o algarismo 9.

As sequências estarão no quadro a seguir (quadro 11)

Quadro 11: Sequencias de números primos a partir de formulações algébricas.

(I)	(II)	(III)	(IV)	(V)	(VI)	(VII)	(VIII)
11	31	23	13	17	7	29	19
41	61	53	43	47	37	59	49
71	91	83	73	77	67	89	79
101	121	113	103	107	97	119	109
131	151	143	133	137	127	149	139
161	181	173	163	167	157	179	169
191	211	203	193	197	187	209	199

Essas sequências nos possibilitam visualizar em particular todos os números que estão dentro da margem dos números ímpares com terminação 1, 3, 7 e 9 como candidatos a número primo. Um outro ponto interessante é que a quantidade de números encontrados para análise, com apenas um valor para n aumenta significativamente

Aplicando as funções I, II, III, IV, V, VI, VII e VIII na planilha do excel, serão definidas sequências em uma planilha e em seguida serão encontrados todos os números primos da planilha através de uma função que usa a ideia do crivo de Aristóstenes com a aproximação inteira da raíz quadrada do número escolhido para análise. Este resultado só será usado se o número for primo, se não, escolhe-se o número abaixo dele que é primo. Assim usa-se a expressão:

=SE(R3=5;R3;SE(MOD(R3;5)=0;" ";SE(R3=7;R3;SE(MOD(R3;7)=0;" ";SE(R3=11;R3;SE(MOD(R3;11)=0;" ";SE(R3=13;R3;SE(MOD(R3;13)=0;" ";SE(R3=17;R3;SE(MOD(R3;17)=0;" ";SE(R3=19;R3;SE(MOD(R3;19)=0;" ";SE(R3=23;R3;SE(MOD(R3;23)=0;" ";SE(R3=29;R3;SE(MOD(R3;29)=0;" ";SE(R3=31;R3;SE(MOD(R3;31)=0;" ";SE(R3=37;R3;SE(MOD(R3;37)=0;" ";SE(R3=41;R3;SE(MOD(R3;41)=0;" ";SE(R3=43;R3;SE(MOD(R3;43)=0;" ";SE(R3=47;R3;SE(MOD(R3;47)=0;" ";SE(R3=53;R3;SE(MOD(R3;53)=0;" ";SE(R3=59;R3;SE(MOD(R3;59)=0;" ";SE(R3=61;R3;SE(MOD(R3;61)=0;" ";SE(R3=67;R3;SE(MOD(R3;67)=0;" ";SE(R3=71;R3;SE(MOD(R3;71)=0;" ";SE(R3=73;R3;SE(MOD(R3;73)=0;" ";SE(R3=79;R3;SE(MOD(R3;79)=0;" ";SE(R3=83;R3;SE(MOD(R3;83)=0;" ";SE(R3=89;R3;SE(MOD(R3;89)=0;" ";SE(R3=97;R3;SE(MOD(R3;97)=0;" ";SE(R3=101;R3;SE(MOD(R3;101)=0;" ";SE(R3=103;R3;SE(MOD(R3;103)=0;" ";SE(R3=107;R3;SE(MOD(R3;107)=0;" ";SE(R3=109;R3;SE(MOD(R3;109)=0;" ";SE(R3=113;R3;SE(MOD(R3;113)=0;" ";SE(R3=127;R3;SE(MOD(R3;127)=0;" ";SE(R3=131;R3;SE(MOD(R3;131)=0;" ";SE(R3=137;R3;SE(MOD(R3;137)=0;" ";SE(R3=139;R3;SE(MOD(R3;139)=0;" ";R3))

Esta função tem um alcance máximo no excel para os números primos de 5 a 139 que significa que 139 é a raiz inteira e primo do número 22800. Observe o quadro (quadro 12)com os primos até 3709

Quadro 12: A utilização do Crivo de Arástotenes e redução do espaço a mostral conduz aos núrneros primos até 3019.

	30n - 19	30n + 1	30n - 7	30n - 17	30n - 13	30n - 23	30n - 1	30n - 11	30n - 19	30n + 1	30n - 7	30n - 17	30n - 13	30n - 23	30n - 1	30n - 11
1	11	31	23	13	17	7	29	19	11	31	23	13	17	7	29	19
2	41	61	53	43	47	37	59	49	41	61	53	43	47	37	59	
3	71	91	83	73	77	67	89	79	71		83	73		67	89	79
4	101	121	113	103	107	97	119	109	101		113	103	107	97		109
5	131	151	143	133	137	127	149	139	131	151			137	127	149	139
6	161	181	173	163	167	157	179	169		181	173	163	167	157	179	
7	191	211	203	193	197	187	209	199	191	211		193	197			199
8	221	241	233	223	227	217	239	229		241	233	223	227		239	229
9	251	271	263	253	257	247	269	259	251	271	263		257		269	
10	281	301	293	283	287	277	299	289	281		293	283		277		
11	311	331	323	313	317	307	329	319	311	331		313	317	307		
12	341	361	353	343	347	337	359	349			353		347	337	359	349
13	371	391	383	373	377	367	389	379			383	373		367	389	379
14	401	421	413	403	407	397	419	409	401	421				397	419	409
15	431	451	443	433	437	427	449	439	431		443	433			449	439
16	461	481	473	463	467	457	479	469	461			463	467	457	479	
17	491	511	503	493	497	487	509	499	491		503			487	509	499
18	521	541	533	523	527	517	539	529	521	541		523				
19	551	571	563	553	557	547	569	559		571	563		557	547	569	
20	581	601	593	583	587	577	599	589		601	593		587	577	599	
21	611	631	623	613	617	607	629	619		631		613	617	607		619
22	641	661	653	643	647	637	659	649	641	661	653	643	647		659	
23	671	691	683	673	677	667	689	679		691	683	673	677			
24	701	721	713	703	707	697	719	709	701						719	709
25	731	751	743	733	737	727	749	739		751	743	733		727		739
26	761	781	773	763	767	757	779	769	761		773			757		769
27	791	811	803	793	797	787	809	799		811			797	787	809	
28	821	841	833	823	827	817	839	829	821			823	827		839	829
29	851	871	863	853	857	847	869	859			863	853	857			859
30	881	901	893	883	887	877	899	889	881			883	887	877		
31	911	931	923	913	917	907	929	919	911					907	929	919
32	941	961	953	943	947	937	959	949	941		953		947	937		
33	971	991	983	973	977	967	989	979	971	991	983		977	967		
34	1001	1021	1013	1003	1007	997	1019	1009		1021	1013			997	1019	1009
35	1031	1051	1043	1033	1037	1027	1049	1039	1031	1051		1033			1049	1039
36	1061	1081	1073	1063	1067	1057	1079	1069	1061			1063				1069
37	1091	1111	1103	1093	1097	1087	1109	1099	1091		1103	1093	1097	1087	1109	
38	1121	1141	1133	1123	1127	1117	1139	1129				1123		1117		1129
39	1151	1171	1163	1153	1157	1147	1169	1159	1151	1171	1163	1153				
40	1181	1201	1193	1183	1187	1177	1199	1189	1181	1201	1193		1187			
41	1211	1231	1223	1213	1217	1207	1229	1219		1231	1223	1213	1217		1229	
42	1241	1261	1253	1243	1247	1237	1259	1249						1237	1259	1249
43	1271	1291	1283	1273	1277	1267	1289	1279		1291	1283		1277		1289	1279

44	1301	1321	1313	1303	1307	1297	1319	1309	1301	1321		1303	1307	1297	1319	
45	1331	1351	1343	1333	1337	1327	1349	1339						1327		
46	1361	1381	1373	1363	1367	1357	1379	1369	1361	1381	1373		1367			
47	1391	1411	1403	1393	1397	1387	1409	1399							1409	1399
48	1421	1441	1433	1423	1427	1417	1439	1429			1433	1423	1427		1439	1429
49	1451	1471	1463	1453	1457	1447	1469	1459	1451	1471		1453		1447		1459
50	1481	1501	1493	1483	1487	1477	1499	1489	1481		1493	1483	1487		1499	1489
51	1511	1531	1523	1513	1517	1507	1529	1519	1511	1531	1523					
52	1541	1561	1553	1543	1547	1537	1559	1549			1553	1543			1559	1549
53	1571	1591	1583	1573	1577	1567	1589	1579	1571		1583			1567		1579
54	1601	1621	1613	1603	1607	1597	1619	1609	1601	1621	1613		1607	1597	1619	1609
55	1631	1651	1643	1633	1637	1627	1649	1639					1637	1627		
56	1661	1681	1673	1663	1667	1657	1679	1669				1663	1667	1657		1669
57	1691	1711	1703	1693	1697	1687	1709	1699				1693	1697		1709	1699
58	1721	1741	1733	1723	1727	1717	1739	1729	1721	1741	1733	1723				
59	1751	1771	1763	1753	1757	1747	1769	1759				1753		1747		1759
60	1781	1801	1793	1783	1787	1777	1799	1789		1801		1783	1787	1777		1789
61	1811	1831	1823	1813	1817	1807	1829	1819	1811	1831	1823					
62	1841	1861	1853	1843	1847	1837	1859	1849		1861			1847			
63	1871	1891	1883	1873	1877	1867	1889	1879	1871			1873	1877	1867	1889	1879
64	1901	1921	1913	1903	1907	1897	1919	1909	1901		1913		1907			
65	1931	1951	1943	1933	1937	1927	1949	1939	1931	1951		1933			1949	
66	1961	1981	1973	1963	1967	1957	1979	1969			1973				1979	
67	1991	2011	2003	1993	1997	1987	2009	1999		2011	2003	1993	1997	1987		1999
68	2021	2041	2033	2023	2027	2017	2039	2029					2027	2017	2039	2029
69	2051	2071	2063	2053	2057	2047	2069	2059			2063	2053			2069	
70	2081	2101	2093	2083	2087	2077	2099	2089	2081			2083	2087		2099	2089
71	2111	2131	2123	2113	2117	2107	2129	2119	2111	2131		2113			2129	
72	2141	2161	2153	2143	2147	2137	2159	2149	2141	2161	2153	2143		2137		
73	2171	2191	2183	2173	2177	2167	2189	2179								2179
74	2201	2221	2213	2203	2207	2197	2219	2209		2221	2213	2203	2207			
75	2231	2251	2243	2233	2237	2227	2249	2239		2251	2243		2237			2239
76	2261	2281	2273	2263	2267	2257	2279	2269		2281	2273		2267			2269
77	2291	2311	2303	2293	2297	2287	2309	2299		2311		2293	2297	2287	2309	
78	2321	2341	2333	2323	2327	2317	2339	2329		2341	2333				2339	
79	2351	2371	2363	2353	2357	2347	2369	2359	2351	2371			2357	2347		
80	2381	2401	2393	2383	2387	2377	2399	2389	2381		2393	2383		2377	2399	2389
81	2411	2431	2423	2413	2417	2407	2429	2419	2411		2423		2417			
82	2441	2461	2453	2443	2447	2437	2459	2449	2441				2447	2437	2459	
83	2471	2491	2483	2473	2477	2467	2489	2479				2473	2477	2467		
84	2501	2521	2513	2503	2507	2497	2519	2509		2521		2503				
85	2531	2551	2543	2533	2537	2527	2549	2539	2531	2551	2543				2549	2539
86	2561	2581	2573	2563	2567	2557	2579	2569						2557	2579	
87	2591	2611	2603	2593	2597	2587	2609	2599	2591			2593			2609	
88	2621	2641	2633	2623	2627	2617	2639	2629	2621		2633			2617		
89	2651	2671	2663	2653	2657	2647	2669	2659		2671	2663		2657	2647		2659
90	2681	2701	2693	2683	2687	2677	2699	2689			2693	2683	2687	2677	2699	2689
91	2711	2731	2723	2713	2717	2707	2729	2719	2711	2731		2713		2707	2729	2719
92	2741	2761	2753	2743	2747	2737	2759	2749	2741		2753					2749

93	2771	2791	2783	2773	2777	2767	2789	2779		2791			2777	2767	2789	
94	2801	2821	2813	2803	2807	2797	2819	2809	2801			2803		2797	2819	
95	2831	2851	2843	2833	2837	2827	2849	2839		2851	2843	2833	2837			
96	2861	2881	2873	2863	2867	2857	2879	2869	2861					2857	2879	
97	2891	2911	2903	2893	2897	2887	2909	2899			2903		2897	2887	2909	
98	2921	2941	2933	2923	2927	2917	2939	2929					2927	2917	2939	
99	2951	2971	2963	2953	2957	2947	2969	2959		2971	2963	2953	2957		2969	
100	2981	3001	2993	2983	2987	2977	2999	2989		3001					2999	
101	3011	3031	3023	3013	3017	3007	3029	3019	3011		3023					3019

Fonte: Condição 'SE' extraído do programa execel.

6.2 SUBSEQUÊNCIAS, A SOMAÇÃO E FUNÇÕES GERADORAS DE PRIMOS

Ao estudar de forma mais aprofundada as sequências dos números primos ímpares { 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, ...}, observa-se que a diferença entre os números em ordem crescente dá uma sequência do tipo { 2, 2, 4, 2, 4, 2, 4, 6, 2, 6, 4, 2, 4, 6, 6, 2, 6, 4, 2, 6, 4, 6, 8, 4, 2, 4, 2, 4, 14, 4, 6, 2, 10, 2, 6, ...}. Após esta análise, passa-se a somar os valores, da nova sequência, em ordem crescente e a definir uma nova sequência que é da seguinte forma {2, 4, 8, 10, 14, 16, 20, 26, 28, 34, 38, 40, 44, 50, 56, 58, 64, 68, 70, 76, 80, 86, 94, 98, 100, 104, 106, 110, 124, 128, 134, 136, 146, 148, 154, ...}. Com estes números passa-se a construir subsequências que estão definidas através das funções abaixo:

- ✓ $Q_1(n) = n^2 - n + 38 \rightarrow (38, 40, 44, 50, 58, 68, 80, ...)$, que somado com 3 ficaria $P_1(n) = n^2 - n + 41 \rightarrow (41, 43, 47, 53, 61, 71, 83, ...)$, que são 40 números primos continuamente para todo $n \in N$.
- ✓ $Q_2(n) = n^2 - n + 14 \rightarrow (14, 16, 20, 26, 34, 44, 56, ...)$, que somado com 3 ficaria $P_2(n) = n^2 - n + 17 \rightarrow (17, 19, 23, 29, 37, 47, 59, ...)$, que são 16 números primos continuamente para todo $n \in N$.
- ✓ $Q_3(n) = 10n^2 - 20n + 26 \rightarrow (16, 26, 56, 106, 176, 266, ...)$, que somado com 3 ficaria $P_3(n) = 10n^2 - 20n + 29 \rightarrow (19, 29, 59, 109, 179, 269, ...)$, que são 19 números primos continuamente para todo $n \in N$.

Estas funções foram encontradas através do processo de somação que se dá pela subtração dos termos consecutivos da sequência definida e isto pode ser feito uma, duas, três, ou mais vezes até que se encontre uma sequência constante, ou seja, todos os termos serão iguais. Depois usa-se a expressão binomial

$$P(n) = \Delta_1 . C_{n,0} + \Delta_2 . C_{n,1} + \Delta_3 . C_{n,2} +... , \quad (1)$$

quantas vezes for o operador Δ_k e k ϵ N, para encontrar a função desejada.

Como por exemplo seja a subsequência (38, 40, 44, 50, 58, 68, 80, ...), usando o operador $\Delta a_n = a_n - a_{n-1}$ da somação tem-se: (2, 4, 6, 8, 10, 12, ...). Repetindo a operação na nova sequência fica (2, 2, 2, 2, 2, ...) que é a sequência constante.

Aplicando a expressão binomial $P(n) = \Delta_1 . C_{n,0} + \Delta_2 . C_{n,1} + \Delta_3 . C_{n,2} +...$, fica:

$Q(n) = 38 . C_{n,0} + 2 . C_{n,1} + 2 . C_{n,2}$

$Q(n) = 38 + 2.(n-1) +2.(n-1).(n-2)/2$

$Q(n) = n^2 - n + 38.$

Acrescentando o número primo 3 na expressão Q(n) encontra-se:

$P(n) = n^2 - n + 41 \rightarrow$(41, 43, 47, 53, 61, 71, 83, ...).

6.3 TESTE DE PRIMALIDADE

No decorrer da história da humanidade muitos matemáticos ou filósofos buscaram uma função para definir os números primos, mas sem sucesso. No entanto, surgiram os testes de primalidades, para tentar suprir a necessidade de uma função e é neste viés que proponho um teste para encontrar números primos. Este processo envolve o algoritmo de Euclides: o mdc de dois números naturais; lema de Euclides, a função inteiro de uma raíz quadrada, o fatorial de um natural, a decomposição de um número fatorial em fatores primos e a relação do mdc de números primos entre si, ou seja, mdc(x,y) = 1. A ideia do Crivo de Erastóstenes, também, está inserida no desenvolvimento deste teste.

Ao analisar o teorema do Crivo de Eratóstenes que é um algoritmo que define números primos em meio a uma quantidade "N" de números naturais. Temos por definição que ao retirar todos os múltiplos dos números primos, a começar do primo 2(dois) até o primo que é menor ou igual a $\sqrt{N}$ será encontrado assim todos os primos desse conjunto U = {1, 2, 3, 4, 5, 6, 7, ..., N}. Por outro lado, se nenhum dos primos entre 2 e $\sqrt{N}$ dividir o número N, este número será primo.

Nesse mesmo entendimento, mas usando a ideia da multiplicação de todos os números primos do conjunto A={1, 2, 3, 4, 5, 6, 7, ..., [$\sqrt{N}$]}, o resultado será um número que pode ser primo com N ou não, ao usar a definição do MDC. Se eles forem primos entre si, N será primo, senão será composto, logo 2.3.5.7.11....P = T, onde P $\leq$ [$\sqrt{N}$] .

O mais interessante é que ao usar o lema de Euclides do MDC para reduzir o resultado do produto em outro número menor que N, o resultado encontrado é um número que pode ser

escrito na forma de produto de potências de fatores primos, ou seja, $p_1^{n_1}.p_2^{n_2}.p_3^{n_3}$ .... . Se um dos números primos p_1, p_2, p_3, ... ,do produto $p_1^{n_1}.p_2^{n_2}.p_3^{n_3}$ ... , dividir N, logo N será composto, caso contrário, será primo.

Desta forma tem-se: MDC(T, N) = MDC(N.q + r, N) = MDC(r, N), onde r < N e $r = p_1^{n_1}.p_2^{n_2}.p_3^{n_3}$ ..., com p_1, p_2, p_3, ... primos e n_1, n_2, n_3, ... natural. Assim, se p_1, p_2, p_3, ... dividir N, MDC(r, N) ≠ 1e N será composto; caso contrário, MDC(r, N) = 1 e N será primo.

Esta mesma análise será feita para todos os elementos do conjunto A, logo o produto 1.2.3.4.5.6.7.8.9..... [√N], que na análise combinatória é um número fatorial, ou seja, [√N]!. Agora tem-se, pelo o teorema de Euclides, acima mencionado, o MDC([√N]!, N) = MDC(N.q_1 + r_1, N) = MDC(r_1, N), onde r_1 < N e $r_1 = p_{11}^{n_{11}}.p_{12}^{n_{12}}.p_{13}^{n_{13}}$ ... com p_{11}, p_{12}, p_{13}, ... primos e n_{11}, n_{12}, n_{13}, ... natural. Assim, se p_{11}, p_{12}, p_{13}, ...dividir N, MDC(r_1, N) ≠ 1 e N será composto; caso contrário, MDC(r_1, N) = 1 e N será primo. O desafio aqui é calcular o número [√N]! que depende diretamente de N e se este for muito grande, teremos um produto de muitos fatores para calcular.

Nos tempos atuais existem os cálculos manuais munido de técnicas matemáticas que duraria muito tempo para resolver, os supercomputadores que podem trabalhar com valores grandes desses números, mas que ainda não é o suficiente. É necessário unir a programação munido com técnicas matemáticas para alcançar esse objetivo de definir se N é primo ou composto. Uma técnica matemática ou teorema da decomposição de um número fatorial em potência de números primos que é definida neste trabalho e é de grade importância para a redução do número [√N]!.

Abaixo a definição desta ideia como teorema e em seguida alguns exemplos. Assim, tem-se:

Teorema 6.1 JR

- ✓ Seja N natural e [√N](função inteiro) = A , então mdc(N,A!) = 1 e N primo.

Exemplificando o teorema:

Exemplo 30

Verifique se 101 e 119 são primos.

Para N = 101 tem-se: A = [√101] =10 → A=7, logo x = 7! = $2^4.3^2.5.7$.

Usando o mdc(7!,101) → mdc($2^4.3^2.5.7$, 101) → mdc[(144-101).35] → mdc[43.35 , 101] → mdc(1505-101.14 , 101) → mdc(91,101). Como 91=7.13 e 7 nem 13 divide 101, então mdc(91,101)=1. Assim 101 é primo.

Para N=119 tem-se: A=[√119] → A =10 → A=7, logo x = 7! = $2^4.3^2.5.7$.
Usando o mdc(7!,119) → mdc($2^4.3^2.5.7$, 119) → mdc[(144-119).35] → mdc[25.35 , 101] → mdc(875-119.7 , 119) → mdc(42,119). Como 42=2.3.7 e 7 divide 119, então mdc(42,119)=7≠1. Assim 119 não é primo.

A expressão definida acima pode ser usada para todo número natural maior que 1(um) com um resultado verdadeiro se N for primo, caso contrário, o resultado será falso se o número N for composto. Assim mdc([√N]!, N) = 1 é uma relação definida para todos os números naturais maiores ou iguais 2.

Pelo teorema de Wilson este número N será primo se satisfazer a congruência

$$(N - 1)! \equiv -1 mod\ N \qquad (2)$$

e com isso de a verifica deste teorema que está relacionado ao espaço amostral de 1 até (N – 1) em um conjunto de números naturais que o produto deles é (N – 1)!.

Pelo teorema de Eratóstenes o espaço amostral {1, 2, 3, ...,(N – 1)} será reduzido para 1 até [√N], ou seja, uma redução importante para os cálculos do crivo definido através de uma tabela onde os números compostos são retirados e os números que permanecem são os números primos.

Esta redução é primordial para o cálculo do fatorial e do novo teste de primalidade proposto acima que define se N é primo pelo mdc([√N]!, N) = 1. Nesta mesma linha de pensamento para a determinação de números primos surgiu uma segunda ideia através da expressão do arranjo $A'_{[\sqrt{N}],[[\sqrt{N}]/2]}$ definida no conjunto B= {[√N], [√N]-1, [√N]-2, [√N]-3, ..., ([√N]/2) +1} retirada de A={1, 2, 3, 4, 5, 6, 7, ..., [√N]}, onde a expressão $(A'_{[\sqrt{N}],[[\sqrt{N}]/2]})$ representa o produto de todos números do conjunto B., ou seja, $A'_{[\sqrt{N}],[[\sqrt{N}]/2}$ = √N]. ([√N]-1). ([√N]-2). ([√N]-3). .... .(([√N]/2) +1) . No caso da expressão[√N] será sempre usado valores pares, mas se der ímpar soma-se a ele uma unidade.

Assim, a expressão MDC([√N]!, N) = 1 será reduzido para MDC([√N]. ([√N]-1). ([√N]-2). ([√N]-3). .... .(([√N]/2) +1) , N) = 1 ou MDC($A'_{[\sqrt{N}],[[\sqrt{N}]/2]}$, N) = 1 que facilitará ainda mais o resultado final para a definição ou caracterização de N.

Exemplo31

Verifique se 101 e 119 são primos.

Resolução:

Para N = 101

$[\sqrt{101}] = 10$

$A'_{10,\mathbf{5}} = 10.9.8.7.6 = 30240$

$MDC(A'_{10,\mathbf{5}}, 101) = MDC(30240, 101) = MDC(30240\text{-}101.299, 101) = MDC(41, 101) = 1.$

Como 41 e 101 são primos entre si, 101 será primo.

Para N = 119

$[\sqrt{101}] = 10$

$A'_{10,\mathbf{5}} = 10.9.8.7.6 = 30240$

$MDC(A'_{10,\mathbf{5}}, 101) = MDC(30240, 119) = MDC(30240\text{-}119.254, 101) = MDC(14, 119) = 7.$

Como 14 = 2.7 e sabendo que 7 divide 119, logo 14 e 119 não são primos entre si. Assim,119 não é primo.

A expressão $A'_{[\sqrt{\mathbf{N}],[[\sqrt{\mathbf{N}]/\mathbf{2}]}}}/2^{[N]/2}$ representa o produto de todo número ímpar definido através do produto dos elementos do conjunto B dividido pela potência $2^{[N]/2}$, ou seja, o produto de todos os elementos ímpares do conjunto A. Esse resultado pode ser reduzido ainda mais, se divido por 5 quantas vezes for necessário, ou seja, até que a divisão não dê mais exata, pois pela regra de divisibilidade, um número só será dividido por 5 quando o algarismo da unidade for 5(cinco) ou 0(zero) sendo este critério de fácil observação. Caso se queira simplificar por 3 fica ao critério do observador. Desta forma ficará mais rápido a identificação do número N que deve ser ímpar neste caso.

A Expressão $MDC\ (A'_{[\sqrt{\mathbf{N}],[[\sqrt{\mathbf{N}]/\mathbf{2}]}}}, N) = 1$ pode ser definida como uma função para $[\sqrt{N}] = 2k$, para todo $k \in N^*$. Dessa forma sendo remodelada a expressão para

$$MDC(A'_{\mathbf{2k,k}} ; [(2k\text{-}1)^2, (2k+1)^2 \text{ -}1]) = 1 \qquad (3)$$

onde $[(2k\text{-}1)^2, (2k+1)^2 \text{ -}1]$ é um intervalo para cada k natural diferente de zero e o arranjo um número natural definido para o intervalo para que MDC que é a função encontre cada primo impar no intervalo. Assim, K será o domínio da função, o contradomínio da função será todos ao naturais e a imagem os números primos ímpares definido pelo MDC no intervalo. Como por exemplo:

Para $k = 1 \rightarrow MDC(A'_{2,\mathbf{1}}; [1, 8]) = 1 \rightarrow A'_{2,\mathbf{1}} = \mathbf{2} \rightarrow Im=\{3, 5, 7\}$; o número 1 não se define e o número 2 é primo e par.

Para k = 2 → MDC(A'$_{4,2}$; [9, 24]) = 1 → A'$_{4,2}$ = 4.3 → Im={11, 13, 17, 19, 23}

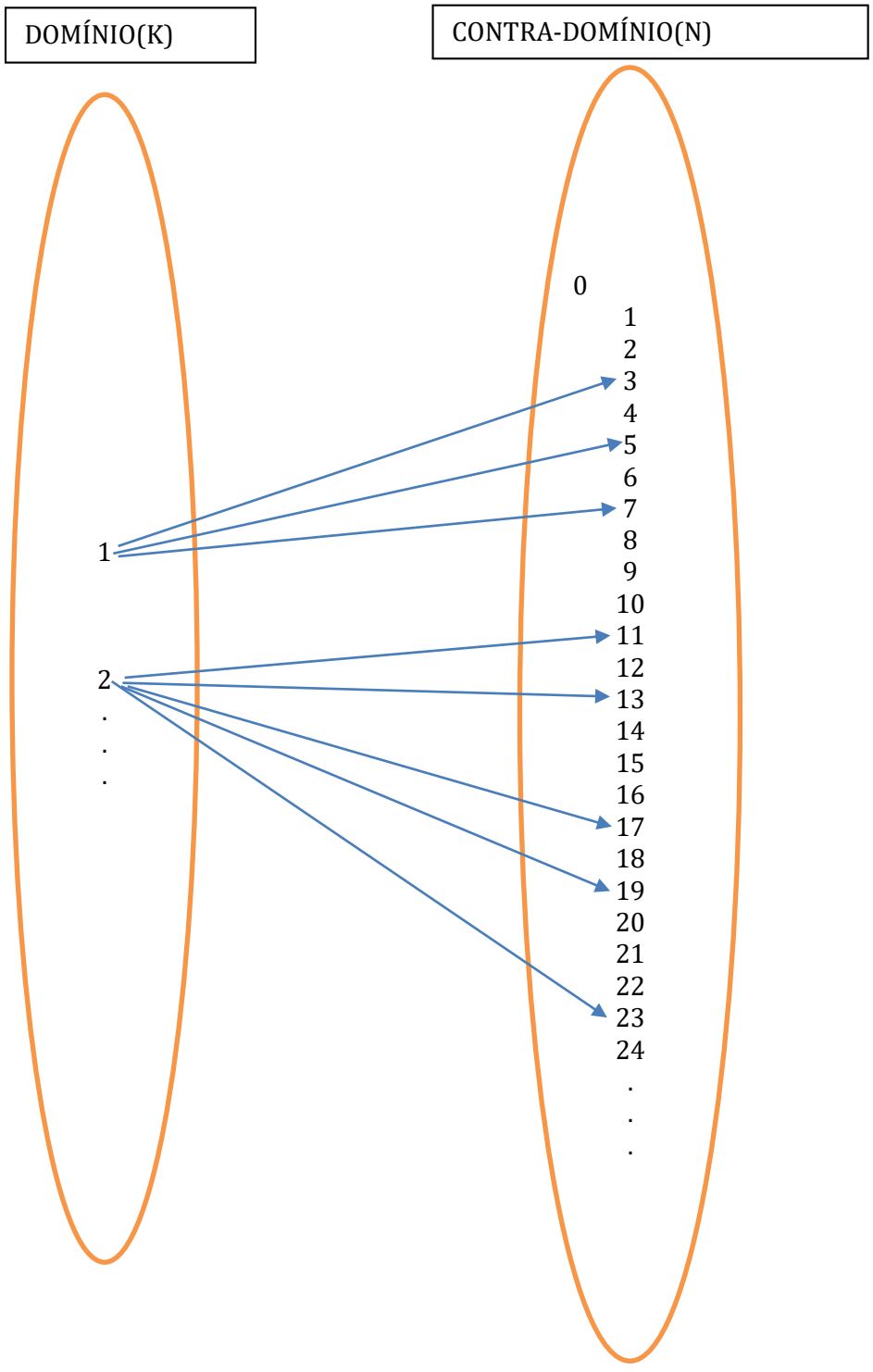
Para k = 3 → MDC(A'$_{6,3}$; [25, 48]) = 1 → A'$_{6,3}$ = 6.5.4→ Im={29, 31, 37, 41, 43, 47}

.....

E assim infinitamente.

Usando o diagrama de flechas tem-se (figura 4):

Figura 4: Correspondência Biunívoca para determinar números primos



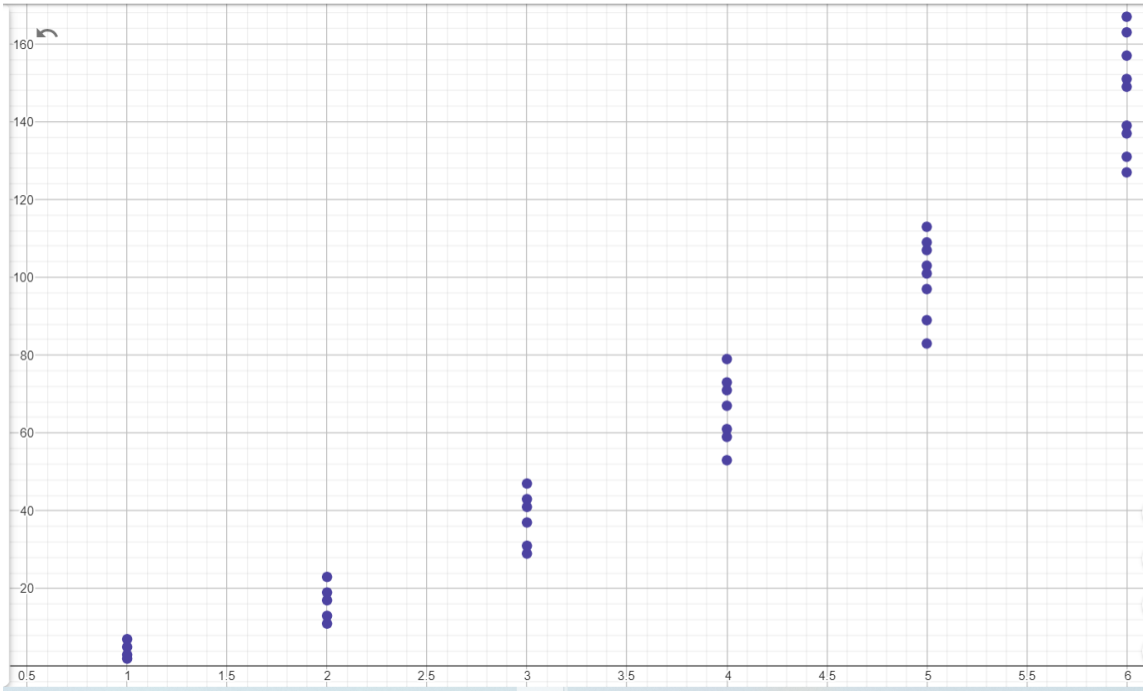
Fonte: Da própria autoria

Construindo o plano cartesiano (quadro 13)

Tabela 1: Achado de números primos a partir da expressão $MDC(A'_{2k,k} ; [(2k-1)^2, (2k+1)^2 -1]) = 1$

Valores do domínio nos N	**$MDC(A'_{2k,k} ; [(2k-1)^2, (2k+1)^2 -1]) = 1$**	**Números primos (Imagem)**
1	$MDC(A'_{2,1} ; [1, 8]) = 1$	3, 5, 7
2	$MDC(A'_{4,2} ; [9, 24]) = 1$	11, 13, 17, 19, 23
3	$MDC(A'_{6,3} ; [25, 48]) = 1$	29, 31, 37, 41, 43, 47
4	$MDC(A'_{8,4} ; [49, 80]) = 1$	53, 59, 61, 67, 71, 73, 79
5	$MDC(A'_{10,5} ; [81, 120]) = 1$	83, 89, 97, 101, 103, 107, 109, 113
6	$MDC(A'_{12,6} ; [121, 168]) = 1$	127, 131, 137, 139, 149, 151, 157, 163, 167
...	**...**	**...**

EIXO Y



EIXO X

Fonte: Da própria autoria

6.4 EQUAÇÕES DIOFANTINAS

Este resultado do MDC, também, nos direciona para equações diofantinas da forma x.a + y.b = 1, para todo “a” e “b” pertencente ao conjunto dos inteiros. Desta forma, a equação possui infinitas soluções da forma: w = a + y.t ; k = b –x.t , para todo t ϵ Z e x<y.

A saber conforme o exemplo,

Como 101 é primo, logo mdc(7!, 101)→mdc(91,101)=1, tem-se:

91a + 101b = 1, aplicando a divisão euclidiana, fica a =10 e b = -9 uma das soluções da equação. Considere a divisão:

	1	9
101	91	10
10	1	

Resolvendo fica: 91 = 9.10 + 1(i) e 101 = 1.91 + 10 (ii), substituindo ii em i, fica: 91 = 9.(101 – 1.191) + 1 → 91- 9.101 + 9.91 = 1 → 10.91 -9.101 = 1 → a=10 e b=-9 .

As demais soluções serão do tipo w = 10 +101t e k = -9 -91t , para todo t ϵ Z.

6.5 CONGRUÊNCIA

A congruência introduzida por Gauss e estudada por Wilson em seu teste de primalidade dada pela expressão (p - 1)! ≡ -1mod p , pode-se conjecturar uma expressão x.R ≡ 1 mod y, para todo R ϵ Z. Esta congruência só servirá para números “y” primos, pois se o número “y” for composto o mdc(x, y) ≠ 1.

Exemplificando:

Os números 7, 11 e 21 são primos?

Usando y=7, tem-se:

Por Wilson fica: (7-1)! ≡ -1 mod 7 → 6! ≡ -1 mod 7 → 721/7 = 13

Novo teste : (√7!, 7) =1 → (2!, 7) = 1 → (2,7) = 1

O número 7 é primo.

Usando y=11, tem-se:

Por Wilson fica: (11-1)! ≡ -1 mod 11 → 10! ≡ -1 mod 11 → (10+1)/11 = 1

Novo teste : (√11!, 11) =1 → (3!, 11) = 1 → (6,11) = 1

O número 11 é primo.

Usando y=21, tem-se:

Por Wilson fica: (21-1)! ≡ -1 mod 21 → 20! ≡ -1 mod 21 → (0+1)/21→1/21

Novo teste : (√21!, 21) =1 → (3!, 21) = 1 → (6,21) =3 ≠ 1

O número 21 não é primo.

6.6 SEQUÊNCIA IMPORTANTE

A sequência ($\frac{\sqrt{2}}{2}$, $\frac{\sqrt{3}}{3}$, $\frac{\sqrt{5}}{5}$, $\frac{\sqrt{7}}{7}$, $\frac{\sqrt{11}}{11}$, $\frac{\sqrt{13}}{13}$, $\frac{\sqrt{17}}{17}$, $\frac{\sqrt{19}}{19}$,...) representa a divisão da √p por p que é a relação de redução do número "p" em outro número [√p] inteiro que é o extremo de uma sequência de 1 a [√p] de números inteiros que satisfazem a definição "Seja N natural e [√N](função inteiro) = A , então mdc(N,A!) = 1 e N primo.".

Esta sequência ($\frac{\sqrt{2}}{2}$, $\frac{\sqrt{3}}{3}$, $\frac{\sqrt{5}}{5}$, $\frac{\sqrt{7}}{7}$, $\frac{\sqrt{11}}{11}$, $\frac{\sqrt{13}}{13}$, $\frac{\sqrt{17}}{17}$, $\frac{\sqrt{19}}{19}$,...) definida pela função $f(p) = \frac{\sqrt{P}}{P}$ ou $f(p) = \frac{1}{\sqrt{P}}$ para todo p pertencente aos números naturais diferente de zero, mostra o percentual, que representa a necessidade de uma sequência de números primos enumeráveis para definir um número primo no intervalo [1,p], logo, quanto maior o p aumentar, menor é a divisão de √p/p ou 1/√p, o que implica no limite definido por $\lim_{p\to+\infty} \frac{\sqrt{p}}{p}$ = 0 ou $\lim_{p\to+\infty} \frac{1}{\sqrt{p}}$ = 0.

6.7 RELAÇÃO IMPORTANTE

As tabelas abaixo representam as sequências de números com terminação 1,3, 7 e 9 que estão se relacionando através do teste de Eratóstenes e o novo teste de primalidade com a escrita verdadeiro ou falso (quadros 14, 15 e 16) que representam as funções definidas.

Quadro 14: Diferentes expressões algébricas para achados de números primos.

	30n – 19	30n + 1	30n – 7	30n - 17	30n – 13	30n - 23	30n - 1	30n - 11
1	11	31	23	13	17	7	29	19
2	41	61	53	43	47	37	59	49
3	71	91	83	73	77	67	89	79
4	101	121	113	103	107	97	119	109
5	131	151	143	133	137	127	149	139
6	161	181	173	163	167	157	179	169
7	191	211	203	193	197	187	209	199
8	221	241	233	223	227	217	239	229
9	251	271	263	253	257	247	269	259
10	281	301	293	283	287	277	299	289
11	311	331	323	313	317	307	329	319
12	341	361	353	343	347	337	359	349

Fonte: Da própria autoria

Quadro 15: Diferentes expressões algébricas para achados de números primos com uso do crivo de Eratóstenes.

30n – 19	30n + 1	30n – 7	30n – 17	30n - 13	30n - 23	30n - 1	30n - 11
11	31	23	13	17	7	29	19
41	61	53	43	47	37	59	
71		83	73		67	89	79
101		113	103	107	97		109
131	151			137	127	149	139
	181	173	163	167	157	179	
191	211		193	197			199
	241	233	223	227		239	229
251	271	263		257		269	
281		293	283		277		
311	331		313	317	307		
		353		347	337	359	349

Fonte: Da própria autoria

Quadro 16:Diferentes expressões algébricas para achados de números primos com o novo teste – MDC

30n – 19	30n + 1	30n – 7	30n – 17	30n - 13	30n - 23	30n - 1	30n - 11
Verdadeiro	Verdadeiro	Verdadeiro	Verdadeiro	Verdadeiro	Verdadeiro	Verdadeiro	Verdadeiro
Verdadeiro	Verdadeiro	Verdadeiro	Verdadeiro	Verdadeiro	Verdadeiro	Verdadeiro	Falso
Verdadeiro	Falso	Verdadeiro	Verdadeiro	Falso	Verdadeiro	Verdadeiro	Verdadeiro
Verdadeiro	Falso	Verdadeiro	Verdadeiro	Verdadeiro	Verdadeiro	Falso	Verdadeiro
Verdadeiro	Verdadeiro	Falso	Falso	Verdadeiro	Verdadeiro	Verdadeiro	Verdadeiro
Falso	Verdadeiro	Verdadeiro	Verdadeiro	Verdadeiro	Verdadeiro	Verdadeiro	Falso
Verdadeiro	Verdadeiro	Falso	Verdadeiro	Verdadeiro	Falso	Falso	Verdadeiro
Falso	Verdadeiro	Verdadeiro	Verdadeiro	Verdadeiro	Falso	Verdadeiro	Verdadeiro
Verdadeiro	Verdadeiro	Verdadeiro	Falso	Verdadeiro	Falso	Verdadeiro	Falso
Verdadeiro	Falso	Verdadeiro	Verdadeiro	Falso	Verdadeiro	Falso	Falso
Verdadeiro	Verdadeiro	Falso	Verdadeiro	Verdadeiro	Verdadeiro	Falso	Falso
Falso	#Núm!	Verdadeiro	Falso	Verdadeiro	Verdadeiro	Verdadeiro	Verdadeiro

Fonte: Da própria autoria

O quadro 16, são todos os números definidos pelas funções f(n) = 30n – 19 , f(n) = 30n + 1, f(n) = 30n – 7, f(n) = 30n – 17, f(n) = 30n – 13, f(n) = 30n – 23, f(n) = 30n – 1, f(n) = 30n – 11 para todo n pertencente aos naturais maiores que zero. O quadro15 é o teste do crivo de Aristostenes pelo excel usando as funções "=SE(....)" e "=MOD(....)" e o quadro 16 o novo teste de primalidade pelo excel usando a função "=MDC(....)".

CONCLUSÃO

A construção da dissertação abordada foi perpassar no capítulo 2 pela evolução dos números e seus criadores com um olhar mais sucinto e direcionado para o objeto de estudo que foi o número primo através de um novo teste de primalidade embasado no teorema, no lema de Euclides e no teorema do Crivo de Eratóstenes. Neste trabalho procurou fazer necessário a menção da biografia de Euclides e Eratóstenes pelas contribuições que trouxeram à luz da comunidade científica e para a sociedade.

Dessa maneira, o capítulo 2 deixou em aberto para o leitor pesquisar e se aprofundar na compreensão da História (surgimento), como um todo, e da biografia de cada autor. Esse segundo capitulo pode ser útil para que o aluno consiga compreender como aconteceu o desenvolvimento histórico dos números primos por meio dos filósofos matemáticos.

O capítulo 3 procurou situar o aluno na expectativa da BNCC de modo que o professor possa construir uma metodologia voltada para questões problemas que seja compreensível ao nível do aluno, pois nesse ponto, tornou-se possível mostrar o que a BNCC elabora nas habilidades e competências estratégias de ensino que conduza o aluno a uma aprendizagem de primalidade com um rigor contextualizado onde o professor desse ser o articular e mentor de uma construção metodológica capaz de promover um processo de ensino e aprendizagem curioso e motivador.

A abordagem do capítulo 4 trouxe algumas relevantes propriedades, definições, teoremas e demonstrações do conjunto dos números naturais e inteiros que são exploradas para a compreensão do que é um número natural, inteiro, composto e primo à criação e execução de funções e testes de primalidades determinísticos e probabilísticos que buscou facilitar e melhorar os estudos científicos e o benefício para a sociedade a partir de um formalismo matemático capaz de mostrar os diferentes aspectos peculiares de cada número estudado no referente capítulo.

Com o prosseguimento da leitura, o capítulo 5 ficou destinado para análise dos diferentes testes conhecidos na literatura, permitindo que afluísse o determinístico e o probabilístico levando a determinar quando um número natural foi composto ou primo. Para um melhor concisão e clareza, houve no decorrer de cada teste vários exemplos teve como intuito facilitar compreensão de como aplicar ou usar o teorema exposto.

Não se preocupou desenvolver demonstrações de cada teste, sendo necessário apenas os teoremas e os exemplos de como se procede para definir o número se foi primo ou não, pois

deixou-se em aberto para que o leitor curioso pudesse fazer uma pesquisa à parte para entender como seriam possíveis a construção de um formalismo matemático muito mais robusto, portanto, este caso, o leitor pode ter a liberdade de pesquisar.

Apesar de todo os desenvolvimentos dos capítulos precedentes, a questão primordial era atingir o objetivo da construção de novo teste de primalidade elencado no capítulo 6, que surgiu da análise do teorema do Crivo de Eratóstenes e do teorema e lema de Euclides (MDC). A ideia nova veio a somar com os novos testes existentes para a definição de um número primo, elencando a sequências e funções extraídas, respectivamente, da sequência dos números primos {2, 3, 5, 7, 11, 13, 17, 19, 23, ...} e das funções 6n + 1 e 6n – 1, que gerariam os números primos em sua estrutura. O programa Excel, teve uma grande participação à análise das sequências e funções à definição do número primo. As comparações realizadas com o novo teste e com os outros testes definido no trabalho, foram de cruciais à confirmação da veracidade modelo inovador.

Na análise realizada naquele capítulo, deu-se a descoberta de uma função através do MDC e o arranjo ligado ao fatorial que em síntese, selecionou de um espaço amostral onde existem diferentes números, somente aqueles que conduzem a especificamente, aos números primos e com base nesse critério de seleção, construísse uma correspondência biunívoca tendo domínio (em todo número natural diferente de zero) e um contradomínio (em todo número natural e imagem em todo número primo ímpar).

Apesar da sequência que caracterizou que não se necessita de muitos números para encontrar um número primo no infinito, restringisse a sequência de números apenas do ponto de vista analítico, necessitando a construção de uma análise muito mais ampla em que a modelagem computacional seria necessária para elaborar sequencias maiores de primalidades.

Naquele capítulo a razão que $f(p) = \frac{\sqrt{P}}{P}$ mostrou que para p tendo ao infinito, conduz a $f(p) = 0$. Nesse caso, a última sequência de números primos pode conduzir a um número muito grande de primalidade que somente a modelagem matemática ou computacional podem sequenciar e se for usado o crivo de Erastóstenes, torna-se difícil e complicado de determinar a sequência de primos.

REFERÊNCIAS

JAQUES, M. The Degrees of Knowledge. Tradução de Gerald B. Phelan. New York: Charles Scribner's Sons, 1959. p. 35-36.

ROSA, M. S. Números complexos: uma abordagem histórica para a aquisição do conceito. 1998. 170 f. Dissertação (Mestrado em Educação Matemática) – Curso de Matemática, Departamento de Matemática, Pontifícia Universidade Católica de São Paulo, São Paulo, 1998.

PORTOLAN, J. et al. **A importância do ensino de números complexos no ensino médio, na visão dos professores de matemática, em alguns municípios da região oeste do Paraná**. 2017. Dissertação (Mestrado) – Universidade Tecnológica Federal do Paraná, Curitiba, 2017.

DEWEY, John. A criança e o programa escolar. In: **DEWEY, J. Os Pensadores**. Abril Cultural, 1980.

CAMARGO RIZEL, Ary. Números primos. Dissertação (Mestrado) – Belo Horizonte, 2014.

GOMES DOS SANTOS, Alex. Conceitos e testes de primalidade: um olhar a partir de enunciados de problemas de um livro didático do sexto ano do ensino fundamental. Vitória, 2022.

AMERICAN PHYSICAL SOCIETY. "This Month in Physics History: June, ca. 240 B.C. Eratosthenes Measures the Earth," 2006. Disponível em: http://www.aps.org/publications/apsnews/200606/history.cfm. Acesso em: 25 jul. 2024.

BOYER, C. B. História da Matemática. São Paulo: Ed. da Universidade de São Paulo, 1974.

DARELA, Eliane; COAN CARDOSO, Marleide; CAMILO DA ROSA, Rosana. História da Matemática. Livro didático. 3. ed. Palhoça: Universidade do Sul de Santa Catarina, Unisul Virtual, 2011.

ROLLER, Duane W. Eratosthenes' Geography: Fragments Collected and Translated, with Commentary and Additional Material. Princeton: Princeton University Press, 2010.

CAJORI, F. Uma história da Matemática. Rio de Janeiro: Ciência Moderna, 2007.

BONGIOVANNI, V. As duas maiores contribuições de Eudoxo de Cnido: a teoria das proporções e o método de exaustão. **UNIÓN - Revista Iberoamericana de Educação Matemática**, n. 2, p. 91-110, 2005. Disponível em: http://www.fisem.org/web/union/revistas/2/Union_002_008.pdf. Acesso em: 25 jul. 2024.

HEFEZ, Abramo. Iniciação à Aritmética. Rio de Janeiro: Instituto de Matemática Pura e Aplicada, 2012.

HEFEZ, Abramo. Aritmética. Rio de Janeiro: Sociedade Brasileira de Matemática, 2016.

BRUCE, J. W. A really trivial proof of the Lucas-Lehmer primality test. **American Mathematical Monthly**, v. 100, n. 4, p. 370-371, 1993.

RIBENBOIM, Paulo. Números Primos: Velhos Mistérios e Novos Recordes. Rio de Janeiro: Instituto de Matemática Pura e Aplicada, 2014.

AGRAWAL, Manindra; KAYAL, Neeraj; SAXENA, Nitin. Primes is in P. Indian Institute of Technology Kanpur, 2006. Disponível em: http://www.cse.iitk.ac.in/users/manindra/algebra/primality_v6.pdf. Acesso em: 25 jul. 2024.

BRAGA, Bruno da Rocha. Algoritmo AKS – Primalidade de um número em tempo polinomial. Rio de Janeiro: Universidade Federal do Rio de Janeiro, 2002.

SOLOVAY, R.; STRASSEN, V. A fast Monte-Carlo test for primality. **SIAM Journal on Computing**, v. 6, n. 1, p. 84-85, 1978.

EUCLIDES. Os elementos de Euclides. Tradução e introdução de Irineu Bicudo. São Paulo: Editora UNESP, 2009.

DE OLIVEIRA, R.; LIMA, V. T.; BERTUOLA, A. C. "Aristarco revisitado". **Revista Brasileira de Ensino de Física**, v. 38, p. 1-12, 2016.

NASA SPACE SCIENCE DATA COORDINATED ARCHIVE. Earth Fact Sheet, 2021. Disponível em: https://nssdc.gsfc.nasa.gov/planetary/factsheet/earthfact.html. Acesso em: 14 dez. 2023.

NEWTON, Robert R. "The sources of Eratosthenes measurement of the Earth." **Quarterly Journal of the Royal Astronomical Society**, v. 21, p. 379-386, 1980.

EVES, H. Introdução à História da Matemática. Campinas: Editora da UNICAMP, 2004.

BERTRAND, Billy. Geometrias Não-Euclidianas: História e Aplicações. Chapecó: 2019.

HEATH, T. L. Euclid and the Traditions About Him. In: **Euclid, Elements**. Cambridge: University Press, 1908. p. 1-6.

DU SAUTOY, Marcus. A Música dos Números Primos: A história de um problema não resolvido na matemática. Rio de Janeiro: Zahar, 2007.

HEFEZ, Abramo. Elementos de Aritmética. São Paulo: Sociedade Brasileira de Matemática, 2012.

SUAPESQUISA. "Quem foi Eratóstenes." Disponível em: https://www.suapesquisa.com/quemfoi/eratostenes.htm. Acesso em: 10 jul. 2023, às 16:54.

EBIOGRAFIA. "Euclides." Disponível em: https://www.ebiografia.com/euclides/. Acesso em: 10 jul. 2023, às 17:36.

TODAMATERIA. "História dos números: origem e evolução dos números." Disponível em: https://www.todamateria.com.br/historia-dos-numeros-origem-e-evolucao-dos-numeros/. Acesso em: 12 jul. 2023, às 13:45.

TODAMATERIA. “História dos números: origem e evolução dos números.” Disponível em: https://www.todamateria.com.br/historia-dos-numeros-origem-e-evolucao-dos-numeros/. Acesso em: 13 jul. 2023, às 13:30.

TODAMATERIA. “Análise combinatória.” Disponível em: https://www.todamateria.com.br/analise-combinatoria/. Acesso em: 17 jul. 2023, às 15:30.

PEREIRA DE ANDRADE, Ricardo. Testes de Primalidade: Uma Análise Matemática dos Algoritmos Determinísticos e Probabilísticos. Fortaleza: 2017.

AUSUBEL, D. P. A aprendizagem significativa: a teoria de David Ausubel. São Paulo: Moraes, 1982.